РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Цифровой страж

Key_P1 MultiClet

Аннотация

Настоящий документ является руководством по эксплуатации информационной системы «Key_P1 MultiClet Цифровой страж». В документе приведены общие сведения об устройстве Key_P1, его функциях, особенностях установки и эксплуатации. Перед установкой и эксплуатацией устройства Key_P1 необходимо внимательно ознакомиться с настоящим руководством. Применение устройства Key_P1 должно дополняться общими мерами предосторожности и физической безопасности при работе с ПК. Устройство доступно для заказа в розницу по телефону или через сайт. Криптографические функции не могут быть изменены пользователем. Устройство запатентовано производителем ОАО "Мультиклет". ПО "Менеджер Key_P1"устанавливается пользователем самостоятельно, дальнейшая поддержка осуществляется только путём обновления версии ПО.

Внимание: начальная инициализация Key_P1, а также генерация случайных и корпоративных ключей должны производиться на доверенном компьютере.

Содержание

Список сокращений

ПК — персональный компьютер;

АС — автоматизированная система;

ПО — программное обеспечение;

ОЗУ — оперативное запоминающее устройство;

СКЗИ — средство криптографической защиты информации;

PIN — пароль для доступа к устройству;

ОС — операционная система;

ИС — информационная система;

Key_P1 — Цифровой страж «Key_P1 MultiClet».

1 Общие сведения

1.1 Описание и назначение

Рис. 1. Цифровой страж Key_P1 MultiClet

Key_P1 (рис. 1) это многофункциональная информационная система, защищенная криптографически и имеющая в своем составе аппаратно-программное шифрование по ГОСТ 28147-89.

Key_P1 - разработан на базе российского мультиклеточного процессора с универсальной не фон-неймановской архитектурой. Это многофункциональное устройство обезопасит данные от потери, кражи и несанкционированного доступа. В Key_P1 аппаратно реализован набор всех самых необходимых функций и алгоритмов защиты информации, а также набор драйверов и библиотек для использования криптографических функций. Key_P1 предназначен для применения на ПК, функционирующих под управлением WindowsXP, Windows 7, Windows 8, Linux 2.6.x, Linux 3.x. (MacOS в плане развития ПО).

Основной функционал Key_P1 заключается в следующем:

- создание иерархического доступа к информации. Существует возможность разграничить права доступа пользователей к зашифрованной информации (например, между отделами предприятия или по видам выполняемых работ (проектов));

- создание синхронизированных ключей для удаленного обмена информацией закрытого доступа по открытым каналам передачи данных;

- шифрование файлов на жестком диске ПК или съемных носителях (USB флэш-дисках, MicroSD, MiniSD, MMC и SD картах);

- создание шифрованных областей данных на съемных накопителях (USB флэш-дисках, MicroSD, MiniSD, MMC и SD картах);

- хранение пользовательских паролей и логинов в защищенной памяти устройства. Доступ к этой памяти предоставляется только после ввода аутентифицирующей информации (PIN). Эта функция позволяет обезопасить парольные данные для доступа к открытым почтовым ресурсам типа mail.ru от несанкционированного доступа;

- предотвращение утечки информации с корпоративных компьютеров на съемные накопители;

- ведение "лог-журнала" основных событий, совершаемых пользователем (в журнале описываются события, непосредственно связанные с функционалом устройства).

Пояснение к описанию функционала устройства приведено в таблице ниже:

Иерархический доступ к информации	В Key_P1 MultiClet предусмотрено разграничение прав доступа к зашифрованным файлам. Служба безопасности предприятия будет иметь возможность создавать различные разграничения прав по отделам. При этом руководитель будет иметь доступ ко всем файлам. Сотрудники компании могут кодировать файлы для своих коллег с помощью программы Corporate Key_P1 Manager при наличии соответствующего уровня доступа.
Контроль персонала	Служба информационной безопасности предприятия может заблокировать возможность записи информации с корпоративных компьютеров на съемные накопители. Для этого устанавливается режим «только чтение», который позволит Key_P1 аппаратно заблокировать любую несанкционированную запись конфиденциальных данных, вирусов или других программ на накопитель. Т.е. записать информацию на накопитель в этом режиме не получится, пользователю понадобиться получить разрешение службы информационной безопасности для возможности записи на накопители.
Защита от шпионских флешек (проблема badUSB)	Key_P1 разрешает подключение только обычных накопителей информации, работа «устройств-шпионов» (представляются одновременно клавиатурой и накопителем) будет заблокирована.
Запрет на отключение	Устройство Key_P1 сохраняет в «лог журнал» основные события, совершаемые пользователем. Просмотр «лог журнала» может быть закрыт для пользователя. Для разблокировки просмотра необходимо ввести ПИН-код администратора. Таким образом, работник не может незаметно изъять устройство Key_P1 для записи на флэш-накопитель корпоративных данных, так как все попытки отключения будут зафиксированы службой безопасности.
Сотрудник в командировке	Пользователи могут создать одинаковые ключи для обмена зашифрованными сообщениями друг с другом или головным офисом компании в случае обмена данными во время деловых поездок с помощью открытой электронной почты и других интернет-ресурсов.
Надежное шифрование	Шифрование информации возможно на накопителях и компьютере. Шифрование осуществляется по алгоритму ГОСТ 28147-89 с шириной ключа 256 бит. Шифрование алгоритмом ГОСТ28147-89 на накопителях осуществляется защищенным методом – по секторам (вскрытие потребует тысячи лет машинного времени).
Неуязвимость данных	Пользователь имеет возможность создания резервных копий зашифрованной информации, таким образом, при потере или повреждении устройства Key_P1 и(или) накопителя пользователь сможет восстановить свою информацию. В случае потери устройство бесполезно для злоумышленника. Потерянное устройство Key_P1 нельзя использовать ни в каких целях, связанных с шифрованием и дешифрованием. Из потерянного устройства нельзя извлечь информацию о принципах работы аналогичных устройств.
Поддержка разных накопителей	Устройство поддерживает работу с накопителями типа SD, micro SD и USB. Также существует возможность использования USB удлинителей, если размер посадочного USB порта на компьютере недостаточен.
Использование разных ОС	Поддерживается работа устройства в операционных системах WindowsXP, Windows 7, Windows 8, Linux 2.6.x, Linux 3.x и в разработке MacOS.
Сейф для паролей	Устройство позволяет сохранять пользовательские пароли и логины на внутреннюю защищенную память устройства Key_P1. В дальнейшем пользователь может, кликнув мышкой, скопировать логин в буфер обмена операционной системы и вставить в нужное поле для ввода логина. Аналогичную операцию можно проделать для пароля. Этим мы обеспечиваем удобное использование и хранение своих паролей, а также защищаемся от кейлогеров на ПК.
Быстрое криптопреобразование	Устройство Key_P1 MultiClet позволяет провести быстрое шифрование или расшифрование информации. Таким образом пользователи могут легко и быстро обмениваться зашифрованными текстовыми сообщениями, которые пересылаются с помощью электронной почты, различных систем обмена сообщениями (например skype), социальных сетей и т.д.

1.2 Организационные меры по защите информации

Для эффективного применения устройства Key_P1, поддержания необходимого уровня защищенности ПК и информационных ресурсов АС необходимо обеспечить:

- Сохранность устройства Key_P1;

- Хранение в тайне кода доступа к устройству (PIN-кода);

Помимо этих мер необходимо осуществлять регулярное регламентное резервное копирование зашифрованных данных и ключей шифрования для возможности восстановления этой информации на новом устройстве Key_P1. Более подробно процедура резервного копирования и восстановления устройства описана в главе 2.6. «Инициализация устройства»

ЗАПРЕЩАЕТСЯ:

- оставлять без контроля после ввода ключевой информации либо иной конфиденциальной информации вычислительные средства, на которых эксплуатируется Key_P1;

- вносить какие-либо изменения в программное обеспечение Key_P1;

- осуществлять несанкционированное администратором безопасности копирование ключевых носителей;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и другие средства отображения информации;

- использовать ключевые носители в режимах, не предусмотренных функционированием Key_P1;

- записывать на ключевые носители постороннюю информацию;

- вскрывать корпус устройства.

1.3 Системные требования

Перед тем как приступать к установке и настройке устройства Key_P1 необходимо удостовериться в том, что ваша рабочая станция соответствует минимальным системным требованиям. Данные требования приведены в таблице 1.

Таблица 1. Системные требования.

Совместимость с операционными системами	• WindowsXP (SP3); • Windows 7; • Windows 8; • Linux 2.6.x; • Linux 3.x.
Необходимые аппаратные условия	USB-порт

1.4 Маркировка устройства

Маркировка устройства Key_P1 наносится с обратной стороны корпуса.

Рис. 2. Маркировка устройств

1.5 Технические характеристики

Таблица 2. Технические характеристики.

Назначение	устройство предназначено для шифрования небольших объёмов конфиденциальной информации
Скорость работы	с открытым разделом накопителя до 3,2 Мбит/с, с закрытым разделом и шифрование без накопителя - до 1,2 Мбит/с
Поддерживаемые типы портов USB	1.1, 2.0, 3.0
Поддерживаемые типы накопителей	USB, SD, microSD, miniSD, MMC
Количество случайных ключей	1024
Количество синхронных ключей	104
Количество корпоративных ключей	512
Групп корпоративных ключей	512
Количество записей логинов и паролей	200
Групп для логинов и паролей	32
Количество записей журнала событий	1024
Количество записей журнала времени	1024
Длина ключа шифрования	для распространяемых в РФ устройств Key_P1 - 256 бит, для распространяемых за пределами РФ устройств Key_P1 - 56 бит

2 Установка и настройка устройства Key_P1

2.1 Описание установки и настройки устройства

Первым шагом необходимо подключить устройство Key_P1 Multiclet к USB порту, а затем в списке подключенных устройств (под Windows это раздел "Мой компьютер") найти Key_P1 и открыть его (например с помощью двойного щелчка левой клавишей мышки). После того, как отобразится файл readme, его необходимо открыть. Далее кликнуть по ссылке "Загрузить ПО" в зависимости от установленной операционной системы. Перед началом работы с устройством Key_P1 Multiclet необходимо установить загруженное ранее приложение Key_P1 Manager. После этого, в соответствии с текущим руководством пользователя, необходимо с помощью приложения Key_P1 Manager выполнить следующие шаги:

1) Установить внутреннюю прошивку устройства

2) Провести инициализацию устройства

3) Провести инициализацию накопителей

Установка внутренней прошивки описана в раздела "Обновление внутреннего программного обеспечения".

Инициализация устройства включает следующие шаги:

1)Установку ключей в количестве 1024 штук

2)Установку PIN кода администратора

3)Установку PIN кода пользователя

4)Установку тревожного PIN кода

5)Установку имени устройства

Инициализация накопителей USB и SD типа включает следующие шаги:

1)Разбиение на два раздела (открытый и закрытый)

2)Установку меток разделов

Следует отметить, что количество накопителей не ограничено, но при этом максимальный размер закрытого раздела ограничен пределом в 2 Гигабайта, а максимальный размер открытого раздела - 1 Терабайтом. Приложение Key_P1 Manager достаточно один раз установить с помощью программного пакета, загруженного с сайта. Возможно

установить приложение на съемный носитель(или просто скопировать папку Key_P1 Software) для необходимой ОС, тогда в дальнейшем для использования устройства не потребуется установка ПО на ПК. Если требуется работа под ОС Windows и ОС Linux, то необходимо скопировать на накопитель две версии приложения.

2.2 Установка программного обеспечения

Первым шагом необходимо подключить устройство Key_P1 к USB порту персонального компьютера. После этого устройство отобразится в системе в качестве съёмного носителя(см пример для ОС Windows 8 на рис. 3).

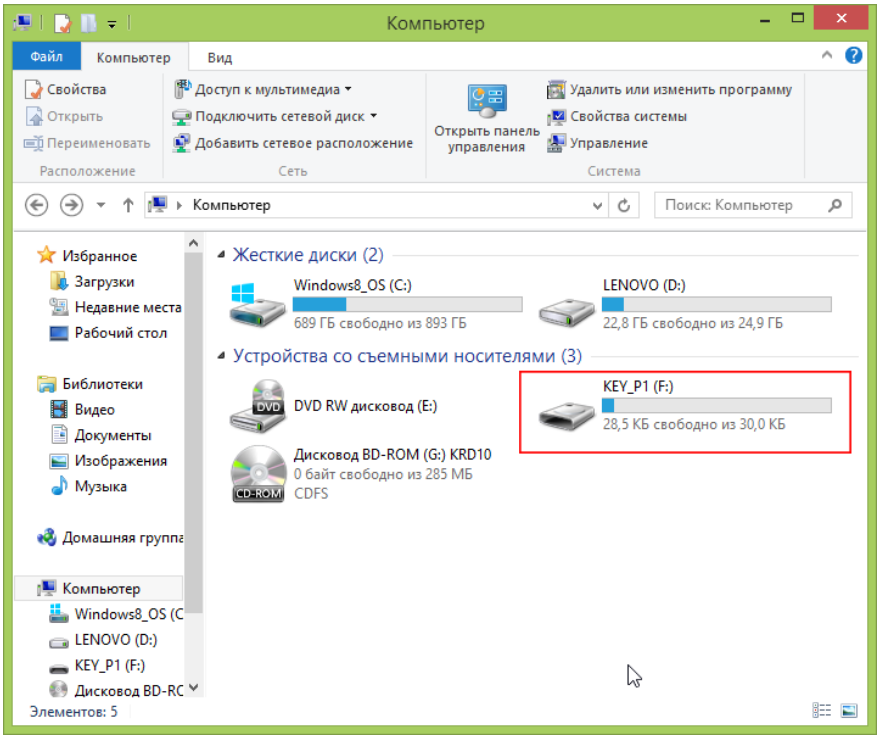

Рис. 3. Первое включение устройства Key_P1 MultiClet

Следующим шагом открываем(например с помощью двойного щелчка левой клавиши мыши) съемный носитель Key_P1 и находим файл readme в формате html. Пример отображения файла приведен на рис. 4

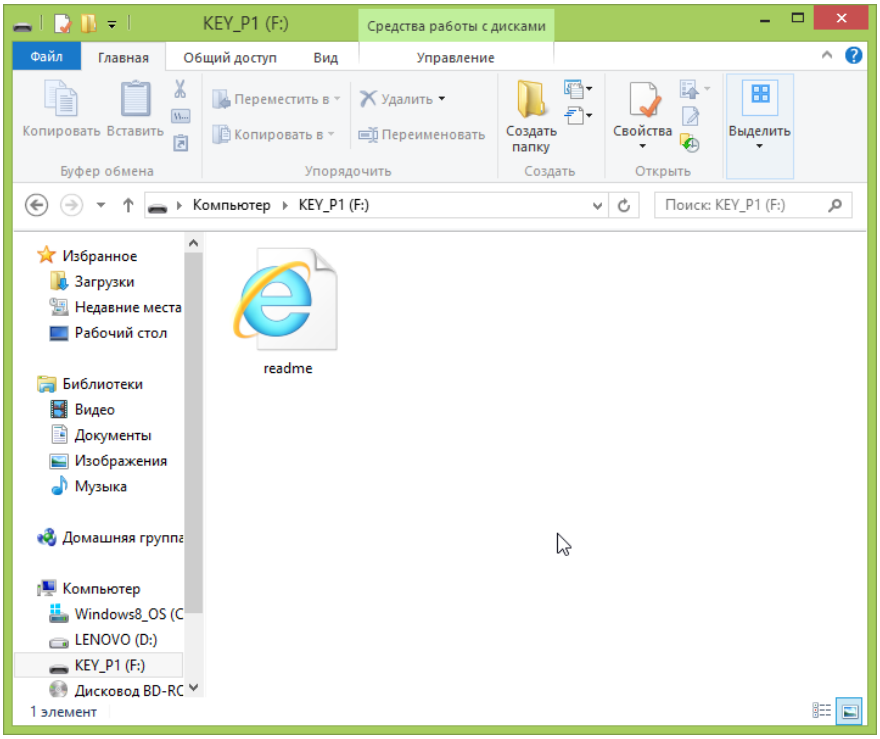

Рис. 4. Файл помощи на устройстве Key_P1 MultiClet

Для получения необходимой информации о загрузке ПО и доступной документации по устройству Key_P1 MultiClet открываем(например с помощью двойного щелчка левой клавиши мыши) файл readme. Если по каким-то причинам файл не открылся браузером, установленным по умолчанию, то следует открыть данный файл с помощью любого установленного в системе интернет браузера. Например для Windows 8 щелкаем правой клавишей мыши по файлу readme и выбираем пункт "открыть с помощью". Далее выбираем любой установленный в системе браузер. Содержимое файла readme представлено на рис. 5

Рис. 5. Содержимое файла помощи на устройстве Key_P1 MultiClet

В зависимости от установленной операционной системы на персональном компьютере необходимо перейти по соответствующей ссылке. Для загрузки ПО на ОС Windows необходимо перейти по ссылке "(Windows) Загрузить ПО".

Если по каким-то причинам загрузка ПО не началась, то необходимо перейти вручную по ссылкам приведенным ниже:

1)Если на персональном компьютере установлена ОС семейства Windows, то следует выбрать ссылку:

http://multiclet.com/docs/PO/Key_P1/Key_P1_Software_Installer.exe.

2)Если на персональном компьютере установлена ОС семейства Linux, то следует выбрать ссылку:

http://multiclet.com/docs/PO/Key_P1/Key_P1_Software_Installer.tar.gz.

Для установки программного обеспечения на персональный компьютер необходимо запустить установочный файл **Key_P1_Software_Installer.exe** (Для ОС Windows) либо **Key_P1_Software_Installer.tar.gz** (для ОС Linux).

Произойдет запуск мастера установки приложения (окно мастера установки приведено на рис. 6) Для начала установки ПО нажмите кнопку "Далее".

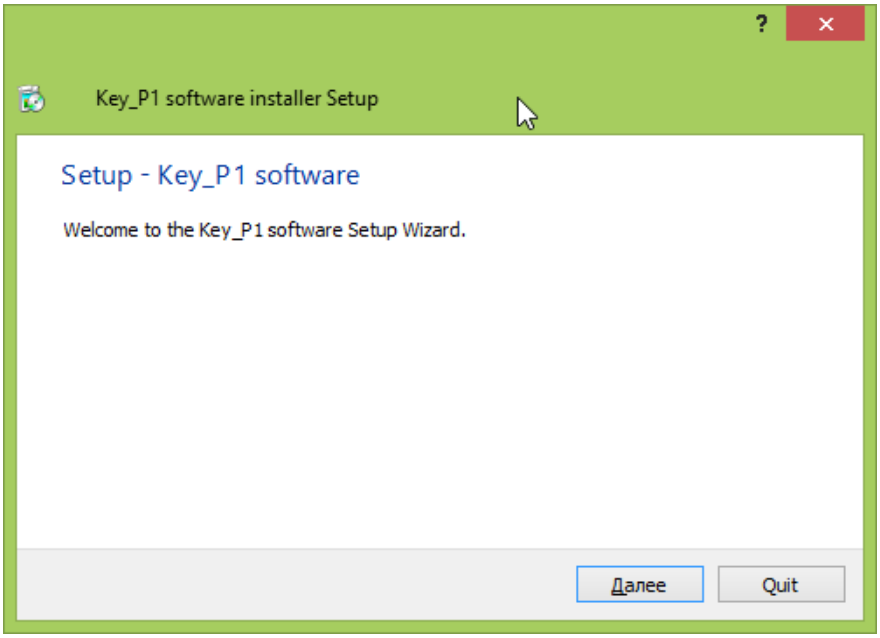

Рис. 6. Окно запуска мастера установки ПО

Мастер установки предложит выбрать путь для установки ПО. По умолчанию задан путь "C:/Multiclet/Key_P1_software". Окно для выбора пути представлено на рис. 7 После указания пути нажмите кнопку "Далее".

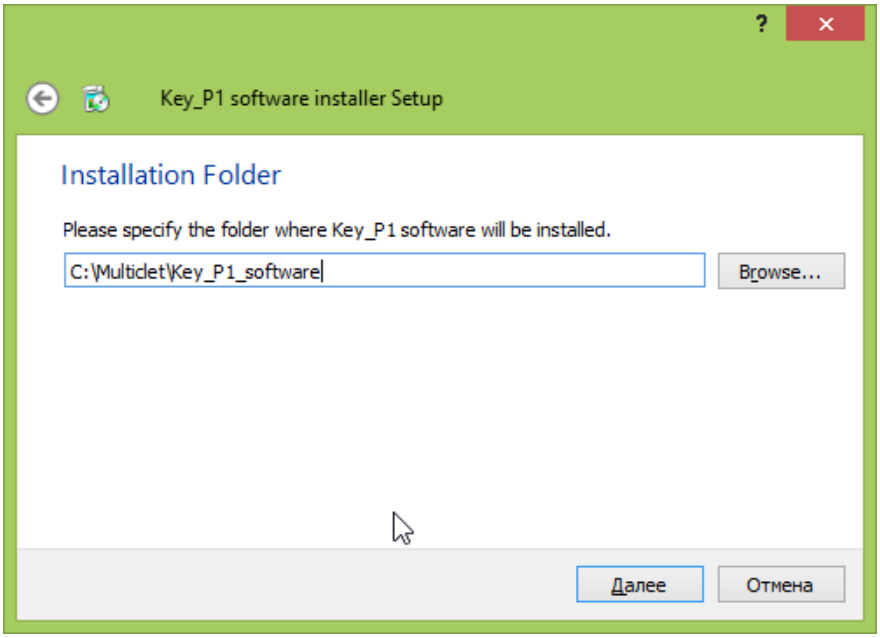

Рис. 7. Окно выбора пути для установки ПО

Затем появится окно для выбора компонентов для установки. В данный момент доступен только один компонент. Для продолжения установки нажмите кнопку "Далее". Окно выбора устанавливаемых компонентов представлено на рис. 8

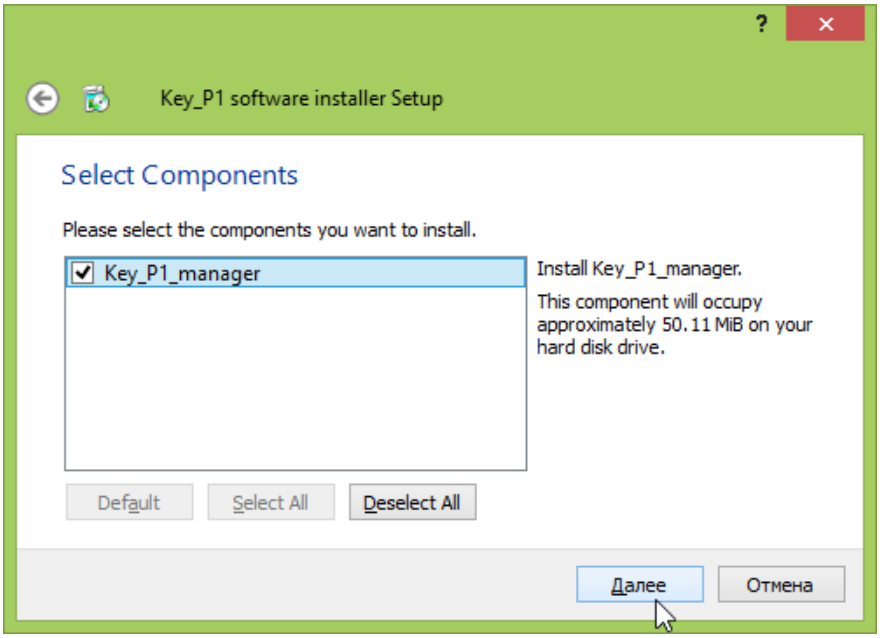

Рис. 8. Окно выбора компонентов установки

В появившемся окне нажмите кнопку "Далее"для продолжения установки ПО. Окно для просмотра параметров установки представлено на рис. 9

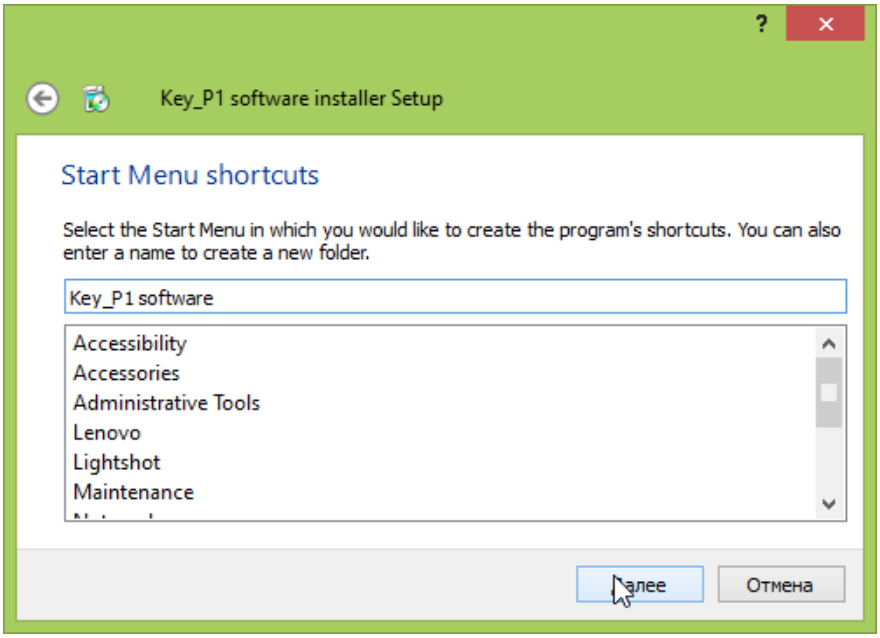

Рис. 9. Окно для просмотра параметров установки

По окончанию установки в появившемся окне необходимо нажать кнопку "Завершить". Окно завершения установки представлено на рис. 10

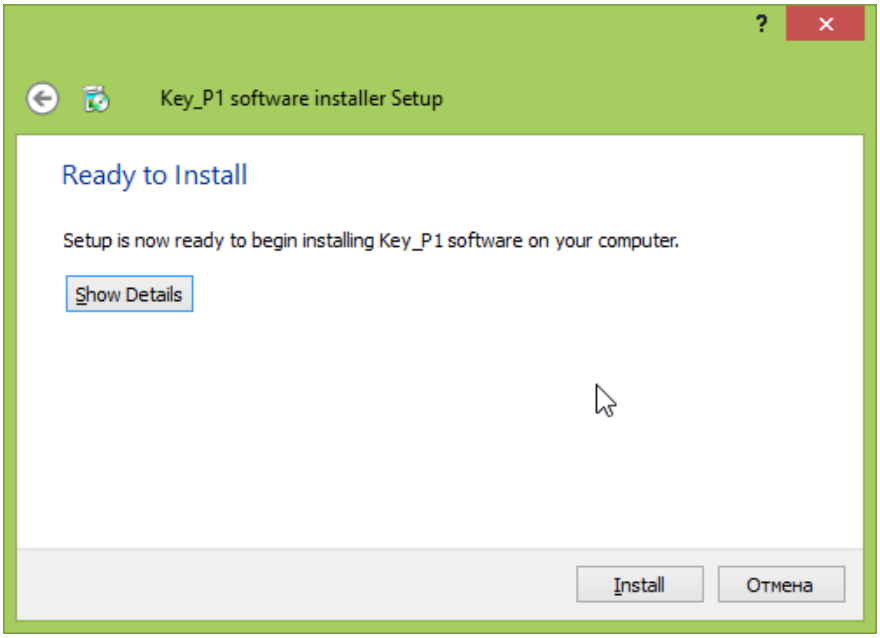

Рис. 10. Окно завершения установки

2.3 Запуск приложения Key_P1 Manager

После того, как весь комплект программного обеспечения установлен на ПК, необходимо запустить приложение **Key_P1 Manager**. Для этого требуется запустить ярлык на рабочем столе вашего ПК **Key_P1_Manager.lnk** либо запустить приложение, например для ОС Windows 7 следующим образом **Пуск->Все программы->Key_P1->Key_P1 Manager**.

После запуска приложения, в правом нижнем углу рабочего стола (панель задач) должен отобразиться ярлык Key_P1 менеджер (Обведен красным прямоугольником на рис. 11).

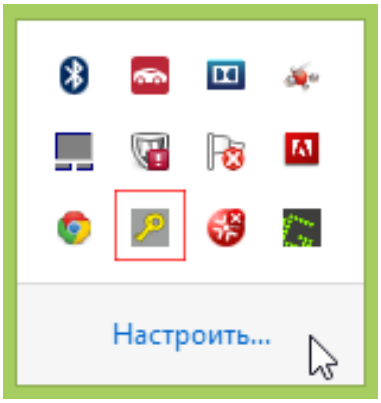

Рис. 11. Отображение значка на панели задач

Для запуска приложения и корректной работы с устройством Key_P1 на ПК с ОС Linux необходим уровень прав доступа **root**.

2.4 Описание интерфейса приложения Key_P1 Manager

Главное меню приложения Key_P1 Manager выглядит так, как показано на рис. 12.

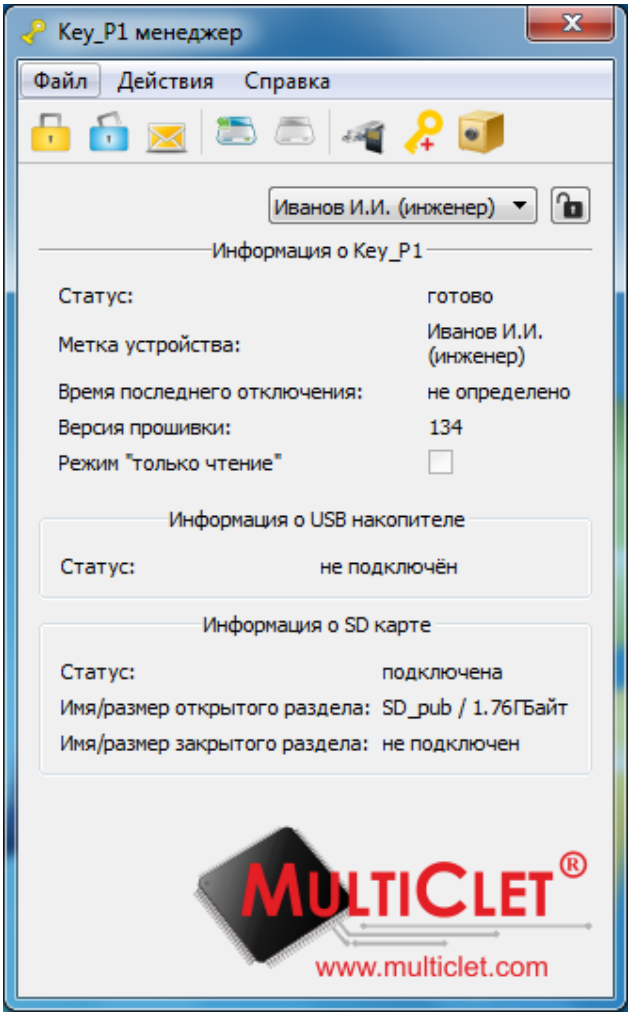

Рис. 12. Главное меню Key_P1 Manager

Меню состоит из следующих элементов:

1) Верхняя панель вкладок **Файл, Действия** и **Справка**. Вкладка **Файл** состоит из команд **Закрыть** и **Выход**. Запуск команды **Закрыть** приведет к сворачиванию приложения в трей (приложение будет отображаться на панели задач). Запуск команды **Выход** приведет к закрытию приложения.

Вкладка **Действия** включает в себя следующие команды: **Шифрование файлов, Расшифрование файлов, Быстрое криптопреобразование, Подключить закрытый раздел, Отключить закрытый раздел, Управление накопителями, Управление синхронными ключами, Хранилище аутентификационных данных**

Вкладка **Действия** содержит подменю **Администрирование**, которое, в свою очередь, содержит следующие пункты: **Управление режимом "только чтение Обновить прошивку, Инициализировать устройство, Изменить метку Key_P1, Изменить PIN администратора, Изменить PIN пользователя, Изменить тревожный PIN, Управление корпоративными ключами, Журнал событий**. Описание данных команд будет изложено далее. Содержимое вкладки **Действия** приведено на рис. 13.

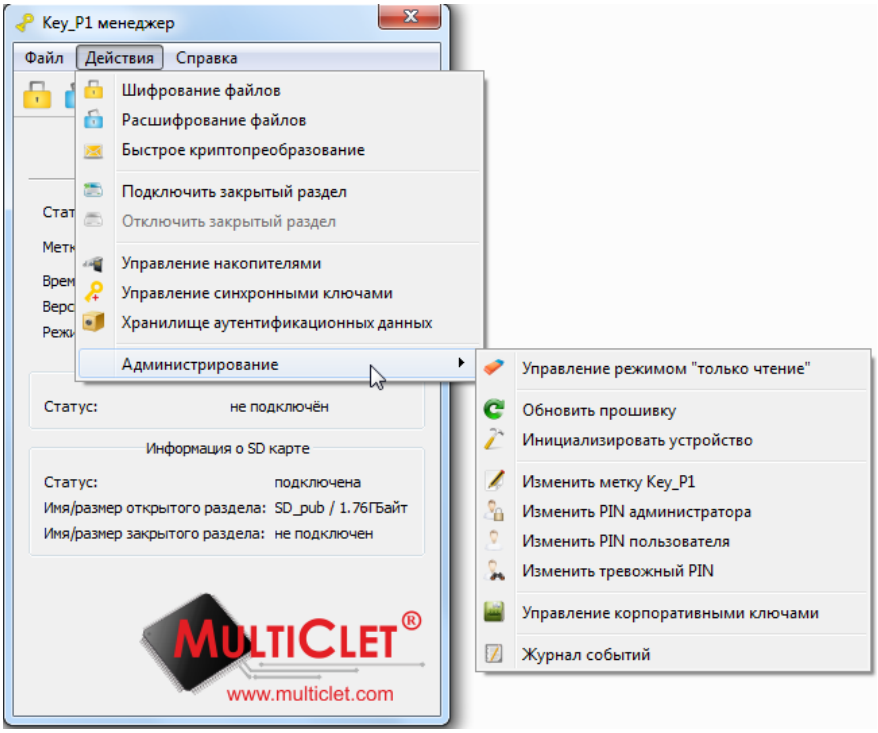

Рис. 13. Вкладка "Действия"Key_P1 Manager

Вкладка **Справка** выдает справочную информацию о работе с приложением. Содержимое вкладки **Справка** приведено на рис. 14.

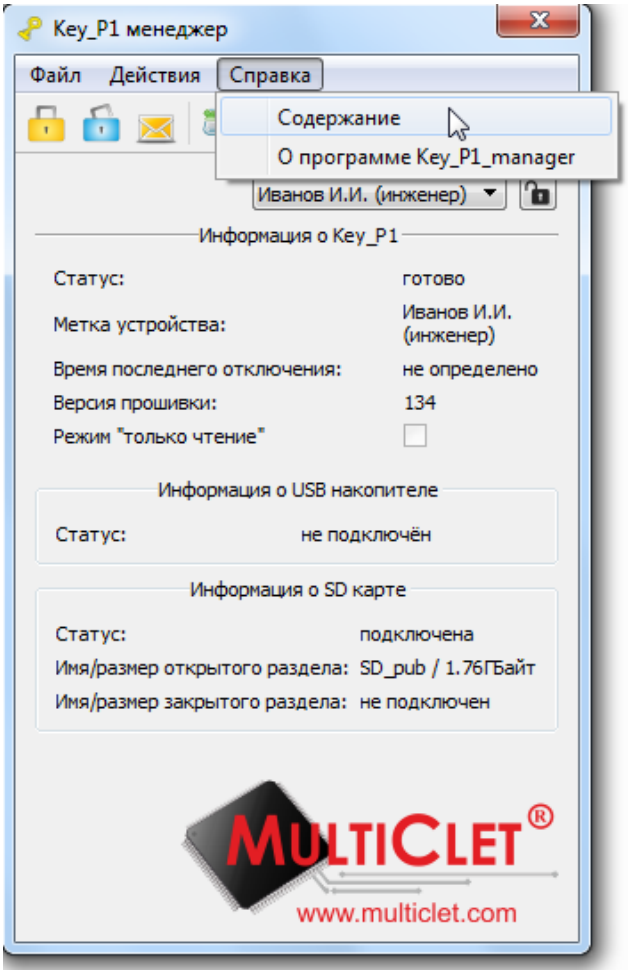

Рис. 14. Вкладка "Справка"Key_P1 Manager

2) Панель инструментов. Полностью дублирует все команды из вкладки **Действия** за исключением пункта **Администрирование**. Панель инструментов на рис. 15 выделена красным цветом.

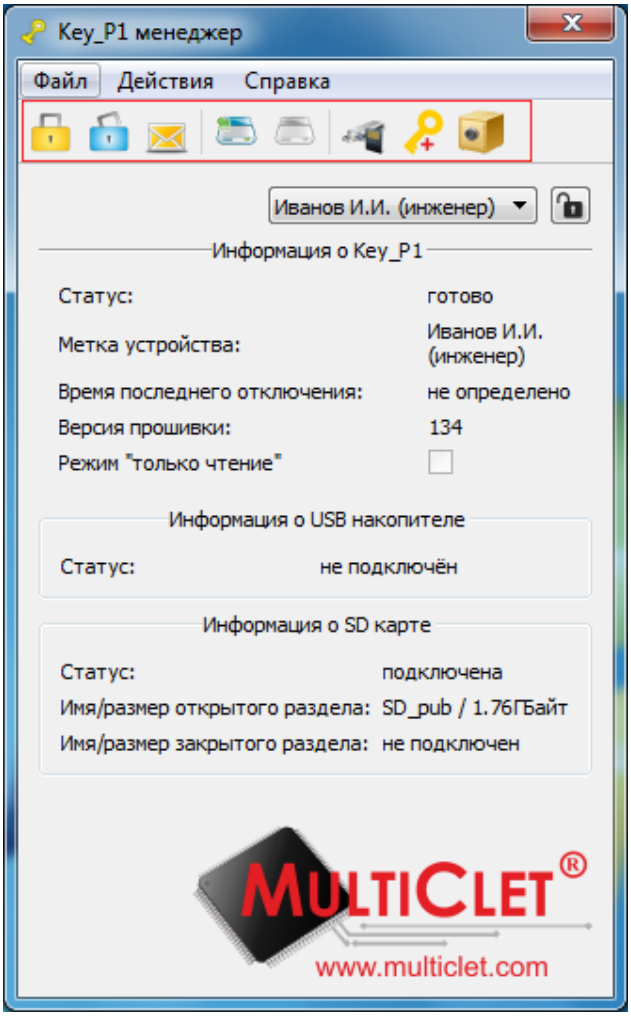

Рис. 15. Панель инструментов Key_P1 Manager

3) Выпадающий список подключенных устройств Key_P1 представлен на рис. 16 (выделен красным цветом). В этом списке отображаются все подключенные устройства с отображением меток.

