

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

Cı	писон	к сокращений	4
1	Оби	щие сведения	5
	1.1	Описание и назначение	5
	1.2	Организационные меры по защите информации	8
	1.3	Системные требования	9
	1.4	Маркировка устройства	9
	1.5	Технические характеристики	10
2	Уста	тановка и настройка устройства Key_P1	11
	2.1	Описание установки и настройки устройства	11
	2.2	Установка программного обеспечения	13
	2.3	Запуск приложения Key_P1 Manager	21
	2.4	Описание интерфейса приложения Key_P1 Manager	22
	2.5	Обновление внутреннего программного обеспечения	28
	2.6	Инициализация устройства	33
	2.7	Изменение PIN администратора	42
	2.8	Изменение PIN пользователя	44
	2.9	Изменение тревожного PIN	47
	2.10	Изменение метки устройства	49
3	Исп	пользование устройства Кеу_Р1	51
	3.1	Управление накопителями	51
		3.1.1 Создание закрытого раздела на USB накопителе	51
		3.1.2 Создание закрытого раздела на SD карте	55
		3.1.3 Подключение закрытого раздела на USB накопителе	59
		3.1.4 Подключение закрытого раздела на SD карте	62
		3.1.5 Отключение закрытого раздела	65
		3.1.6 Использование закрытого раздела	67
		3.1.7 Удаление закрытого раздела	68
	3.2	Управление синхронными ключами	70
		3.2.1 Добавление синхронных ключей	70
		3.2.2 Удаление синхронных ключей	74
	3.3	Шифрование файлов	77
	3.4	Расшифрование файлов	84



	3.5	Быстрое криптопреобразование	89
	3.6	Управление корпоративными ключами	93
		3.6.1 Пример создание иерархического доступа	99
		3.6.2 Шифрование информации корпоративными ключами	107
		3.6.3 Расшифрование информации корпоративными ключами	110
	3.7	Ограничение доступа к съемным носителям	112
	3.8	Журнал действий пользователя	115
	3.9	Хранилище аутентификационных данных	117
4	Час	то возникающие вопросы	126
5	Лис	ст регистрации изменений	127



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 Кеу Р1 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	В Key_P1 MultiClet предусмотрено разграничение прав доступа к зашифрованным фай-
информации	лам. Служба безопасности предприятия будет иметь возможность создавать различные
	разграничения прав по отделам. При этом руководитель будет иметь доступ ко всем фай-
	лам. Сотрудники компании могут кодировать файлы для своих коллег с помощью про-
	граммы 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 Лля этого
	ровать любую несанкционированную запись конфиденциальных данных, вирусов или дру-
	гих программ на накопитель. 1.е. записать информацию на накопитель в этом режиме не
	получится, пользователю понадооиться получить разрешение служоы информационной
	оезопасности для возможности записи на накопители.
Защита от шпионских	Key_P1 разрешает подключение только обычных накопителей информации, работа
флешек (проблема	«устройств-шпионов» (представляются одновременно клавиатурой и накопителем) будет
badUSB)	заблокирована.
Запрет на отключение	Устройство Key_P1 сохраняет в «лог журнал» основные события, совершаемые пользова-
	телем. Просмотр «лог журнала» может быть закрыт для пользователя. Для разблокировки
	просмотра необходимо ввести ПИН-код администратора. Таким образом, работник не мо-
	жет незаметно изъять устройство Кеу_Р1 для записи на флэш-накопитель корпоративных
	данных, так как все попытки отключения будут зафиксированы службой безопасности.
Сотрудник в командиров-	Пользователи могут создать одинаковые ключи для обмена зашифрованными сообщени-
ке	ями друг с другом или головным офисом компании в случае обмена данными во время
	деловых поездок с помощью открытой электронной почты и других интернет-ресурсов.
Належное шифрование	Шифрование информации возможно на накопителях и компьютере. Шифрование осу-
	пествляется по алгоритму ГОСТ 28147-89 с шириной ключа 256 бит. Шифрование алгорит-
	мом ГОСТ28147-89 на накопителях осуществляется защишенным методом – по секторам
	(вскрытие потребует тысячи лет машинного времени).
Неуязвимость данных	Пользователь имеет возможность создания резервных копий защифрованной информации
пеульниесть данных	таким образом, при потере или повреждении устройства Кеу. Р1 и(или) накопителя поль-
	зователь сможет восстановить свою информацию. В случае потеря устроиство осснолезно
	для элоумышленника. Потерянное устроиство ксу_11 нельзя использовать ни в каких
	целях, связанных с шифрованием и дешифрованием. Из потерянного устроиства нельзя
	извлечь информацию о принципах расоты аналогичных устроиств.
поддержка разных нако-	устроиство поддерживает расоту с накопителями типа SD, micro SD и USB. Также суще-
пителей	ствует возможность использования USB удлинителей, если размер посадочного USB порта
	на компьютере недостаточен.
Использование разных	Поддерживается работа устройства в операционных системах WindowsXP, Windows 7,
OC	Windows 8, Linux 2.6.х, Linux 3.х и в разработке MacOS.
Сейф для паролей	Устройство позволяет сохранять пользовательские пароли и логины на внутреннюю защи-
	щенную память устройства Кеу_Р1. 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 обеспечива-
	ем удобное использование и хранение своих паролей, а также защищаемся от кейлогеров
	на ПК.
Быстрое криптопреобра-	Устройство Key_P1 MultiClet позволяет провести быстрое шифрование или расшифро-
зование	вание информации. Таким образом пользователи могут легко и быстро обмениваться за-
	шифрованными 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 AC необходимо обеспечить:

- Сохранность устройства Кеу_Р1;

- 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 систе-	• WindowsXP (SP3);
мами	• Windows 7;
	• Windows 8;
	• Linux 2.6.x;
	• Linux 3.x.
Необходимые аппаратные условия	USB-порт

1.4 Маркировка устройства

Маркировка устройства Кеу_Р1 наносится с обратной стороны корпуса.



14 – 2014 год выпуска партии

Рис. 2. Маркировка устройств



1.5 Технические характеристики

Таблица 2. Технические характеристики.

Назначение	устройство предназначено для		
	шифрования небольших объё-		
	мов конфиденциальной инфор-		
	мации		
Скорость работы	с открытым разделом накопите-		
	ля до 3,2 Мбит/с,		
	с закрытым разделом и шифро-		
	вание 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 Кеу_Р1 - 256 бит,		
	для распространяемых за пре-		
	делами РФ устройств Кеу_Р1 -		
	56 бит		



2 Установка и настройка устройства Кеу Р1

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 OC, тогда в дальнейшем для использования устройства не потребуется установка ПО на ПК. Если требуется работа под OC Windows и OC 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 OC Windows 8 на рис. 3).

💭 I 💽 🚺 🖛 I Компьютер – 🗖 🗙						
Файл Компьюте	р Вид ^ 🕐					
Свойства Сткрыть Сткрыть Переименовать Расположение	№ Доступ к мультимедиа *					
 Избранное Загрузки Недавние мес Рабочий стол 	 Жесткие диски (2) Windows8_OS (C;) 689 ГБ свободно из 893 ГБ Устройства со съемными носителями (3) 					
🕽 Библиотеки ा Видео ⊡ Документы ш Изображения Ј Музыка К Домашняя груп	Состанование Состанование КЕУ_Р1 (F:) ОКОВОД ВО-ROM (G:) ККР10 28,5 КБ свободно из 30,0 КБ Состанование Состанование					
Компьютер Windows8_OS Image: Lenovo (D:) Ima	s (C -RC ➤ ﷺ ■					

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



👝 l 💽 🚹 = l	KEY_P1 (F:)	Средства работы с д	исками			×
Файл Главная Об	іщий доступ Вид	Управление				^ ?
Копировать Вставить	💽 Переместить в 👻	🗙 Удалить 🔹	Создать папку	Свойства	на странать Выделить	
Буфер обмена	Упоряд	очить	Создать	Открыть		
🛞 👻 🕇 👝 🕨 K	омпьютер → КЕУ_Р1 (F:)	~	С Поиск:	KEY_P1 (F:)	Q.
 Избранное Загрузки Недавние места Рабочий стол Библиотеки Видео Документы Цзображения Музыка Домашняя группе 	readme		Ν			
			2			
Компьютер						
Windows8_OS (C						
KEY P1 (E:)						
Дисковод BD-RC ¥						
1 элемент						:==

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



Key_P1 MultiClet

<u>1) Подробное описание устройства Key_P1 Multiclet</u> <u>2)(Windows) Загрузить ПО</u> <u>3)(Linux) Загрузить ПО</u> <u>4) Форум Key_P1 Multiclet</u>
Вопросы и пожелания принимаются по электронной почте: sale@multiclet.com, micron@fointec.ru
1) Documents and more information about Key_P1 Multiclet 2)(Windows) Download Software 3)(Linux) Download Software 4) Forum Key_P1 Multiclet

Questions and suggestions please email to: sale@multiclet.com, micron@fointec.ru

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 OC 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 OC Windows) либо **Key P1 Software Installer.tar.gz** (для OC Linux).