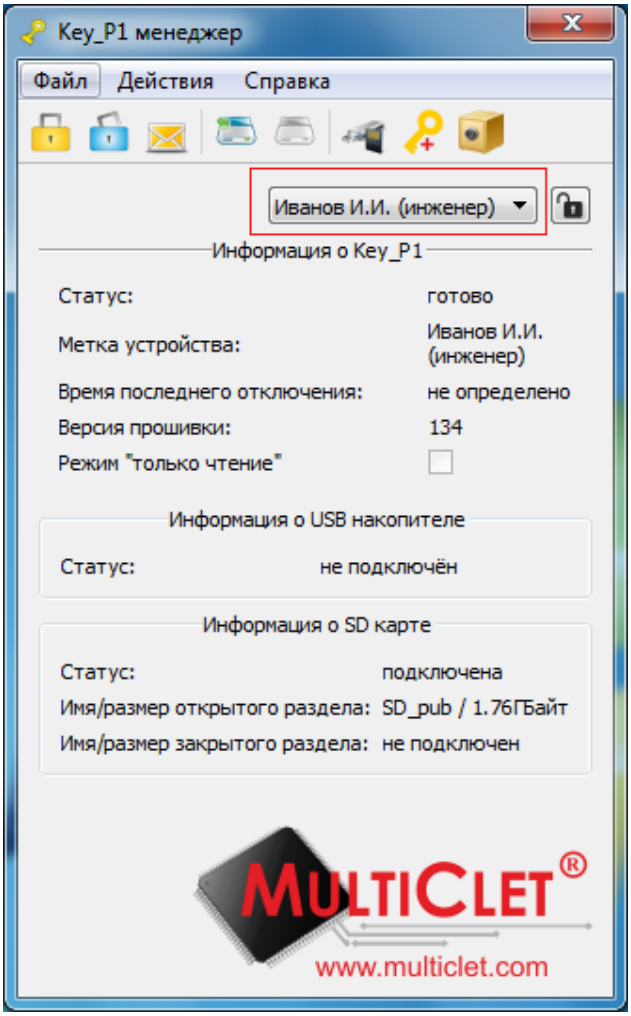

Рис. 16. Список подключенных к ПК устройств Key_P1

4) Кнопка **Разблокировки PIN кода пользователя** на рис. 17 выделена красным цветом.

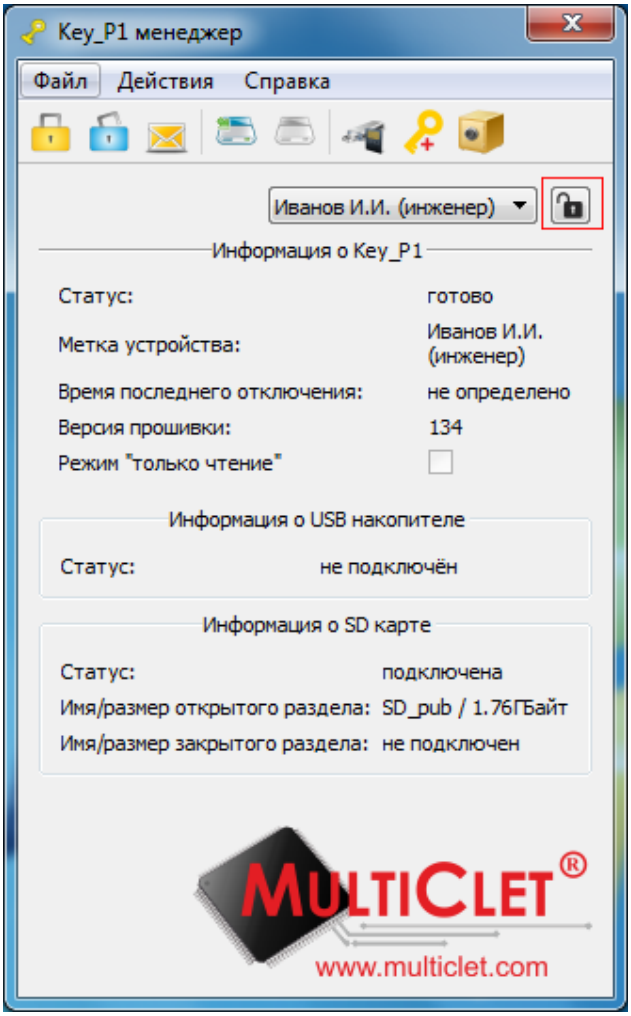

Рис. 17. Кнопка разблокировки PIN пользователя

5) Область **Информация о Key_P1**. Данная область включает в себя **Статус (состояние устройства), Метку устройства (Имя устройства), Время последнего отключения устройства, Версию прошивки, Режим "только чтение"**.

6) Область **Информация о USB накопителе**. Данная область включает в себя **Статус (состояние накопителя), Имя/размер открытого раздела, Имя/размер закрытого раздела**

7) Область **Информация о SD карте**. Данная область включает в себя **Статус (состояние SD карты), Имя/размер открытого раздела, Имя/размер закрытого раздела**

2.5 Обновление внутреннего программного обеспечения

Обновление внутреннего программного обеспечения (далее по тексту – прошивка) необходимо осуществлять регулярно, поскольку каждая следующая версия прошивки делает работу приложения Key_P1 Manager более стабильной и функциональной.

Запустите приложение Key_P1 Manager. Подключите устройство Key_P1 Multiclet к свободному USB порту ПК, после чего появится собщение с предложением провести установку прошивки на устройство (в случае первого подключение устройства к ПК), см рис.18. Нажмите кнопку "Yes"для продолжения. Обновление прошивки и её установка на новое устройство - идентичные процедуры с запуском мастера обновления прошивки.

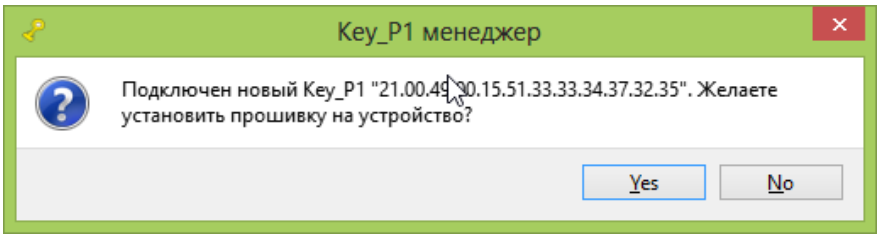

Рис. 18. Установка прошивки

Для обновления прошивки устройства вручную необходимо в главном меню приложения последовательно выбрать вкладку **Действия**, перейти в подменю **Администрирование** и выбрать пункт **Обновить прошивку** (рис. 19).

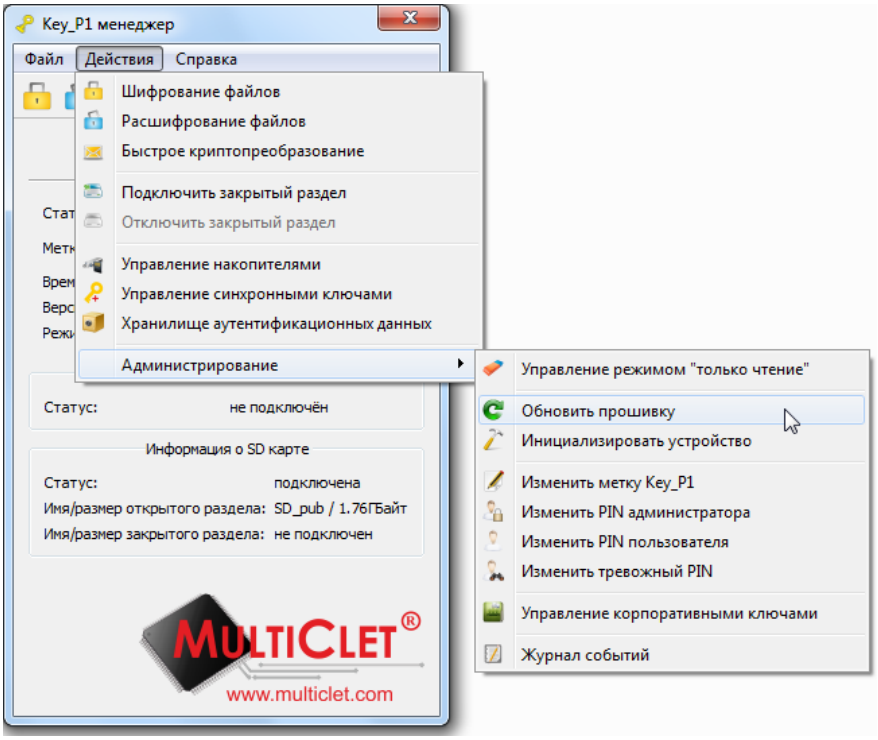

Рис. 19. Обновление прошивки

Откроется окно **Мастер обновления прошивки Key_P1** (рис. 20). Для продолжения процедуры следует нажать кнопку «Далее». Для прекращения операции по обновлению прошивки необходимо нажать кнопку «Отмена».

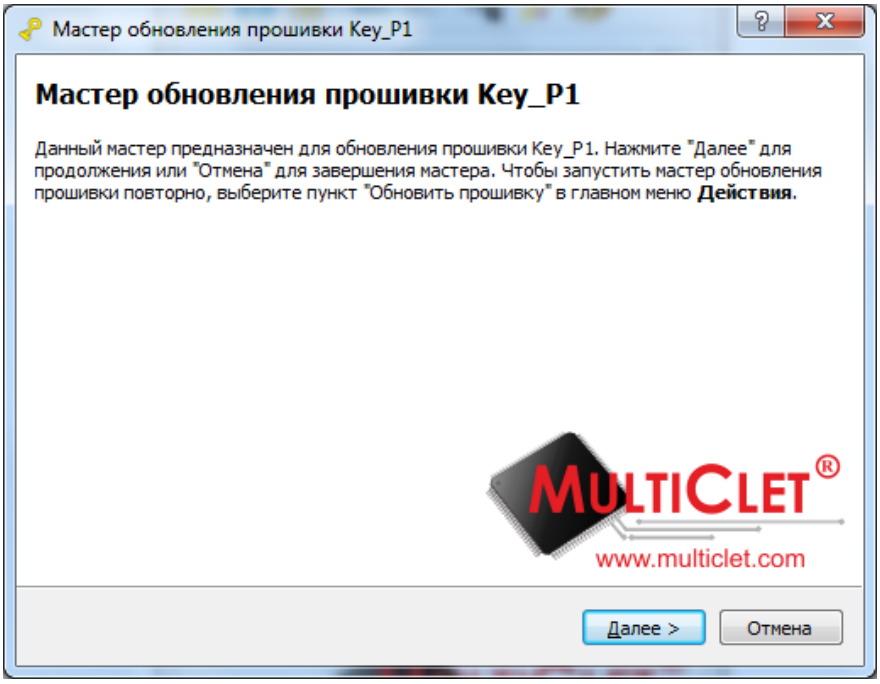

Рис. 20. Мастер обновления прошивки Key_P1

Следующее окно - это выбор источника обновления. Предлагается два варианта установки обновления: с сайта http://multiclet.com или с помощью заранее загруженного файла (рис. 21).

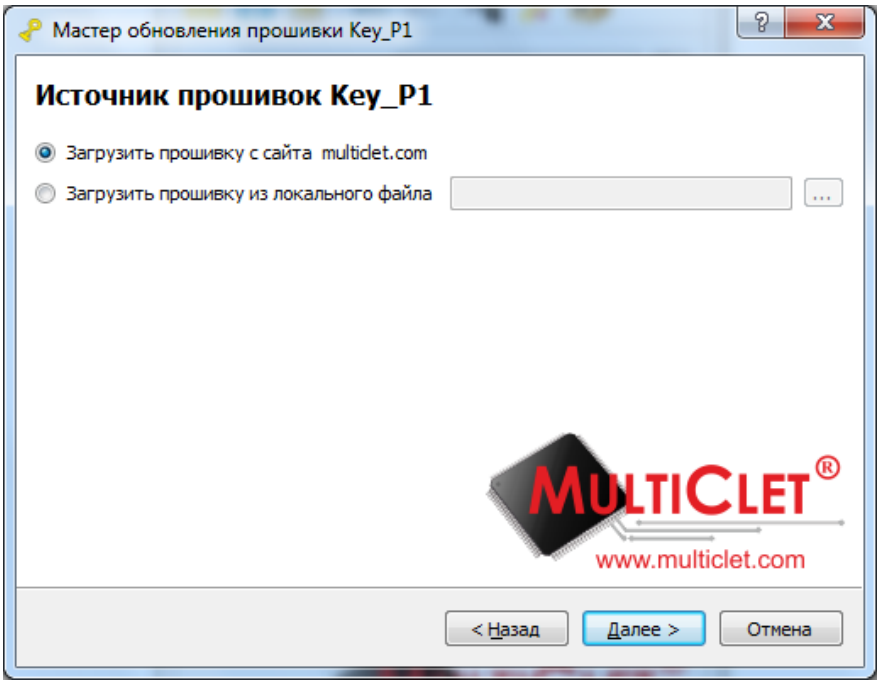

Рис. 21. Источник обновления прошивки

По умолчании загрузка прошивки будет выполнена с сайта http://multiclet.com, для чего необходим доступ в сеть интернет. Произойдет автоматическое подключение к сайту и появится окно **Список прошивок Key_P1** (рис. 22) со списком всех вариантов прошивок, доступных для установки. Для продолжения установки необходимо выбрать нужную прошивку и нажать кнопку «Далее».

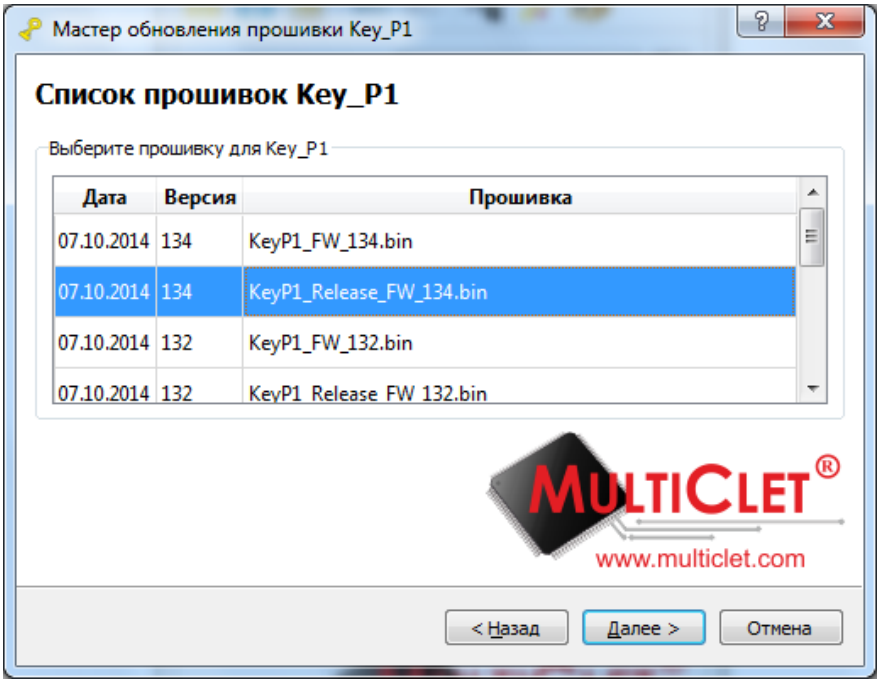

Рис. 22. Список прошивок Key_P1

Если требуется обновить прошивку из локального файла, то необходимо выбрать пункт **Загрузить прошивку из локального файла** (рис. 23).

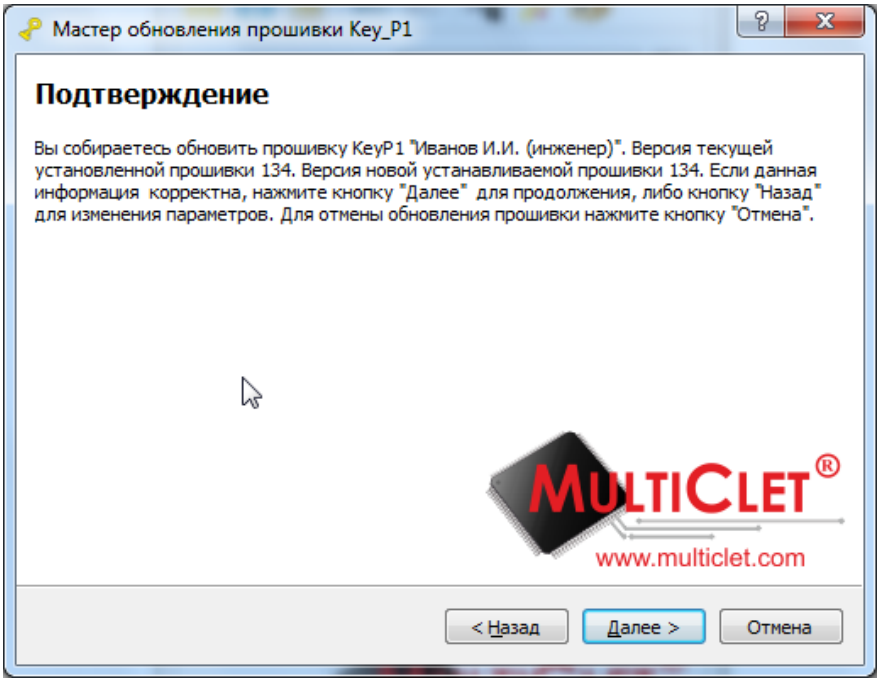

Рис. 23. Загрузка прошивки из локального файла

Далее следует указать путь к этому файлу (рис. 24).

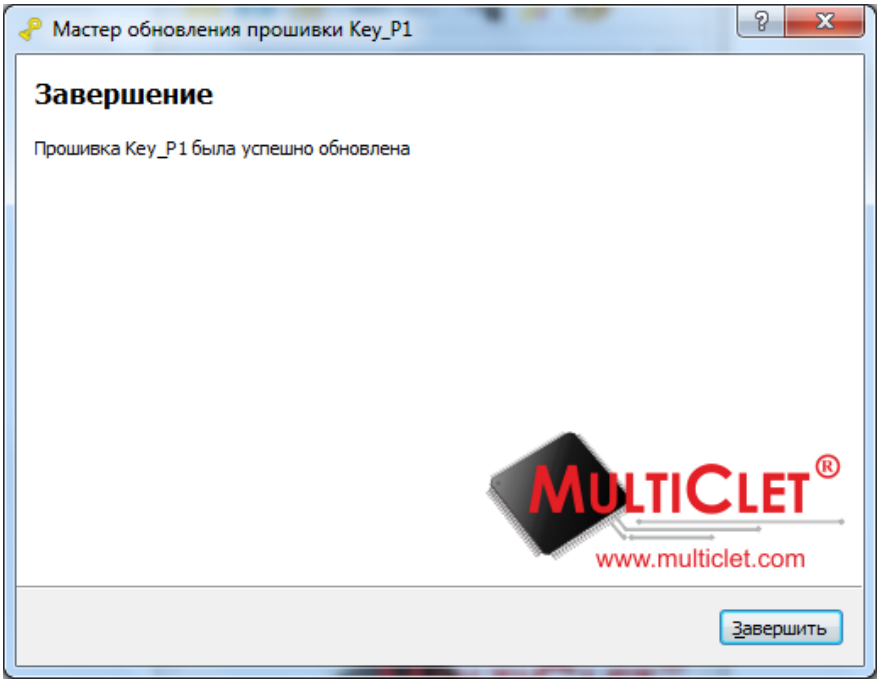

Рис. 24. Загрузка прошивки из локального файла

Для подтверждения обновления необходимо ввести PIN администратора и нажать кнопку «OK». Далее запустится процесс обновления.

2.6 Инициализация устройства

Следующим этапом необходимо произвести инициализацию устройства. После запуска приложения Key_P1 Manager необходимо подключить устройство Key_P1 Multiclet. Должно появиться сообщение с предложением провести инициализацию(если устройство не инициализировано), см рис.25. Для продолжения нажмите кнопку "Yes".

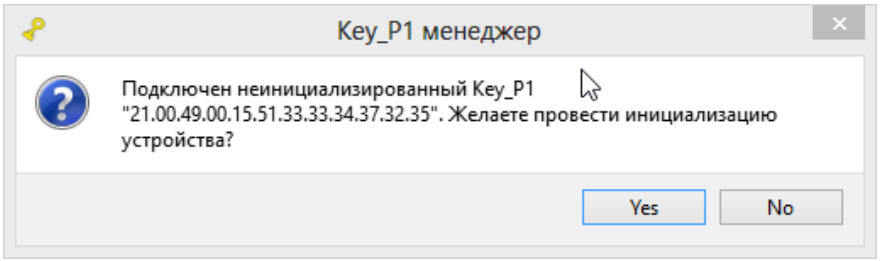

Рис. 25. Окно старта инициализации устройства Key_P1

Запустится мастер инициализации устройства, см рис.26. Также мастер инициализации устройства можно запустить вручную, для этого в главном меню устройства необходимо выбрать вкладку **Действия**, выбрать подменю **Администрирование** и пункт **Инициализировать устройство**.

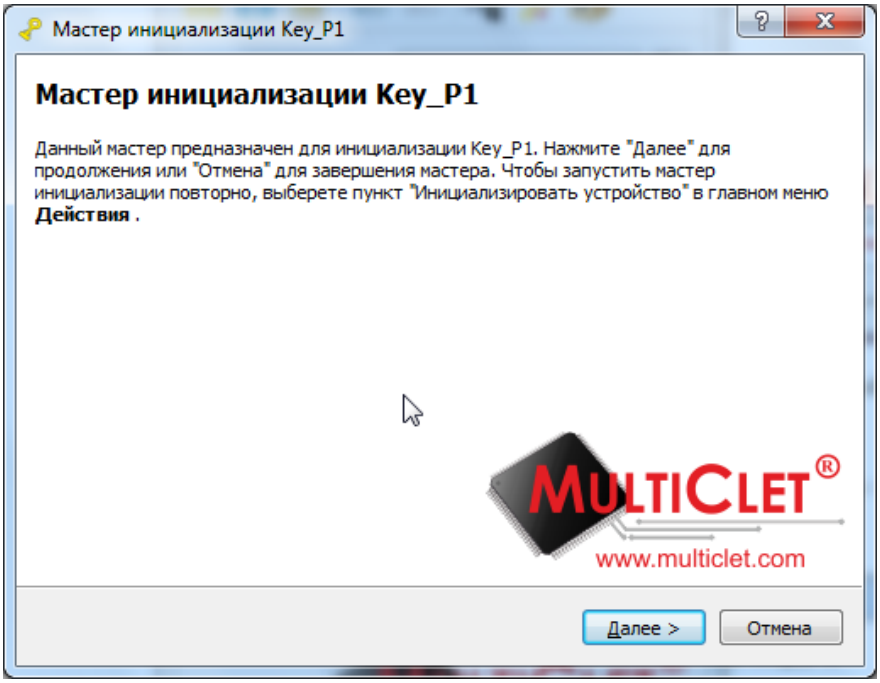

Рис. 26. Мастер инициализации устройства Key_P1

Для продолжения процедуры необходимо нажать на кнопку «Далее». Для прекращения

процедуры инициализации следует нажать на кнопку «Отмена».

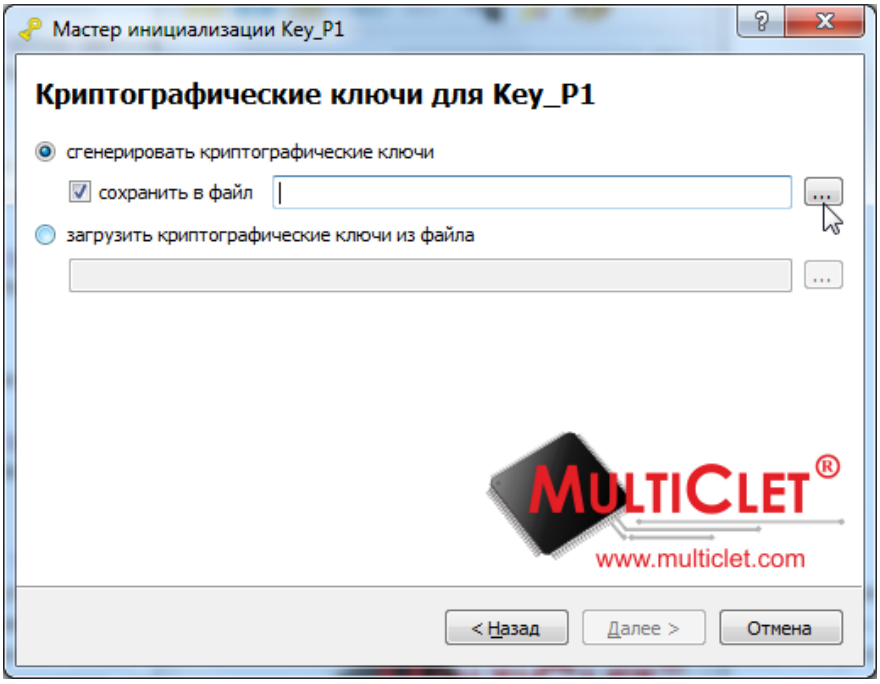

Рис. 27. Параметры инициализации устройства Key_P1

На первом этапе инициализации устройства необходимо задать параметры инициализации (рис. 27).

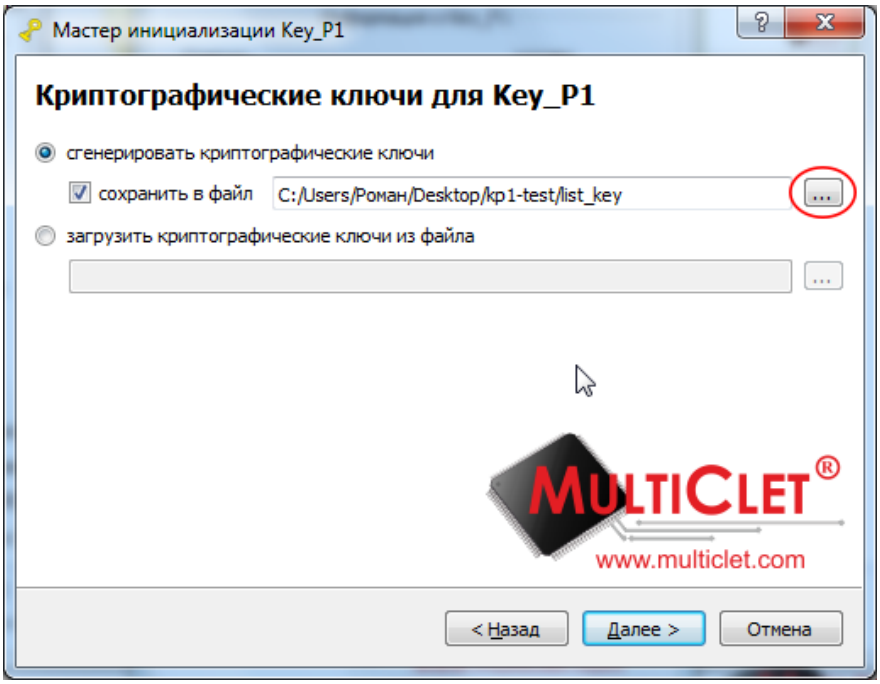

Рис. 28. Параметры инициализации устройства Key_P1

Сначала необходимо отметить «галочкой» строку **сгенерировать криптографические ключи**. Генерацию ключей необходимо производить на доверенном компьютере. По умолчанию все ключи будут храниться во внутренней памяти устройства, но есть возможность сделать резервную копию ключей. В этом случае при утере устройства будет возможность восстановить криптографические ключи и перенести их на новое устройство Key_P1. Для создания резервной копии ключей необходимо поставить «галочку» в строке **сохранить в файл** и перейти к выбору директории сохранения файла(кнопка выделена красным цветом на рис. 28). Далее следует выбрать путь и имя файла для сохранения и нажать кнопку "Сохранить"(рис. 29).

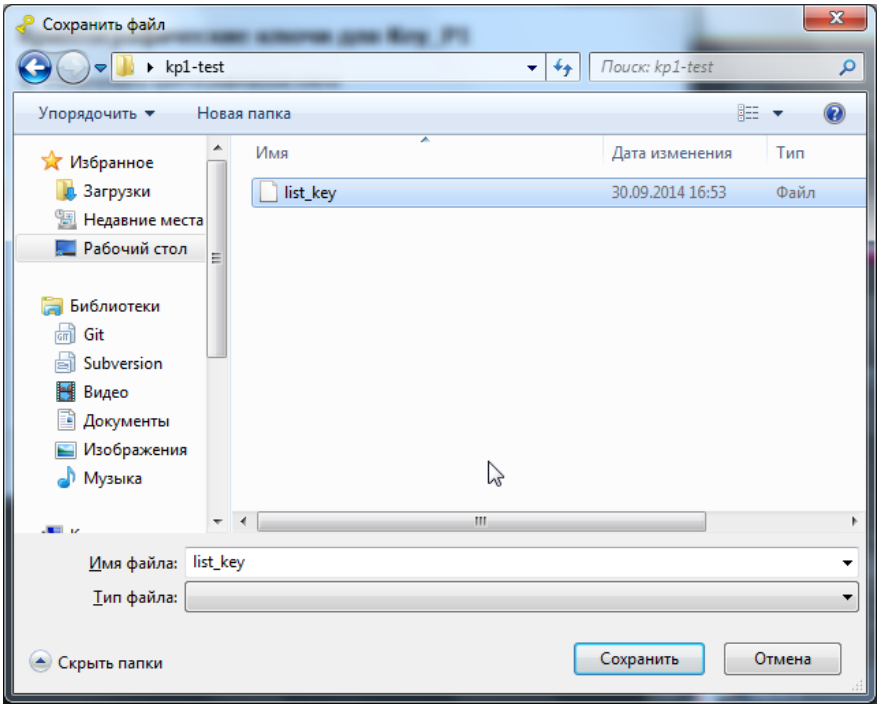

Рис. 29. Задание пути для сохранения резервной копии ключей

Если необходимо восстановить заранее сохраненные криптографические ключи, то следует отметить строку **загрузить криптографические ключи из файла** и нажать на кнопку, которая находится справа (выделена красным цветом) (рис. 30) выбрать ранее сохраненный файл с ключами.

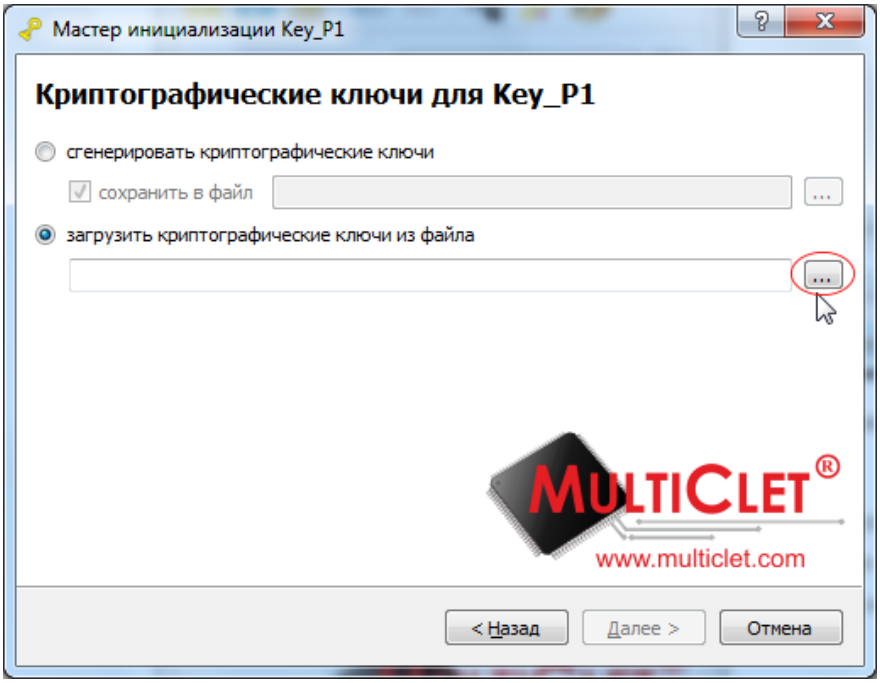

Рис. 30. Задание пути для загрузки из резервной копии ключей

Продолжение процедуры следует после нажатия на кнопку «Далее», а для прекращения процедуры следует нажать на кнопку «Отмена». В появившемся окне **PIN администратора** (рис. 31) необходимо задать PIN администратора (при использовании устройства в компании ввод PIN администратора, тревожный PIN, и PIN пользователя является прерогативой службы информационной безопасности или уполномоченного сотрудника) и нажать «Далее». Минимальное количество символов - 4, максимальное количество символов - 16, заглавные и строчные буквы различаются.

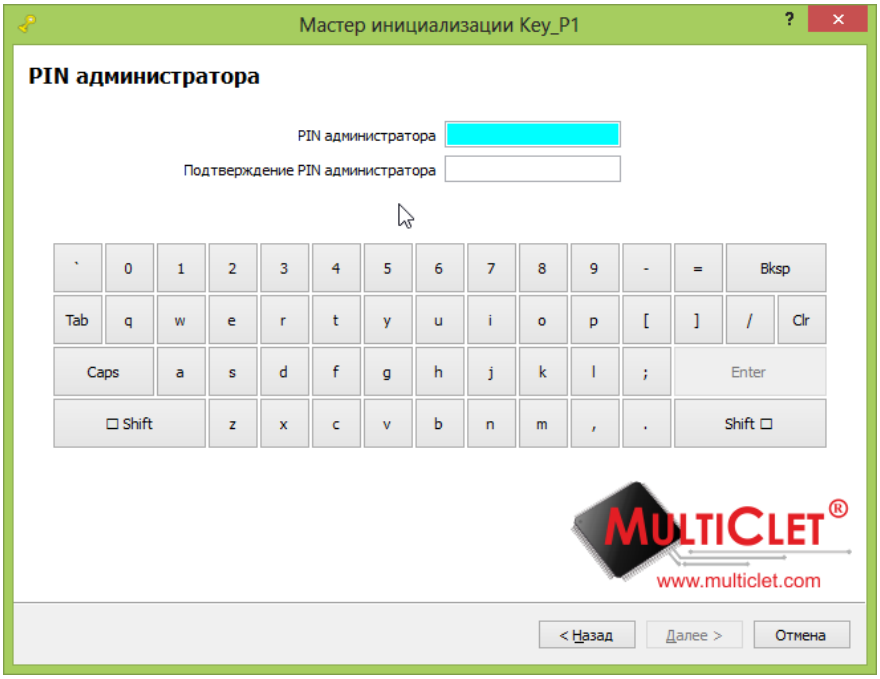

Рис. 31. Ввод PIN администратора

В появившемся окне **PIN пользователя** (рис. 32) необходимо задать PIN пользователя и нажать «Далее». Минимальное количество символов - 4, максимальное количество символов - 16, заглавные и строчные буквы различаются.

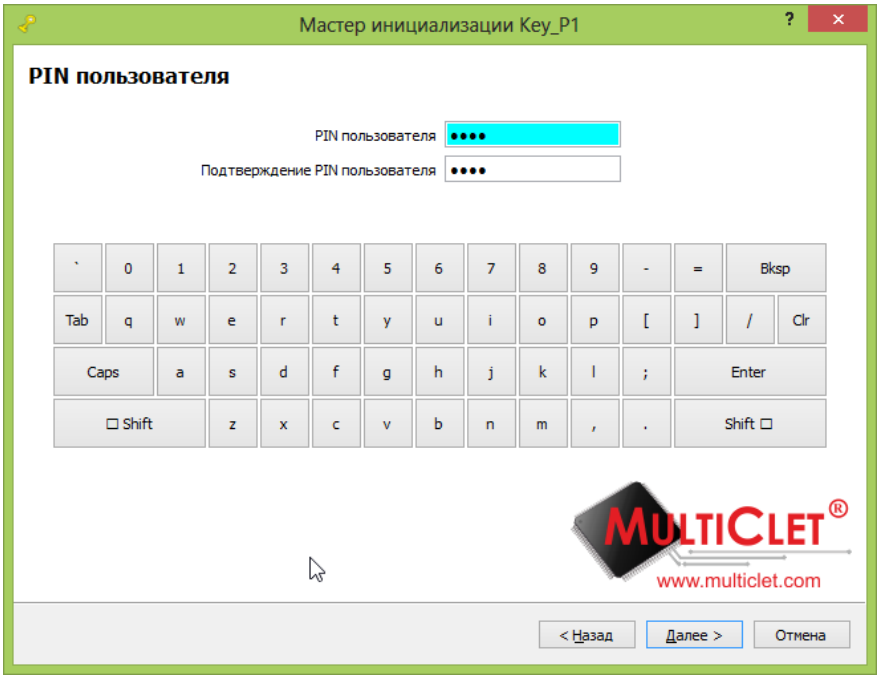

Рис. 32. Ввод PIN пользователя

В появившемся окне **Тревожный PIN** (рис. 33) необходимо задать тревожный PIN и нажать «Далее». Использование тревожного PIN необходимо для моментального удаления всех данных с устройства Key_P1. При установке тревожного PIN необходимо убедиться, чтобы он не совпадал с PIN пользователя. В случае их совпадения тревожный PIN код не сработает. Минимальное количество символов - 4, максимальное количество символов - 16, заглавные и строчные буквы различаются.

Примечание: при инициализации устройства можно отказаться от ввода тревожного PIN кода. Для этого необходимо отсавить поля для ввода пустыми и нажать кнопку "Далее". Таким образом тревожный PIN код не будет задан.

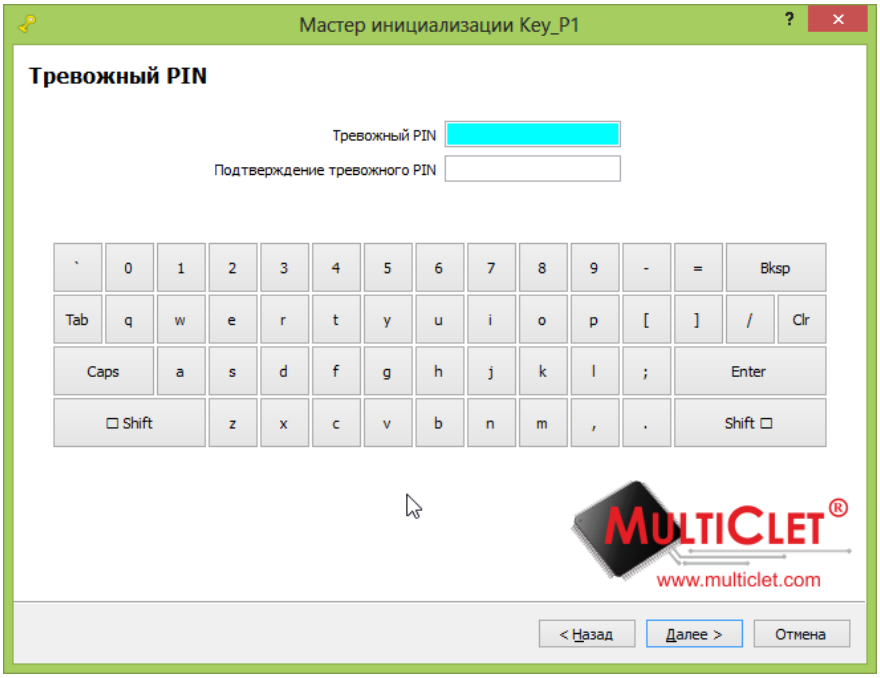

Рис. 33. Ввод тревожного PIN

Далее нужно задать имя устройства (рис. 34). Максимальное количество символов доступных для ввода - 128. В качестве метки можно указать ФИО пользователя или комбинацию имени и названия подразделения. Например, «Иванов Иван Иванович» или «Иванов И.И.(инженер)».

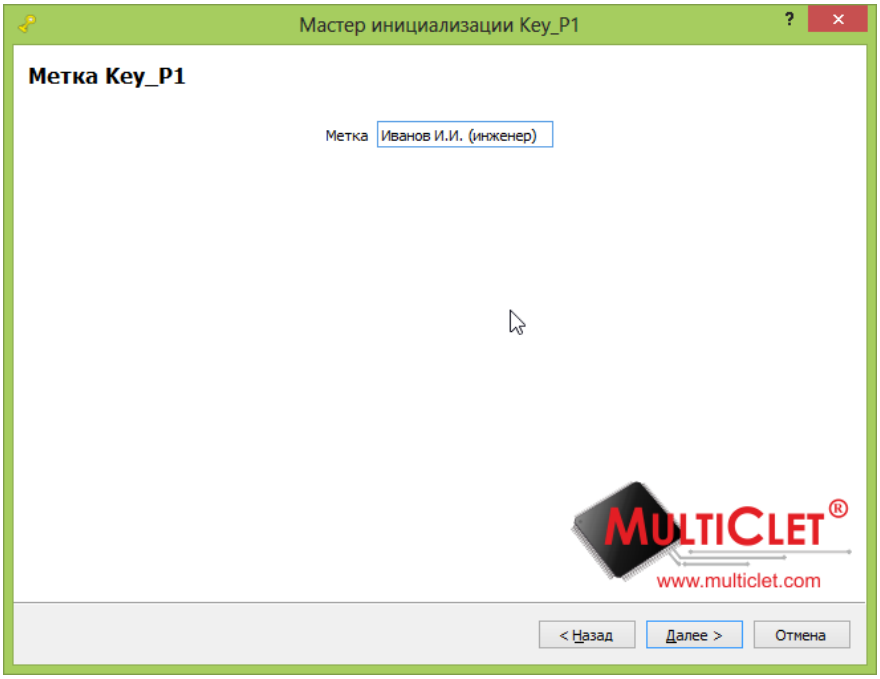

Рис. 34. Ввод имени устройства

Необходимо проверить параметры инициализации (рис. 35) и нажать кнопку «Далее».

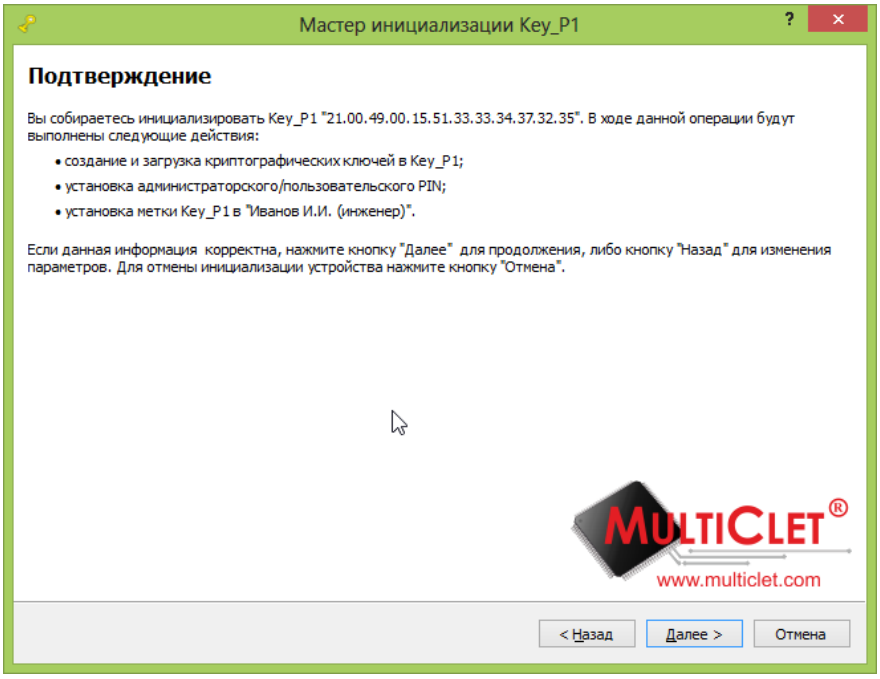

Рис. 35. Параметры инициализации

Запускается процесс инициализации по завершении которого необходимо нажать кнопку «Завершить» (рис. 36).

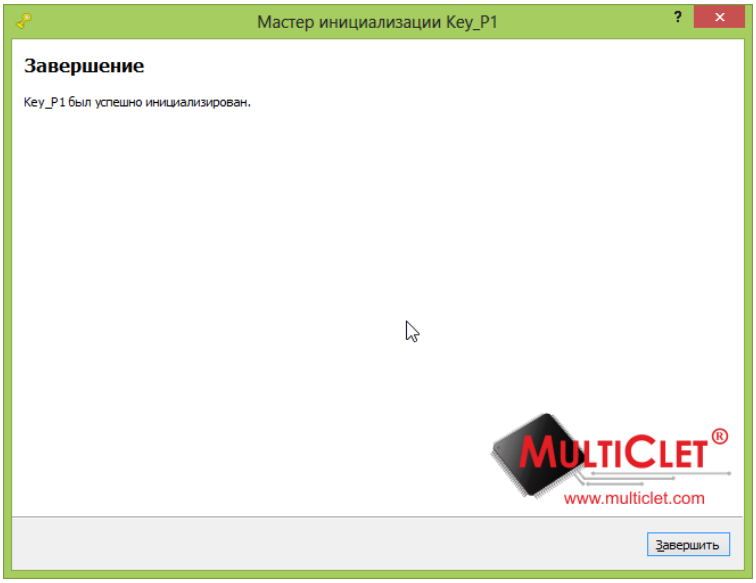

Рис. 36. Завершение инициализации

Инициализация устройства Key_P1 завершена. В главном меню устройство будет отображаться под своей меткой (именем): «Иванов И. И.» (рис. 37).

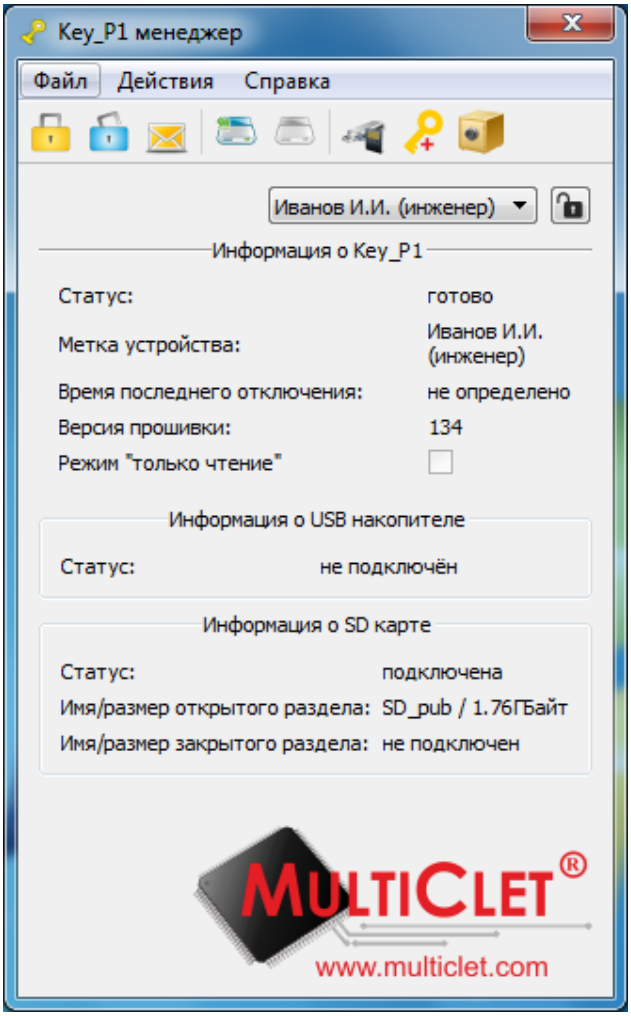

Рис. 37. Главное меню после инициализации устройства

2.7 Изменение PIN администратора

Для того, чтобы выполнить операцию по изменению PIN администратора, следует выбрать вкладку **Действия**, перейти в подменю **Администрирование** и выбрать пункт **Изменить PIN администратора** (рис. 38)

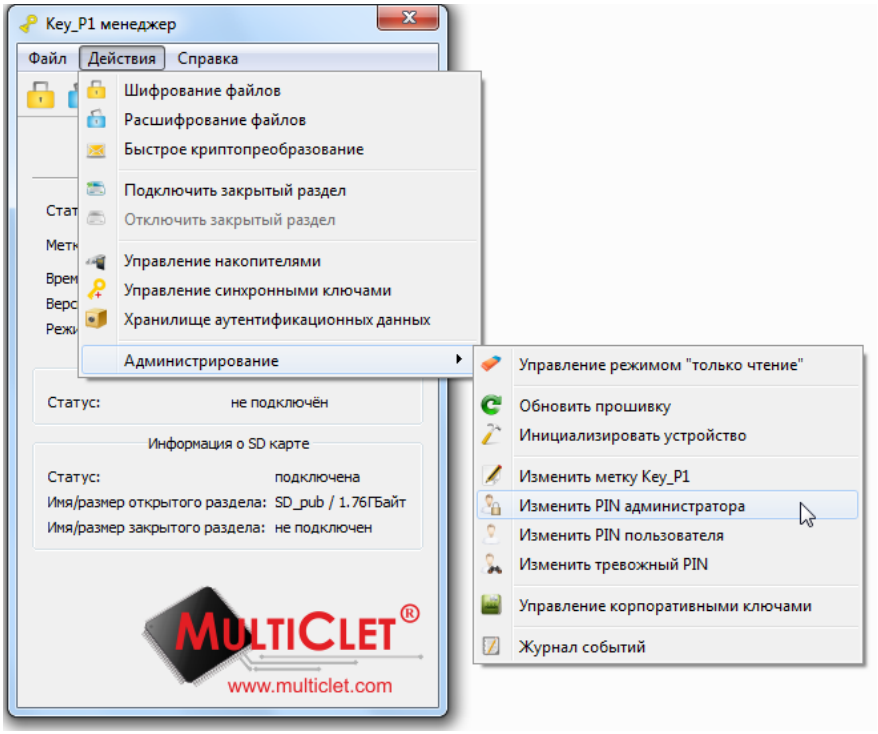

Рис. 38. Выбор команды для смены PIN администратора

В появившемся окне (рис. 39) следует ввести старый PIN администратора в строке **Текущий PIN администратора**, ввести новый PIN в строках **Новый PIN администратора** и **Подтверждение нового PIN администратора**. После выполнения этих действий необходимо нажать кнопку «OK» для сохранения изменений. Максимальное количество попыток для ввода PIN - 10, в случае 10 неправильных попыток ввода PIN администратора будет заблокирован. После этого необходимо удалить все данные с помощью специальной утилиты, а затем провести заново процедуру инициализации (Процедура инициализации описана в главе 2.6).

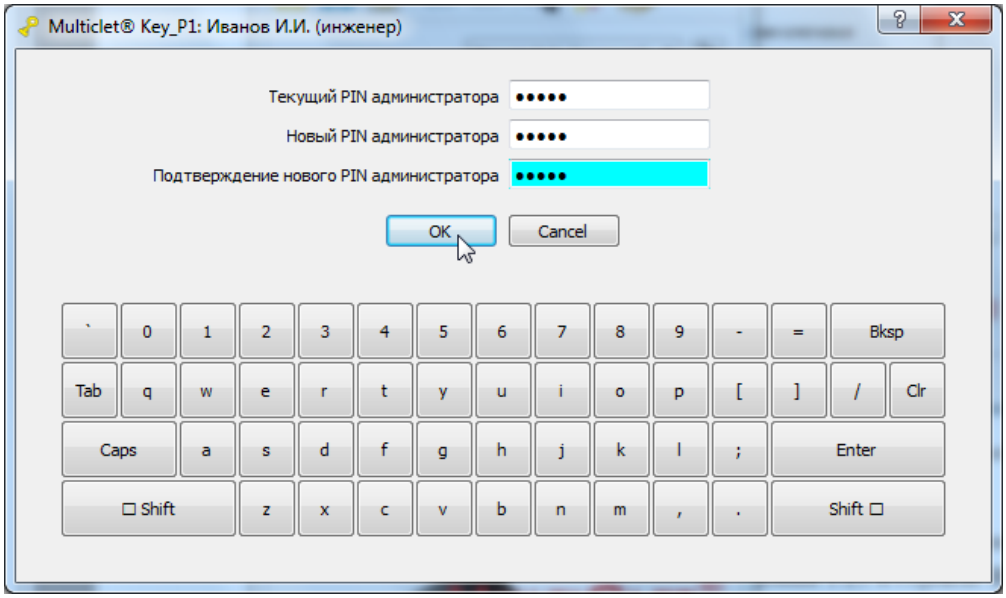

Рис. 39. Окно смены PIN администратора

2.8 Изменение PIN пользователя

Для того, чтобы выполнить операцию по изменению PIN пользователя, следует выбрать вкладку **Действия**, перейти в подменю **Администрирование** и выбрать команду **Изменить PIN пользователя** (рис. 40)

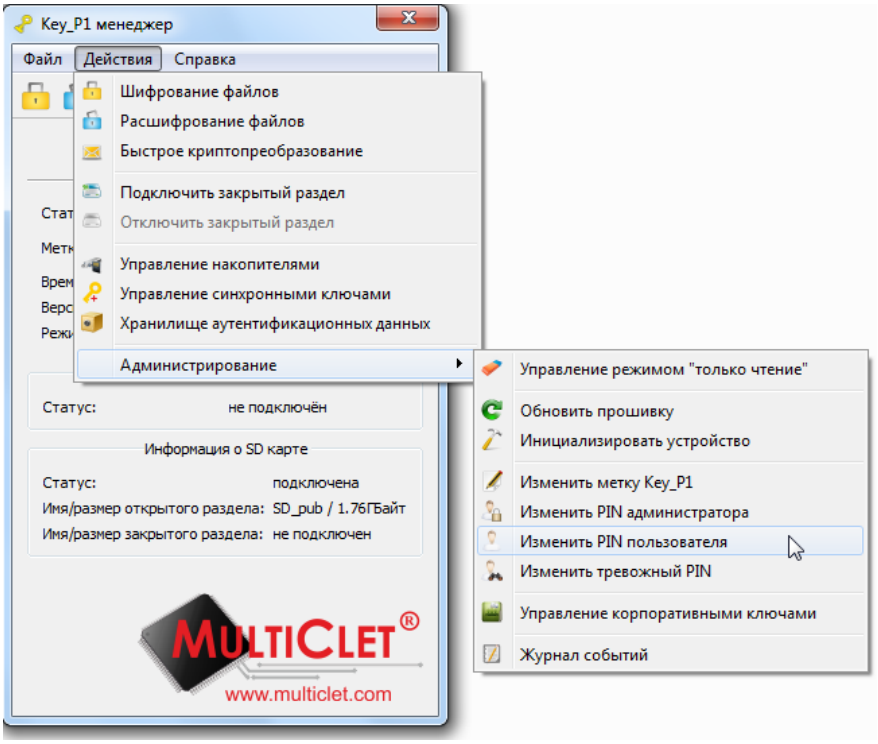

Рис. 40. Выбор команды для смены PIN пользователя

В появившемся окне, в строке **Выберите логин** следует выбрать с помощью какого PIN следует произвести смену PIN пользователя. Данное действие можно осуществить путем ввода текущего PIN пользователя либо текущего PIN администратора.

1) Использование PIN пользователя (рис. 41). Следует выбрать в строке **Логин** «пользователь». Далее в строке **Текущий PIN пользователя** следует ввести текущий PIN пользователя, а затем ввести новый PIN пользователя в строках **Новый PIN пользователя** и **Подтверждение нового PIN пользователя**. После выполнения этих действий необходимо нажать кнопку «OK» для сохранения изменений. Максимальное количество попыток для ввода PIN пользователя - 10, в случае 10 неправильных попыток ввода PIN пользователя будет заблокирован. Для его разблокировки необходимо воспользоваться PIN администратора.

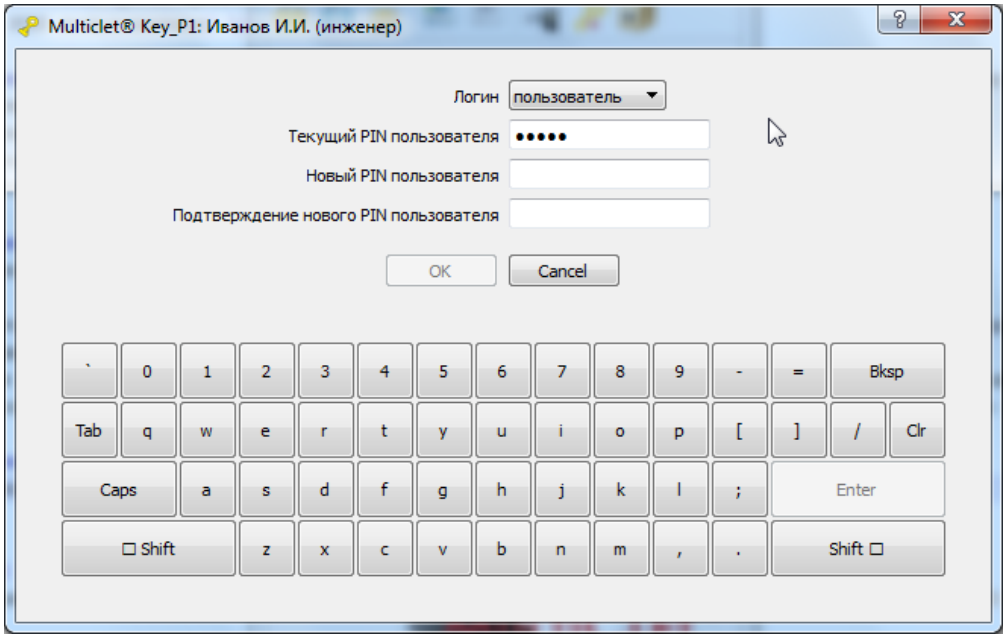

Рис. 41. Изменение PIN пользователя самим пользователем

2) Использование PIN администратора (рис. 42). Следует выбрать в строке **Логин** «администратор». Далее в строке **Текущий PIN администратора** следует ввести текущий PIN администратора, а затем ввести новый PIN пользователя в строках **Новый PIN пользователя**. После выполнения этих действий необходимо нажать кнопку «OK» для сохранения изменений. и **Подтверждение нового PIN пользователя**. Максимальное количество попыток для ввода PIN администратора - 10, в случае 10 неправильных попыток ввода PIN администратора будет заблокирован. После этого необходимо удалить все данные с помощью специльной утилиты, а затем провести заново процедуру инициализации (Процедура инициализации описана в главе 2.4).

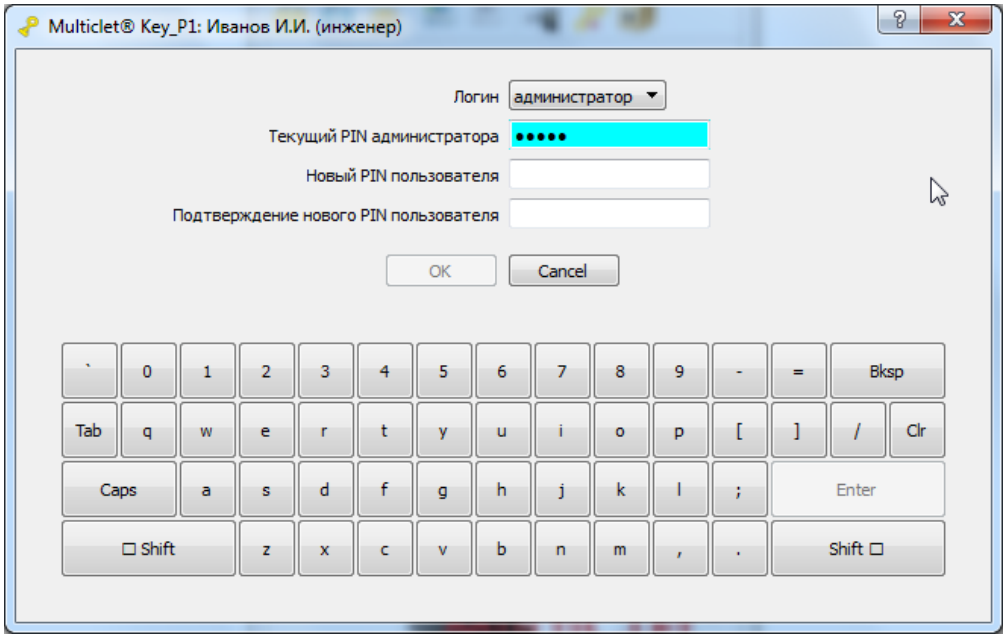

Рис. 42. Изменение PIN пользователя администратором

2.9 Изменение тревожного PIN

Для того, чтобы выполнить операцию по изменению тревожного PIN, следует выбрать вкладку **Действия**, перейти в подменю **Администрирование** и выбрать пункт **Изменить тревожный PIN** (рис. 43)

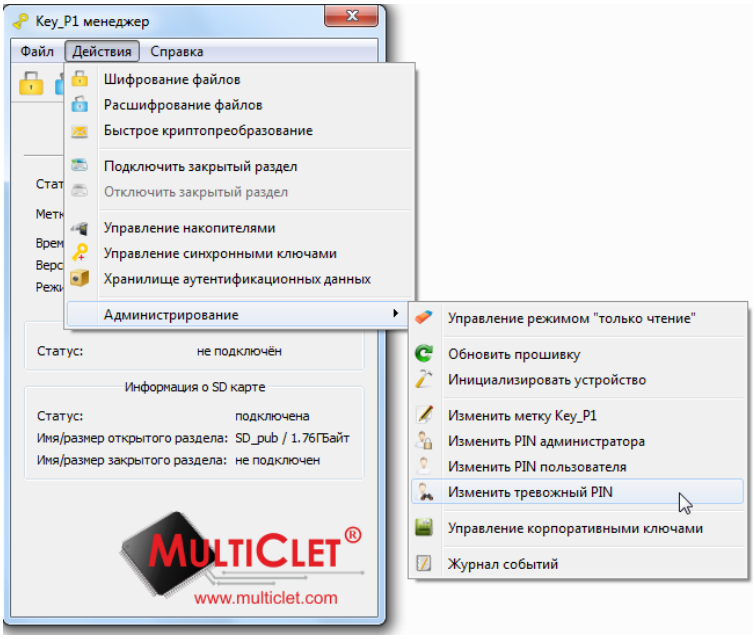

Рис. 43. Изменение тревожного PIN

В появившемся окне (рис. 44) следует ввести текущий PIN пользователя в строке **PIN пользователя**, а также ввести новый тревожный PIN в строках **Тревожный PIN** и **Подтверждение тревожного PIN**. После выполнения этих действий необходимо нажать кнопку «OK» для сохранения изменений.

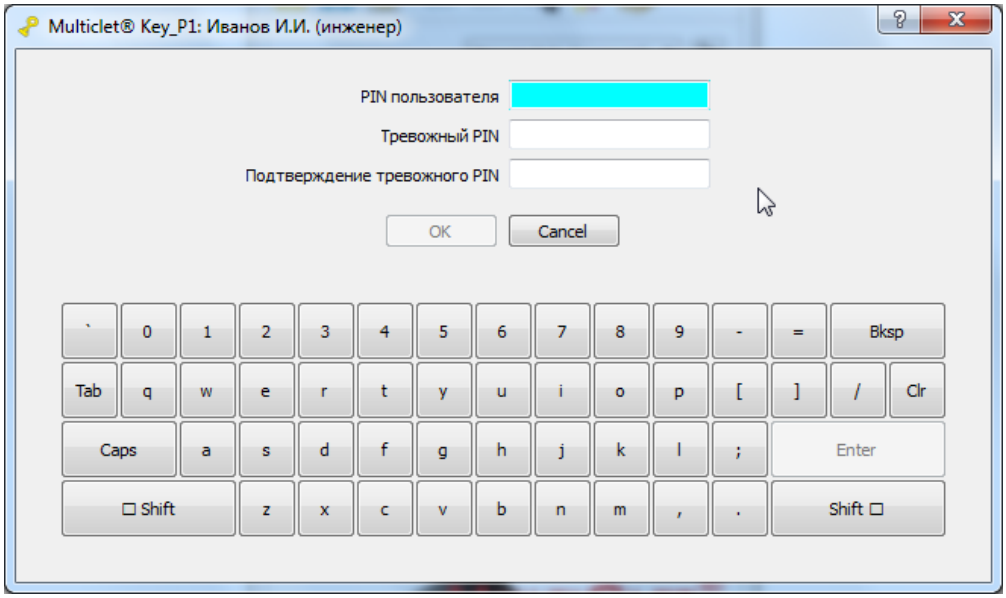

Рис. 44. Изменение тревожного PIN

2.10 Изменение метки устройства

Для того, чтобы выполнить операцию по изменению метки (имени) устройства, следует выбрать вкладку **Действия** перейти в подменю **Администрирование** и выбрать пункт **Изменить метку Key_P1** (рис. 45). Данная операция может выполняться только администратором.

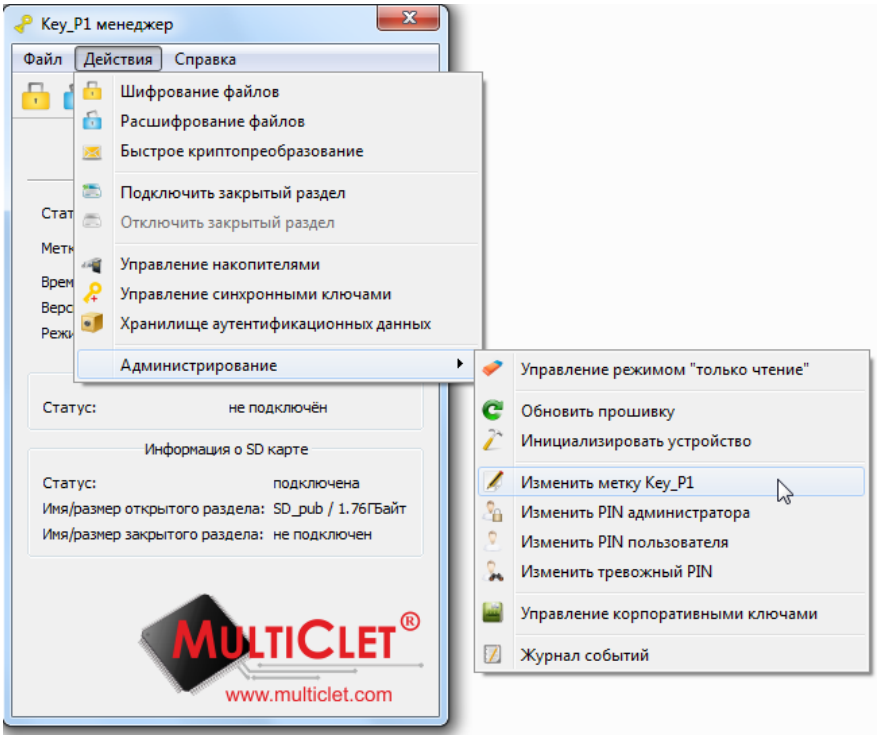

Рис. 45. Изменение метки устройства

В появившемся окне, в строке **Метка устройства** (рис. 46) следует ввести новую метку (имя) устройства и нажать кнопку «OK».

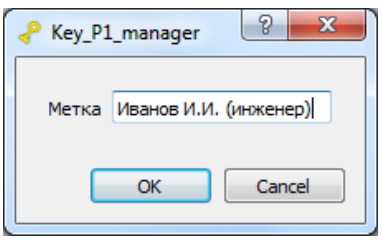

Рис. 46. Ввод метки устройства

Далее следует ввести текущий PIN администратора в строке **PIN администратора** (рис. 47) и нажать кнопку «OK».

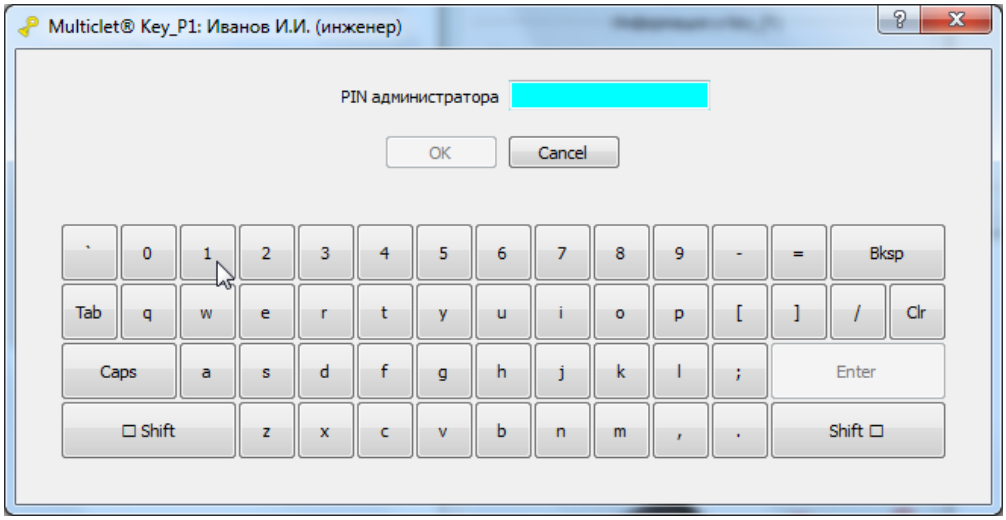

Рис. 47. Ввод PIN администратора

Если все действия были сделаны правильно, то в главном меню приложения, в строке **Метка устройства** будет отображаться новая метка устройства.

3 Использование устройства Key_P1

3.1 Управление накопителями

3.1.1 Создание закрытого раздела на USB накопителе

Для того, чтобы выполнить создание закрытого (шифрованного) раздела на USB накопителе следует последовательно выбрать вкладку **Действия** и выбрать пункт **Управление накопителями** (рис. 48).

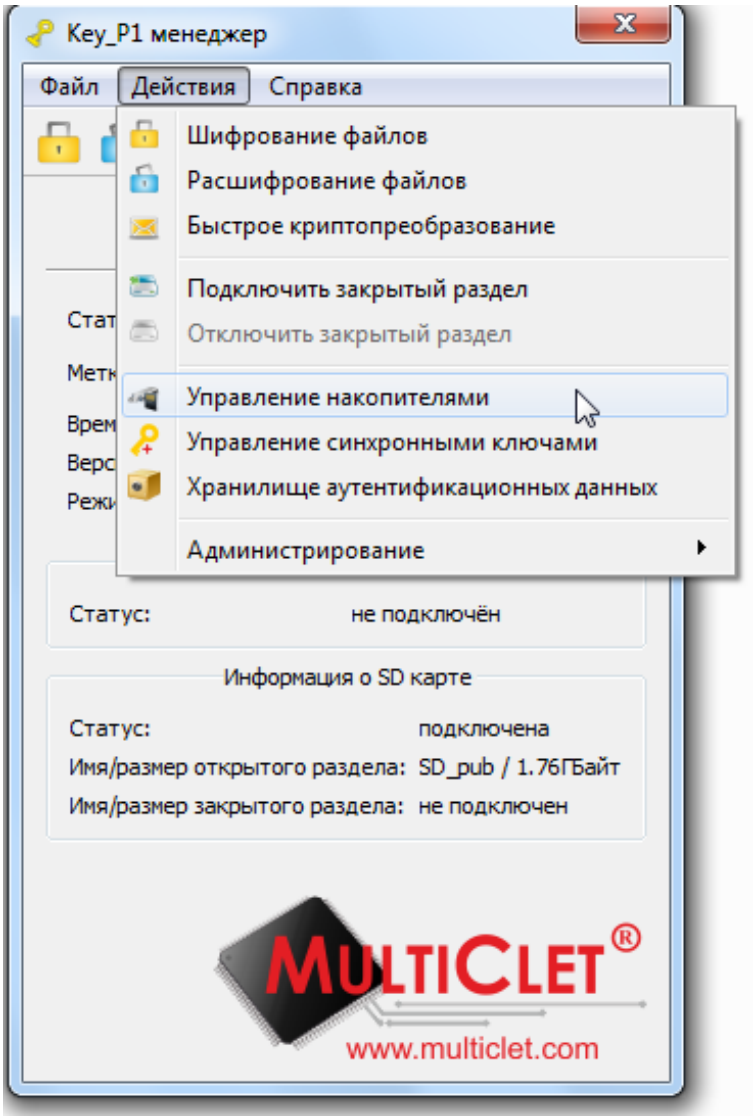

Рис. 48. Управление накопителями

В открывшемся окне **Управление накопителями** (рис. 49) следует выбрать в стро-

ке **Накопитель** «USB накопитель», в строке **Действие** выбрать «Инициализировать накопитель», в строке **Метка открытого раздела** ввести имя открытого раздела, в строке **Размер открытого раздела** указать размер открытого раздела, в строке **Метка закрытого раздела** ввести имя закрытого раздела, в строке **Размер закрытого раздела** указать размер закрытого раздела.

Внимание: в результате запуска процесса инициализации накопителя будет произведено его форматирование и все данные на нём будут удалены.

После выполнения всех действия необходимо нажать «OK».(рис. 49).

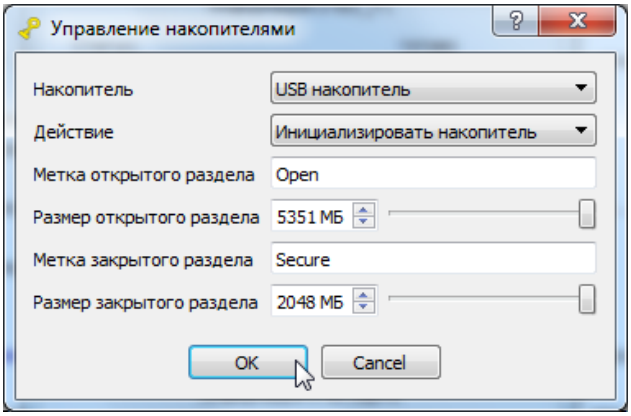

Рис. 49. Инициализация накопителя

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK» (рис. 50).

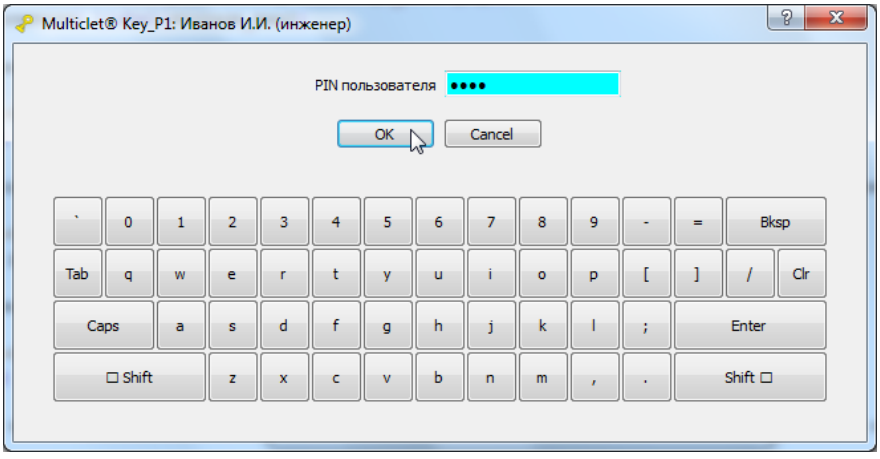

Рис. 50. Ввод PIN пользователя

Появится окно с предложением подключить закрытый раздел (рис. 51). Следует отметить «галочкой» закрытый раздел, который необходимо подключить и нажать «OK».

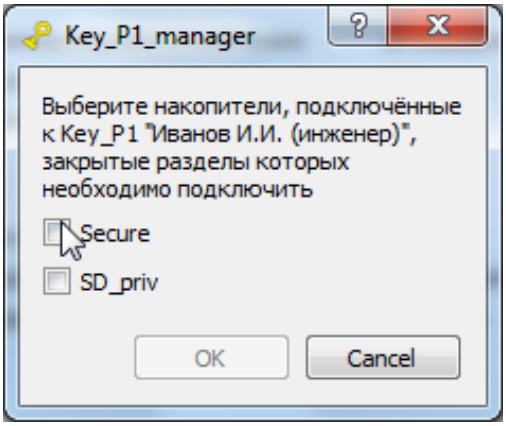

Рис. 51. Подключения закрытого раздела

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK» (рис. 52).