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



	?	×
🗞 Key_P1 software installer Setup		
Setup - Key_P1 software		
Welcome to the Key_P1 software Setup Wizard.		
Дал	iee Qu	uit

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".



	?	x
Installation Folder		
Please specify the folder where Key_P1 software will be installed.		
C:\Multiclet\Key_P1_software	Brows	se
\searrow		
Далее	Отме	ена

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



	? ×
) 😸 Key_P1 software installer Setup	
Select Components	
Please select the components you want to install.	
✓ Key_P1_manager	Install Key_P1_manager.
Def <u>a</u> ult <u>S</u> elect All <u>D</u> eselect All	This component will occupy approximately 50.11 MiB on your hard disk drive.
	Далее Отмена

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



				? ×
🕞 👸 Key_	P1 software installer Se	tup		
Start Menu	shortcuts			
Select the Start enter a name to	Menu in which you would create a new folder.	like to create the	program's shortcuts.	You can also
Key P1 softwar	e			
Accessibility				•
Accessories				
Administrativ	e Tools			
Lenovo				
Lightshot				
Maintenance				
KI 1 I				
			Далее	Отмена

Рис. 9. Окно для просмотра параметров установки

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



	?	×
) 😸 Key_P1 software installer Setup		
Ready to Install		
Setup is now ready to begin installing Key_P1 software on your computer.		
Show Details		
\triangleright		
Install	Отме	ена

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 OC 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.

ዯ Кеу_Р1 менеджер	X			
Файл Действия Справка				
🗗 🛅 🖂 🗂 🐗	<mark>ନ</mark> 🗊			
Иванов И.И. (инженер) 🔻 ն			
Информация о Кеу_Г	P1			
Статус:	готово			
Метка устройства:	Иванов И.И. (инженер)			
Время последнего отключения:	не определено			
Версия прошивки:	134			
Режим "только чтение"				
Информация о USB накопителе				
Статус: не подкл	ючён			
Информация о SD кар	те			
Статус: по	дключена			
Имя/размер открытого раздела: SD	_pub / 1.76ГБайт			
Имя/размер закрытого раздела: не подключен				
www.multiclet.com				

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 Кеу_Р1, 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"Кеу_P1 Manager

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



Кеу_Р1 менеджер				
Файл Действия Справка				
Содержа О програ	ние 🔓 мме Key_P1_manager			
Иванов И.И.	. (инженер) 🔻 🚹			
Информация о Кеу	_P1			
Статус:	готово			
Метка устройства:	Иванов И.И. (инженер)			
Время последнего отключения:	не определено			
Версия прошивки:	134			
Режим "только чтение"				
Информация о USB накопителе				
Статус: не подн	ключён			
Информация о SD карте				
Статус: г	подключена			
Имя/размер открытого раздела: 5	SD_pub / 1.76ГБайт			
Имя/размер закрытого раздела: не подключен				
WDLTICLET® www.multiclet.com				

Рис. 14. Вкладка "Справка"Кеу_Р1 Manager

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



ℯ Кеу_Р1 менеджер	×			
Файл Действия Справка				
🗗 🔂 🔀 🖾 🐗	<mark>ନ</mark> 🗐			
Иванов И.И.	. (инженер) 🔻 🍙			
Информация о Кеу	_P1			
Статус:	готово			
Метка устройства:	Иванов И.И. (инженер)			
Время последнего отключения:	не определено			
Версия прошивки:	134			
Режим "только чтение"				
Информация о USB нак	Информация о USB накопителе			
Статус: не поди	ключён			
Информация о SD к	арте			
Статус: г	подключена			
Имя/размер открытого раздела: 5	SD_pub / 1.76ГБайт			
Имя/размер закрытого раздела: н	не подключен			
WWW.multiclet.com				

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.



	×				
Файл Действия Справка					
🔓 🔂 🔀 🗂 🐗	<mark>ନ</mark> 🗐 👘				
Иванов И.И.	Иванов И.И. (инженер) 🔻 🚹				
Информация о Кеу_	P1				
Статус:	готово				
Метка устройства:	Иванов И.И. (инженер)				
Время последнего отключения:	не определено				
Версия прошивки:	134				
Режим "только чтение"					
Информация о USB накопителе					
Статус: не подкл	лючён				
Информация о SD ка	рте				
Статус: по	одключена				
Имя/размер открытого раздела: SI)_pub / 1.76ГБайт				
Имя/размер закрытого раздела: не	е подключен				
WWW.multiclet.com					

Рис. 16. Список подключенных к ПК устройств Кеу_Р1

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



Кеу_Р1 менеджер	×		
Файл Действия Справка			
🗗 🔂 🖂 🗂 🛋	2 🗊		
Иванов И.И	. (инженер) 🔻 🔳		
Информация о Кеу	/_P1		
Статус:	готово		
Метка устройства:	Иванов И.И. (инженер)		
Время последнего отключения:	не определено		
Версия прошивки:	134		
Режим "только чтение"			
Информация о USB нак	опителе		
Статус: не под	ключён		
Информация о SD к	арте		
Статус:	подключена		
Имя/размер открытого раздела:	SD_pub / 1.76ГБайт		
Имя/размер закрытого раздела:	не подключен		
www.multiclet.com			

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 Кеу_Р1



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

Растер обновления прошивки Кеу_Р1	8 ×
Источник прошивок Кеу_Р1	
Эагрузить прошивку с сайта multiclet.com	
🔘 Загрузить прошивку из локального файла	
	www.multiclet.com
	< <u>Н</u> азад Далее > Отмена

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».



₽ N	Ластер обн	новления	прошивки Кеу_Р1	
Cr	ІИСОК П ыберите пр	ІРОШИ рошивку д	вок Кеу_Р1	
	Дата	Версия	Прошивка	
(07.10.2014	134	KeyP1_FW_134.bin	
(07.10.2014	134	KeyP1_Release_FW_134.bin	
C	07.10.2014	132	KeyP1_FW_132.bin	
C	07.10.2014	132	KeyP1 Release FW 132.bin	
	WDLTICLET® www.multiclet.com			
	< <u>Н</u> азад Далее > Отмена			

Рис. 22. Список прошивок Кеу_Р1

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 «ОК». 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».

Мастер инициализации Кеу_Р1	8 X
Криптографические ключи для Кеу_Р1	
 сгенерировать криптографические ключи 	
🔽 сохранить в файл	
🔘 загрузить криптографические ключи из файла	3
www.m	ulticlet.com
<hr/>	> Отмена

Рис. 27. Параметры инициализации устройства Key_P1

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

Мастер инициализации	и Кеу_Р1
Криптографичес	ские ключи для Кеу_Р1
осгенерировать криптог	графические ключи
🔽 сохранить в файл	C:/Users/Роман/Desktop/kp1-test/list_key
🔘 загрузить криптографи	ические ключи из файла
	\searrow
	•
	WDLTICLET®
	< <u>Н</u> азад Далее > Отмена

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).

	an amore and Kry .71		— X
🕞 🗢 📕 🕨 kp1-te	• • •	Поиск: kp1-test	٩
Упорядочить 🔻 Н	зая папка	8=	• 🔞
🔆 Избранное	Имя	Дата изменения	Тип
〕 Загрузки	list_key	30.09.2014 16:53	Файл
📃 Недавние места			
📃 Рабочий стол			
 Библиотеки Git Subversion Видео Документы Изображения Музыка 	6		
	٠ [+
<u>И</u> мя файла: lis	key		-
<u>Т</u> ип файла:			•
🔿 Скрыть папки		Сохранить	Отмена

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.


Р Мастер инициализации Кеу_Р1
Криптографические ключи для Кеу_Р1
🔘 сгенерировать криптографические ключи
🗸 сохранить в файл
загрузить криптографические ключи из файла
WDLTICLET® www.multiclet.com
< <u>Н</u> азад Далее > Отмена

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.