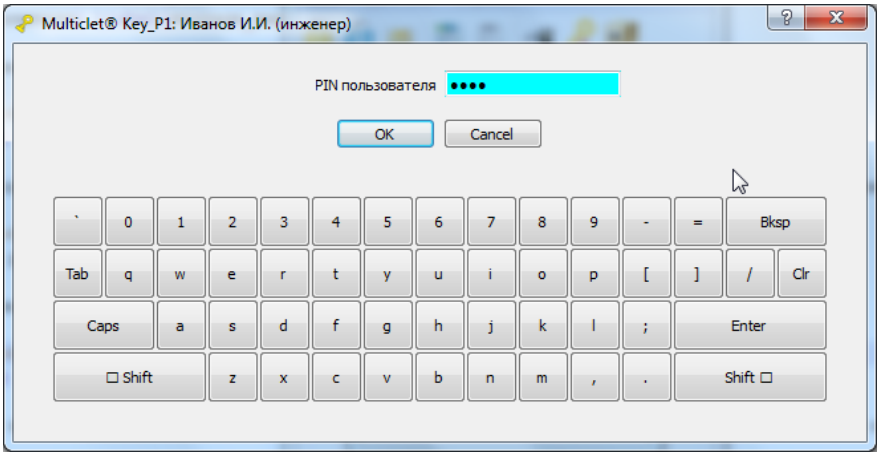

Рис. 52. Ввод PIN пользователя

После выполнения этих действий в главном меню в поле **Информация о USB накопителе** появится информация о созданых разделах. В операционной системе закрытый раздел будет отображаться отдельным диском в списке устройств со съемными носителями (рис. 53).

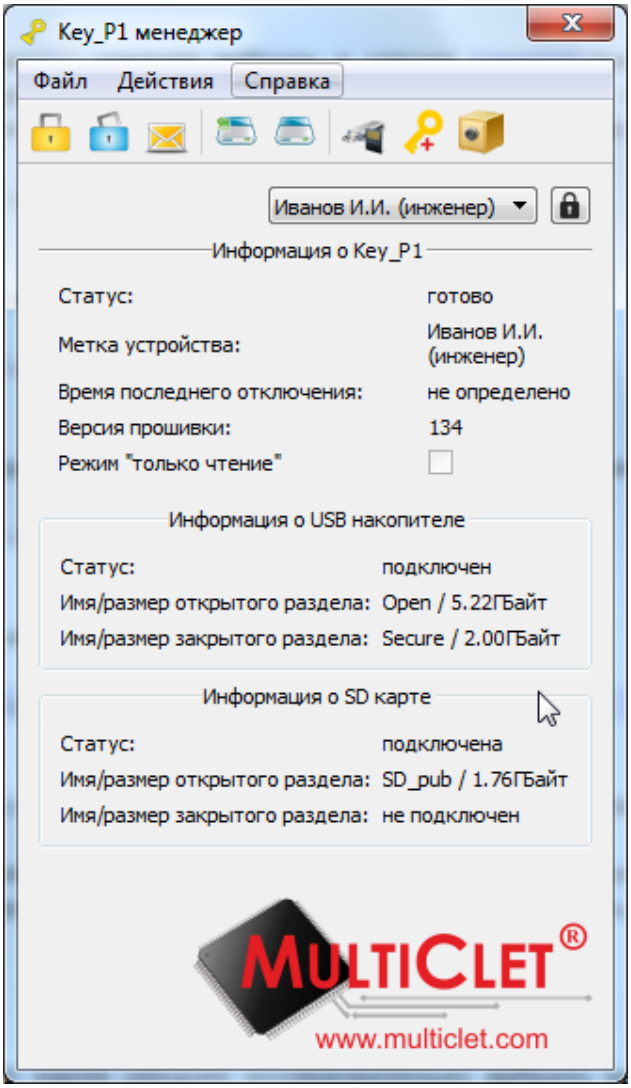

Рис. 53. Главное меню приложения

Для того, чтобы выполнить операцию по изменению имени разделов или форматированию закрытого раздела, необходимо последовательно выбрать вкладку **Действия** перейти в подменю **Администрирование** и выбрать пункт **Управление накопителями**. В открывшемся окне **Управление накопителями** следует выбрать в строке **Накопитель** «USB накопитель», в строке **Действие** выбрать необходимое действие с накопителем. Далее следует произвести все необходимые изменения.

3.1.2 Создание закрытого раздела на SD карте

Для того, чтобы выполнить создание закрытого (шифрованного) раздела на SD карте, следует последовательно выбрать вкладку **Действия** и пункт **Управление накопителями** (рис. 54).

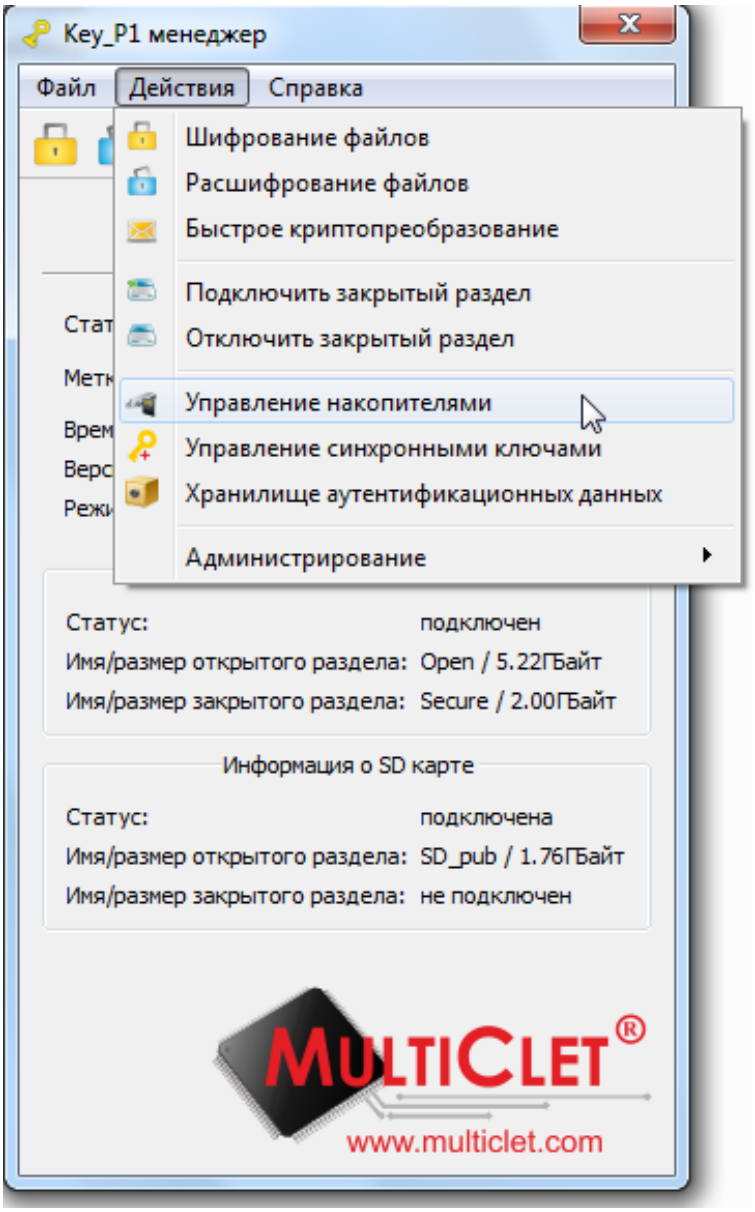

Рис. 54. Управление накопителями

В открывшемся окне **Управление накопителями** (рис. 55) следует выбрать в строке **Накопитель** «SD карта», в строке **Действие** выбрать «Инициализировать накопитель», в строке **Метка открытого раздела** ввести имя открытого раздела, в строке **Размер открытого раздела** указать размер открытого раздела, в строке **Метка за-**

крытого раздела ввести имя закрытого раздела, в строке **Размер закрытого раздела** указать размер закрытого раздела.

Внимание: в результате запуска процесса инициализации накопителя будет произведено его форматирование и все данные на нём будут удалены.

После выполнения всех действий необходимо нажать «OK».

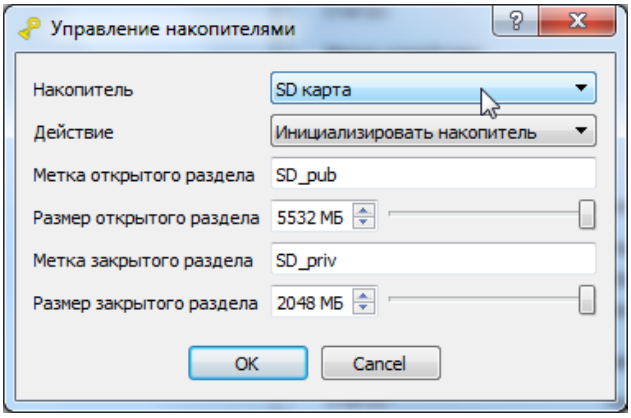

Рис. 55. Инициализация накопителя

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK» (рис. 56).

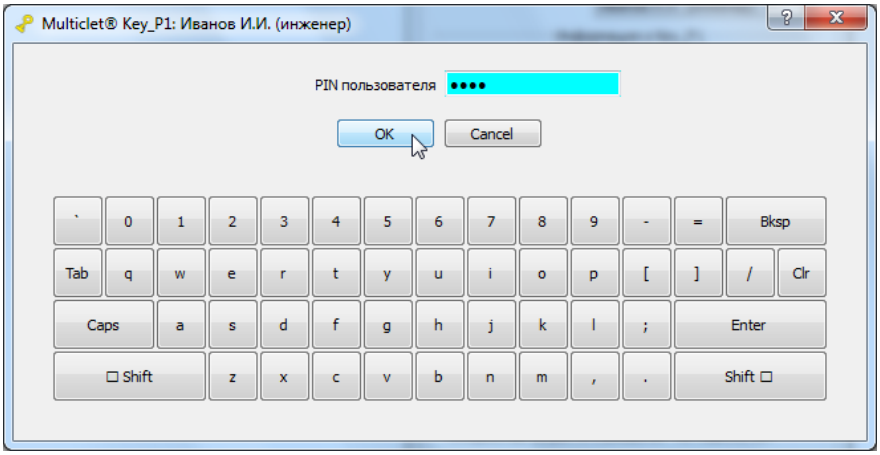

Рис. 56. Ввод PIN пользователя

Появится окно с предложением подключить закрытый раздел (рис. 57), здесь следует отметить «галочкой» подключаемый раздел и нажать «OK».

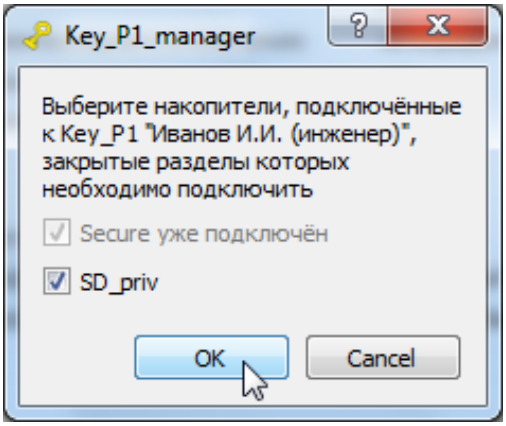

Рис. 57. Подключение закрытого раздела

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK» (рис. 58).

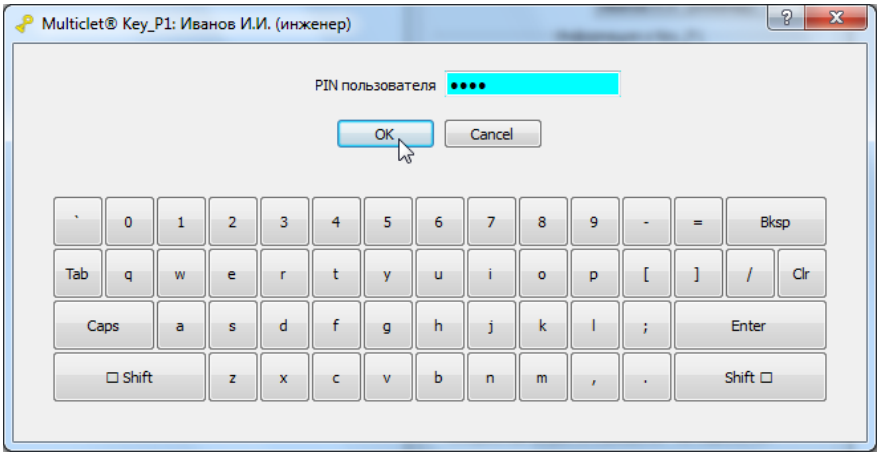

Рис. 58. Ввод PIN пользователя

После выполнения этих действий в главном меню в поле **Информация о SD карте** появится информация о созданых разделах. В операционной системе закрытый раздел будет отображаться отдельным диском в списке устройств со съемными носителями(рис. 59).

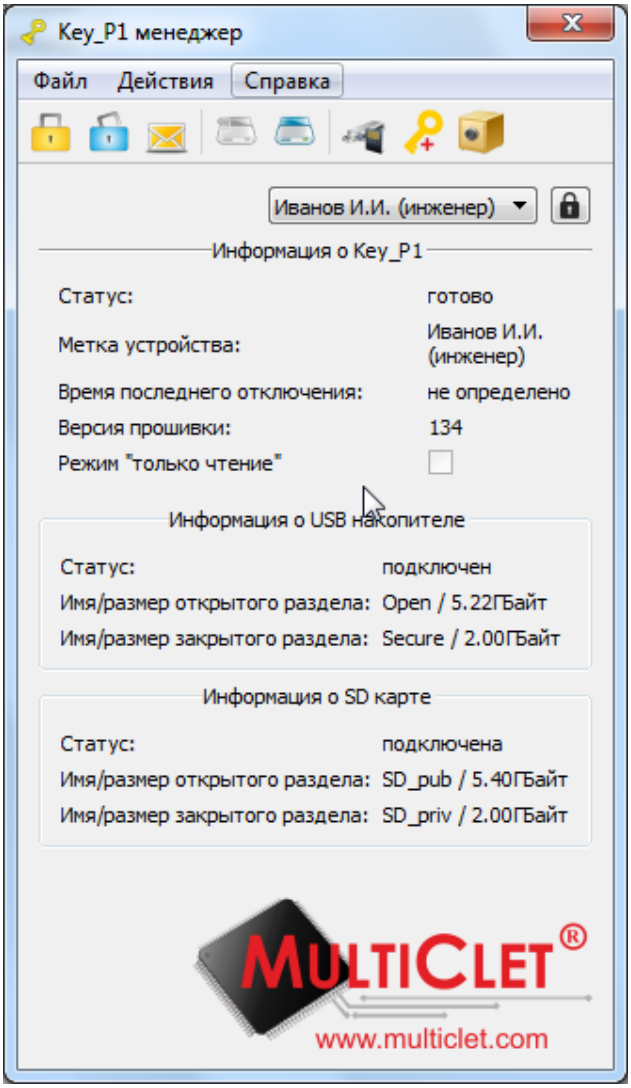

Рис. 59. Главное меню приложения

Для того, чтобы выполнить операцию по изменению имени разделов или форматированию закрытого раздела, необходимо последовательно выбрать вкладку **Действия** и команду **Управление накопителями**. В открывшемся окне **Управление накопителями** следует выбрать в строке **Накопитель** «SD карта», в строке **Действие** выбрать необходимое действие с накопителем. Далее следует произвести все необходимые изменения.

3.1.3 Подключение закрытого раздела на USB накопителе

Для того, чтобы выполнить процедуру подключения созданного ранее закрытого раздела (ов) на USB накопителе, необходимо последовательно выбрать вкладку **Действия** и команду **Подключить закрытый раздел** (рис. 60).

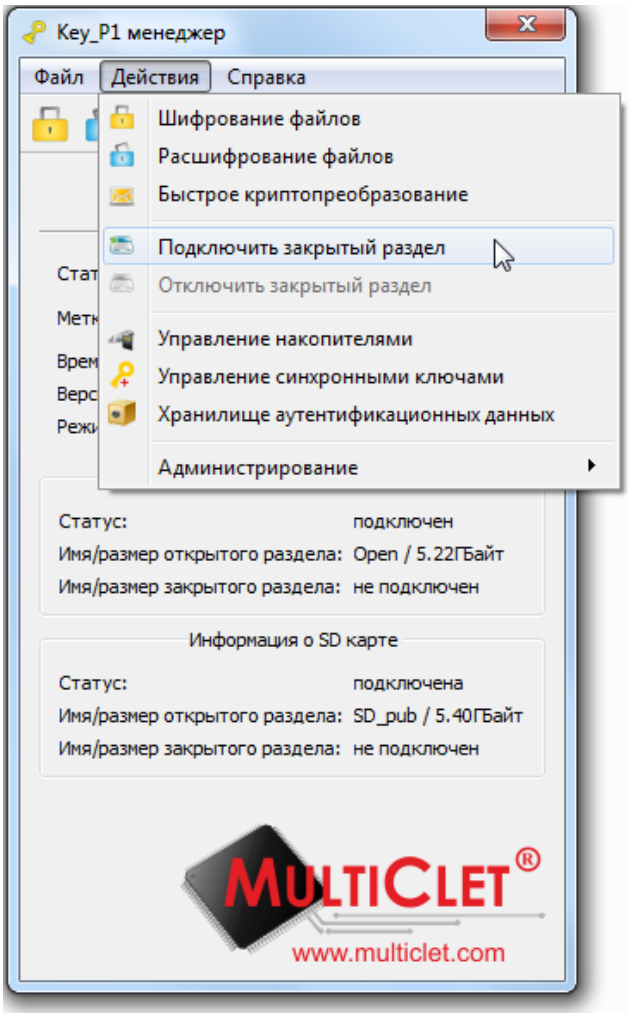

Рис. 60. Подключение закрытого раздела

В открывшемся окне необходимо отметить «галочкой» закрытый раздел, который следует подключить и нажать «ОК» (рис. 61).

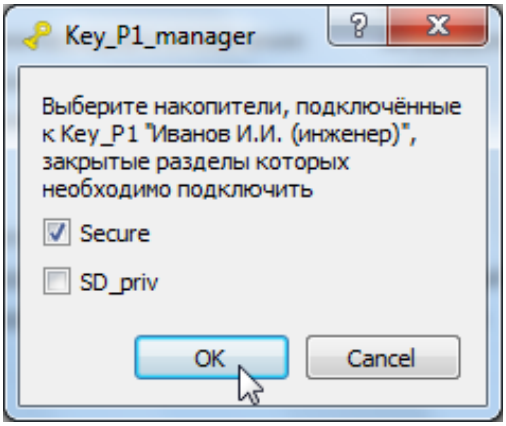

Рис. 61. Выбор накопителя

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK» (рис. 62).

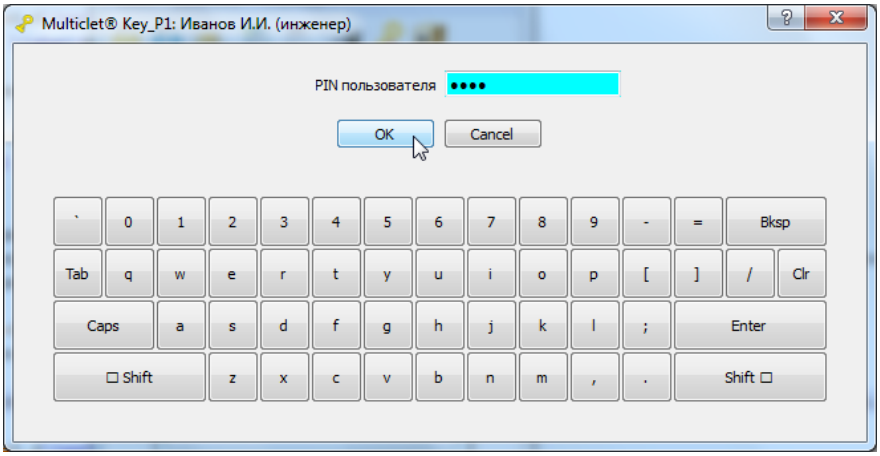

Рис. 62. Ввод PIN пользователя

Главное меню приложения примет вид как на рис. 63

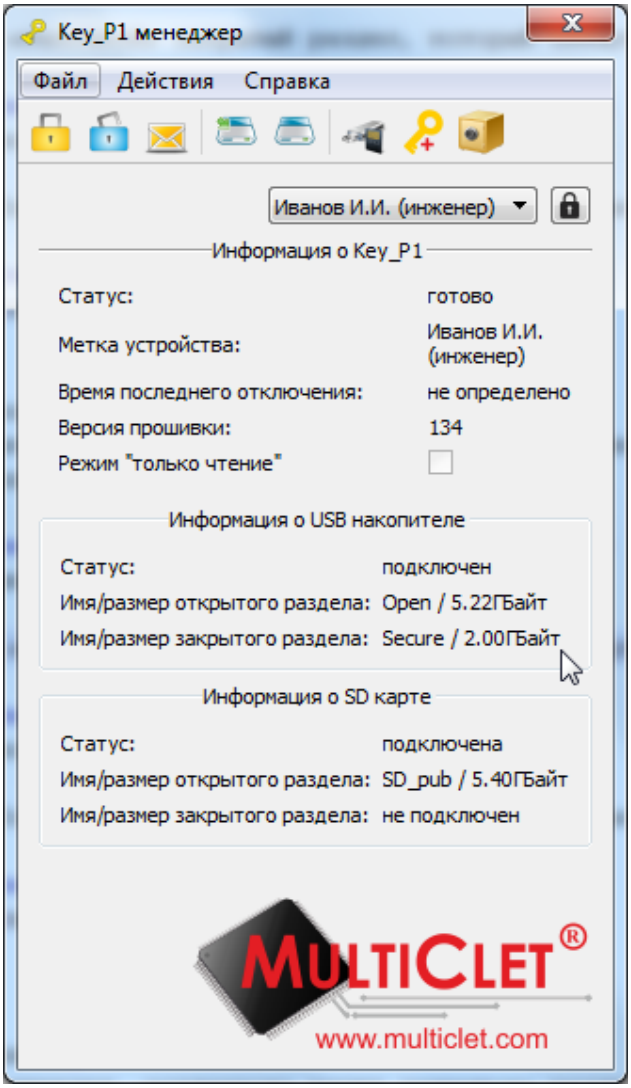

Рис. 63. Главное меню приложения

3.1.4 Подключение закрытого раздела на SD карте

Для того, чтобы выполнить процедуру подключения созданного ранее закрытого раздела (ов) на SD карте, необходимо последовательно выбрать вкладку **Действия** и команду **Подключить закрытый раздел** (рис. 64).

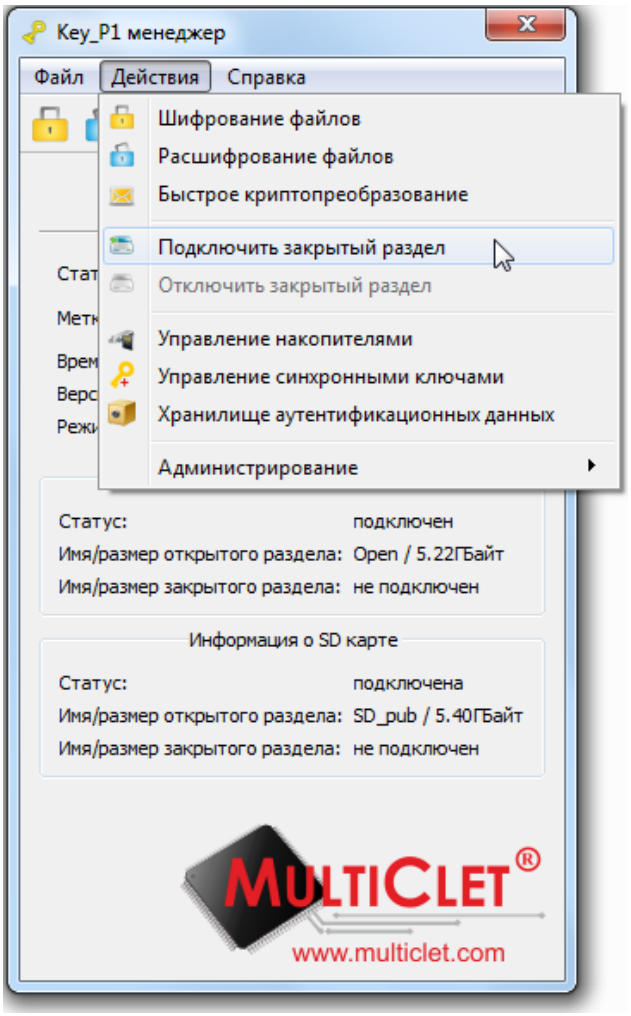

Рис. 64. Подключение закрытого раздела

В открывшемся окне необходимо отметить «галочкой» закрытый раздел, который следует подключить и нажать «ОК» (рис. 65).

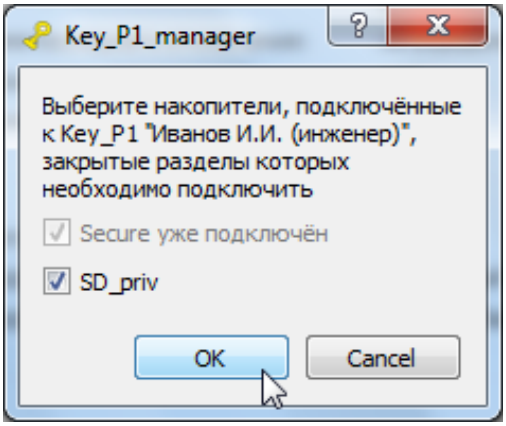

Рис. 65. Выбор накопителя

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK» (рис. 66).

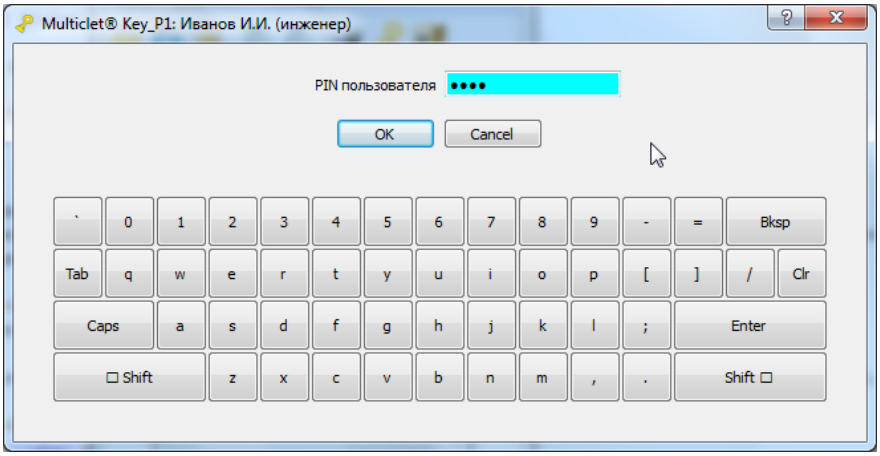

Рис. 66. Ввод PIN пользователя

Главное меню приложения примет вид как на рис. 67

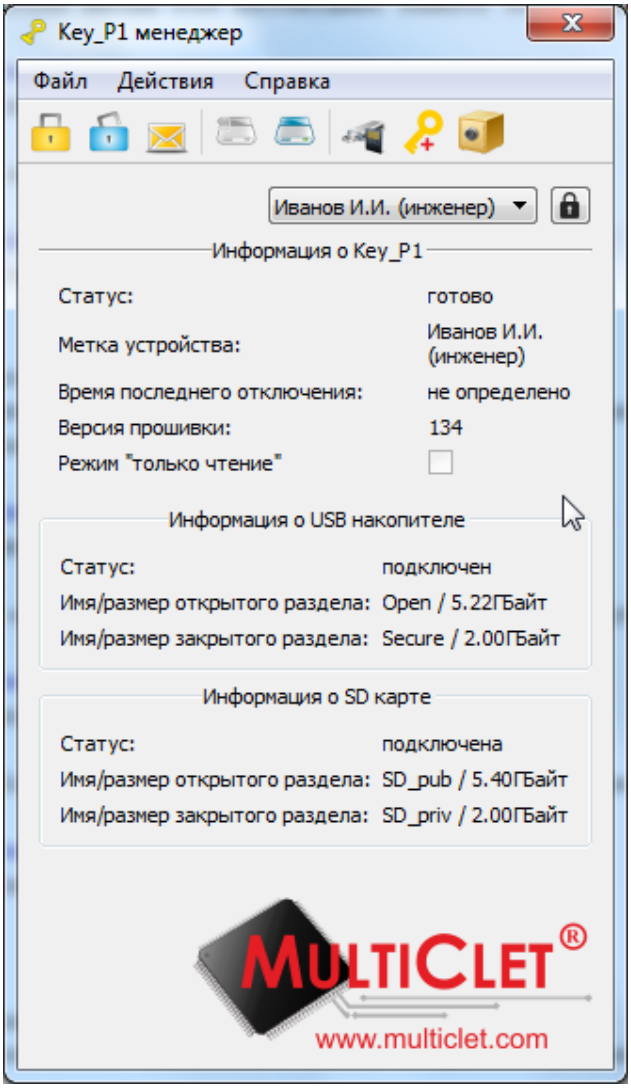

Рис. 67. Главное меню приложения

3.1.5 Отключение закрытого раздела

Для того, чтобы выполнить процедуру отключения созданного ранее закрытого раздела (ов), необходимо последовательно выбрать вкладку **Действия** и команду **Отключить закрытый раздел** (рис. 68).

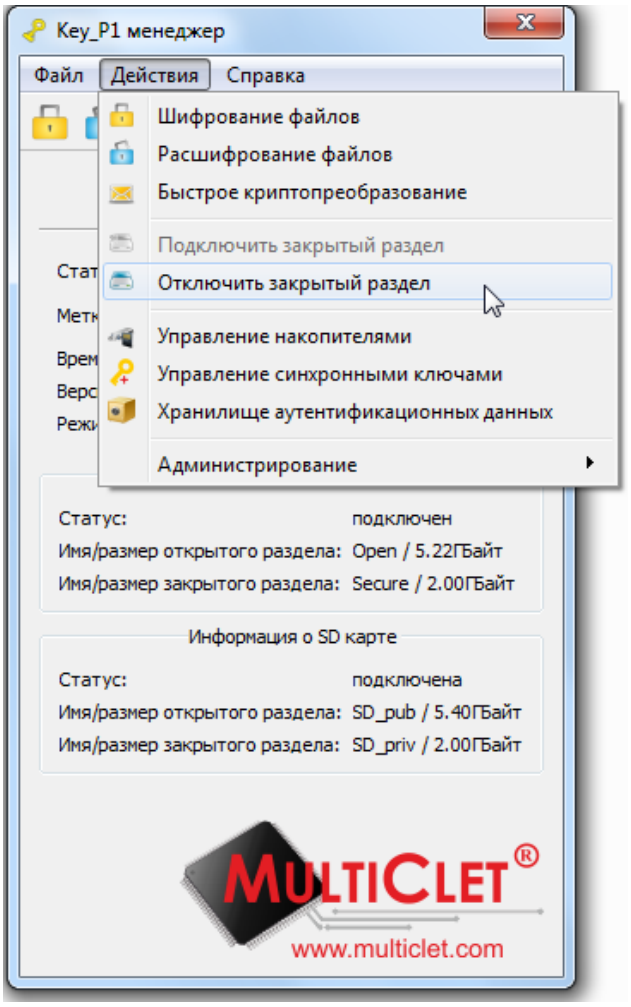

Рис. 68. Отключение закрытого раздела

В открывшемся окне необходимо отметить «галочкой» закрытый раздел, который следует отключить и нажать «OK» (рис. 69).

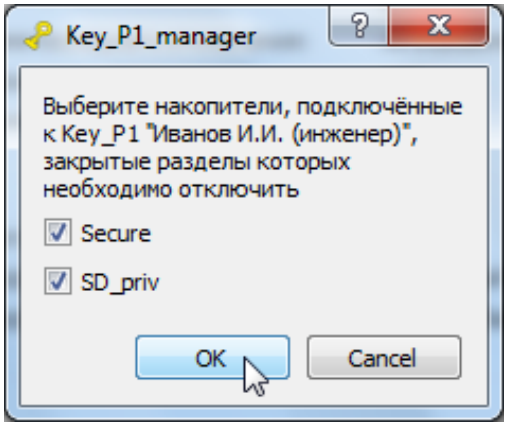

Рис. 69. Выбор накопителя

Главное меню приложения примет вид как на рис. 70

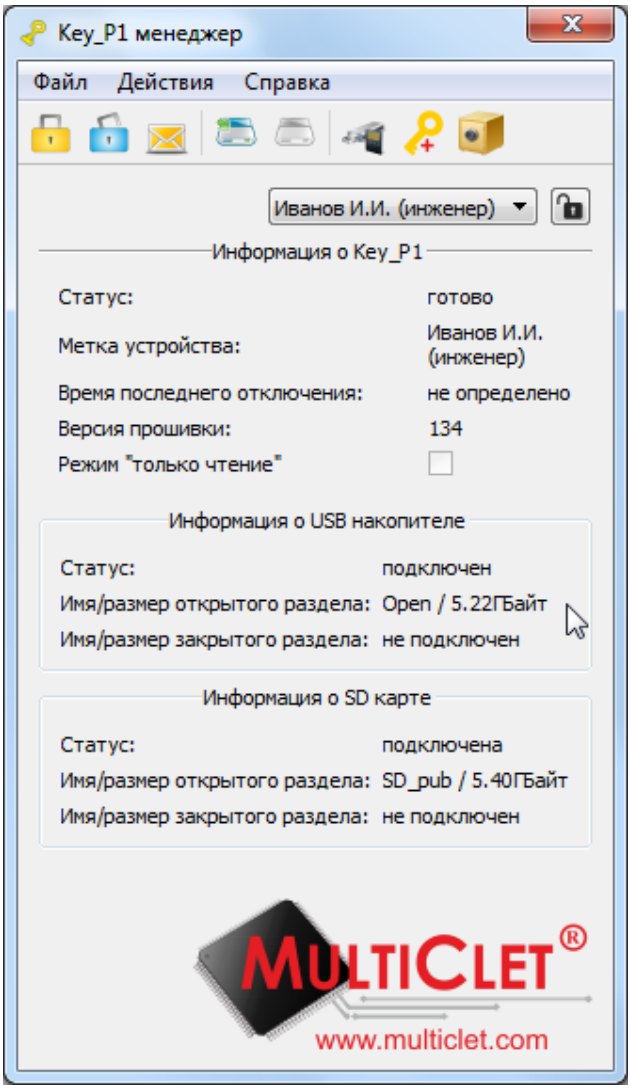

Рис. 70. Главное меню приложения

3.1.6 Использование закрытого раздела

Закрытый раздел необходим для хранения информации в зашифрованном виде. Для того, чтобы зашифровать информацию, необходимо копировать файл (ы) в ранее созданный закрытый раздел. Данную операцию можно выполнить как с помощью команды ОС «Копирование», так и с помощью с помощью «перетаскивания» файла (ов) в закрытый раздел (рис. 71).

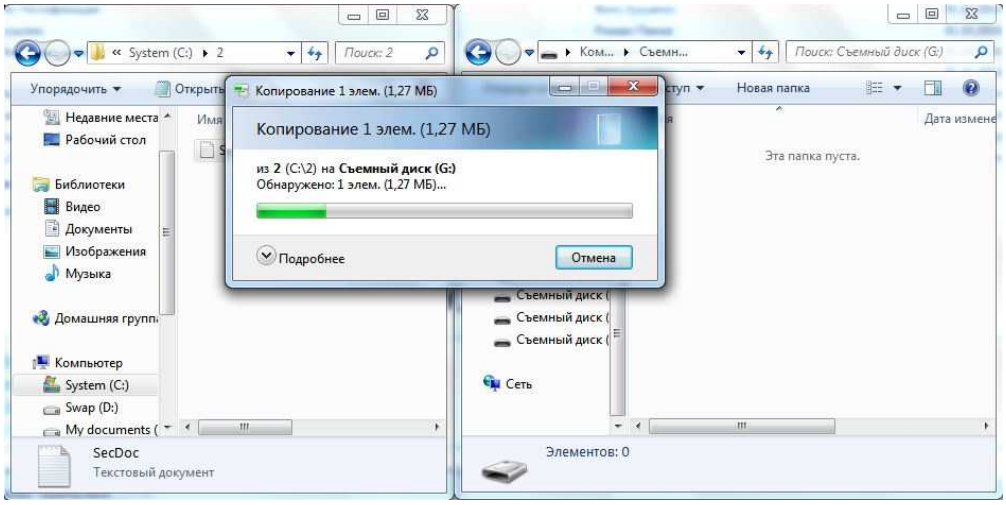

Рис. 71. Копирование информации в закрытый раздел

Данная процедура идентична как для закрытого раздела, созданного на USB накопителе, так и для закрытого раздела, созданного на SD карте.

Для того, чтобы расшифровать находящийся в закрытом разделе файл (ы), достаточно копировать файл (ы) из закрытого раздела в любое, доступное для переноса файла, место файловой системы.

3.1.7 Удаление закрытого раздела

Для того, чтобы выполнить удаление закрытого (шифрованного) раздела на USB накопителе, следует последовательно выбрать вкладку **Действия** и выбрать пункт **Управление накопителями** (рис. 72).

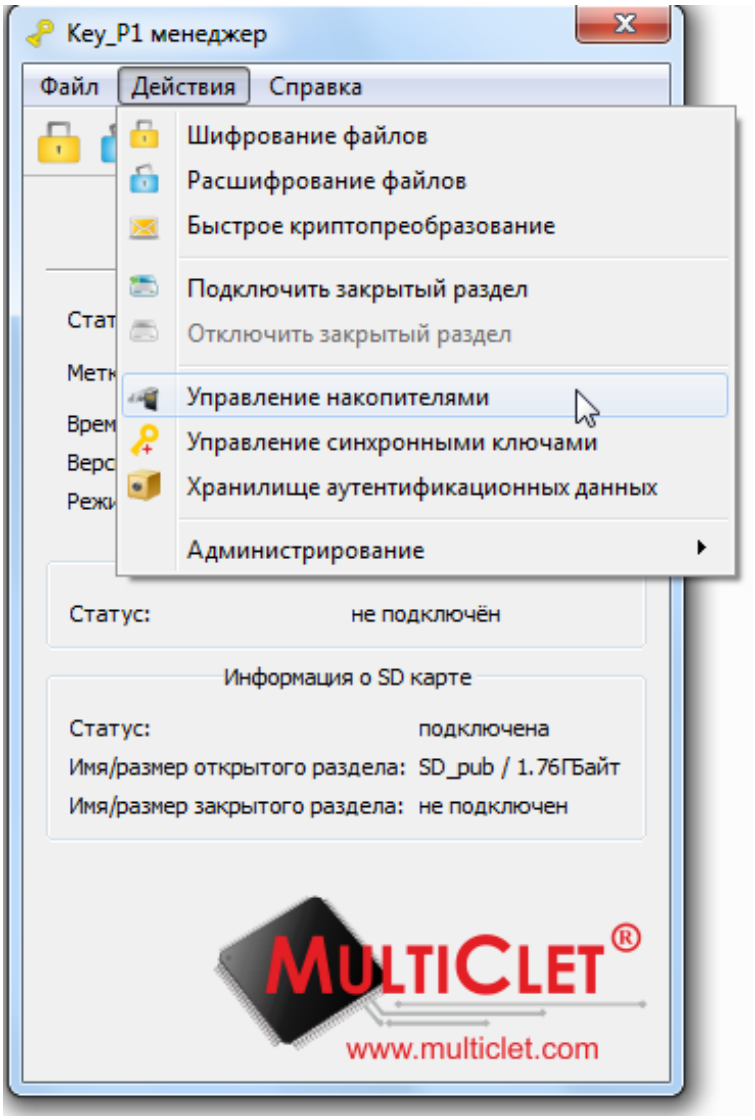

Рис. 72. Управление накопителями

В открывшемся окне **Управление накопителями** (рис. 73) следует выбрать в строке **Накопитель** «USB накопитель»(или «SD накопитель»), в строке **Действие** выбрать «Инициализировать накопитель», в строке **Метка закрытого раздела** ввести имя закрытого раздела, в строке **Размер закрытого раздела** указать размер закрытого раздела равным **0** Мбайт, в строке **Метка открытого раздела** ввести имя открытого раздела, в строке **Размер открытого раздела** указать максимально возможный

размер открытого раздела.