< ₽					N	Ластер	о иниц	циали	зации	Key_F	°1				? ×
PI	V ад	мини	істра	тора	1										
			По,	дтверж,	Р. цение Р.	IN адми IN адми	нистрат нистрат	opa]			
							6					1			
	•	0	1	2	3	4	5	6	7	8	9	-	=	Bk	sp
	Tab	q	w	e	r	t	У	u	i	o	р	[]	1	Clr
	Ca	ps	а	s	d	f	g	h	j	k	1	;		Enter	
		🗆 Shift		z	x	c	v	b	n	m				Shift 🗆	
												N	LTI	C	.ET®
												W	ww.m	ulticlet	.com
										<	: <u>Н</u> азад	l	<u>1</u> алее >		Отмена

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.

~					N	Ластер	о иниц	циал	изации	Key_F	°1				?	×
PI	N по	льзо	вате	ля												
			ſ	Тодтвер	ждение	PIN no.	пьзовато	еля [еля [••••]				
	•	0	1	2	3	4	5	6	7	8	9	-	=	Bk	SD	
	Tab	q	w	e	r	t	у	u	i	0	p	[]	1	Clr	
	Ca	ps	a	s	d	f	g	h	j	k	Т	;		Enter		Ī
		🗆 Shift		z	x	с	v	b	n	m	,	•		Shift 🗆		
						6						N	LTI ww.m		ET	• ®
										<	: <u>Н</u> азад	l	<u>1</u> алее >		Отмен	a

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.

P					Ν	Ластер	о ини	циали	зации	Key_P	1				?	×
Тр	ево	кный	i PIN	I												
				Подтв	ержден	Трев ие трев	зожный ожного	PIN PIN]				
	•	0	1	2	3	4	5	6	7	8	9	-	=	Bk	sp	
	Tab	q	w	e	r	t	у	u	i	o	р	[]	1	Clr	
	Ca	ps	a	s	d	f	g	h	j	k	I	;		Enter		
		🗆 Shift		z	x	с	v	ь	n	m		•		Shift 🗆		
							[r				NU	LT		E	n
										<	<u>Н</u> азад		<u>Д</u> алее >	•	Отмен	ıa

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)».



 	Мастер инициализации Кеу_Р1	?	×
Метка Кеу_Р1			
	Метка Иванов И.И. (инженер)		
	2		
	WOLTIC	LE let.co	T [®]
	< <u>Н</u> азад Далее >	Отме	на

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).



Кеу_Р1 менеджер	×
Файл Действия Справка	
🖥 🛅 🖂 🗂 🛋	t 🔑 🗐 👘
Иванов И.И	1. (инженер) 🔻 🚹
Информация о Ке	y_P1
Статус:	готово
Метка устройства:	Иванов И.И. (инженер)
Время последнего отключения:	не определено
Версия прошивки:	134
Режим "только чтение"	
Информация о USB на	копителе
Статус: не под	цключён
Информация о SD н	карте
Статус:	подключена
Имя/размер открытого раздела:	SD_pub / 1.76ГБайт
Имя/размер закрытого раздела:	не подключен
	TICLET ® .multiclet.com

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)

	енеджер		
Стат Врем Режи Стат Стат	Стравка Шифрование файлов Расшифрование файлов Быстрое криптопреобразование Подключить закрытый раздел Отключить закрытый раздел Управление накопителями Управление синхронными ключами Хранилище аутентификационных данных		
Статус:	Администрирование не подключён	ľ ć	Управление режимом "только чтение" Обновить процияку
Статус:	Информация о SD карте подключена	2 Z	Основно прошлаку Инициализировать устройство Изменить метку Кеу_Р1
Имя/разме Имя/разме	ер открытого раздела: SD_pub / 1.76ГБайт ер закрытого раздела: не подключен	2	Изменить PIN администратора Изменить PIN пользователя Изменить тревожный PIN
			Управление корпоративными ключами Журнал событий
	www.muticlet.com		

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 иниицализации (Процедура инициализации описана в главе 2.6).



P Multiclet	Р Multiclet® Кеу_Р1: Иванов И.И. (инженер)														
	Текущий PIN администратора ••••• Новый PIN администратора ••••• Подтверждение нового PIN администратора ••••• ОК Cancel														
•	0	1	2	3	4	5	6	7	8	9	-	=	Bksp		
Tab	q	w	e	r	t	У	u	i	0	р	[]	-/ -	Ir	
Ca	ps	а	s	d	f	g	h	j	k	I	;		Enter		
	🗆 Shift		z	x	c	v	Ь	n	m	,	•		Shift 🗆		

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)

🖓 Key_	Р1 м	енеджер		
Файл	<u>Дей</u> б 20 20 20 20 20 20 20 20 20 20 20 20 20	йствия Справка Шифрование файлов Расшифрование файлов Быстрое криптопреобразование Подключить закрытый раздел Отключить закрытый раздел Управление накопителями		
Врем Верс Режи	2 I	Управление синхронными ключами Хранилище аутентификационных данных		
Стат	yc:	Администрирование	 C 	Управление режимом "только чтение" Обновить прошивку
Стат Имя/	гус: разме	Информация о SD карте подключена ер открытого раздела: SD_pub / 1.76ГБайт	2	Инициализировать устройство Изменить метку Кеу_Р1 Изменить РIN администратора
Имя/	разме	ер закрытого раздела: не подключен	2	Изменить PIN пользователя 🔓 Изменить тревожный PIN
		www.multiclet.com		Управление корпоративными ключами Журнал событий

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.



~ N	P Multiclet® Кеу_Р1: Иванов И.И. (инженер)														
	Логин пользователь 🔻														
	Текущий PIN пользователя														
	Новый PIN пользователя														
	Подтверждение нового PIN пользователя														
	OK Cancel														
	OK Cancel														
	•	0	1	2	3	4	5	6	7	8	9	-	=	Bksp	
	Tab	q	w	e	r	t	У	u	i	•	р	[]	/ Clr	
	Ca	ps	a	s	d	f	g	h	j	k	I	;		Enter	
		🗆 Shift		z	x	c	v	Ь	n	m	,	•		Shift 🗆	

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).



A Multiclet	® Key_	Р1: Ива	нов И.	И. (инж	енер)	-		٩.		_			? ×		
	Логин администратор 🔻														
	Текущий PIN администратора														
	Новый PIN пользователя														
	Подтверждение нового PIN пользователя														
	OK Cancel														
•	0	1	2	3	4	5	6	7	8	9	-	=	Bksp		
Tab	q	w	e	r	t	у	u	i	0	p	[]	/ Clr		
Ca	ips	a	s	d	f	g	h	j	k	-	;		Enter		
	□ Shift		z	x	c	v	b	n	m	,	•		Shift 🗆		

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)

🥜 Key_	Р1 м	енеджер	X			
Файл Стат Метк Врем Верс	<u>Деі</u> 6 2 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3	ствия Справи Шифрование и Расшифрован Быстрое крип Подключить за Отключить за Управление на Управление си	а файлов roпреобразование акрытый раздел срытый раздел икопителями икопителями икоронными ключами			
Режи		Администрир	ование	•	~	Управление режимом "только чтение"
Стат	yc:	Информация	не подключён а о SD карте		C Z	Обновить прошивку Инициализировать устройство
Стат Имя/ Имя/	ус: разм разм	р открытого раз р закрытого раз	подключена дела: SD_pub / 1.76ГБайт дела: не подключен		× 2 2	Изменить метку Кеу_Р1 Изменить PIN администратора Изменить PIN пользователя
			WWW.multiclet.com			Узменить тревожный РЛО 😡 Управление корпоративными ключами Журнал событий

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.



💡 Mult	Multiclet® Кеу_Р1: Иванов И.И. (инженер)														
	РІN пользователя Тревожный РІN Подтверждение тревожного РІN ОК Cancel									C	5				
	•	0	1	2	3	4	5	6	7	8	9	-	=	Bksp	
Та	ab	q	w	e	r	t	У	u	i	0	р	[]		Clr
	Caps	s	a	s	d	f	g	h	j	k	I	;		Enter	
		3 Shift		z	x	c	v	Ь	n	m	,	•		Shift 🗆	

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.