Внимание: в результате запуска процесса инициализации накопителя будет произведено его форматирование и все данные на нём будут удалены.

После выполнения всех действия необходимо нажать «OK».(рис. 73).

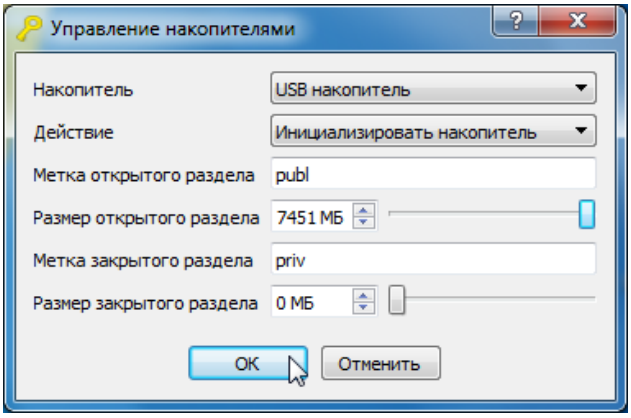

Рис. 73. Удаление закрытого раздела

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK». Дождаться выполнения процедуры инициализации. Затем отключить и заново подключить устройство Key_P1. В результате закрытый раздел будет удалён и появится сообщение, что накопитель не инициализирован.

3.2 Управление синхронными ключами

Синхронные ключи необходимы для того, чтобы пользователи могли создавать одинаковые ключи для обмена зашифрованными сообщениями друг с другом или головным офисом компании в случае обмена закрытыми данными во время деловых поездок с помощью открытой электронной почты и других интернет-ресурсов.

3.2.1 Добавление синхронных ключей

Перед тем как приступить к созданию синхронных ключей, абонентам, которые планируют пересылать шифрованную информацию, необходимо обменяться между собой следующими данными: № алгоритма (первый, второй или третий), начальное значение (кодовое слово или фраза). Данные необходимы для того, чтобы были сформированы одинаковые ключи у всех абонентов.

Для того, чтобы выполнить процедуру создания синхронных ключей, необходимо последовательно выбрать вкладку **Действия** и команду **Управление синхронными ключами** (рис. 74).

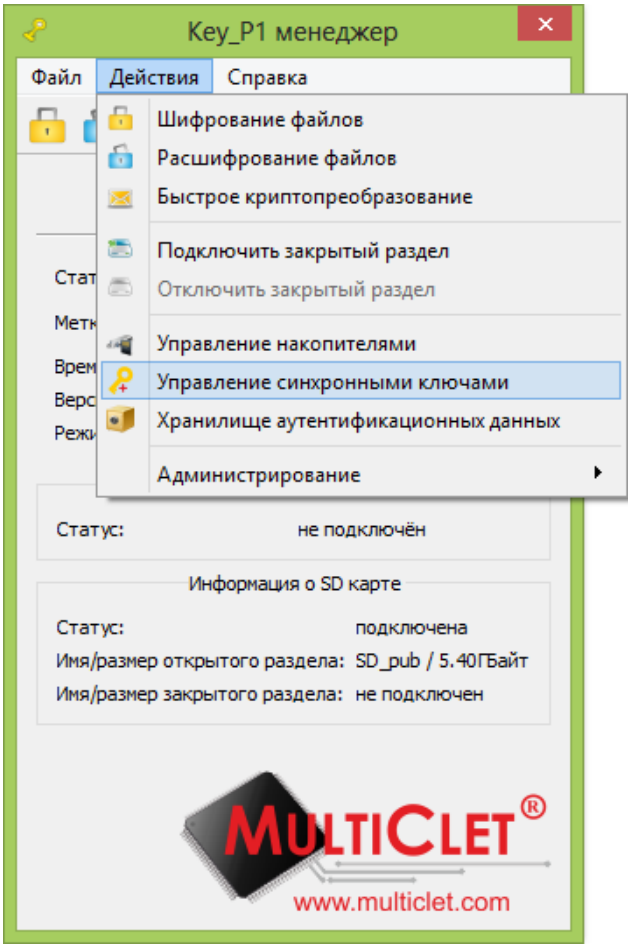

Рис. 74. Управление синхронными ключами

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK» (рис. 75).

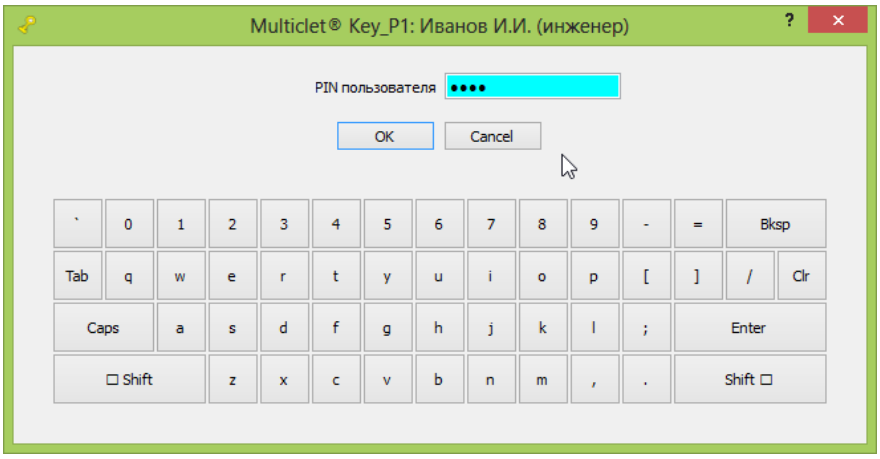

Рис. 75. Ввод PIN пользователя

В открывшемся окне **Управление синхронными ключами** (рис. 76) необходимо нажать кнопку «Добавить».

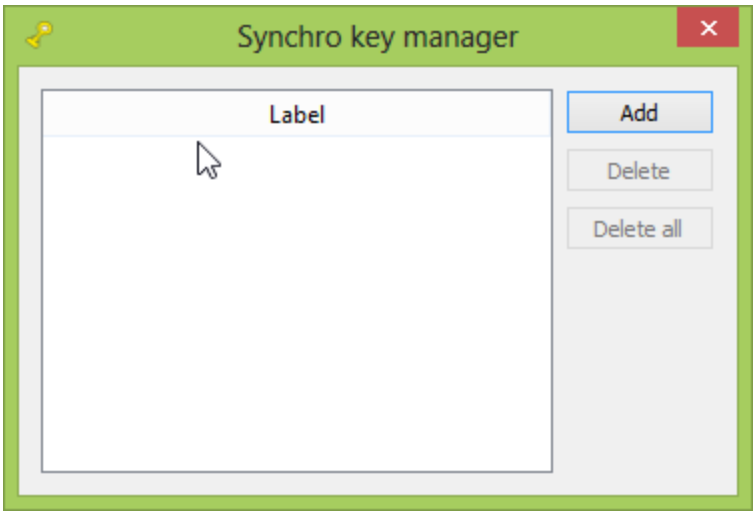

Рис. 76. Управление синхронными ключами

В открывшемся окне **Добавление синхронных ключей** (рис. 77), необходимо указать **Алгоритм**, по которому будет осуществляться шифрование, в строке **Описание** указать описание синхронных ключей, в строке **Начальное значение** и **Подтверждение начального значения** необходимо ввести слово или фразу, по которой будут формироваться синхронные ключи. После выполнения всех действий необходимо нажать «OK».

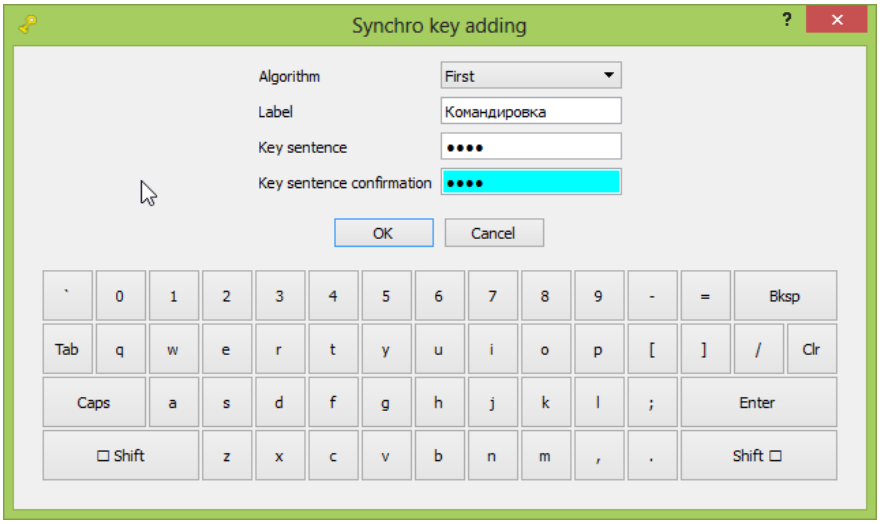

Рис. 77. Добавление синхронных ключей

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK» (рис. 78).

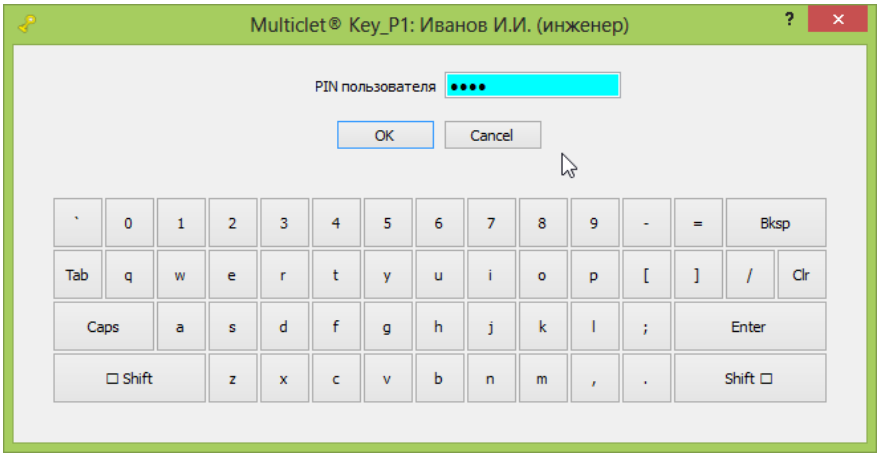

Рис. 78. Ввод PIN пользователя

После выполнения этих действий, в окне **Управление синхронными ключами** (рис. 79) будет отображаться информация о синхронных ключах.

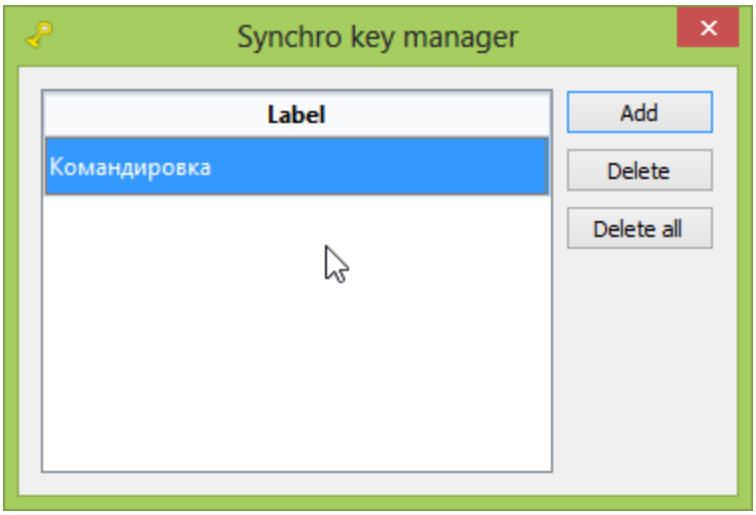

Рис. 79. Управление синхронными ключами

3.2.2 Удаление синхронных ключей

Для того, чтобы выполнить процедуру удаления синхронных ключей, необходимо последовательно выбрать вкладку **Действия** и команду **Управление синхронными ключами** (рис. 80).

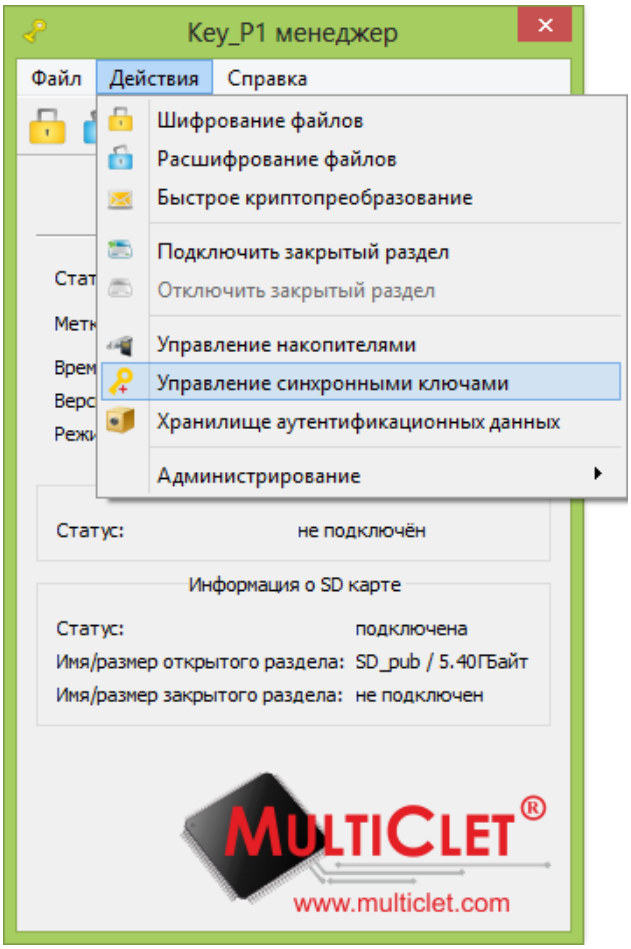

Рис. 80. Управление синхронными ключами

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK» (рис. 81).

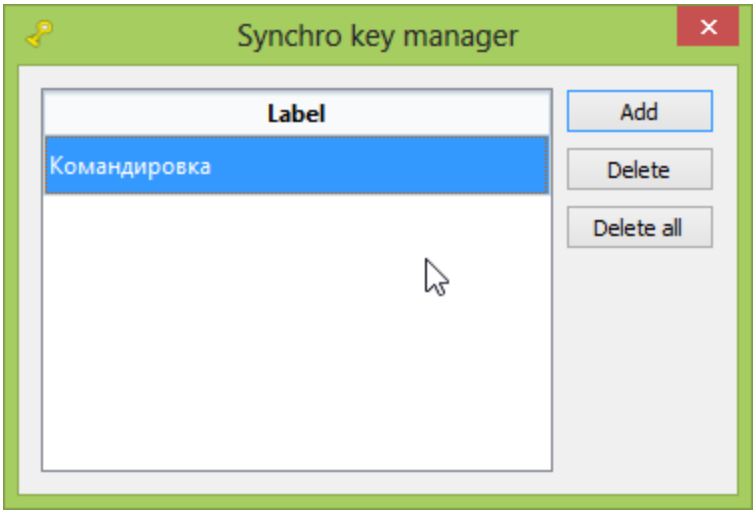

Рис. 81. Ввод PIN пользователя

В открывшемся окне **Управление синхронными ключами** (рис. 82) необходимо выделить набор ключей, который требуется удалить и нажать кнопку «Удалить». Если требуется удалить все наборы ключей, то следует нажать кнопку «Удалить все».

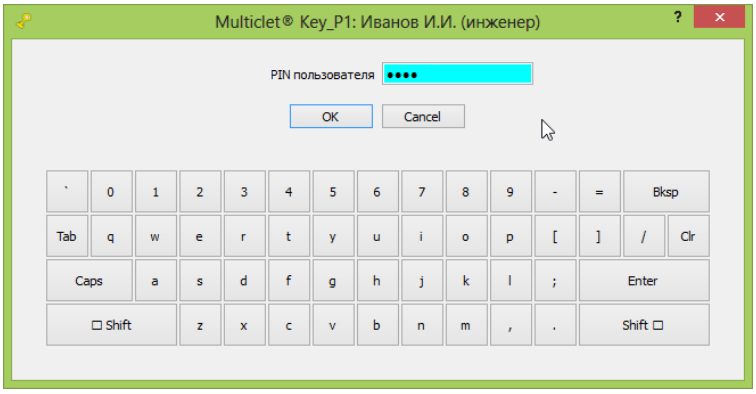

Рис. 82. Удаление синхронных ключей

Появится окно с вопросом о подтверждении удаления. Необходимо нажать «Yes» (рис. 83).

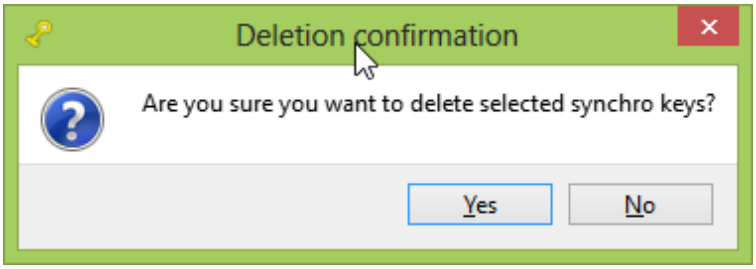

Рис. 83. Удаление ключей

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK» (рис. 84).

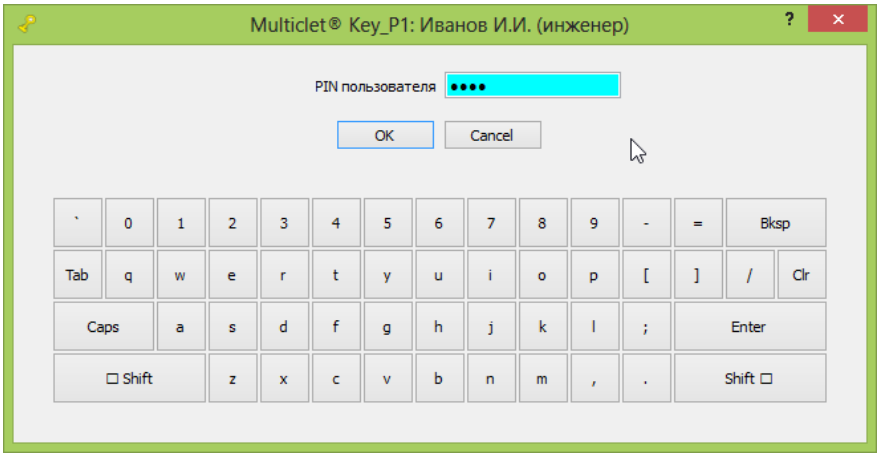

Рис. 84. Ввод PIN пользователя

3.3 Шифрование файлов

Шифрование файлов на устройстве Key_P1 осуществляется следующими способами:

1) **автоматически при копировании файлов на закрытый раздел** инициализированного накопителя: в этом случае файлы на накопителе будут зашифрованы на накопителе по группам секторов при помощи нескольких ключей из 1024 созданных при инициализации устройства.

2) выбором метода шифрования в пункте "Шифрование файлов": в этом случае шифрование файлов может осуществляться одним из 3-х способов:

- **случайным ключом** (несколькими ключами из 1024-х, заданных при инициализации, части одного файла могут быть зашифрованы 1024-мя ключами)

- **синхронизированным ключом** (с помощью выбранного синхронизированного ключа)

- **корпоративным ключом** (одним из нескольких ключей, предназначенных для шифрования файлов выбранной корпоративной группы)

Для того, чтобы выполнить процедуру шифрования файлов, необходимо последовательно выбрать вкладку **Действия** и команду **Шифрование файлов**(рис. 85).

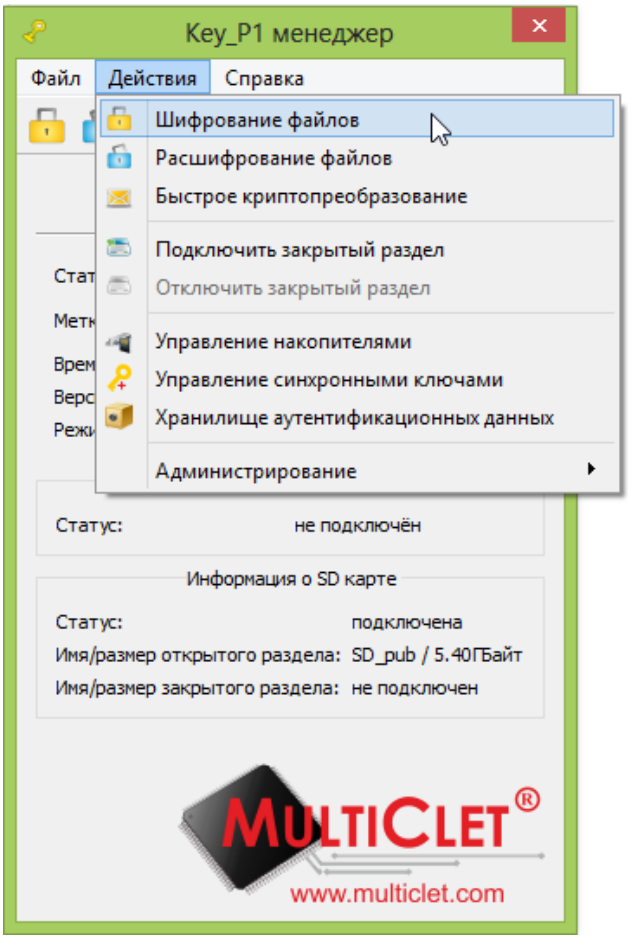

Рис. 85. Шифрование файлов

Появится окно **Шифрование файлов**(рис. 86). В поле **Исходные директории и файлы для зашифрования** необходимо, используя кнопки **Добавить файлы** и **Добавить директорию** добавить для зашифрования файлы и/или директорию (будут зашифрованы все файлы директории).

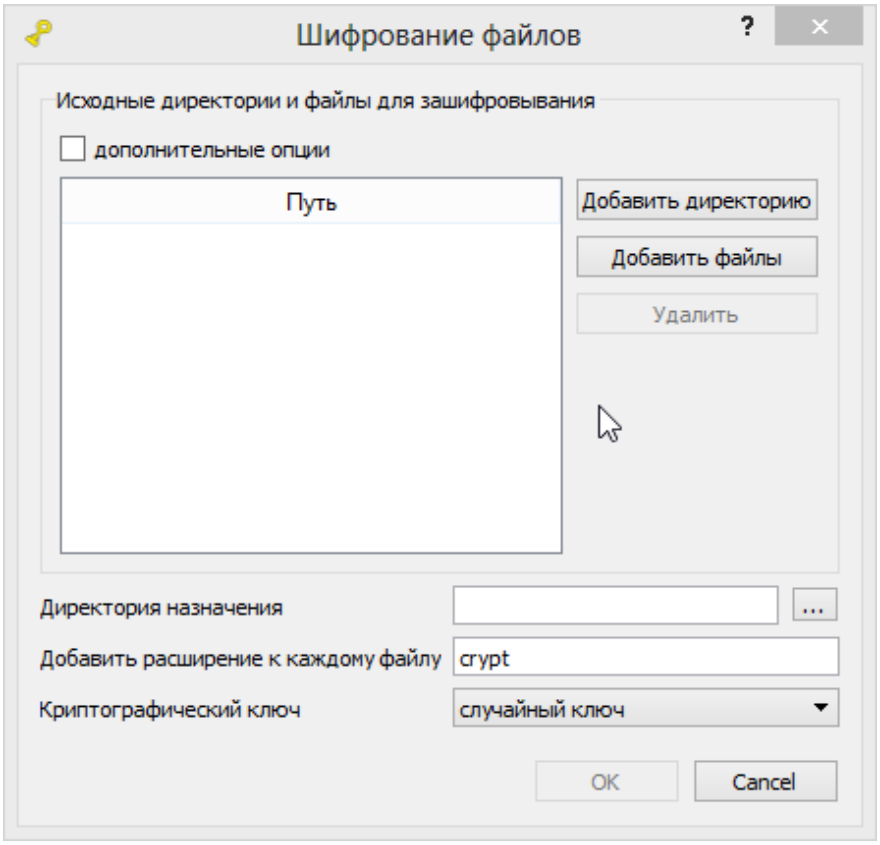

Рис. 86. Шифрование файлов

Для примера нажимаем кнопку **Добавить директорию** и выбираем папку **input**. Таким образом, все файлы в выбранной директорию будут в дальнейшем зашифрованы. Выбор директории иллюстрируется на рис. 87

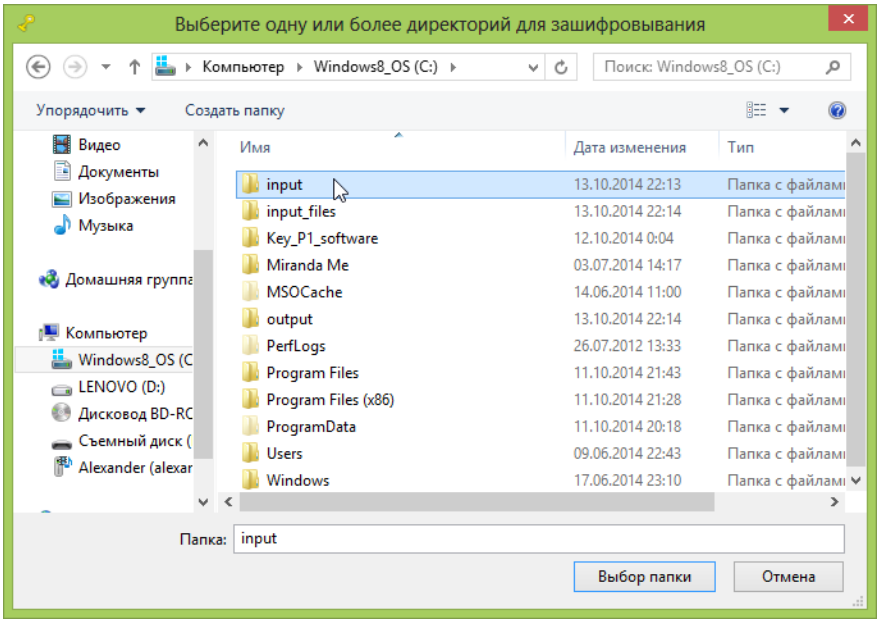

Рис. 87. Выбор директории

Следующим шагом нажмём кнопку **Добавить файлы** и выберем два файла, которые собираемся зашифровать.

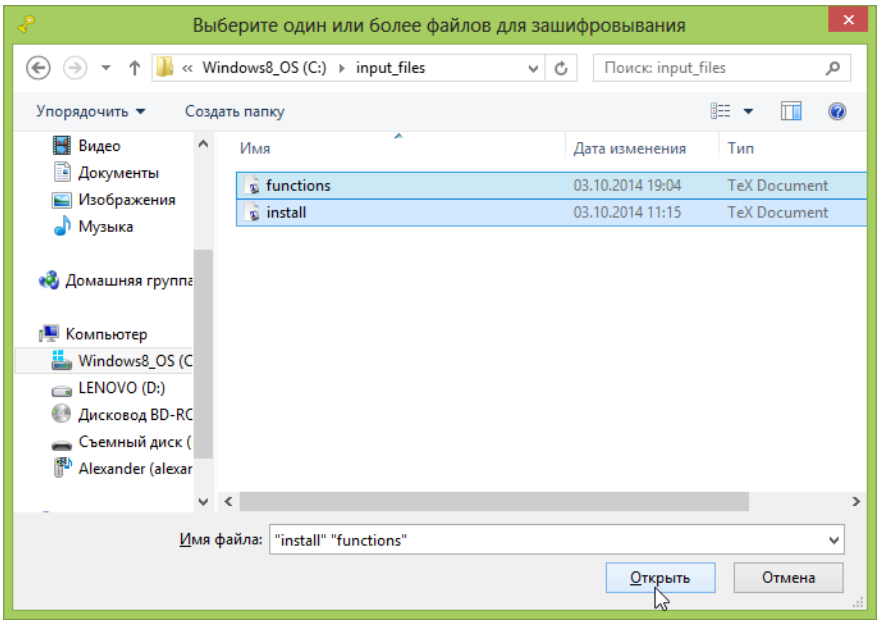

Рис. 88. Выбор файлов

В основном окне для шифрования осталось указать выходную директорию (путь для сохранения зашифрованных файлов) и тип ключа шифрования. Текущий вид окна для шифрования представлен на рис. 89.

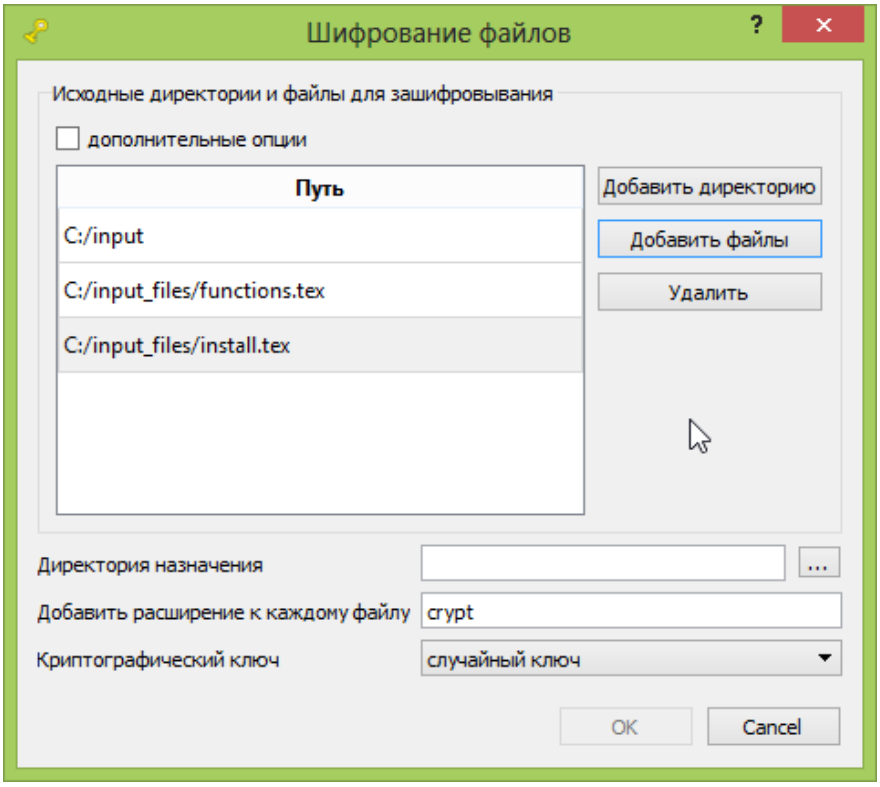

Рис. 89. Окно для шифрования

Теперь выберем директорию размещения зашифрованных файлов как показано на рис. 90.

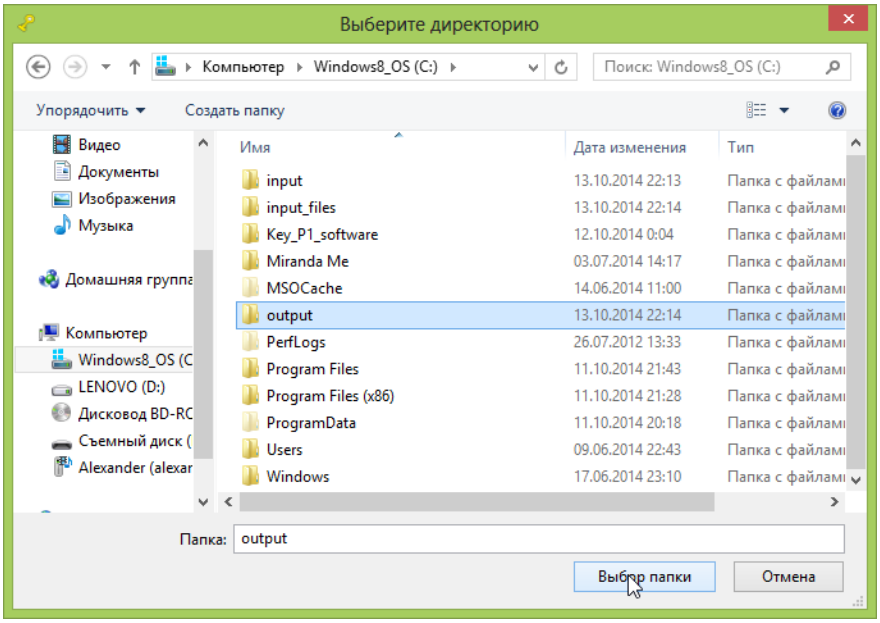

Рис. 90. Выбор директория назначения

В окне для шифрования выберем тип криптографического ключа (в нашем примере выбран "случайный"). Окно для шифрования примет вид представленный на рис. 91. Для начала шифрования файлов нажмите клавишу "OK".

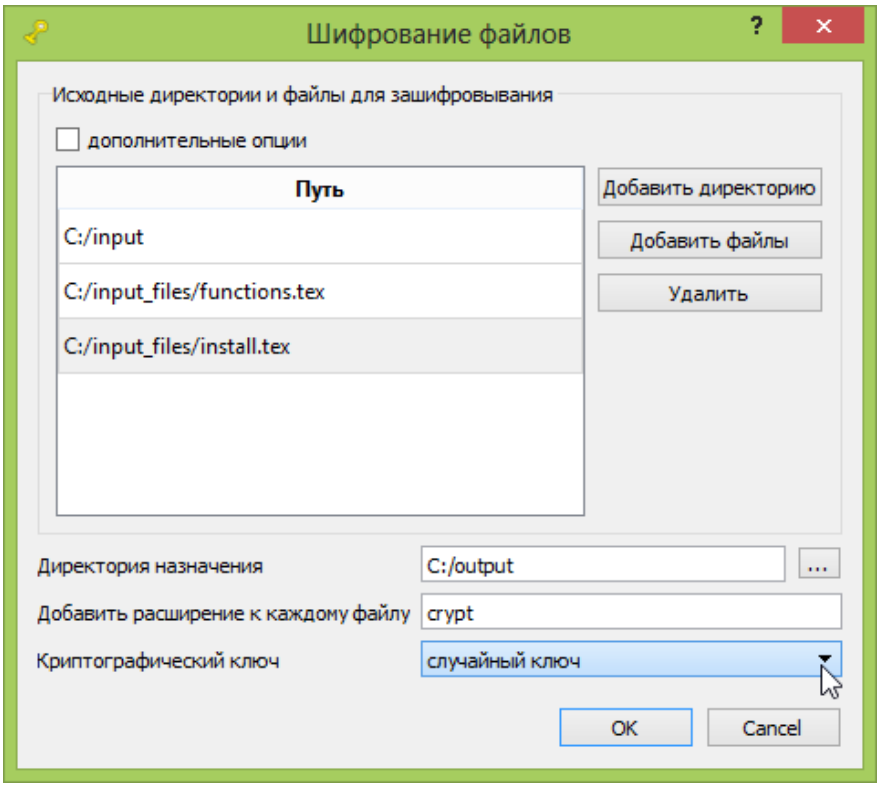

Рис. 91. Выбор директория назначения

Если в поле **Исходные директории и файлы для зашифрования** была добавлена директория, то после установки "галочки"в строке дополнительные опции можно установить следующие параметры (рис. 92):

1)Шаблон файла. Определяет файлы с каким расширением требуется зашифровать. По умолчанию будут зашифрованы все файлы входящие в директорию.

2)Рекурсивно. Если стоит «галочка» в поле этого параметра, все файлы вложенных директорий этой директории будут зашифрованы. Если «галочки» нет, тогда будут зашифрованы файлы только указаной директории.

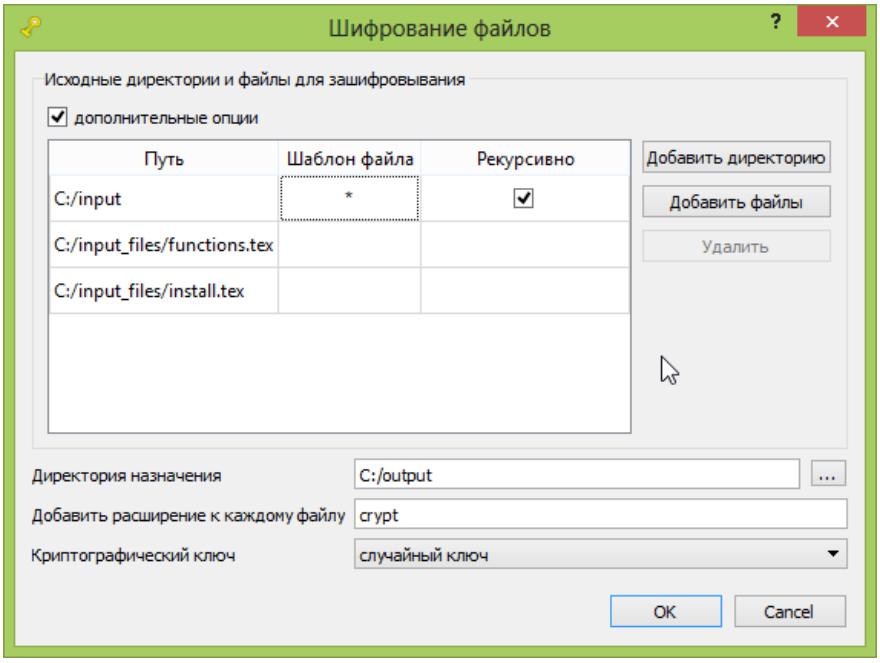

Рис. 92. Шифрование файлов с дополнительными параметрами

Для того, чтобы удалить файлы или директорию из списка **Исходные директории и файлы для зашифрования**, необходимо выделить необходимый файл и/или директорию и нажать кнопку «Удалить».

В строке **Добавить расширение к каждому файлу** есть возможность указать расширение, которое должно быть у файлов после зашифрования. По умолчанию файлы после зашифрования будут иметь расширение «crypt». В строке **Криптографический ключ** необходимо выбрать ключ, с помощью которого будет произведена процедура шифрования. Доступны три варианта ключей: случайный, синхронный и корпоративный. После выполнения всех этих действий необходимо нажать кнопку «OK» для запуска процедуры зашифрования.

3.4 Расшифрование файлов

Для того, чтобы выполнить процедуру расшифрования файлов необходимо последовательно выбрать вкладку **Действия** и команду **Расшифрование файлов**(рис. 93).

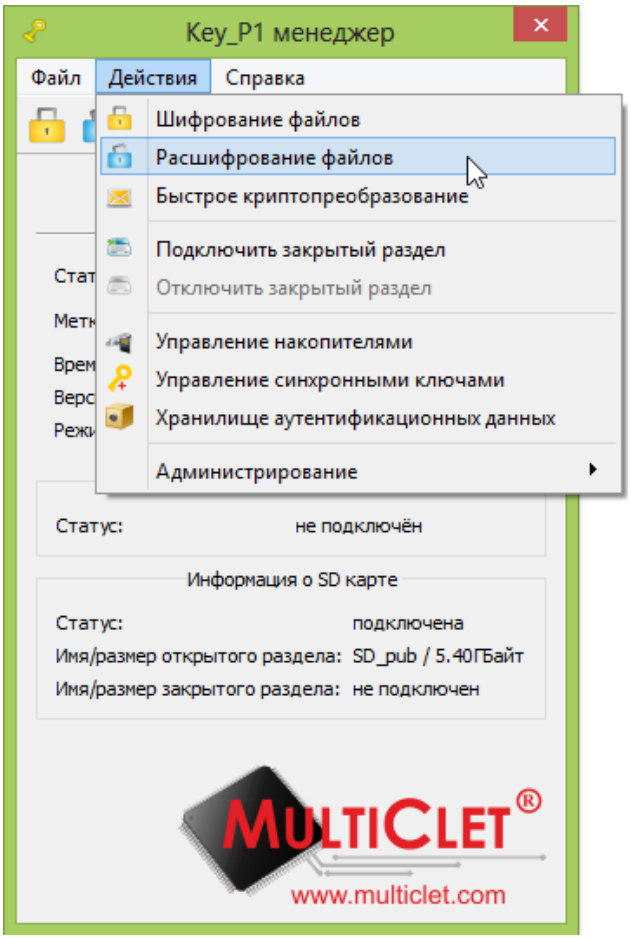

Рис. 93. Расшифрование файлов

Появится окно **Расшифрование файлов**(рис. 94). В поле **Исходные директории и файлы для расшифрования** необходимо используя кнопки **Добавить файлы** и **Добавить директорию** добавить для расшифрования файлы и/или директорию (будут расшифрованы все файлы директории).

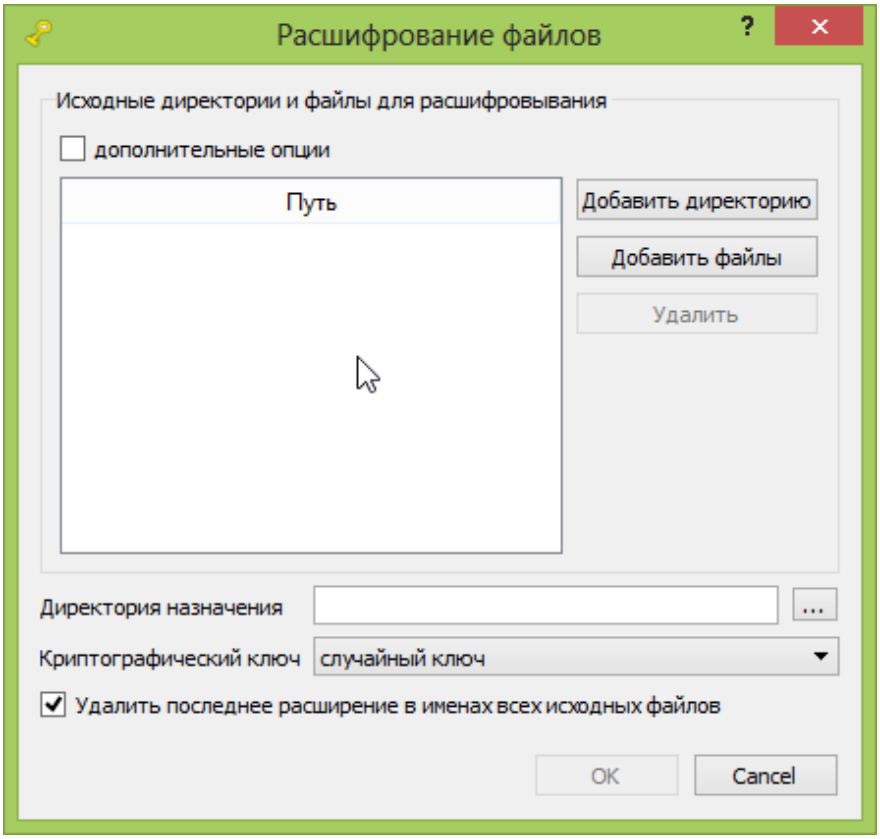

Рис. 94. Расшифрование файлов

Для примера добавим директорию для файлов, которые хотим расшифровать. И добавим директорию назначения для размещения расшифрованных данных. На рис. 95 изображен пример выбора директорий.

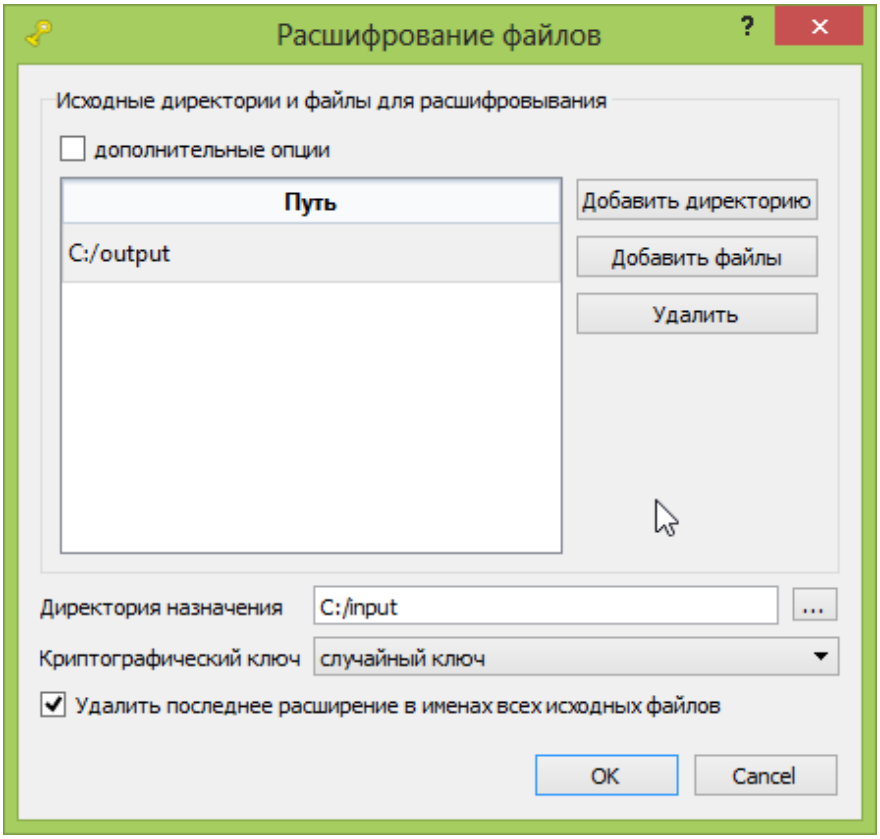

Рис. 95. Выбор директорий

Выберем тип криптографического ключа - синхронизированный ключ и укажем на ключ с меткой "Командировка". Для быстрого перехода к управлению синхро ключами доступна кнопка "Управление". Полученный вид окна представлен на рис. 96.

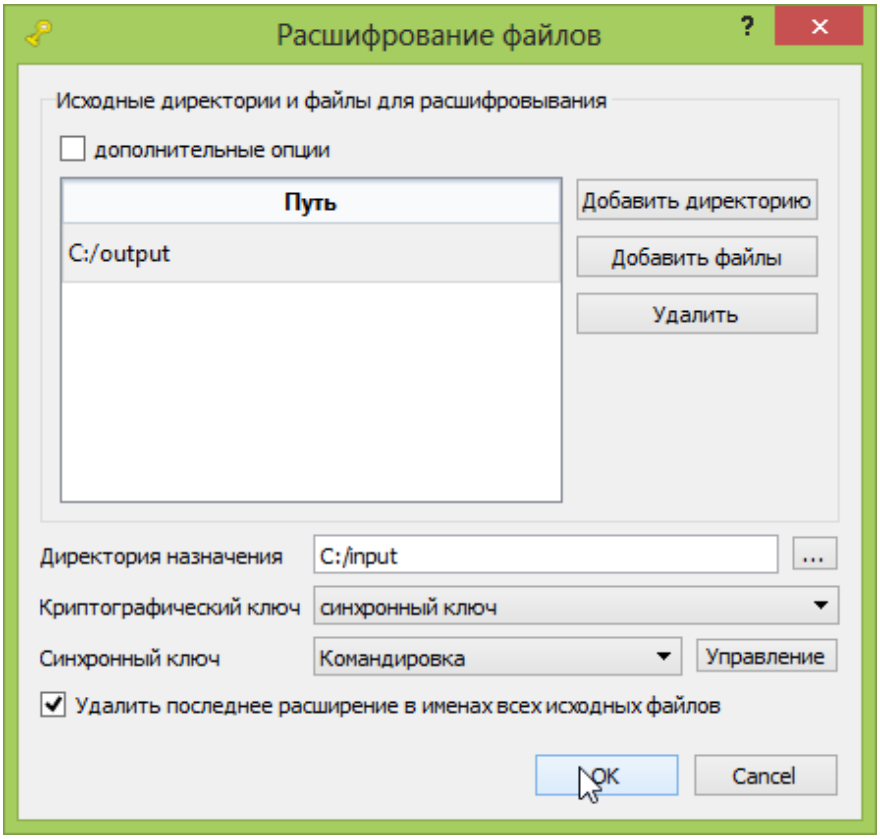

Рис. 96. Выбор директорий

Если в поле **Исходные директории и файлы для расшифрования** была добавлена директория, то после установки "галочки"в строке дополнительные опции можно установить следующие параметры (рис. 97):

1)Шаблон файла. Определяет файлы с каким расширением требуется расшифровать. По умолчанию будут расшифрованы все файлы входящие в директорию.

2)Рекурсивно. Если стоит «галочка» в поле этого параметра, все файлы вложенных директорий этой директории будут расшифрованы. Если «галочки» нет, тогда будут расшифрованы файлы только указаной директории.

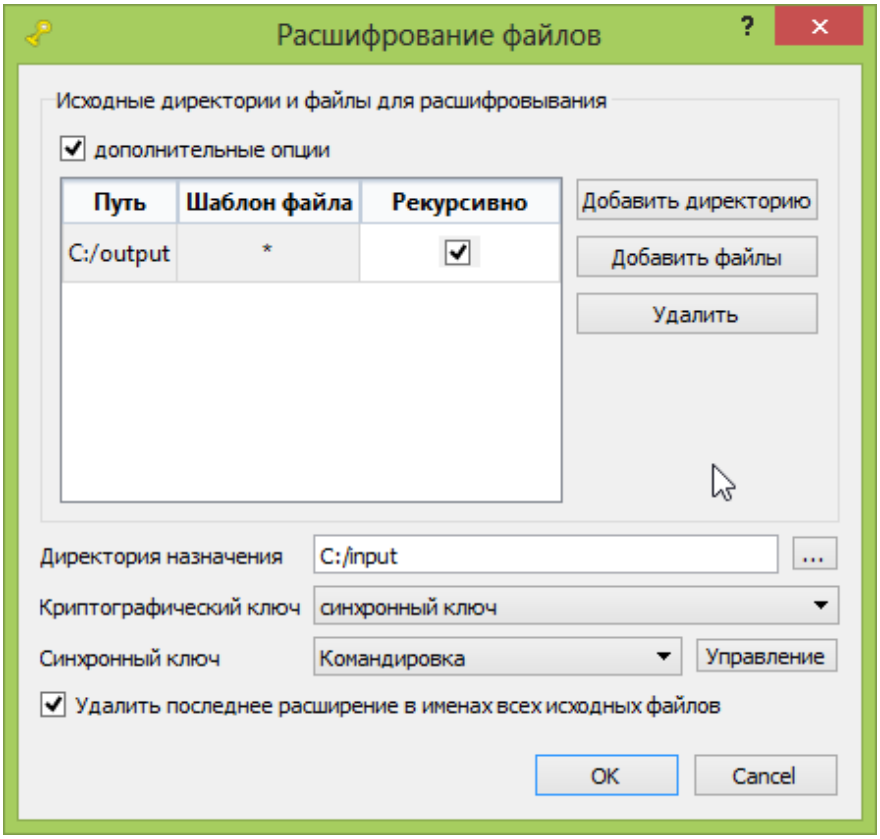

Рис. 97. Расшифрование файлов

Для того, чтобы удалить файлы или директорию из списка **Исходные директории и файлы для расшифрования**, необходимо выделить необходимый файл и/или директорию и нажать кнопку «Удалить».

В строке **Директория назначения** следует указать путь, где будут сохранены расшифрованные данные. В строке **Добавить расширение к каждому файлу** есть возможность указать расширение, которое должно быть у файлов после расшифрования. По умолчанию файлы после расшифрования будут иметь расширение «crypt». В строке **Криптографический ключ** необходимо выбрать ключ, с помощью которого будет произведена процедура расшифрования. Доступны три варианта ключей: случайный, синхронный и корпоративный. В строке **Удалить последнее расширение в именах всех исходных файлов** есть возможность поставить «галочку». В таком случае у всех исходных файлов после расшифрования будет удалено расширение. После выполнения всех этих действий необходимо нажать кнопку «OK» для запуска процедуры расшифрования.

3.5 Быстрое криптопреобразование

Быстрое криптопреобразование необходимо для быстрого шифрования или дешифрования текстовых сообщений. Для того, чтобы начать работу с быстрым криптопреобразованием, необходимо последовательно выбрать вкладку **Действия** и выбрать пункт **Быстрое криптопреобразование**(рис. 98).

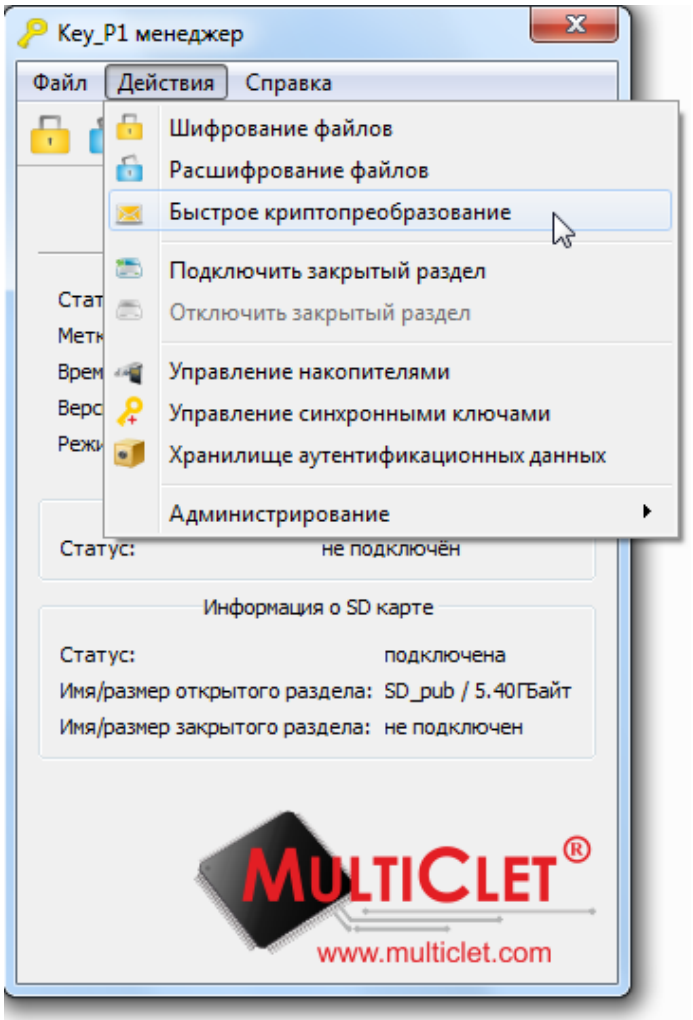

Рис. 98. Выбор элемента

Появится окно для шифрования и дешифрования текстовых сообщений (рис. 99).

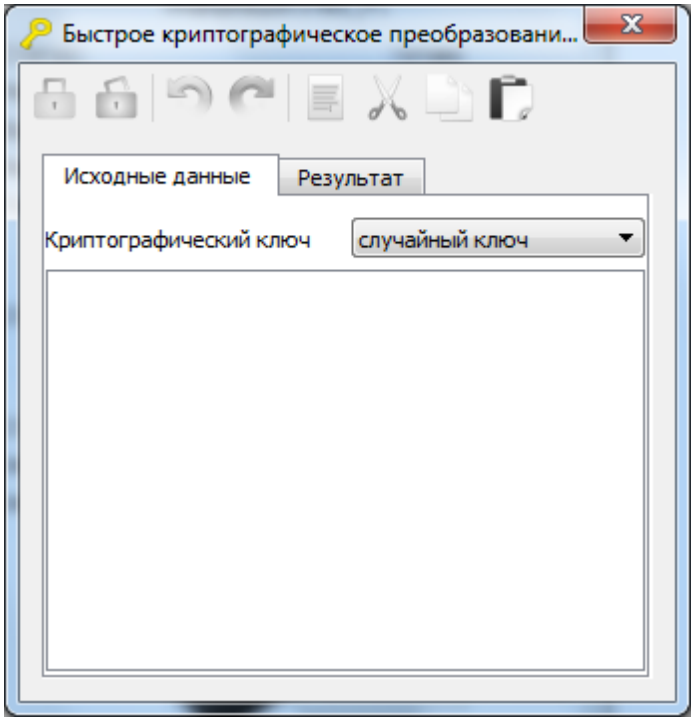

Рис. 99. Быстрое криптопреобразование

Для примера в текстовом поле вкладки **Исходные данные** введём сообщение для шифрования, как показано на рис. 100

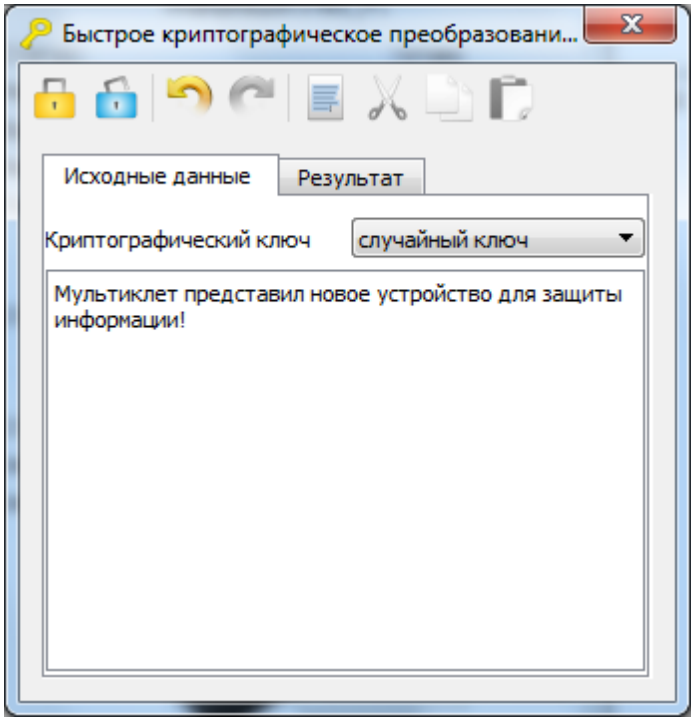

Рис. 100. Пример сообщения для шифрования

После ввода текстового сообщения станет активной панель инструментов (выделено красным цветом на рис. 101)

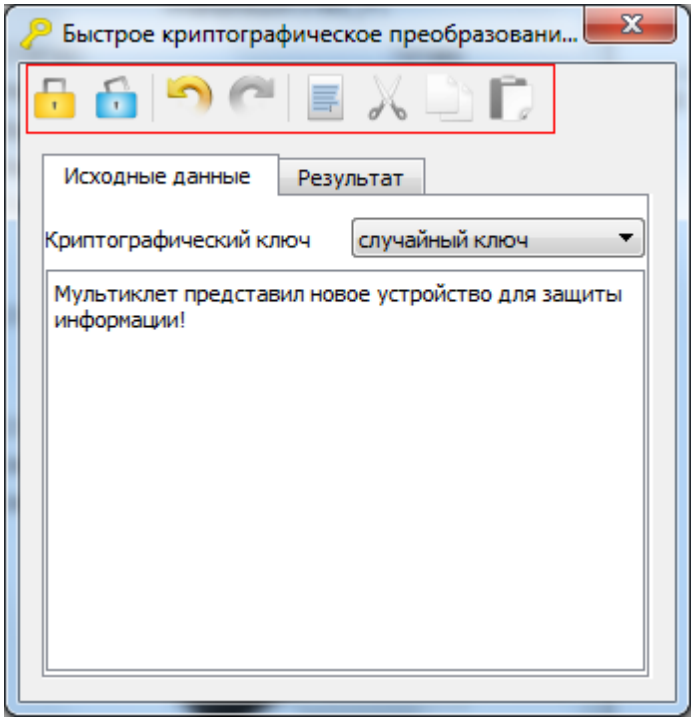

Рис. 101. Панель инструментов

Элементы панели инструментов:

1) **Шифрование сообщения**

2) **Дешифрование сообщения**

3) **Отменить**

4) **Вернуть**

5) **Выделить всё**

6) **Вырезать**

7) **Копировать**

8) **Вставить**

В поле **Криптографический ключ** может быть установлен один из следующих вариантов: случайный, синхронный и корпоративный. После нажатия кнопки **Шифрование сообщения** и выбора криптографического ключа появится окно ввода PIN пользователя, см рис. 102.

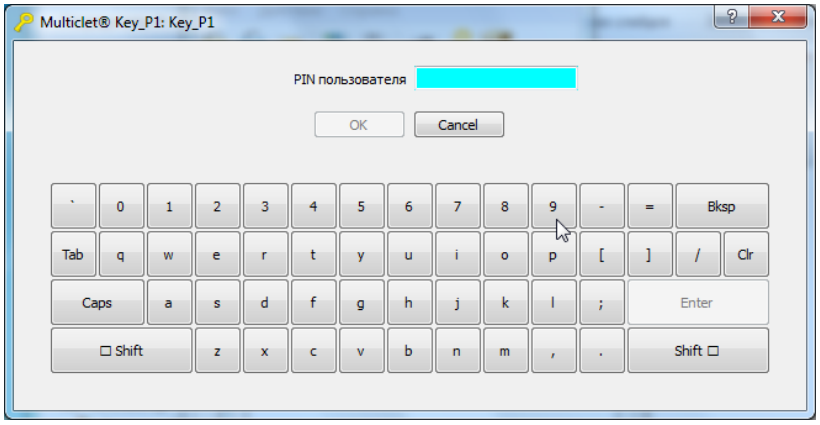

Рис. 102. Ввод PIN пользователя

В случае успешного ввода PIN пользователя отобразится содержимое вкладки **Результат**, как показано на рис. 103. Зашифрованную фразу можно выделить средствами ОС или нажав кнопку **Выделить всё** на панели инструментов. Затем можно зайти в почтовый клиент, соцсеть и др. и средствами ОС вставить полученное сообщение.

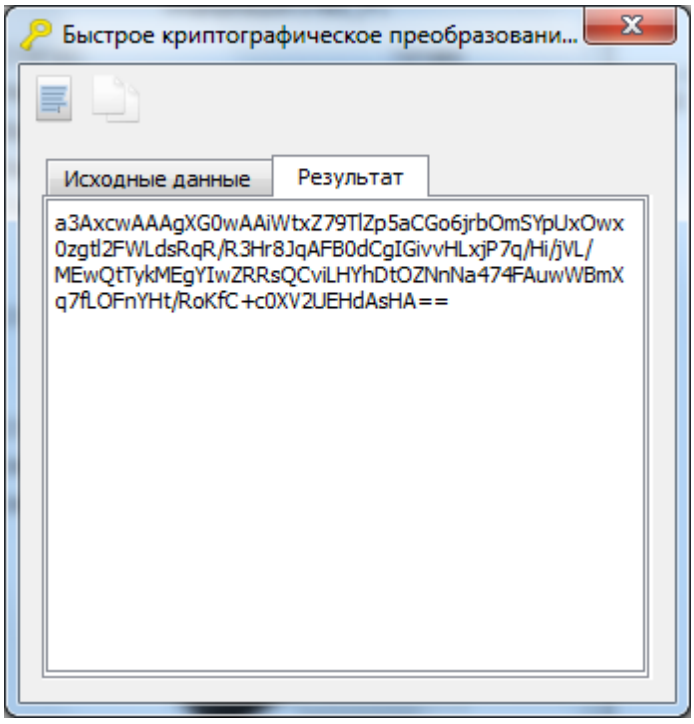

Рис. 103. Результат шифрования

Дешифрование сообщения происходит аналогичным образом.

3.6 Управление корпоративными ключами

Для того, чтобы начать работу с корпоративными ключами, необходимо последовательно выбрать вкладку **Действия** перейти в подменю **Администрирование** и выбрать пунтк **Управление корпоративными ключами**(рис. 104).

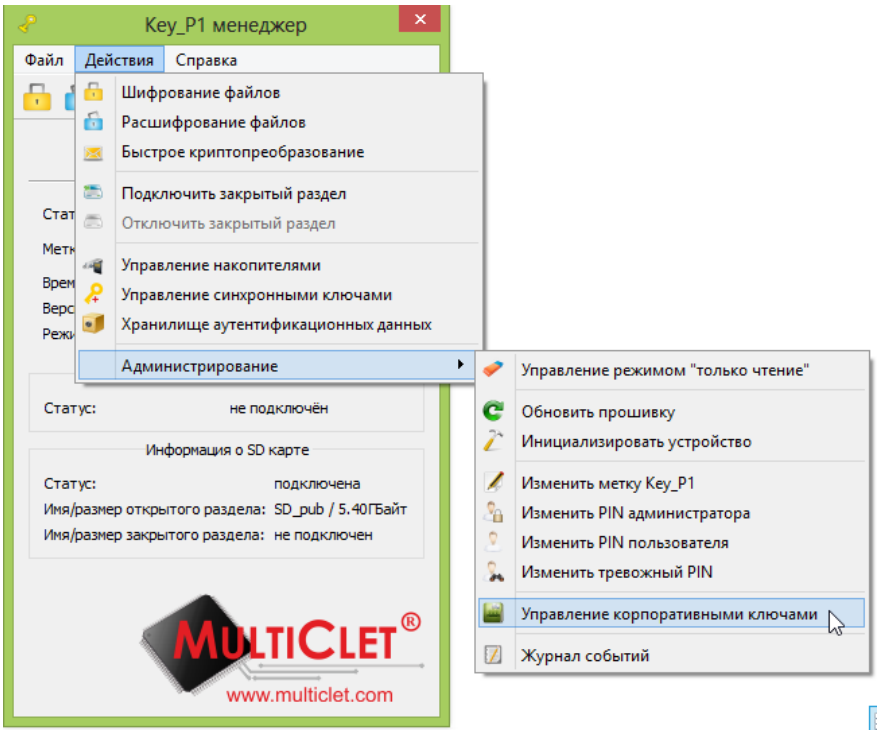

Рис. 104. Управление корпоративными ключами

Появится окно ввода PIN администратора. После ввода PIN необходимо нажать «OK» (рис. 105).

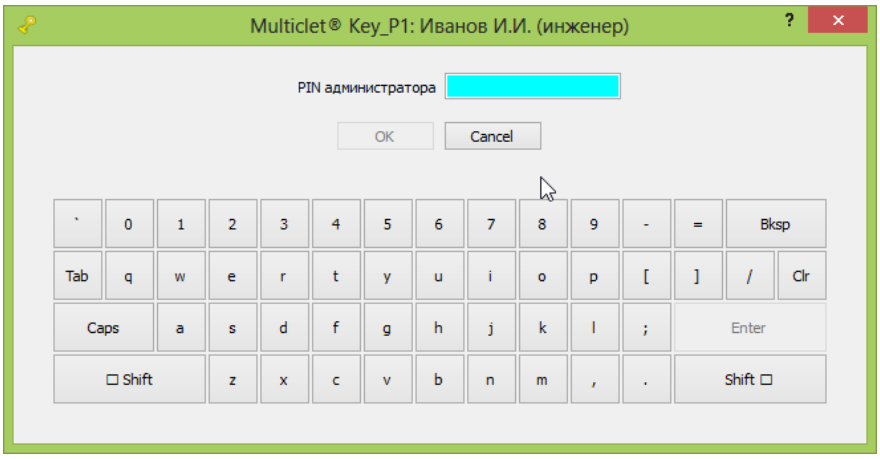

Рис. 105. Ввод PIN администратора

Появится меню **Управление корпоративными ключами** (рис. 106).

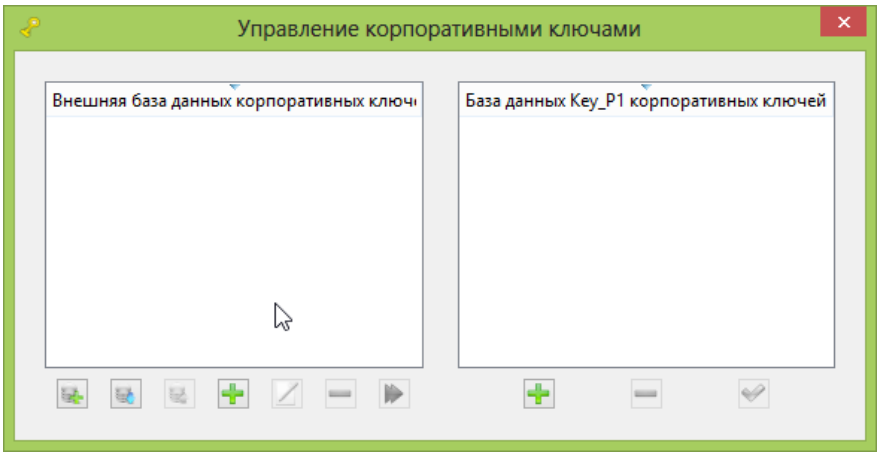

Рис. 106. Управление корпоративными ключами

Данное меню делится на два окна: **Внешняя база данных корпоративных ключей** и **База данных Key_P1 корпоративных ключей**. Внешняя база - является структурой ключей предприятия, а база Key_P1 - допуском конкретного пользователя. Администратор службы безопасности предприятия после формирования внешней базы корпоративных ключей переносит необходимые группы ключей на устройства сотрудников компании. Рекомендуется производить данную операцию на доверенном ПК. Данная операция производится только по ПИН коду администратора, для лучшего понимания приведён пример создания иерархического доступа в пункте 3.6.1 Управление внешней базой данных корпоративных ключей осуществляется посредством выполнения следующих команд представленных в виде иконок слева направо (рис. 107)(выделено красным цветом):

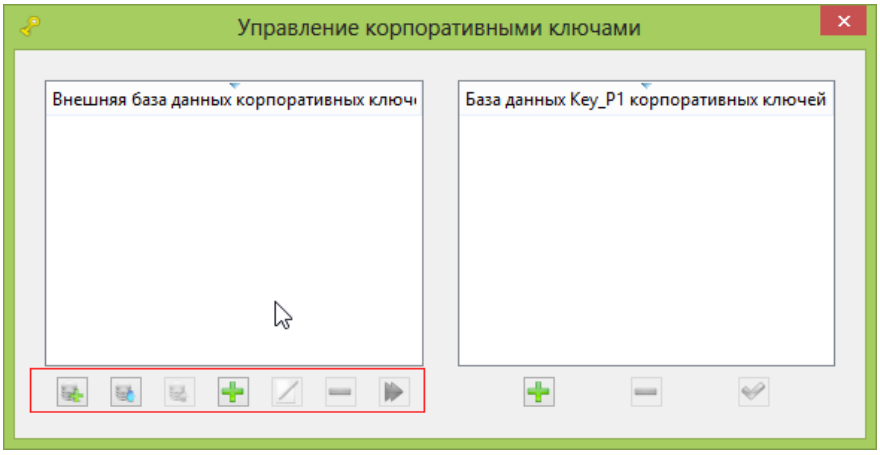

Рис. 107. Управление корпоративными ключами

Рассмотрим элементы панели инструментов для управления внешней базой корпоративных ключей:

1) **Создать новую базу данных корпоративных ключей** - выполнение процедуры по созданию новой базы;

2) **Открыть базу данных корпоративных ключей** - выполнение процедуры по открытию ранее созданой базы из файла;

3) **Сохранить базу данных корпоративных ключей** - выполнение процедуры по сохранению текущей базы в файл;

4) **Добавить группу корпоративных ключей в базу данных** - выполнение процедуры по добавлению группы корпоративных ключей. Для выполнения этой операции необходимо указать имя группы и количество ключей (рис. 108);

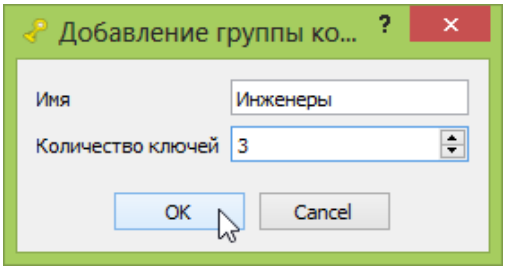

Рис. 108. Добавление группы корпоративных ключей

Группа будет иметь метку "Инженеры"и для данной группы будут сгенерированы 3 ключа. После нажатия кнопки "OK"появится окно представленное на рис. 109.

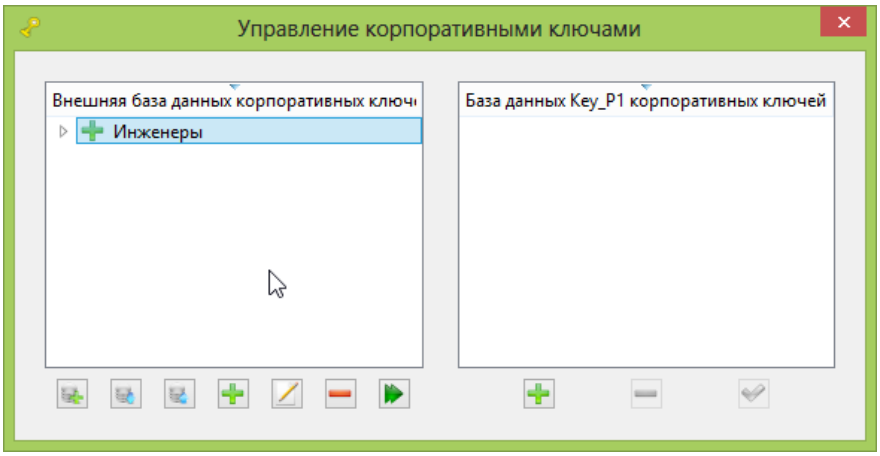

Рис. 109. Добавление группы корпоративных ключей

5) **Редактировать группу корпоративных ключей в базе данных** - при выпол-

нении данной команды возможно внесение изменений в имя группы корпоративных ключей, окно для изменения метки группы представлено на рис. 110

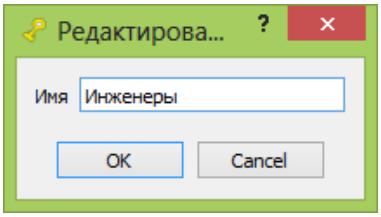

Рис. 110. Изменение метки группы корпоративных ключей

6) **Удалить группу корпоративных ключей из базы данных** - выполнение процедуры по удалению группы корпоративных ключей из базы.

Управление базой данных Key_P1 корпоративных ключей осуществляется посредством выполнения следующих команд представленных в виде иконок слева направо (рис. 111)(выделено красным цветом):

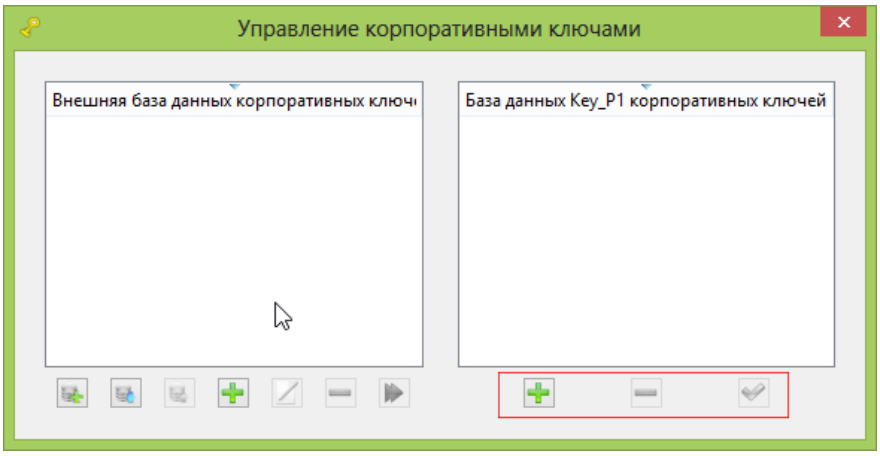

Рис. 111. Управление корпоративными ключами

1) **Добавить группу корпоративных ключей в базу данных Key_P1** - выполнение процедуры по добавлению группы корпоративных ключей в базу Key_P1. Для выполнения этой операции необходимо указать имя группы и количество ключей (рис. 112);

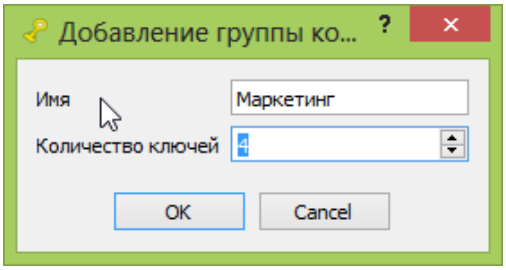

Рис. 112. Добавление группы корпоративных ключей

2) **Удалить группу корпоративных ключей из базы данных Key_P1** - выполнение процедуры по удалению группы корпоративных ключей из базы Key_P1;

3) **Применить изменения в базе данных Key_P1** - сохранение всех изменений в базе данных Key_P1. При выполнении этой команды появится окно ввода PIN администратора (рис. 113). После ввода PIN необходимо нажать «OK».