💡 Key_	Р1 м	енедже	p	×			
Файл	Дей	іствия	Справка				
🗗 🚺	-	Шифр	оование файлов				
		Расши	ифрование файлов рое криптопреобразова	ние			
	-	Полкл	лючить закрытый разде	л			
Стат		Отклн	очить закрытый раздел				
Метк	e 🍯	Управ	ление накопителями				
Верс	2	Управ. Управ	ление синхронными кл	ючами			
Режи	-	лрани	плище аутентификацио	нных данных		•	
	_	Адми	нистрирование		•		Управление режимом "только чтение"
Стат	yc:		не подключён			7	Обновить прошивку
		Ин	формация о SD карте		Ż	2	Инициализировать устройство
Стат	yc:		подключ	ена		ļ	Изменить метку Кеу_Р1
Имя/	разме разме	ер откры ер закры	ытого раздела: SD_pub / итого раздела: не подкл	1.76ГБайт	4	6	Изменить PIN администратора
						2	Изменить PIN пользователя Изменить тревожный PIN
			MIN TIC	I FT [®]			эправление корпоративными ключами
					E/	6	Журнал событий
			www.multicle	et.com			

Рис. 45. Изменение метки устройства

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

Key_P1	_manager ? X	Γ
Метка	Иванов И.И. (инженер)	
	OK Cancel	

Рис. 46. Ввод метки устройства

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



~	Multicle	et® Key_	Р1: Ива	нов И.	И. (инж	енер)					-	-	•		2	x
					PI	IN админ	нистрат	ора								
							OK		Cancel							
	•	0	1	2	3	4	5	6	7	8	9	-	=	Bks	sp	
	Tab	q	w	e	r	t	у	u	i	•	p	[]	-	Clr	
		Caps		s	d	f		h	i	k				Enter		
														chift III		
		L) Shift		Z	×	C	V	D	n	m	'	·		Shirt 🗆		

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.



Использование устройства Кеу Р1 3

Управление накопителями 3.1

Создание закрытого раздела на USB накопителе 3.1.1

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

🥐 Key_	Р1 ме	неджер		— X	
Файл	Дей	ствия Спра	авка		
	6	Шифровани	ие файлов		
	6	Расшифров	вание файлов		
	\mathbf{x}	Быстрое кр	иптопреобразова	ание	
	-	Подключит	гь закрытый разде	ел	
Стат		Отключить	закрытый раздел	1	
Метн	<i></i>	Управление	е накопителями	N	
Врем	2	Управление	е синхронными кл	лючами	
Bepo	•	Хранилище	е аутентификацио	онных данных	
PC/W	1	Алминистр	ирование		•
	_	, Munucib	npossine		
Стат	гус:		не подключён		
		Информа	ция о SD карте		
Стат	гус:		подключ	ена	
Имя/	/разме	р открытого р	раздела: SD_pub/	1.76ГБайт	
Имя	разме	р закрытого р	раздела: не подкл	ючен	
			WWW.multicl	ELET [®] et.com	

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.

🖓 Управление накопителя	ми ? Х
Накопитель	USB накопитель 💌
Действие	Инициализировать накопитель 🔻
Метка открытого раздела	Open
Размер открытого раздела	5351 M5 🍨
Метка закрытого раздела	Secure
Размер закрытого раздела	2048 МБ 🚔
ОК	Cancel

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

Рис. 49. Инициализация накопителя

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

~ N	Iulticlet	t® Key_	Р1: Ива	нов И.І	И. (инж	енер)									?	x
	РІN пользователя															
	OK Cancel															
	Ò	0	1	2	3	4	5	6	7	8	9	-	=	Bk	sp	
	Tab	q	w	e	r	t	У	u	i	•	P	[]	/	Clr	
	Ca	aps	a	s	d	f	g	h	j	k	-	;		Enter		
		🗆 Shift		z	x	c	v	Ь	n	m	,	•		Shift 🗆		

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».



Key_P1_manager	? x
Выберите накопители, под к Key_P1 "Иванов И.И. (ин закрытые разделы которы необходимо подключить	цключённые женер)*, ых
Secure	
SD_priv	
ОК	Cancel

Рис. 51. Подключения закрытого раздела

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

~ N	Multiclet® Кеу_Р1: Иванов И.И. (инженер)														
	PIN пользователя														
							ОК		Cancel						
														2	
	` 0 1 2 3 4 5 6 7 8 9 - = Bksp									,					
	Tab	q	w	e	r	t	У	u	i	0	p	[]		Clr
	Ca	ps	a	s	d	f	g	h	j	k	-	;		Enter	

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).



Кеу_Р1 менеджер	×
Файл Действия Справка	
🗗 🛅 🖂 🗂 🛋	i 名 🗊 👘
Иванов И.И	1. (инженер) 🔻 🔒
Информация о Ке	y_P1
Статус:	готово
Метка устройства:	Иванов И.И. (инженер)
Время последнего отключения:	не определено
Версия прошивки:	134
Режим "только чтение"	
Информация о USB нан	копителе
Статус:	подключен
Имя/размер открытого раздела:	Open / 5.22ГБайт
Имя/размер закрытого раздела:	Secure / 2.00ГБайт
Информация о SD н	карте
Статус:	подключена
Имя/размер открытого раздела:	SD_pub / 1.76ГБайт
Имя/размер закрытого раздела:	не подключен
MUL	TICLET ®
www	.multiclet.com

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).

🥜 Кеу_Р1 ме	енеджер									
Файл Дей	ствия Справка									
🕂 🔓	Шифрование файлов									
6	🛅 Расшифрование файлов									
2	Быстрое криптопреобразование									
	Подключить закрытый раздел									
Стат 👝	Отключить закрытый раздел									
Врем	Управление накопителями									
Bend	Управление синхронными ключами									
Режи	Хранилище аутентификационных данных									
	Администрирование	•								
Статус:	подключен									
Имя/разме	р открытого раздела: Open / 5.22ГБайт									
Имя/разме	р закрытого раздела: Secure / 2.00ГБайт									
	Информация о SD карте	Ŀ								
Статус:	подключена									
Имя/разме	р открытого раздела: SD_pub / 1.76ГБайт									
Имя/разме	р закрытого раздела: не подключен									
	WULTICLET® www.multiclet.com									

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 раз**дела 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 «ОК».

🥐 Управление накопителя	ми 8 х
Накопитель	SD карта 🗸
Действие	Инициализировать накопитель 🔻
Метка открытого раздела	SD_pub
Размер открытого раздела	5532 МБ 🚔
Метка закрытого раздела	SD_priv
Размер закрытого раздела	2048 M5 🚔
ок	Cancel

Рис. 55. Инициализация накопителя

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

₽ №	lulticlet	® Key_	Р1: Ива	нов И.	И. (инж	енер)					_			2	? <mark>x</mark>
	РІN пользователя														
	OK Cancel														
		0	1	2	3	4	5	6	7	8	9	-	=	Bksp	`
	Tab	q	w	e	r	t	У	u	i	0	р	[]	1	Clr
	Ca	ps	a	s	d	f	g	h	j	k	I	;		Enter	
		🗆 Shift		z	x	c	v	Ь	n	m	,	•		Shift 🗆	

Рис. 56. Ввод PIN пользователя

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



🖓 Key_P1_manager 🛛 🔋 🗾 🗙
Выберите накопители, подключённые к Key_P1 "Иванов И.И. (инженер)",
закрытые разделы которых необходимо подключить
✓ Secure уже подключён
SD_priv
OK Cancel

Рис. 57. Подключение закрытого раздела

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

~ N	lulticlet	® Key_	Р1: Ива	нов И.	И. (инж	енер)					_	_	-	?	x
						PIN no.	ъзоват	еля 🔸	••						
	OK Cancel														
· 0 1 2 3 4 5 6 7 8 9 - =							=	Bksp							
	Tab	q	w	e	r	t	У	u	i	0	p	[]	/ Clr	
	Caps a			s	d	f	g	h	j	k	I	;	Enter		
	□ Shift				x	c	v	ь	n	m	,	•		Shift 🗆	

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).



	×
Файл Действия Справка	
🗗 🛅 🖂 🖾 🏹	r 🔑 🗊 🔷 1
Иванов И.І	1. (инженер) 🔻 🔒
Информация о Ке	y_P1
Статус:	ГОТОВО
Метка устройства:	Иванов И.И. (инженер)
Время последнего отключения:	не определено
Версия прошивки:	134
Режим "только чтение"	
Информация о USB на	копителе
Статус:	подключен
Имя/размер открытого раздела:	Open / 5.22ГБайт
Имя/размер закрытого раздела:	Secure / 2.00ГБайт
Информация о SD	карте
Статус:	подключена
Имя/размер открытого раздела:	SD_pub / 5.40ГБайт
Имя/размер закрытого раздела:	SD_priv / 2.00ГБайт
MDL	TICLET [®]

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).

Файл [Действия Справка									
	🖬 Шифрование файлов									
	🛅 Расшифрование файлов									
i	🗾 Быстрое криптопреобразование									
	🗂 Подключить закрытый раздел 💦									
Стат	🗂 Отключить закрытый раздел									
Метк	Управление накопителями									
Врем	Управление синхронными ключами									
Верс Режи	Хранилище аутентификационных данных									
	Администрирование									
Стату	с: подключен									
Имя/ра	азмер открытого раздела: Open / 5.22ГБайт									
Имя/ра	азмер закрытого раздела: не подключен									
	Информация о SD карте									
Стату	с: подключена									
Имя/ра	азмер открытого раздела: SD_pub / 5.40ГБайт									
Имя/ра	азмер закрытого раздела: не подключен									
	WWW.multiclet.com									

Рис. 60. Подключение закрытого раздела

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



Key_P1_manager	2	x						
Выберите накопители, под к Key_P1 "Иванов И.И. (ин	цключ женер	іённые))",						
закрытые разделы которых необходимо подключить								
Secure	Secure							
SD_priv								
ОК	Can	cel						

Рис. 61. Выбор накопителя

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

~ N	P Multiclet® Key_P1: Изанов И.И. (инженер)															
	РІN пользователя															
	OK Cancel															
	•	0	1	2	3	4	5	6	7	8	9	-	=	Bks	p	
	Tab	q	w	e	r	t	У	u	i	0	р	[]	1	Clr	
	Caps a s d f g h j k l ; Enter															
	□ Shift z x c v b n m , . Shift □															

Рис. 62. Ввод PIN пользователя

Главное меню приложения примет вид как на рис. 63



Кеу_Р1 менеджер	X
Файл Действия Справка	
🗗 🛅 🖂 🚐 🐗	1 🔑 🗊 👘
Иванов И.И	1. (инженер) 🔻 🔒
Информация о Ке	y_P1
Статус:	готово
Метка устройства:	Иванов И.И. (инженер)
Время последнего отключения:	не определено
Версия прошивки:	134
Режим "только чтение"	
Информация о USB на	копителе
Статус:	подключен
Имя/размер открытого раздела:	Open / 5.22ГБайт
Имя/размер закрытого раздела:	Secure / 2.00ГБайт
Информация о SD и	карте
Статус:	подключена
Имя/размер открытого раздела:	SD_pub / 5.40ГБайт
Имя/размер закрытого раздела:	не подключен
MDL	TICLET®
www	.multiclet.com

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).

Файл Дей	іствия Справка									
🕂 🗗 🗗	Шифрование файлов									
6	Расшифрование файлов									
X	🛃 Быстрое криптопреобразование									
2	Подключить закрытый раздел									
Стат 👝	Отключить закрытый раздел									
Метн	Управление накопителями									
Врем 🔎	Управление синхронными ключами									
Верс Режи	Хранилище аутентификационных данных									
	Администрирование									
Статус:	подключен									
Имя/разме	ер открытого раздела: Open / 5.22ГБайт									
Имя/разме	ер закрытого раздела: не подключен									
	Информация о SD карте									
Статус:	подключена									
Имя/разме	ер открытого раздела: SD_pub / 5.40ГБайт									
Имя/разме	р закрытого раздела: не подключен									
	WWW.multiclet.com									

Рис. 64. Подключение закрытого раздела

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





Рис. 65. Выбор накопителя

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

~ N	Р Multiclet® Key_P1: Иванов И.И. (инженер)															
	PIN пользователя															
	OK Cancel															
	•	0	1	2	3 4 5 6 7 8 9						-	=	Bksp			
	Tab	q	w	e	r	t	У	u	i	0	р	[]	1	Clr	
	Caps a s d f g h j k l ; Enter															
	□ Shift z x c v b n m , . Shift □															

Рис. 66. Ввод PIN пользователя

Главное меню приложения примет вид как на рис. 67



Кеу_Р1 менеджер	×
Файл Действия Справка	
🗗 🛅 🖂 🗂 🛋	t 🔑 🗊 👘
Иванов И.	И. (инженер) 🔻 🔒
Информация о Ке	ey_P1
Статус:	готово
Метка устройства:	Иванов И.И. (инженер)
Время последнего отключения:	не определено
Версия прошивки:	134
Режим "только чтение"	
Информация о USB на	копителе
Статус:	подключен
Имя/размер открытого раздела:	Open / 5.22ГБайт
Имя/размер закрытого раздела:	Secure / 2.00ГБайт
Информация о SD	карте
Статус:	подключена
Имя/размер открытого раздела:	SD_pub / 5.40ГБайт
Имя/размер закрытого раздела:	SD_priv / 2.00ГБайт
	TICLET [®]

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).

🖓 Key_P	1 менеджер
Файл [Действия Справка
-	🔂 Шифрование файлов
	🕤 Расшифрование файлов
1	🙍 Быстрое криптопреобразование
	🗂 Подключить закрытый раздел
Ciai	🗂 Отключить закрытый раздел
Метк Врем	ча Управление накопителями
Bepc	Управление синхронными ключами
Режи	Хранилище аутентификационных данных
	Администрирование
Стату	с: подключен
Имя/ра	азмер открытого раздела: Open / 5.22ГБайт
Имя/ра	азмер закрытого раздела: Secure / 2.00ГБайт
	Информация о SD карте
Стату	с: подключена
Имя/ра	азмер открытого раздела: SD_pub / 5.40ГБайт
Имя/ра	азмер закрытого раздела: SD_priv / 2.00ГБайт
	WWW.multiclet.com

Рис. 68. Отключение закрытого раздела

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



Key_P1_manager	?	x
Выберите накопители, по, к Key_P1 "Иванов И.И. (ин	аключ женер	іённые))",
закрытые разделы которы необходимо отключить	ыX	
Secure		
SD_priv		
ок	Can	cel

Рис. 69. Выбор накопителя

Главное меню приложения примет вид как на рис. 70

Кеу_Р1 менеджер	×										
Файл Действия Справка											
🗗 🛅 🖂 篙 🦱	t 🔑 🗊 👘										
Иванов И.І	И. (инженер) 🔻 🛅										
Информация о Кеу_Р1											
Статус:	готово										
Метка устройства:	Иванов И.И. (инженер)										
Время последнего отключения:	не определено										
Версия прошивки:	134										
Режим "только чтение"											
Информация о USB на	копителе										
Статус:	подключен										
Имя/размер открытого раздела:	Open / 5.22ГБайт										
Имя/размер закрытого раздела:	не подключен 45										
Информация о SD	карте										
Статус:	подключена										
Имя/размер открытого раздела:	SD_pub / 5.40ГБайт										
Имя/размер закрытого раздела:	не подключен										
MOL	TICLET®										

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 OC «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).

Key_P1	менеджер									
Файл Д	ействия Справка									
🗗 🗗	Шифрование файлов									
	Расшифрование файлов									
	Быстрое криптопреобразование									
2	Подключить закрытый раздел									
Стат 🥭	🗄 Отключить закрытый раздел									
Метк	👔 Управление накопителями									
Врем	Управление синхронными ключами									
Режи	📕 Хранилище аутентификационных данных									
	Администрирование									
Статус	: не подключён									
	Информация о SD карте									
Статус	: подключена									
Имя/раз	змер открытого раздела: SD_pub / 1.76ГБайт									
Имя/раз	Имя/размер закрытого раздела: не подключен									
	WWW.multiclet.com									

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 «ОК».(рис. 73).

Р Управление накопителями							
Накопитель	USB накопитель 🔻						
Действие	Инициализировать накопитель 🔻						
Метка открытого раздела	publ						
Размер открытого раздела	7451 МБ 🊔						
Метка закрытого раздела	priv						
Размер закрытого раздела	0 МБ 🚔						
ок	Отменить						

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).



₽		Ke	у_Р1 менед	жер	x			
Файл	Дей	ствия	Справка					
<u> </u>	6 6 8	Шифр Расши Быстр	ование файлог 1фрование фай ое криптопрес	в йлов образование				
Стат	1	Подкл Отклю	ючить закрыти очить закрыты	ый раздел й раздел				
мети	e 🍕	Управ.	ление накопит	елями				
Врем	<mark>,</mark>	Управ	ление синхрон	ными ключами				
Режи	•	Хранилище аутентификационных данных						
		Админ	нистрирование	2		۲		
Стат	yc:		не под	ключён				
		Инс	формация о SD к	карте				
Стат Имя/ Имя/	гус: разме разме	р откры р закры	того раздела: того раздела:	подключена SD_pub / 5.40ГБай не подключен	іт			
			MULI	TICLET	®			

Рис. 74. Управление синхронными ключами

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

₽	Multiclet® Кеу_Р1: Иванов И.И. (инженер) ?													
					PIN no.	пьзоват	еля 💽	•••]			
						OK		Cancel		2				
										v 				
	0	1	2	3	4	5	6	7	8	9	-	=	= Bksp	
Tab	q	w	e	r	t	У	u	i	o	р	[1	1	Clr
Caps a		s	d	f	g	h	j	k	1	;		Enter		
□ Shift		z	x	с	v	ь	n	m	,			Shift 🗆		
			-		-					'				

Рис. 75. Ввод PIN пользователя


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

<i>₹</i> S	ynchro key manager		×
	Label	Add	
5		Delete	
		Delete all	

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».