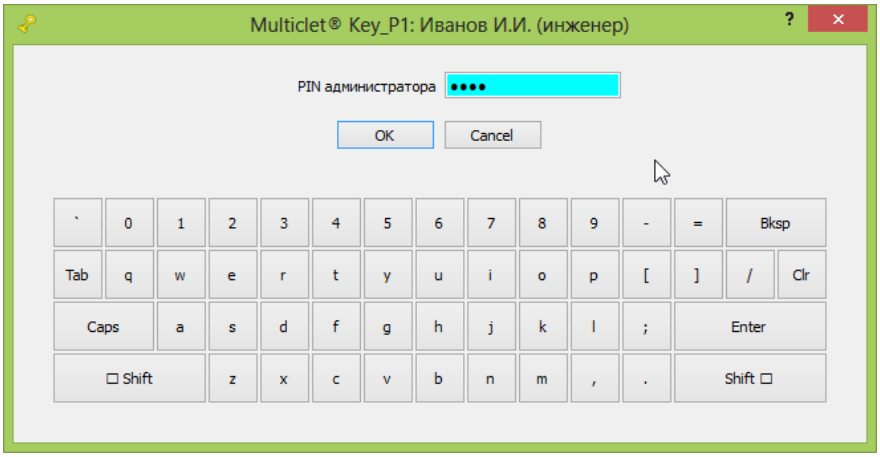

Рис. 113. Ввод PIN администратора

В результате применения изменений в базе корпоративных ключей окно управления ключами примет вид как на рис. 114. Таким образом, на устройстве будет создана корпоративная группа "Маркетинг".

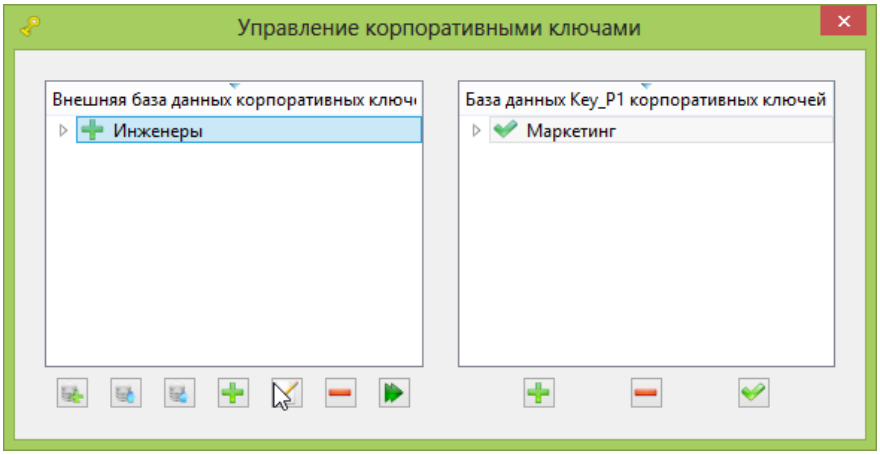

Рис. 114. Управление корпоративными ключами

3.6.1 Пример создание иерархического доступа

Рассмотрим пример организации иерархического доступа на предприятии. Откроем окно «управление корпоративными ключами»(вкладка Действия->Администрирование) и в левой области нажмём кнопку «Добавить группу корпоративных ключей в базу данных» , см рис. 115

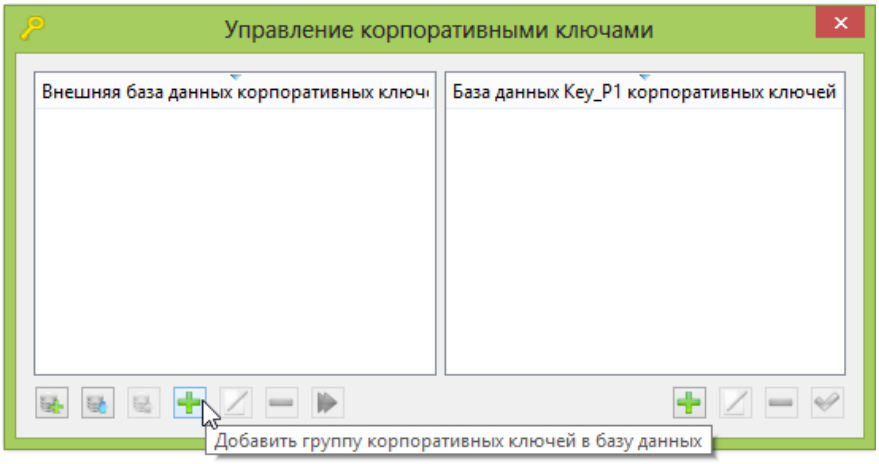

Рис. 115. Окно управление корпоративными ключами

Создадим группу корпоративных ключей «Бухгалтерия» и сгенерируем для данной группы 3 ключа. Сразу отметим, что назначение группе нескольких ключей нисколько не усложнит работу, т.к. устройство Key_P1 автоматически распознаёт наличие у пользователя ключей для расшифрования файла выбранной группы. В дальнейшем поясним данный момент. Пример создания группы показан на рис. 116

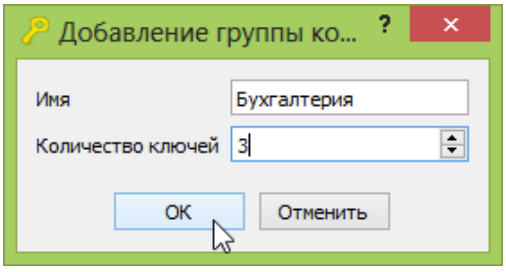

Рис. 116. Создание группы корпоративных ключей

После нажатия кнопки «Ok» данная группа отобразится в области внешней базы корпоративных ключей со значком «плюс», который означает, что группа ключей создана, но не добавлена в базу, см рис. 117

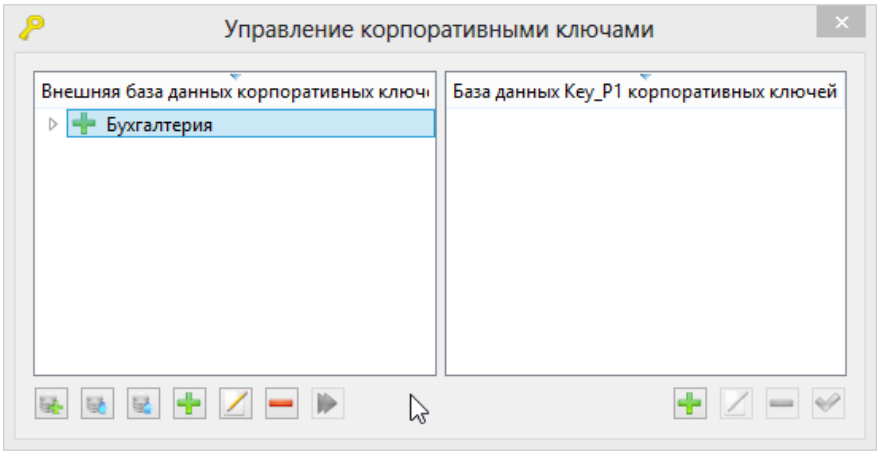

Рис. 117. Создание группы корпоративных ключей

Аналогичным образом добавим группу «Программисты», для которой назначим 2 ключа, которые будут сгенерированы, см рис. 118

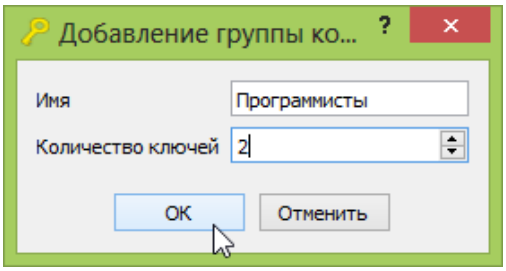

Рис. 118. Создание группы корпоративных ключей

Добавим все необходимые группы во внешнюю корпоративную базу, полученный результат изображен на рис. 119

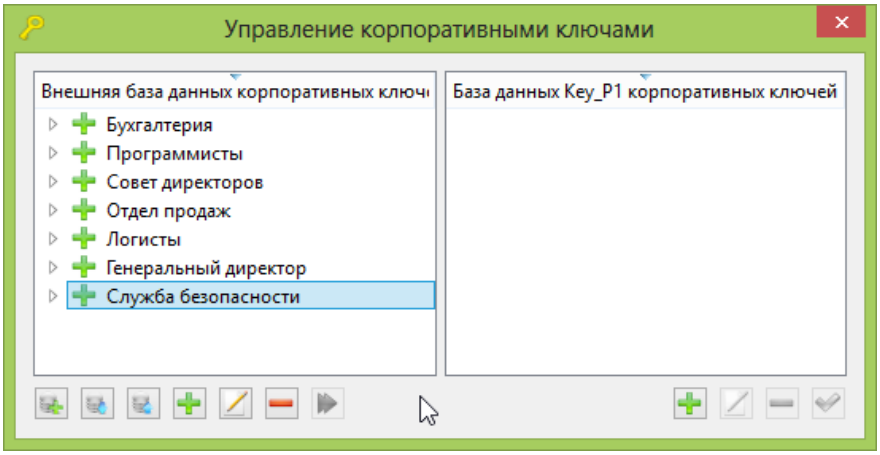

Рис. 119. Создание групп корпоративных ключей

Следующим шагом сохраним созданные группы в файл внешней базы корпоративных ключей, как показано на рис. 120

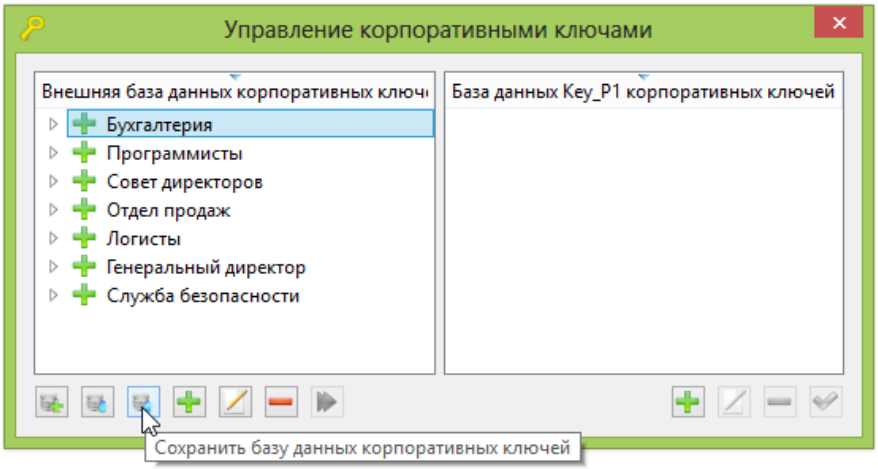

Рис. 120. Сохранение внешней базы групп корпоративных ключей

После нажатия кнопки «сохранить внешнюю базу корпоративных ключей» появится окно для задания имени файла, содержащего базу ключей, см рис. 121

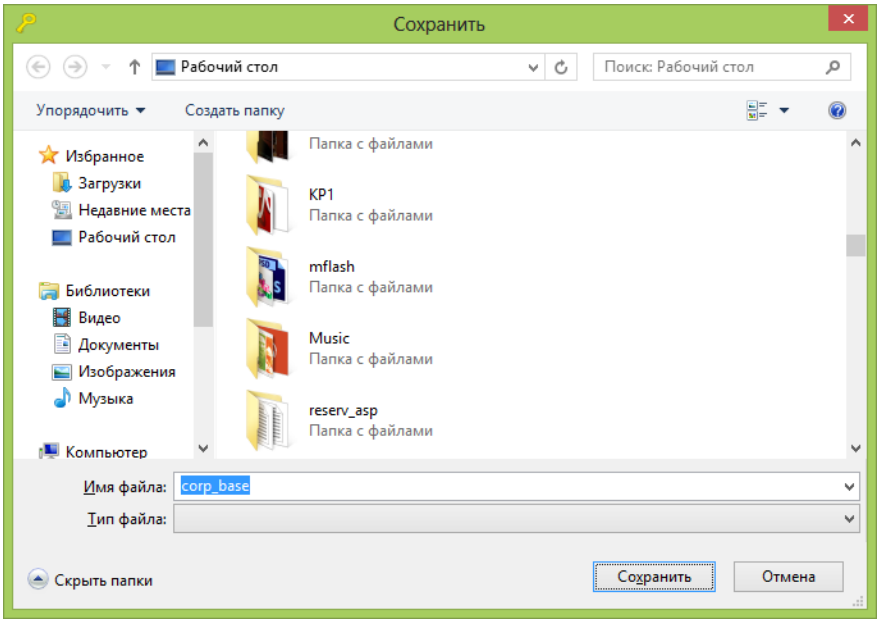

Рис. 121. Сохранение внешней базы групп корпоративных ключей

Данную базу корпоративных ключей администратор службы безопасности должен хранить на доверенном ПК или на защищенном накопителе(например, закрытом разделе, созданном с помощью Key_P1 либо же данный файл можно зашифровать с помощью устройства Key_P1). Процедура организации иерархического доступа заключа-

ется в установке администратором службы безопасности определённого набора групп ключей на пользовательские устройства Key_P1. Предположим, что директору компании необходимо обмениваться информацией со всеми структурными подразделениями компании, тогда администратор службы безопасности переходит в раздел «управление корпоративными ключами» на устройстве Key_P1 директора компании и нажимает кнопку «открыть внешнюю базу корпоративных ключей», как показано на рис. 122

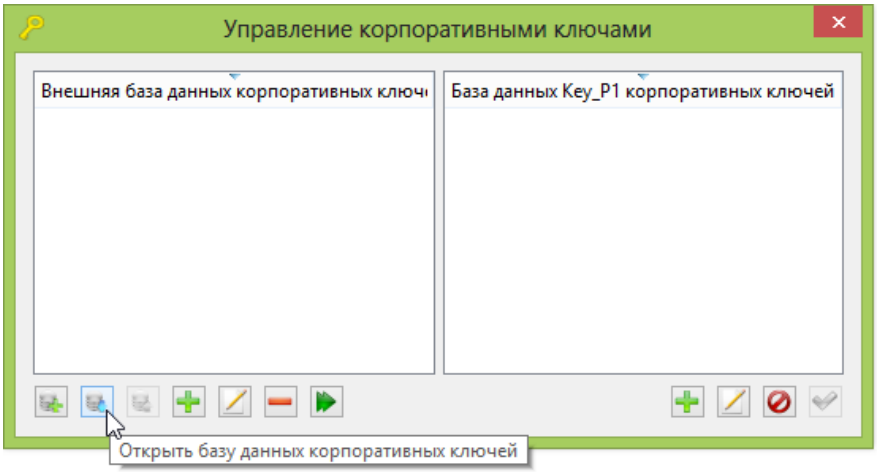

Рис. 122. Управление группами корпоративных ключей

Затем администратор выбирает файл с базой корпоративных ключей и нажимает кнопку «Открыть», как показано на рис. 123

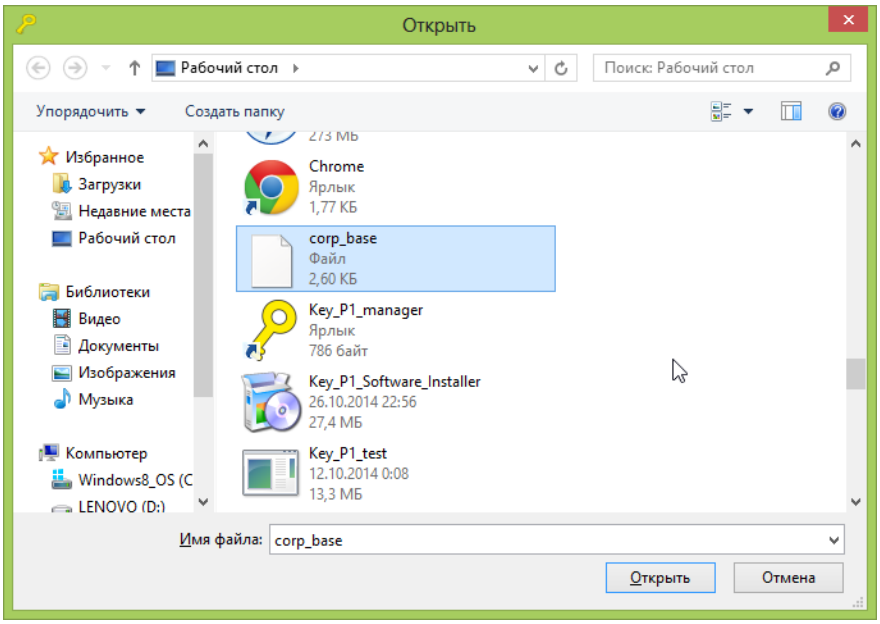

Рис. 123. Открытие внешней базы корпоративных ключей

В левой области окна управления корпоративными ключами отобразится список доступных групп внешней базы, см рис. 124

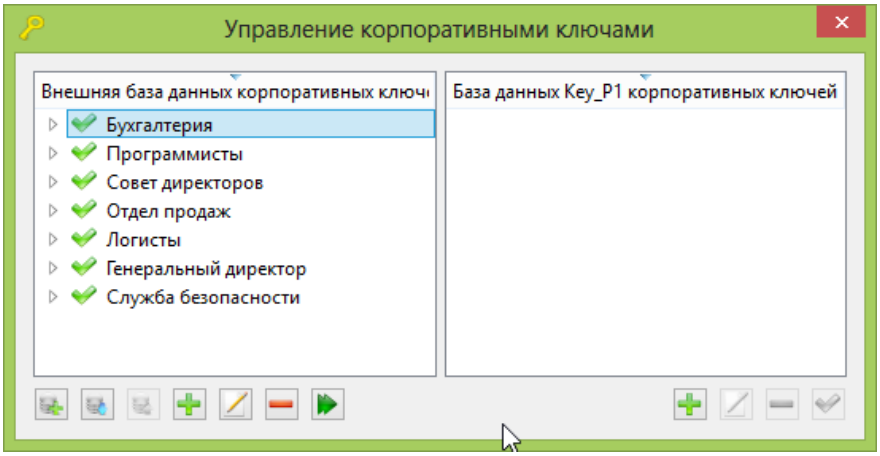

Рис. 124. Группы внешней базы корпоративных ключей

С помощью кнопки «Добавить группу корпоративных ключей» переносим группы из внешней базы на устройство Key_P1 директора компании, см рис. 125

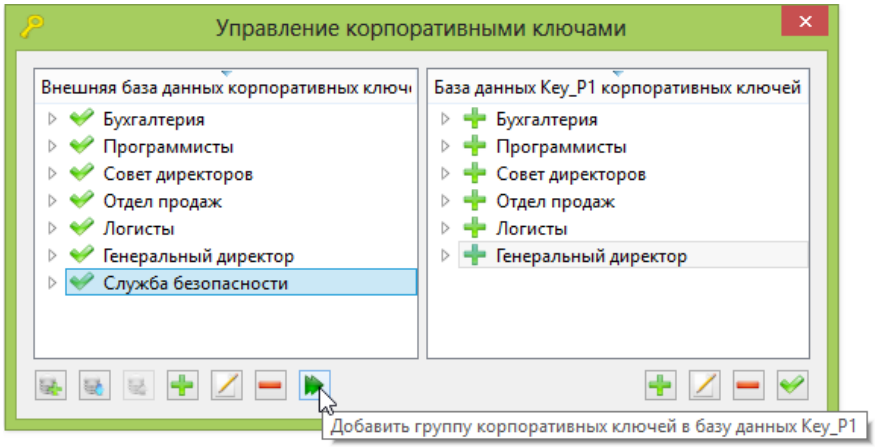

Рис. 125. Установка групп внешней базы корпоративных ключей на устройство

После переноса необходимых групп ключей нажимаем кнопку в правой области «Применить изменения в базе данных Key_P1», как показано на рис. 126

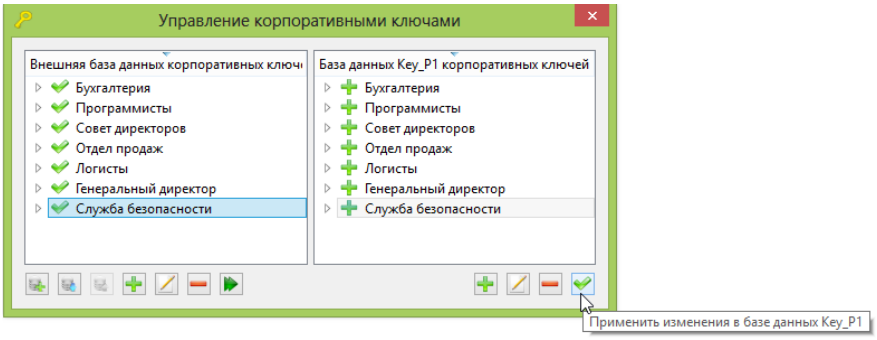

Рис. 126. Установка групп внешней базы корпоративных ключей на устройство

После того, как группы ключей успешно установлены на устройство, у каждой группы отобразится значок «галочка», см рис. 127

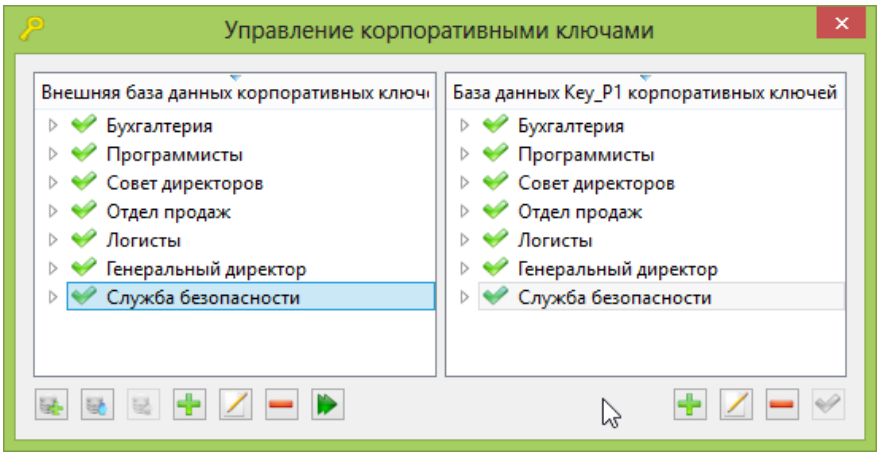

Рис. 127. Группы корпоративных ключей установлены на устройство

Для пользователей, например, отдела «Бухгалтерия» группы ключей устанавливаются аналогичным образом. Добавим группы ключей, которые необходимы отделу «Бухгалтерия», см рис. 128

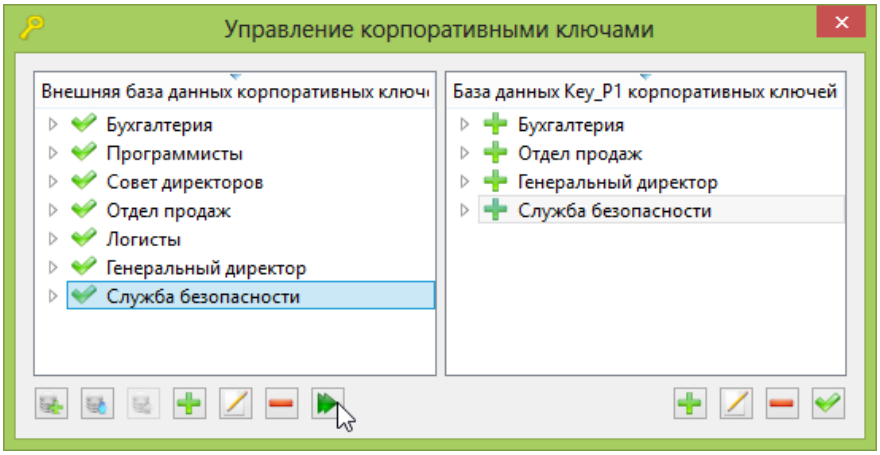

Рис. 128. Группы корпоративных ключей для установки на устройство

Затем нажмём кнопку «Применить изменения в базе данных Key_P1», как показано на рис. 129

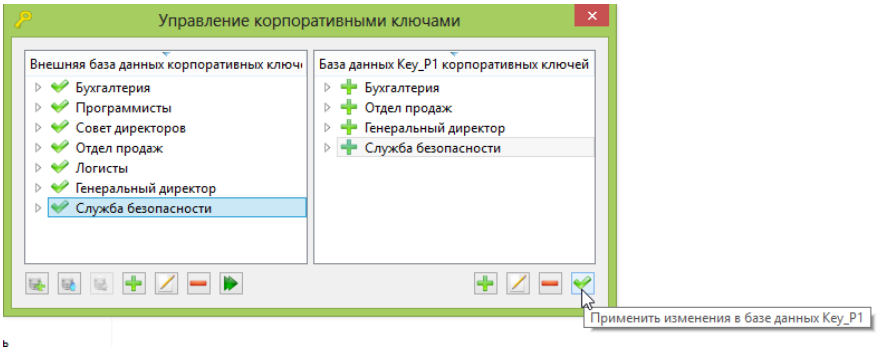

Рис. 129. Установка групп корпоративных ключей на устройство

В результате получим окно, показанное на рис. 130

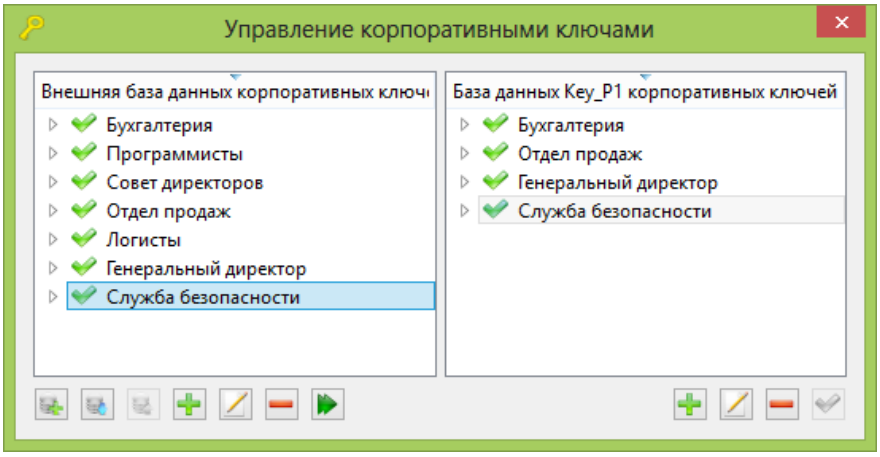

Рис. 130. Группы корпоративных ключей на устройстве

Функции администратора службы безопасности по созданию иерархического доступа на предприятии заканчиваются после установки групп корпоративных ключей для каждого пользователя отдела.

3.6.2 Шифрование информации корпоративными ключами

Шифрование информации корпоративными ключами происходит с помощью единого окна для шифрования информации случайными, синхронными, корпоративными ключами. Перейти в окно «Зашифрование информации» можно с помощью вкладки Действия->Зашифрование информации или с помощью кнопки на панели инструментов, как показано на рис. 131

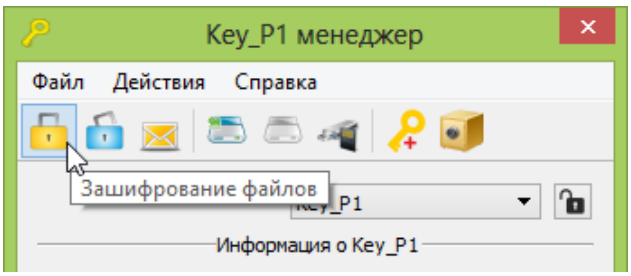

Рис. 131. Шифрование информации

В поле криптографический ключ необходимо выбрать «корпоративный ключ», ввести ПИН код пользователя, после чего появится возможность выбора отдела, для которого необходимо зашифровать информацию, например, «отдел продаж», см рис. 132

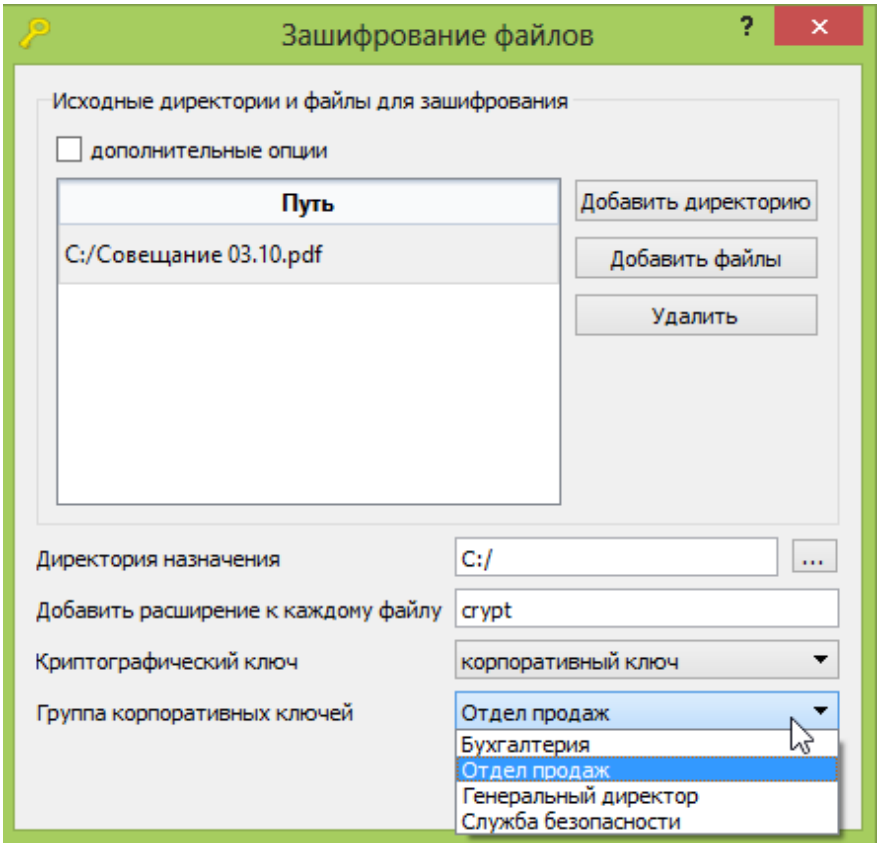

Рис. 132. Окно шифрования информации

Выбор файлов и директорий для шифрования, а также директории назначения подробно описан в главе 3.3(Шифрование файлов). Для запуска шифрования корпоративными ключами для выбранного отдела нажмите кнопку «Ок». Прогресс шифрования можно наблюдать в окне фоновых операций с устройством, как показано на рис. 133

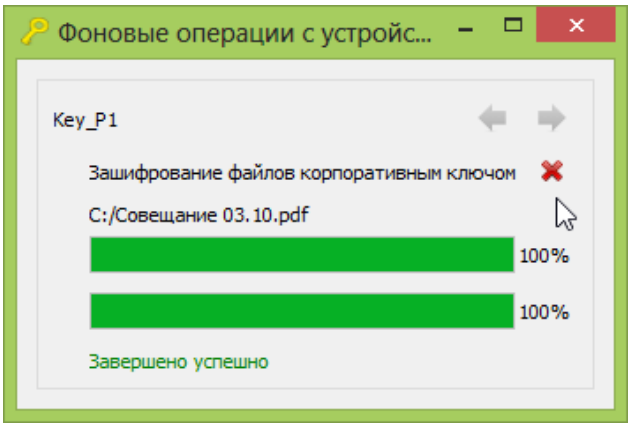

Рис. 133. Прогресс шифрования информации

В результате в директории назначения будет файл, зашифрованный одним из несколь-

ких ключей, которые установлены для выбранного отдела.

3.6.3 Расшифрование информации корпоративными ключами

Расшифрование информации корпоративными ключами происходит с помощью единого окна для расшифрования информации случайными, синхронными, корпоративными ключами. Перейти в окно «Расшифрование информации» можно с помощью вкладки Действия->Расшифрование информации или с помощью кнопки на панели инструментов, как показано на рис. 134

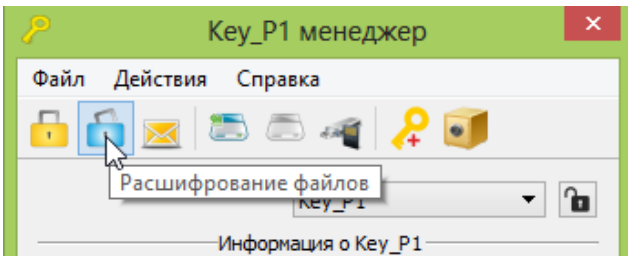

Рис. 134. Расшифрование информации

В поле криптографический ключ необходимо выбрать «корпоративный ключ», ввести ПИН код пользователя, после чего появится возможность выбора отдела, от которого необходимо расшифровать информацию, например, «отдел продаж», см рис. 135

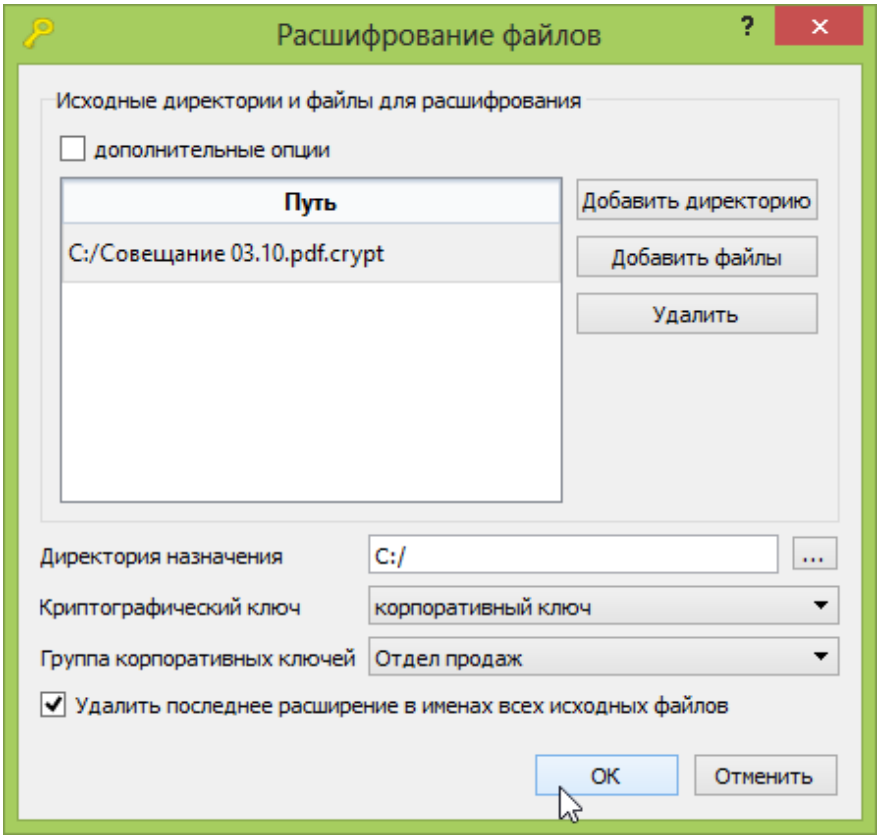

Рис. 135. Окно расшифрования информации

Выбор файлов и директорий для расшифрования, а также директории назначения подробно описан в главе 3.4(Расшифрование файлов). Для запуска расшифрования корпоративными ключами от выбранного отдела нажмите кнопку «Ок». Прогресс расшифрования можно наблюдать в окне фоновых операций с устройством. В результате в директории назначения будет файл, расшифрованный одним из нескольких ключей, которые установлены для выбранного отдела. Устройство Key_P1 определит, есть ли на текущем устройстве ключ для расшифрования информации. И после указания отдела, от которого принят файл и для которого ключ присутствует, файл будет расшифрован.

3.7 Ограничение доступа к съемным носителям

Служба информационной безопасности предприятия может в соответствии с внутренней политикой безопасности заблокировать возможность записи информации с корпоративных компьютеров на съемные накопители. Для этого устанавливается режим «только чтение», который позволит Key_P1 аппаратно заблокировать любую несанкционированную запись конфиденциальных данных, вирусов или других программ на накопитель. Т.е. записать информацию на накопитель в этом режиме не получится. Пользователю необходимо получить разрешение службы информационной безопасности для возможности записи на накопители.

Для того, чтобы выполнить установку режима «только чтение», необходимо последовательно выбрать вкладку **Действия** перейти в подменю **Администрирование** и выбрать пункт **Управление режимом "только чтение"** (см рис. 136)

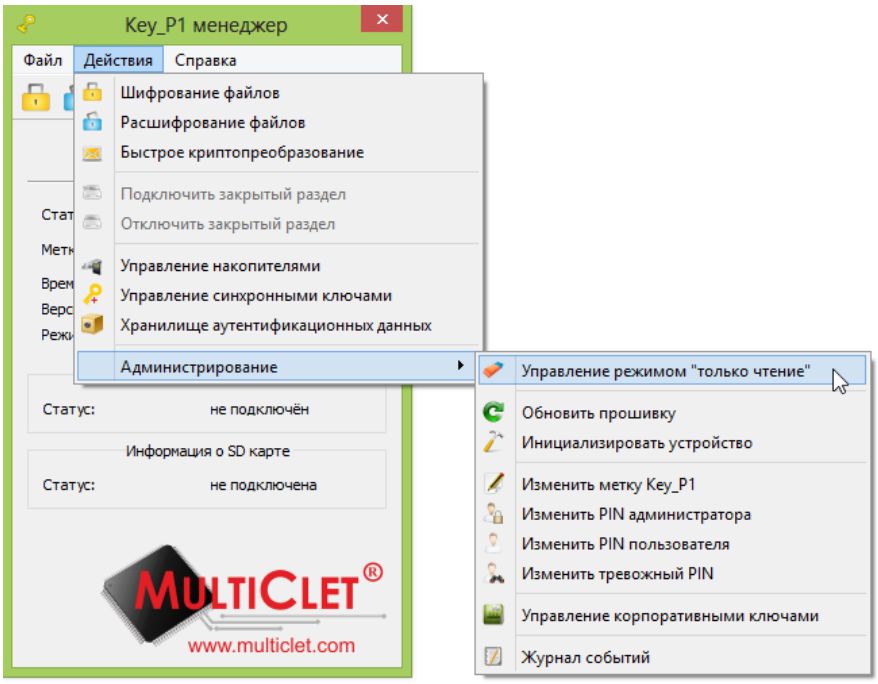

Рис. 136. Управление режимом "только чтение"

После правильного ввода PIN кода администратора появится окно для управления режимом "только чтение". Администратор в праве разрешить пользователю управлять режимом "только чтение"или установить принудительно данный режим(рис. 137).

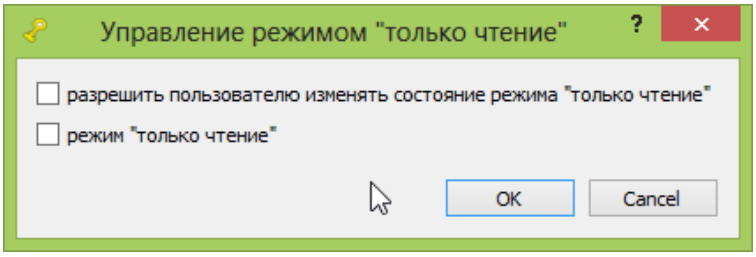

Рис. 137. Ввод PIN кода администратора

В случае установки администратором режима "только чтение"с последующим вводом PIN кода администратора (см рис. 138) в главном меню программы Key_P1 менеджер пользователь увидит установленную "галочку"в строке режим "только чтение"(см рис. 139)

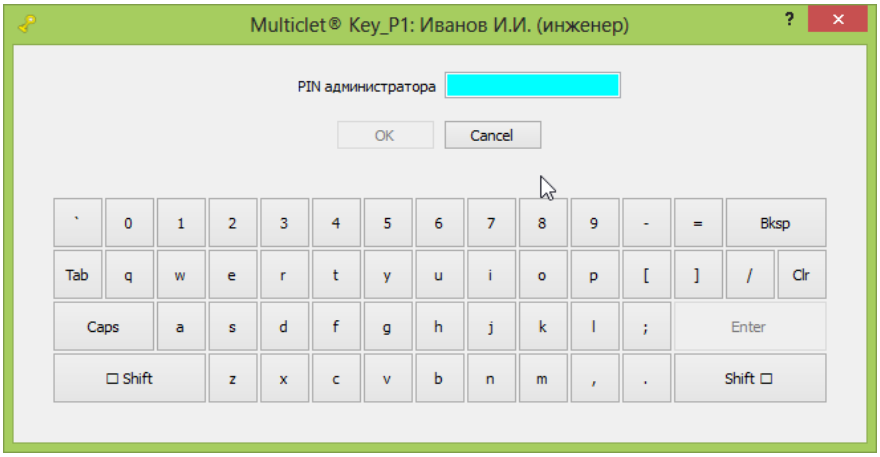

Рис. 138. Ввод PIN кода администратора

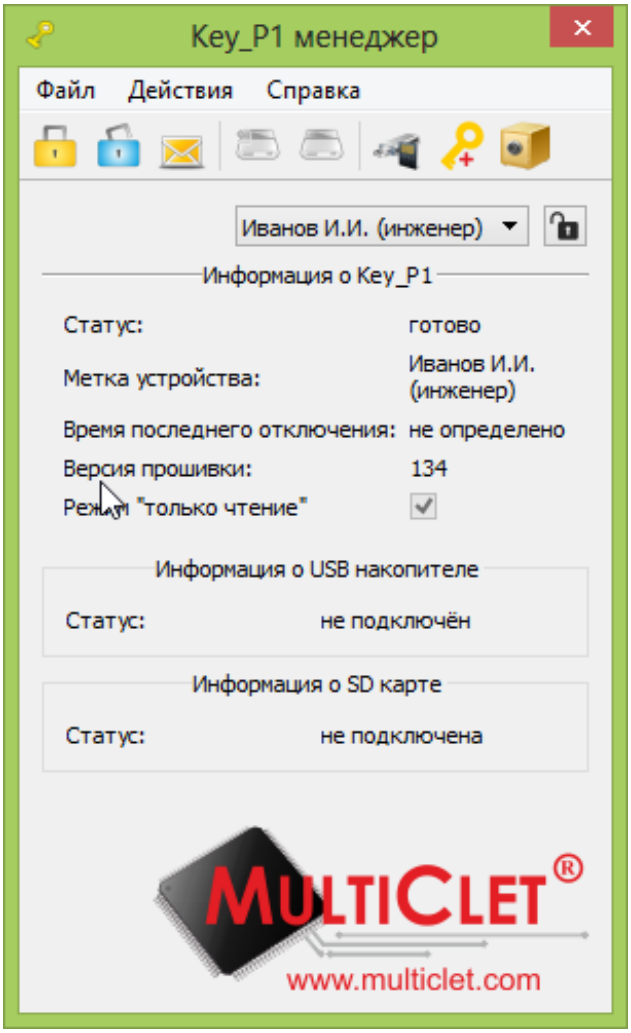

Рис. 139. Главное окно приложения

3.8 Журнал действий пользователя

Устройство Key_P1 ведёт лог-журнал основных действий. В журнал работы устройства заносятся основные действия пользователя с указанием времени. Фиксируется время подключения устройства, разблокировки закрытых разделов и т.д. Таким образом, отключение Key_P1 с целью несанкционированного копирования конфиденциальной информации с корпоративных компьютеров на внешний носитель будет зафиксировано (включая отметку о времени и дате) и доступно службе информационной безопасности.

Для того, чтобы открыть журнал, необходимо последовательно выбрать вкладку **Действия** перейти в подменю **Администрирование** и выбрать пункт **Журнал событий** (см рис. 140)

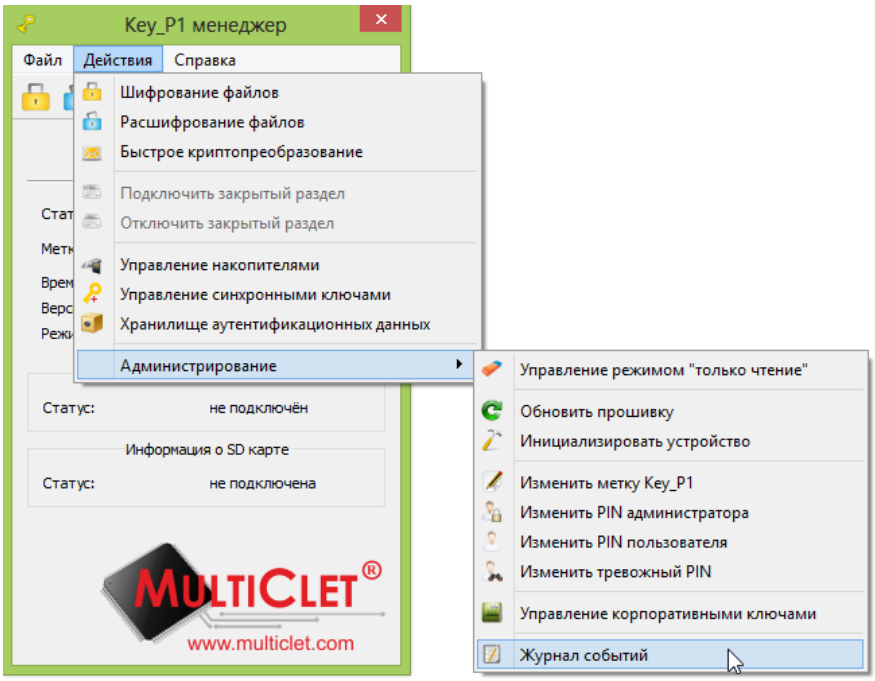

Рис. 140. Журнал событий

Журнал событий состоит из журнала времени отключения/подключения устройства и журнала основных событий, совершаемых пользователем с устройством Key_P1. Окно журнала событий представлено на рис. 141

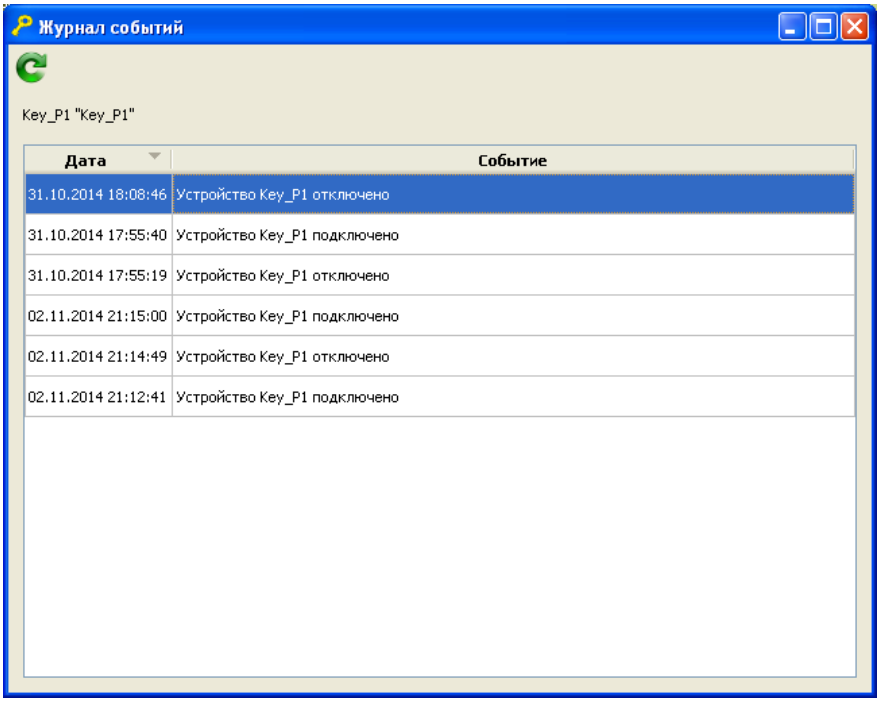

Рис. 141. Журнал времени подключения/отключения устройства

Журнал событий будет активирован после специального бесплатного обновления прошивки устройства.

3.9 Хранилище аутентификационных данных

Устройство позволяет сохранять пользовательские пароли и логины на внутреннюю защищенную память устройства Key_P1. Данная функция позволит, в том числе, обезопасить данные для доступа к общедоступным почтовым ресурсам, таким как: «Mail.ru», «Gmail.com», «Mail.yandex.ru» от несанкционированного доступа, как это произошло осенью 2014 года с 6 млн. записей других пользователей. Это достигается за счет установки сложного и длинного пароля и указания адреса ресурса при добавлении данных в хранилище. Для того, чтобы воспользоваться данной функцией, необходимо последовательно выбрать вкладку **Действия** и команду **Хранилище аутентификационных данных** (рис. 142).

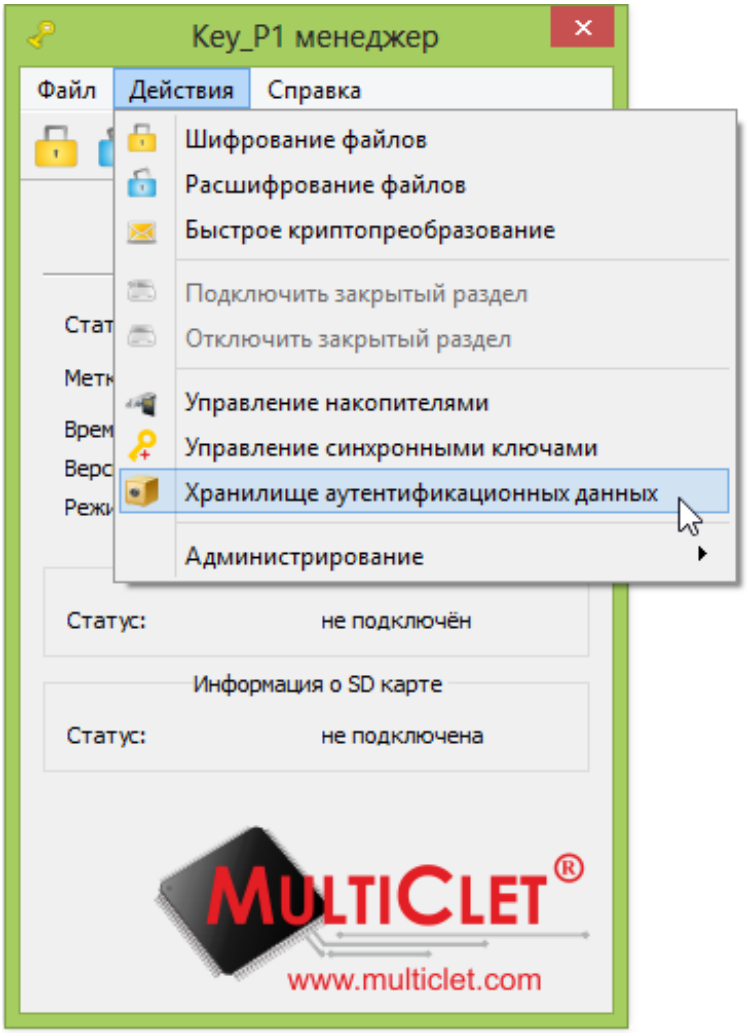

Рис. 142. Хранилище аутентификационных данных

Под аутентификационными данными понимаются логин и пароль к информационному

ресурсу. Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK» (рис. 143).

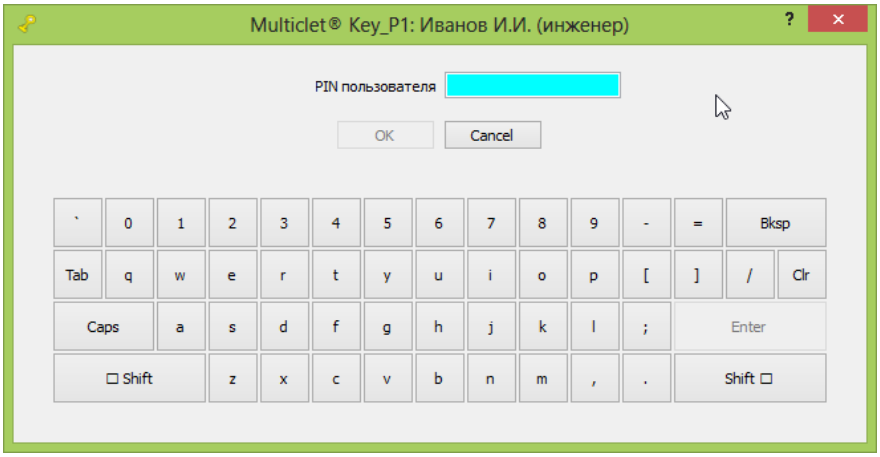

Рис. 143. Ввод PIN пользователя

Появится основное окно **хранилища аутентификационных данных** (рис. 144). Окно состоит из двух частей. В левой части можно создавать группы для паролей к информационным ресурсам определенной тематики. В правой части заносится парольная информация для каждого ресурса. Создадим новую группу «Почта». Для этого необходимо нажать кнопку **Добавить** в левой части.

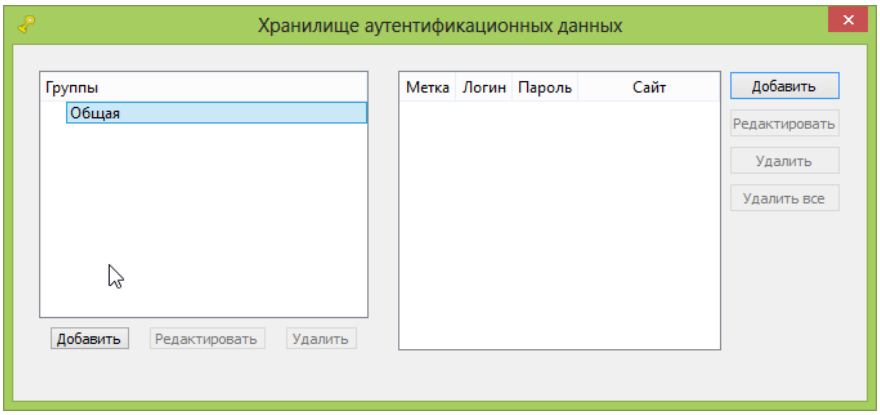

Рис. 144. Окно хранилища

Появится окно для ввода метки (имени) новой группы (рис. 145). После ввода имени необходимо нажать «OK».

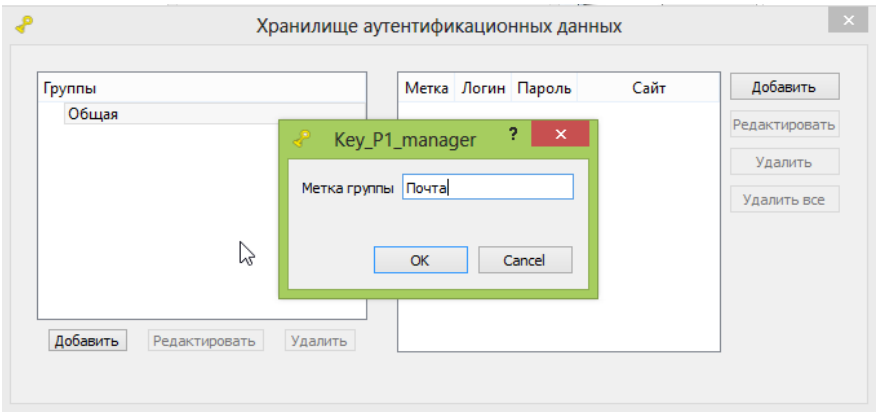

Рис. 145. Метка группы

В левой части появилась новая группа «Почта» (рис. 146). Произведем добавление новых парольных данных для почтового ресурса «Mail.ru». Для этого необходимо нажать кнопку **Добавить** в правой части окна.

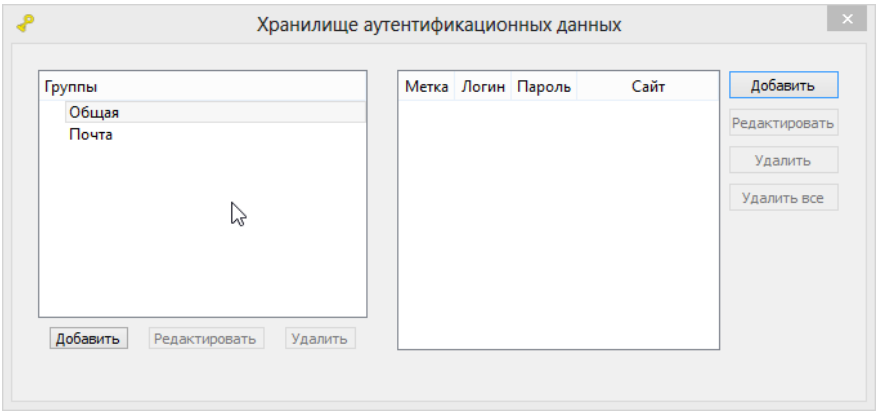

Рис. 146. Окно хранилища

Появится **Окно добавления аутентификационных данных** (рис. 147). В строке **Группа** следует выбрать группу, к которой относится информационный ресурс. В строке **Описание** необходимо добавить описание или назначение информационного ресурса. В строке **Сайт** следует добавить интернет адрес информационного ресурса. В строке **Логин** необходимо ввести логин для доступа к информационному ресурсу. В строке **Пароль** следует ввести пароль для доступа к информационному ресурсу. В строке **Подтверждение пароля** вводится еще раз пароль. После выполнения всех этих действий следует нажать «OK».

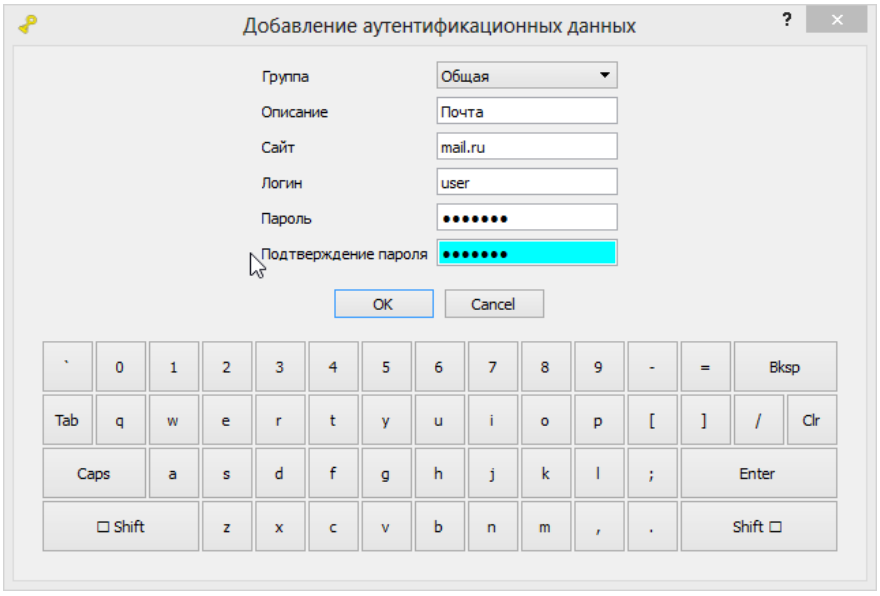

Рис. 147. Окно добавления аутентификационных данных

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK» (рис. 148).

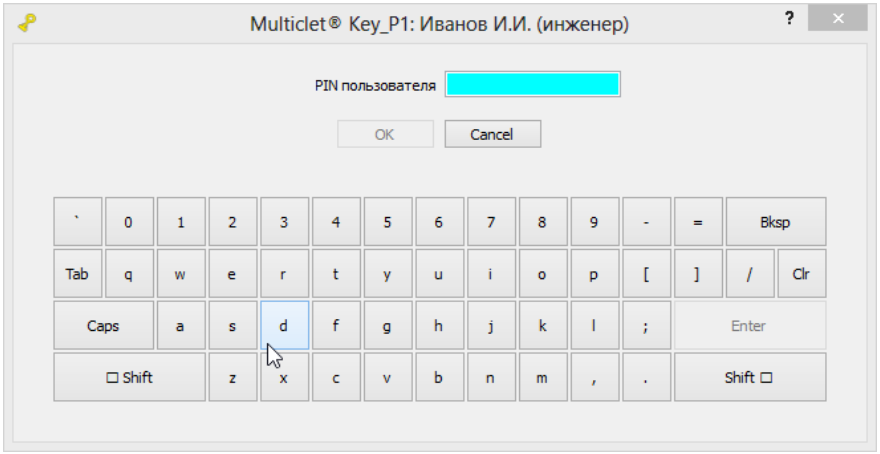

Рис. 148. Ввод PIN пользователя

В правой части основного окна отобразится парольная информация ресурса «Mail.ru» (рис. 149).

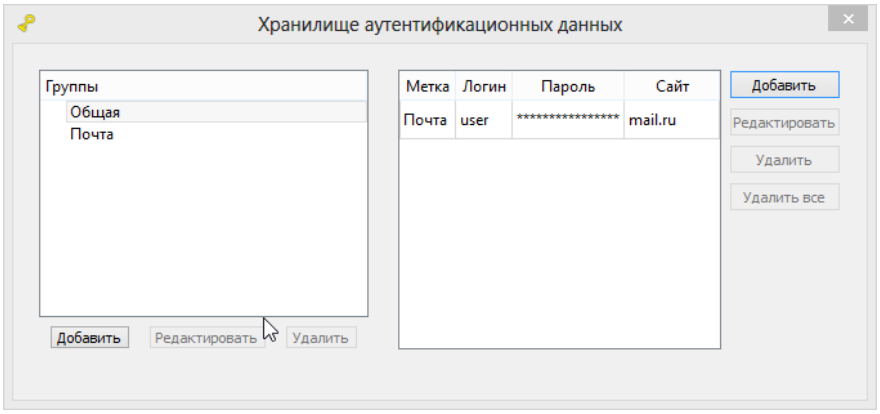

Рис. 149. Окно хранилища

Для того, чтобы произвести копирование данных с целью переноса их в окно авторизации информационного ресурса, сначала следует произвести копирование интернет-адреса ресурса. Для этого следует перевести курсор мыши на поле, находящееся под заголовком **Сайт**, и двойным щелчком левой клавишей мыши осуществить захват данных (рис. 150). При этом в левой части окна появится информация о количестве времени оставшемся для выполнения данной операции.

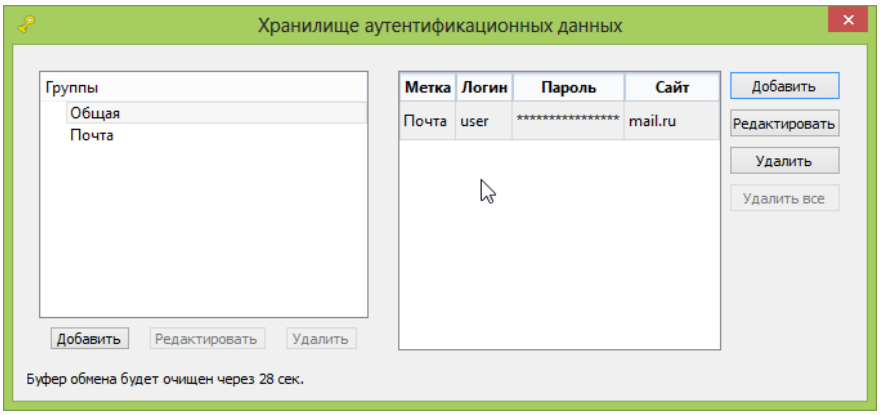

Рис. 150. Копирование данных

Далее необходимо перейти к информационному ресурсу. В нашем случае следует открыть браузер и в адресной строке, нажав на правую кнопку мыши, выполнить команду «Вставить». После чего следует нажать на клавиатуре «Enter». Появится окно авторизации ресурса «Mail.ru»(рис. 151).

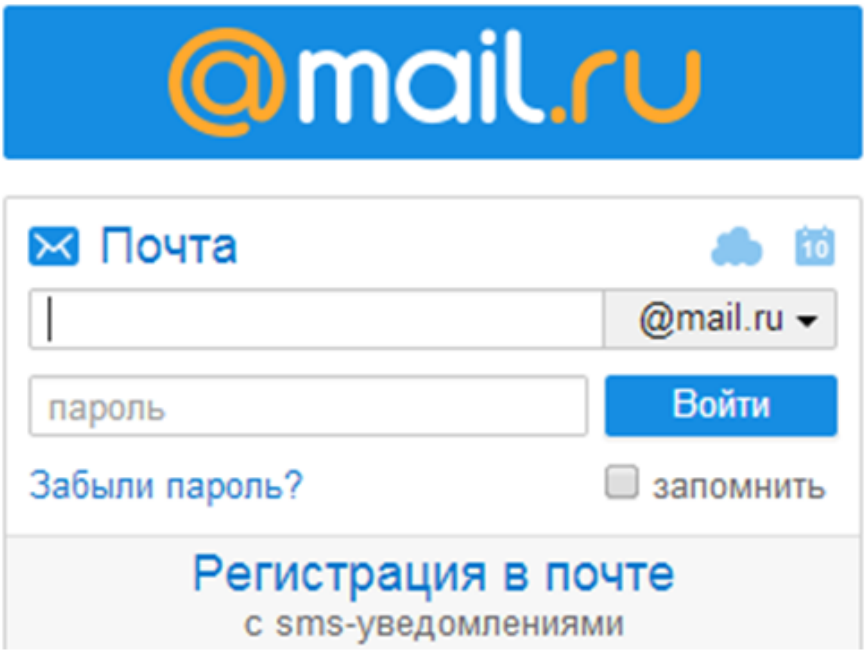

Рис. 151. Окно авторизации

Далее следует произвести копирование логина для доступа к ресурсу. Для этого необходимо перевести курсор мыши на поле под заголовком **Логин** и двойным щелчком левой клавишей мыши осуществить захват данных (рис. 152). При этом в левой части окна появится информация о количестве времени оставшемся для выполнения данной операции. Следующим шагом следует перевести курсор мыши в окне авторизации на строку ввода логина и, нажав на правую кнопку мыши, выполнить команду «Вставить».

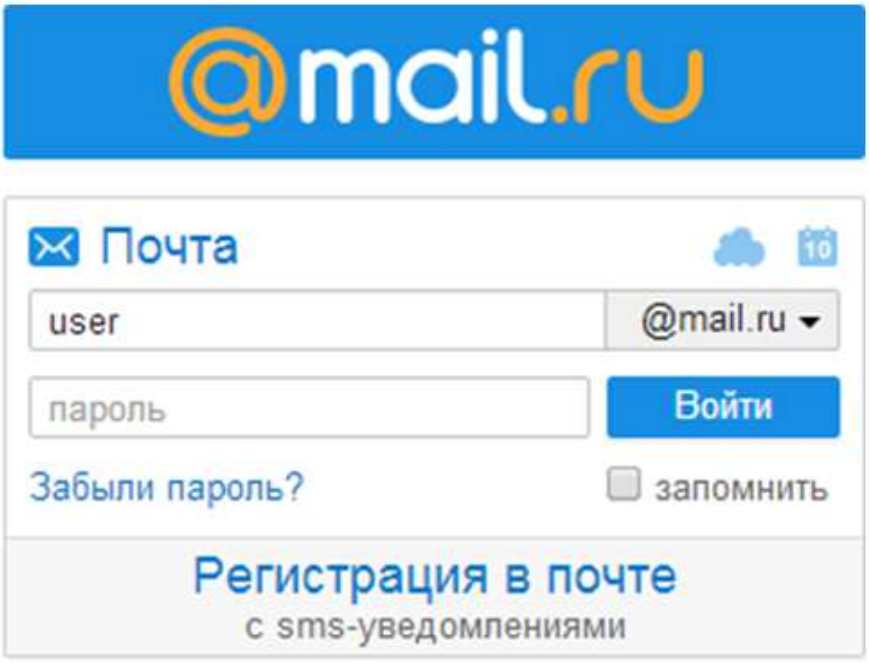

Рис. 152. Окно авторизации

Далее следует произвести копирование пароля для доступа к ресурсу. Для этого необходимо перевести курсор мыши на поле под заголовком **Пароль** и двойным щелчком левой клавишей мыши осуществить захват данных (рис. 153). При этом в левой части окна появится информация о количестве времени оставшемся для выполнения данной операции. Следующим шагом следует перевести курсор мыши в окне авторизации на строку ввода пароля и, нажав на правую кнопку мыши, выполнить команду «Вставить». После этого можно нажать кнопку «Войти» и осуществить вход в информационный ресурс.

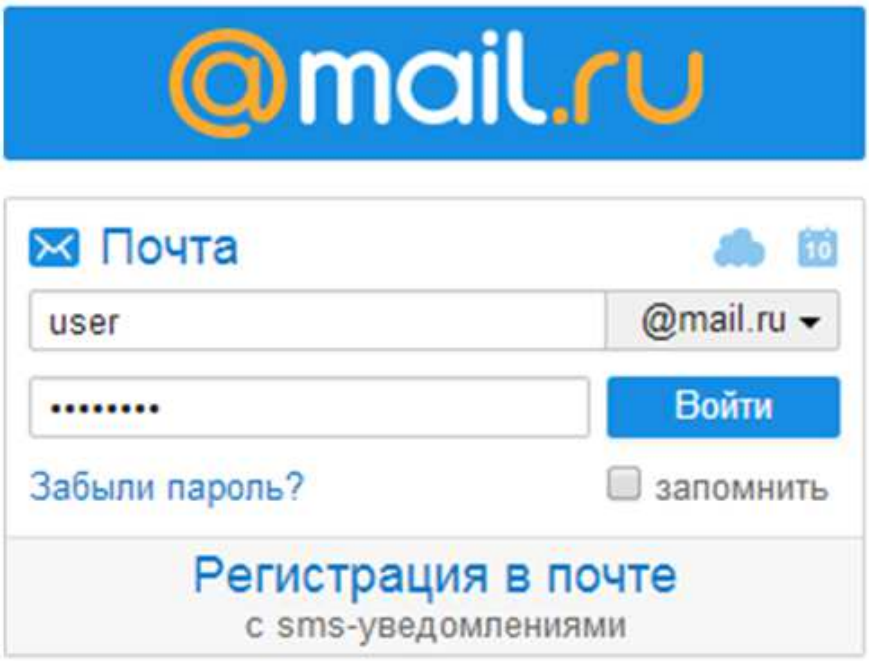

Рис. 153. Окно авторизации

Любые аутентификационные данные можно редактировать. Для того, чтобы выполнить данную процедуру, необходимо в основном окне **хранилища аутентификационных данных** в правой части нажать кнопку **Редактировать** (рис. 154).

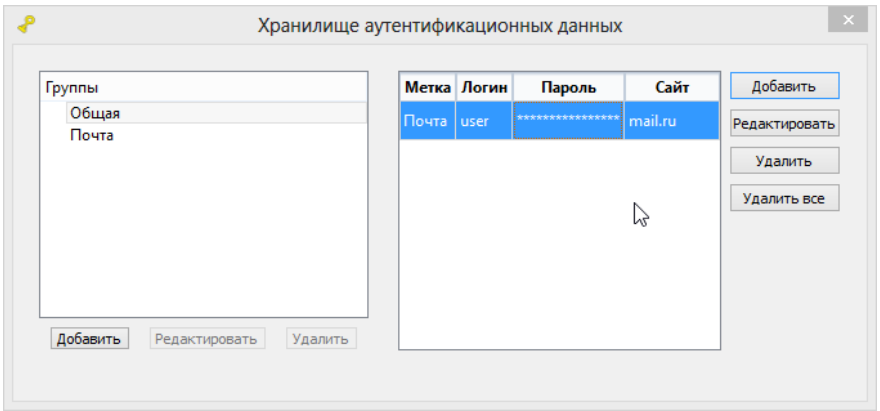

Рис. 154. Редактирование аутентификационных данных

Появится окно редактирования аутентификационных данных (рис. 155). В данном окне можно изменить любую информацию. После выполнения всех операций следует нажать «OK».

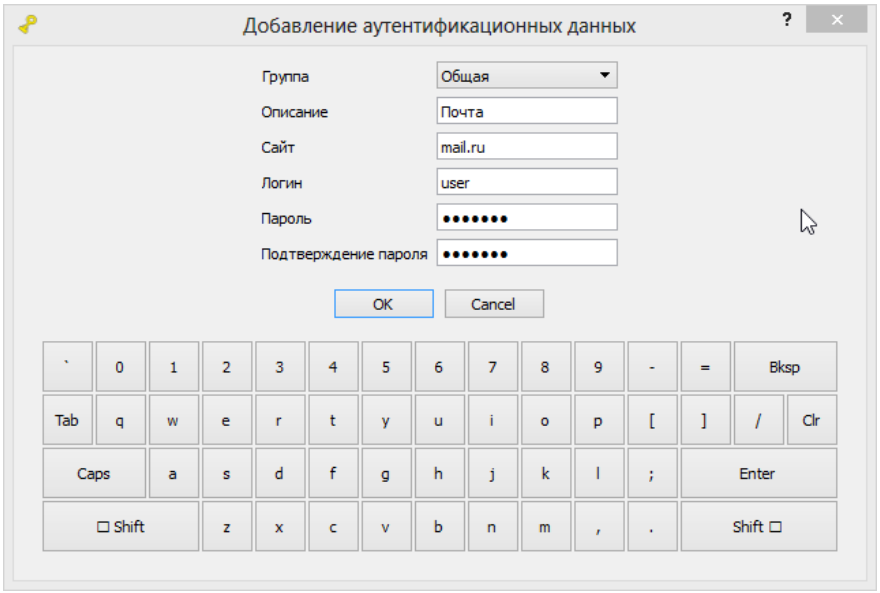

Рис. 155. Редактирование аутентификационных данных

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «OK» (рис. 156).

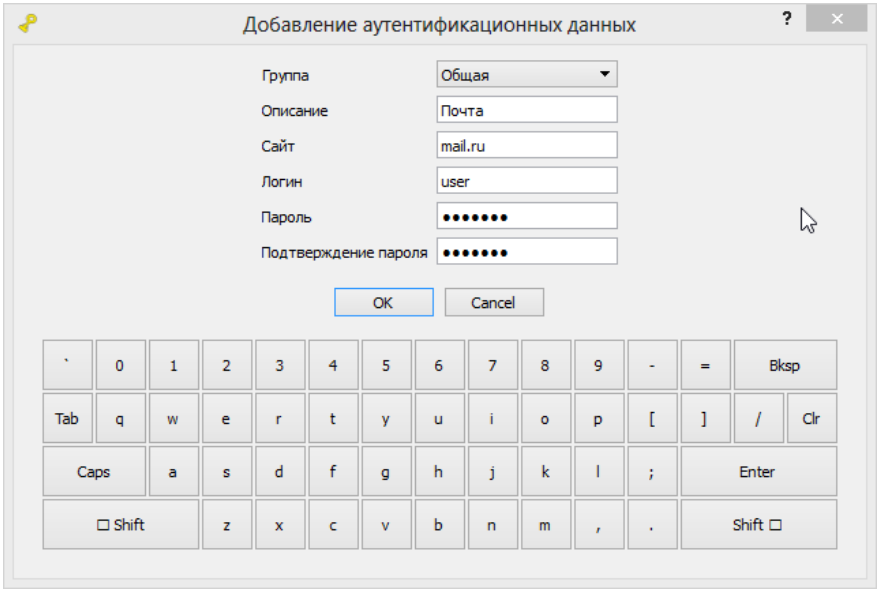

Рис. 156. Ввод PIN пользователя

4 Часто возникающие вопросы

Вопрос 1: *Можно ли использовать личные данные, не являющиеся логином и паролем для доступа к сайту, а, например, номером и cvv кредитной карты? Или такие данные можно только хранить в защищенном виде?*

Ответ: Конечно это сделать можно. Например, номер кредитной карты можно поместить в строку «логин», а cvv в строку «пароль».

Вопрос 2: *Где хранятся ключи шифрования? И можно ли получить установленные на устройство ключи шифрования?*

Ответ: Ключи для шифрования хранятся в защищенной памяти устройства. В целях безопасности из устройства ключи шифрования не получить. Но возможно восстановление устройства, если был сохранен набор ключей при инициализации.

5 Лист регистрации изменений

Номер	Версия	Дата	Описание изменений	Номера страниц
1	0.1	25.08.2015	Начальная версия документации	