)					9	Synchi	o key	adding	g					? ×
				Algorit	hm		Fin	st		•				
	Ко	Командировка												
Key sentence ••••														
	[12		Key se	ntence o	onfirma	tion 🔸	••						
						OK		Cancel						
•	0	1	2	3	4	5	6	7	8	9	-	=	Bk	sp
Tab	q	w	e	r	t	у	u	i	o	р	[]	1	Clr
Ca	ips	а	s	d	f	g	h	j	k	T	;		Enter	
	□ Shift		z	x	с	v	b	n	m	,			Shift 🗆	

Рис. 77. Добавление синхронных ключей

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

www.multiclet.com



					PIN no	льзоват	еля 💽	•••]			
						OK		Cancel	[à				
•	0	1	2	3	4	5	6	7	8	9	-	=	Bł	sp
Tab	q	w	e	r	t	У	u	i	o	р	[]	1	d
Ca	ps	a	s	d	f	g	h	j	k	- 1	;		Enter	
	□ Shift		z	x	с	v	ь	n	m	,			Shift 🗆	

Рис. 78. Ввод PIN пользователя

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

Synchro key manager	×
Label	Add
Командировка	Delete
2	Delete all

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).

~		Key	_Р1 менед	жер	×			
Файл	Действ	ия	Справка					
Стат	 ⊡ □ □ □ □ □ □ □ 	Іифро асшис ыстро одклн тключ	вание файлог фрование фай е криптопрес очить закрыты иить закрыты	в йлов образование ый раздел й раздел				
Метк Врем Верс Режи	✓ Yr ✓ Yr ✓ Yr ✓ Xi	травл травл ранил дмині	ение накопит ение синхрон ище аутентис истрирование	елями ными ключами фикационных да а	нных	•		
Стат	yc:	Инф	не под ормация о SD к	ключён арте				
Стат Имя/ Имя/	Информация о SD карте Статус: подключена Имя/размер открытого раздела: SD_pub / 5.40ГБайт Имя/размер закрытого раздела: не подключен							

Рис. 80. Управление синхронными ключами

Появится окно ввода PIN пользователя. После ввода PIN необходимо нажать «ОК» (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».

8			١	Multic	let® K	ey_P1	: Иван	юв И.	И. (ин	женер)			? ×
	PIN пользователя													
	OK Cancel													
•	` 0 1 2 3 4 5 6 7 8 9 - = Bksp													
Tab	q	w	e	r	t	у	u	i	0	р	ſ]	1	Clr
	Caps	а	s	d	f	g	h	j	k	T	;		Enter	
	□ Shift		z	x	с	v	ь	n	m	,			Shift 🗆	

Рис. 82. Удаление синхронных ключей

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



Рис. 83. Удаление ключей



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

			N	Aulticl	et® K	ey_P1	: Иван	юв И.І	И . (ин	женер))			?	×
РIN пользователя ••••															
						OK		Cancel			\square				
•	0	1	2	3	4	5	6	7	8	9	-	=	Bk	sp	
Tab	q	w	e	r	t	У	u	i	o	р	[]	1	Clr	
Ca	ips	a	s	d	f	g	h	j	k	-T	;		Enter		
	🗆 Shift		z	x	с	v	ь	n	m	,			Shift 🗆		

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).



~		Ke	у_Р1 менед	жер		×				
Файл	Дей	ствия	Справка							
	-	Шифр	ование файло	в	2					
	6	Расш	ифрование фа	йлов	20					
	🗵 Быстрое криптопреобразование									
	💿 Подключить закрытый раздел									
Стат		Отклн	очить закрыть	ій раздел						
Метн	a a	Управ	ление накопи	телями						
Врем	ې	Управ	ление синхро	нными кл	тючами					
Верс Режи	•	Храни	лище аутенти	фикацио	нных дан	ных				
	Администрирование									
Стат	гус:		не по,	дключён						
		Ин	формация о SD	карте						
Стат	ryc:			подключ	ена					
Имя/	разме	р откры	того раздела:	SD_pub /	5.40ГБай	т				
Имя/	разме	р закрь	пого раздела:	не подкл	ючен					
			MDL	TIC .multicle	LET et.com	®				

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).



дополнительные опции	
Путь	Добавить директорию
	Добавить файлы
	Удалить
	l≽
иректория назначения	
обавить расширение к каждому файлу	crypt

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



🔗 Выбе	рите одну или более директорий для зашифро	вывания	
🐑 🌛 👻 🕆 💾 🕨 Ka	омпьютер → Windows8_OS (C:) → v С Пол	иск: Windows8_OS (C:) р	
Упорядочить 🔻 Созд	ать папку	:= 🗸 🔞	
Видео ^	Имя Дата изи	иенения Тип	^
Документы	퉬 input 📐 13.10.20	14 22:13 Папка с файламі	
изооражения	input_files 13.10.20	14 22:14 Папка с файламі	
🚽 і і і і і і і і і і і і і і і і і і і	Key_P1_software 12.10.20	14 0:04 Папка с файламі	
3	Miranda Me 03.07.20	14 14:17 Папка с файламі	
🤜 домашняя группа	MSOCache 14.06.20	14 11:00 Папка с файламі	
· Kauna ana	boutput 13.10.20	14 22:14 Папка с файламі	
Windows? OS (C	PerfLogs 26.07.20	12 13:33 Папка с файламі	
Windowso_03 (C	Program Files 11.10.20	14 21:43 Папка с файламі	
	Program Files (x86) 11.10.20	14 21:28 Папка с файламі	
Одисковод БО-КС	ProgramData 11.10.20	14 20:18 Папка с файламі	
Сьемный диск (🐌 Users 09.06.20	14 22:43 Папка с файламі	
	Windows 17.06.20	14 23:10 Папка с файламі ч	v
- ×	<	>	
Папк	a: input		
	Выб	ор папки Отмена	

Рис. 87. Выбор директории

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

🕜 Выб	ерите один или более файлов для за	шифровывания	×
🔄 🌛 🝷 🕇 📙 « Win	ndows8_OS (C:) > input_files ~ ~	🖒 Поиск: input_fi	les ,p
Упорядочить 🔻 Созда	ть папку		iii 🕶 🔲 🔞
Видео ^	Имя	Дата изменения	Тип
Документы	😼 functions	03.10.2014 19:04	TeX Document
Изображения	😼 install	03.10.2014 11:15	TeX Document
 Домашняя группа Компьютер Windows8_OS (С LENOVO (D:) Дисковод BD-RC Съемный диск (Alexander (alexar 	¢		
l/ug d	aŭ nat "install" "functione"		
<u>ν</u> ιω, φ		<u>О</u> ткрыть	Отмена

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.



₽	Шифрова	ание файлов	? ×
	Исходные директории и файлы для зац	иифровывания	
	дополнительные опции		
	Путь	Добавить директорию	
	C:/input		Добавить файлы
	C:/input_files/functions.tex		Удалить
	C:/input_files/install.tex		
			\searrow
д	иректория назначения		
Д	обавить расширение к каждому файлу	crypt	
K	риптографический ключ	случайный ключ	•
			OK Cancel

Рис. 89. Окно для шифрования

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

۹ ⁹	ите директорию		×
🔄 🄄 🕆 🕇 👗 🕨 K	DS (C:)	🖒 Поиск: Window	vs8_OS (C:) 🔎
Упорядочить 🔻 Соз,			:== 👻 🔞
😸 Видео \land	^	Дата изменения	Тип ^
📑 Документы		13.10.2014 22:13	Папка с файламі
📔 Изображения		13.10.2014 22:14	Папка с файламі
Музыка		12.10.2014 0:04	Папка с файламі
		03.07.2014 14:17	Папка с файламі
🤫 Домашняя группа		14.06.2014 11:00	Папка с файламі
		13.10.2014 22:14	Папка с файламі
мотьютер		26.07.2012 13:33	Папка с файламі
Windows8_US (C		11.10.2014 21:43	Папка с файламі
		11.10.2014 21:28	Папка с файламі
О ДИСКОВОД ВО-КС		11.10.2014 20:18	Папка с файламі
Съемный диск (09.06.2014 22:43	Папка с файламі
Alexander (alexar		17.06.2014 23:10	Папка с файламі 🗸
~			>
Паля			
		Выбрр папки	Отмена

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 "ОК".

	ание файлов	? ×
Исходные директории и файлы для за	шифровывания	
дополнительные опции		
Путь		Добавить директорию
C:/input		Добавить файлы
C:/input_files/functions.tex		Удалить
C:/input_files/install.tex		
Директория назначения	C:/output	
Добавить расширение к каждому файлу	crypt	
Криптографический ключ	случайный ключ	×
		OK Cancel

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.



Ρ	Шифрование файлов 🔹 ?								
Исходные директории и файл	ы для зашифровыван	ния							
✓ дополнительные опции	Шаблон файла	Рекурсивно	Лобавить директорию						
C:/input	*		Добавить файлы						
C:/input_files/functions.tex			Удалить						
C:/input_files/install.tex									
			5						
Директория назначения	C:/output								
Добавить расширение к каждою	чуфайлу crypt								
Криптографический ключ	случайный	ключ	•						
			OK Cancel						

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).

Ŷ		Ke	у_Р1 менед	жер	×				
Файл	Дей	ствия	Справка						
	6	Шифр	ование файло	в					
_	6	Расш	ифрование фа	йлов					
		Быстр	ое криптопре	образование					
	5	Подкл	іючить закрыт	ъй раздел					
Стат		Отклн	очить закрыты	ій раздел					
Метн	e 🍯	Управ	ление накопит	гелями					
Врем	<mark>,</mark>	Управ	ление синхрон	ными ключам	и				
Режи		Хранилище аутентификационных данных							
		Адми	нистрировани	e		+			
Стат	yc:		не под	цключён					
		Ин	формация о SD і	карте					
Стат	yc:			подключена					
Имя/	Имя/размер открытого раздела: SD_pub / 5.40ГБайт Имя/размер закрытого раздела: не подключен								
Имя/									
			MDL.	TICLE	T n				

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).



Pac	шифрование ф	айлов ? ×
Исходные директории и ф	айлы для расшифро и	вывания
Пу	ть	Добавить директорию
		Добавить файлы
		Удалить
	2	
Директория назначения		
Криптографический ключ	случайный ключ	•
 Удалить последнее рась 	ширение в именах во	ех исходных файлов
		OK Cancel

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.



🖓 Расшифрование фа	йлов ? 🗙
Исходные директории и файлы для расшифров	ывания
дополнительные опции	
Путь	Добавить директорию
C:/output	Добавить файлы
	Удалить
	6
Директория назначения C:/input	
Криптографический ключ случайный ключ	•
Удалить последнее расширение в именах все:	х исходных файлов
	OK Cancel

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.



🕜 Pa	сшифрование фай	лов ? ×
Исходные директории и	файлы для расшифровые	зания
дополнительные опц	ии	
Пу	/ть	Добавить директорию
C:/output		Д обавить файлы
		Удалить
Директория назначения	C:/input	
Криптографический ключ	синхронный ключ	•
Синхронный ключ	Командировка	• Управление
 Удалить последнее рас 	ширение в именах всех и	ісходных файлов
		OK Cancel

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.



<i></i> ₹	Расшифрование файлов ? 🗙									
Исходные	директории и о	файлы , ии	для расшифров	выва	ния					
Путь	Шаблон фа	 ійла	Рекурсивно	,	Добавить	директор	рию			
C:/outpu	ıt *		✓		Добави	іть файль	bl			
					Уд	алить				
						3				
Директория	назначения	C:/inpu	ut							
Криптограф	ический ключ	синхронный ключ 🔻								
Синхронныі	ключ	Командировка 👻 Управление								
🖌 Удалити	последнее рас	сширени	ие в именах все	ехис	ходных фай	ілов				
					ОК	Can	cel			

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).

Кеу_Р1 ме	неджер
Файл Дей	ствия Справка
🕂 🔂	Шифрование файлов
6	Расшифрование файлов
	Быстрое криптопреобразование
	ис Подключить закрытый раздел
Иетн	Отключить закрытый раздел
Врем 🐗	Управление накопителями
Bepc 🔑	Управление синхронными ключами
Режи 🥑	Хранилище аутентификационных данных
	Администрирование
Статус:	не подключён
	Информация о SD карте
Статус:	подключена
Имя/размер	р открытого раздела: SD_pub / 5.40ГБайт
Имя/размер	р закрытого раздела: не подключен
	WWW.multiclet.com

Рис. 98. Выбор элемента

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



🔑 Быстрое криптографическое преобразовани 🗾 🏵
e s de ciex de C
Исходные данные Результат
Криптографический ключ

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.



Multiclet	® Key_	P1: Key	_P1		Ξ.				-		+-			?
					PIN no.	пьзоват	еля							
						OK		Cancel						
][
Ì	0	1	2	3	4	5	6	7	8	9	-	=	Bks	p
Tab	q	w	e	r	t	У	u	i	0	P]]		Clr
Ca	ps	a	s	d	f	g	h	j	k	I	;	Enter		
	🗆 Shift		z	x	с	v	Ь	n	m	,	•	Shift 🗆		

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.

🔑 Быстрое криптографическое преобразовани 💌
Исходные данные Результат
a3AxcwAAAgXG0wAAiWtxZ79TlZp5aCGo6jrbOmSYpUxOwx 0zgtl2FWLdsRqR/R3Hr8JqAFB0dCgIGivvHLxjP7q/Hi/jVL/ MEwQtTykMEgYIwZRRsQCviLHYhDtOZNnNa474FAuwWBmX q7fLOFnYHt/RoKfC+c0XV2UEHdAsHA==

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).

	Кеу_Р1 мене,	джер 🛛 🗙			
Файл Деі	ствия Справка				
Стат Врем Верс	Шифрование файл Расшифрование ф Быстрое криптопр Подключить закры Отключить закрыт Управление накопи Управление синхро	ов айлов еобразование тый раздел ый раздел ителями энными ключами			
Режи	Хранилище аутент Администрирован	ификационных данных ие	•		Управление режимом "только чтение"
Статус: Статус: Имя/разми Имя/разми	не по Информация о SD пр открытого раздела пр закрытого раздела	одключён окарте подключена : SD_pub / 5.40ГБайт : не подключен		C 2 2 2 2	Обновить прошивку Инициализировать устройство Изменить метку Key_P1 Изменить PIN администратора Изменить PIN пользователя
		TICLET®		3. 121 121	Изменить тревожный PIN Управление корпоративными ключами Журнал событий

Рис. 104. Управление корпоративными ключами

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

			N	Multic	et® K	ey_P1	: Иван	юв И.	И <mark>. (и</mark> н:	женер))			?
				P	[N адми	нистрат	ора]			
						OK		Cancel						
		1				1	1		G	1		1	1	
•	0	1	2	3	4	5	6	7	8	9	-	=	B	ksp
Tab	q	w	e	r	t	у	u	i	o	р	[]	1	Clr
c	aps	а	s	d	f	g	h	j	k	1	;		Enter	





P	Управление корпо	рат	тивными ключами	×
	Внешняя база данных корпоративных ключи		База данных Кеу_Р1 корпоративных ключей	
	<i>b</i> ³			
			₽ ₽	

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):







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);

🕜 Добавление группы ко ? 🛛 🗙						
Имя	Инженеры					
Количество ключей	3					
ок	Cancel					

Рис. 108. Добавление группы корпоративных ключей

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

Ŷ	Управление корпо	рат	гивными ключами
E	Знешняя база данных корпоративных ключі ▷ 🕂 Инженеры		База данных Кеу_Р1 корпоративных ключей
	\$		
[s s s + Z - Þ		₽ ♥

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

🕹 Pe	дактиров	3a ?	×
Имя	Инженеры		
	OK	Cancel	

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):

Управление корпоративными ключами	×
Внешняя база данных корпоративных ключи База данных Кеу_Р1 корпоративных ключе	i
6	

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);



🖑 Добавление г	руппы ко ? 🛛 🗙
Имя Количество ключей	Маркетинг
ОК	Cancel

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».

			N	Multic	et® K	ey_P1	: Иван	юв И.І	И <mark>. (и</mark> н	женер))			?	×
				PI	IN адми	нистрат	opa 🔸]				
OK Cancel															
											6				
•	0	1	2	3	4	5	6	7	8	9	-	=	Bk	sp	
Tab	q	w	e	r	t	у	u	i	o	р	[]	1	Clr	
Ca	ps	a	s	d	f	g	h	j	k	1	;		Enter		
	□ Shift		z	x	с	v	ь	n	m	,			Shift 🗆		
															_

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".



P	Управление корпо	ративными ключами
	Внешняя база данных корпоративных ключі	База данных Кеу_Р1 корпоративных ключей Маркетинг
L	R R R + R - P	+ •

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

🔑 Добавление группы ко 📍 🗙						
Имя Бухгалтерия						
Количество ключей 3						
ОК Отменить						

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



Управление корпоративными ключами							
Внешняя база данных корпоративных ключ	База данных Кеу_Р1 корпоративных ключей						
Бухгалтерия							

Рис. 117. Создание группы корпоративных ключей

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

Р Добавление группы ко ? ×	
Имя	Программисты
Количество ключей	2
ОК Отменить	

Рис. 118. Создание группы корпоративных ключей

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







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 Кеу Р1 либо же данный файл можно зашифровать с помощью устройства Кеу Р1). 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

Управление корпор	ативными ключами
Внешняя база данных корпоративных ключ	База данных Кеу_Р1 корпоративных ключей ▷
Добавить г	руппу корпоративных ключей в базу данных Кеу_Р

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







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


<i>Р</i> Зашифрован	ие файлов 🛛 ? 🗙
Исходные директории и файлы для заш	ифрования
дополнительные опции	
Путь	Добавить директорию
C:/Совещание 03.10.pdf	Добавить файлы
	Удалить
директория пазначения	
Добавить расширение к каждому файлу	crypt
Криптографический ключ	корпоративный ключ 🔻
Группа корпоративных ключей	Отдел продаж
	Бухгалтерия
	Отдел продаж
	Служба безопасности

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

🔑 Фоновые операции с устройс 🗧	
Key_P1	+ +
Зашифрование файлов корпоративным кли	рчом 💥
С:/Совещание 03.10.pdf	2
	100%
	100%
Завершено успешно	

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



<i>Р</i> Расши	фрование файлов	; ?	×
Исходные директории и файль	а для расшифрования		
дополнительные опции			
Путь	A	обавить директо	орию
С:/Совещание 03.10.pdf.cry	pt	Добавить файл	ы
		Удалить	
Лиректория назначения	C:/		
Криптографический ключ	корпоративный ключ		-
Группа корпоративных ключей	Отдел продаж		•
 Удалить последнее расшире 	ние в именах всех исхо,	дных файлов	
	67	Отме	нить

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)

			N	Aultic	et® K	ey_P1	: Иван	юв И.	И <mark>. (и</mark> н:	женер))			?
				P!	IN админ	нистрат	opa 📘]			
						OK		Cancel						
							1		B			1		
•	0	1	2	3	4	5	6	7	8	9	-	=	B	sp
Tab	q	w	e	r	t	У	u	i	o	р	[]	1	Clr
Ca	ps	а	s	d	f	g	h	j	k	T	;		Enter	
	🗆 Shift		z	x	с	v	ь	n	m	,			Shift 🗆	

Рис. 138. Ввод PIN кода администратора



🕜 Кеу_Р1 менед:	жер 🛛 🗙
Файл Действия Справка	
🗗 🔂 🖂 🖾 🗖	a 🔓 🧊 👘
Иванов И.И. (инженер) 🔻 🚹
Информация о Кез	y_P1
Статус:	готово
Метка устройства:	Иванов И.И. (инженер)
Время последнего отключения	: не определено
Версия прошивки:	134
Режыт "только чтение"	~
Информация о USB нак	копителе
Статус: не под	(ключён
Информация о SD н	карте
Статус: не под	ключена
WWW.m	Ulticlet.com

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



🔑 Журнал событи	й 🗖 🗖 🗖
C	
Key_P1 "Key_P1"	
Дата 🔻	Событие
31.10.2014 18:08:46	Устройство Кеу_Р1 отключено
31.10.2014 17:55:40	Устройство Кеу_Р1 подключено
31.10.2014 17:55:19	Устройство Кеу_Р1 отключено
02.11.2014 21:15:00	Устройство Кеу_P1 подключено
02.11.2014 21:14:49	Устройство Кеу_Р1 отключено
02.11.2014 21:12:41	Устройство Кеу_P1 подключено

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).

			Ν	/lulticl	et® K	ey_P1	: Иван	юв И.І	И. (ин:	женер))			?	×
					PIN no	льзоват ОК	еля	Cancel				C	જે		
•	0	1	2	3	4	5	6	7	8	9	-	=	Bk	sp	
Tab	q	w	e	r	t	у	u	i	o	p	[]	1	Clr	
Ca	aps	a	s	d	f	g	h	j	k	I	;		Enter		
	🗆 Shift		z	x	с	v	ь	n	m	,	•		Shift 🗆		
												·			_

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.

Хранилище ау	тентификационных данных	×
Группы	Метка Логин Пароль Сайт	Добавить
Общая		Редактировать
		Удалить
		Удалить все
3		
Добавить Редактировать Удалить		

Рис. 144. Окно хранилища

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



Группы			Метка	Логин	Пароль	Сайт	Добавить
Общая		2 Kov I	D1 manac	nor ⁽	? ×		Редактировать
			- I_manag	Jei			Удалить
		Метка груп	пы Почта				Удалить все
	ß	[OK	C	ancel		

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».



				Группа	a		06	щая		•				
				Описа	ние		Поч	нта						
				Сайт			mai	l.ru						
				Логин			use	er						
				Парол	ь		••	•••••						
			I	Подтв	ержден	ие паро.	ля 🔸	••••						
						01/								
						UK		Cancel						
	0	1	2	3	4	5	6	7	8	9	-	=	B	сsр
۰ Tab	0 q	1 w	2 e	3 r	4 t	5 y	6 u	7 i	8	9 p	-	=	BI	csp Clr
、 Tab Ca	0 q ps	1 w a	2 e s	3 r d	4 t	5 У д	6 u h	7 i j	8 o k	9 p I	- [;]	Bl / Enter	csp Clr

Рис. 147. Окно добавления аутентификационных данных

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

					PIN no.	льзоват	еля]			
						OK		Cancel						
•	0	1	2	3	4	5	6	7	8	9	-	=	Bk	sp
Tab	q	w	e	r	t	у	u	i	o	р	[]	1	Clr
Ca	aps	a	s	d	f	g	h	j	k	I	;		Enter	
	□ Shift		z	×	c	v	ь	n	m	,			Shift 🗆	

Рис. 148. Ввод PIN пользователя

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



руппы		Метка	Логин	Пароль	Сайт	Добавить
Общая Почта		Почта	user	*****	mail.ru	Редактировать
						Удалить
						Удалить все

Рис. 149. Окно хранилища

Для того, чтобы произвести копирование данных с целью переноса их в окно авторизации информационного ресурса, сначала следует произвести копирование интернетадреса 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.

Группы	Метка	Логин	Пароль	Сайт	Добавить
Общая	Почта	user	*****	mail.ru	Редактировать
					Удалить
		B			Удалить все

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).



C mo	il.ru				
🖂 Почта					
	@mail.ru 👻				
пароль	Войти				
Забыли пароль?	🔲 запомнить				
С sms-уведомлениями					

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».



	iil.ru
🖂 Почта	
user	@mail.ru -
пароль	Войти
Забыли пароль?	🔲 запомнить
Регистраци с sms-уведо	IЯ В ПОЧТЕ млениями

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.



0mc	il.ru
🖂 Почта	
user	@mail.ru 🗸
••••••	Войти
Забыли пароль?	🔲 запомнить
Регистраци с sms-уведо	я в почте млениями

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).

Группы	Метка	Логин	Пароль	Сайт	Добавить
Общая Почта	Почта	user	*****	mail.ru	Редактироваты
				ß	Удалить Удалить все

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».



		Группа Общая 💌												
	Описание Почта													
	Сайт mail.ru													
Логин user														
				Парол	ь		••	•••••						6
				Подтв	ержден	ждение пароля								
						OK		Cancel						
•	0	1	2	3	4	5	6	7	8	9	-	=	Bł	csp
Tab	q	w	e	r	t	У	u	i	o	р	[]	1	Clr
Ca	ps	а	s	d	f	g	h	j	k	1	;		Enter	

Рис. 155. Редактирование аутентификационных данных

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

			Ļ	1обав.	ление	аутен	тифи	кацио	нных,	даннь	IX			?
		Группа Общая 👻												
	Описание Почта													
Сайт mail.ru														
Логин User														
Пароль											2			
Подтверждение пароля											Ū			
						OK		Cancel						
•	0	1	2	3	4	5	6	7	8	9	-	=	Bk	sp
Tab	q	w	e	r	t	у	u	i	o	р	[]	1	Clr
Ca	ps	a	s	d	f	g	h	j	k	I	;		Enter	
							b n m							

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 сvv 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	