Аладдин РД
www.aladdin-rd.ru

JC-Client

Руководство администратора

Версия 1.1

Москва, 2014

Аннотация

Настоящий документ содержит сведения по установке, настройке и работе с ПО JC-Client 6.22. Мы постарались наиболее полно осветить представленную тему и сделать документ удобным для практического применения. Если все же у вас возникли вопросы или пожелания по содержанию, адресуйте их на techwriters@aladdin-rd.ru. Мы будем благодарны за конструктивные замечания и ответим на возникшие вопросы.

По вопросам технической поддержки обращайтесь в ЗАО «Аладдин Р.Д.» по адресу: http://www.aladdin-rd.ru/support/index.php. Таким способом вы всегда сможете отслеживать состояние своей заявки.

Содержание

Введение

JC-Client представляет собой набор утилит, обеспечивающих работу с электронными ключами JaCarta в операционных системах семейства Windows. Таким образом, электронные ключи JaCarta можно использовать для интерактивного входа в систему, ЭЦП, доступа к VPN, а также для работы с большинством приложений, разработанных для использования со смарт-картами и поддерживающих стандарты CAPI, PKCS#11 и Minidriver.

Пользовательский интерфейс JC-Client представлен набором утилит, которые предоставляют администратору инструменты для работы с электронными ключами JaCarta, а также позволяют задавать политики использования устройств пользователями. С помощью утилит в составе ПО JC-Client пользователи могут выполнять базовые операции с электронными ключами JaCarta, такие как смена пароля или просмотр сведений о сертификатах в памяти электронных ключей JaCarta.

Для работы с электронными ключами JaCarta также может использоваться дополнительное ПО IDProtect Admin. IDProtect Admin не входит в стандартную поставку JC-Client, однако его описание и сценарии работы с ним также представлены в настоящем руководстве.

Примечание:

Электронные ключи JaCarta также можно использовать для биометрической аутентификации (аутентификации по отпечатку пальца). Сведения, касающиеся такого использования, представлены в документе *Использование JaCarta для биометрической аутентификации в среде Windows*.

Изменения в новой версии

Текущая версия JC-Client содержит следующие нововведения.

- Реализована поддержка криптографии на основе эллиптических кривых через интерфейс PKCS#11.
- Поддержка Windows 8.1 Update 1/2012.
- Служба смарт-карт на компьютере, на который устанавливается JC-Client, переводится в режим автоматического запуска.

Описание пакетов установки

Дистрибутив JC-Client включает следующие пакеты установки (см. таблицу ниже).

Файл	Описание
JC-Client.msi (32-бит) JC-Clientx64.msi (64-бит)	Устанавливает JC-Client на рабочую станцию. Необходимо, чтобы в одной папке с файлом установки находился соответствующий пакет: JC-Client.msi - Data2.cab JC-Clientx64.msi – Data1.cab
Data1.cab Data2.cab	Пакеты, необходимые для установки JC-Client. Данные файлы должны находиться в одной папке с файлом установки (см. выше).

Системные требования

Перед установкой JC-Client удостоверьтесь в том, что компьютер соответствует минимальным требованиям.

Требования к аппаратному и программному обеспечению рабочей станции

Поддерживаемые операционные системы	• Windows XP SP3 (32-бит) • Windows XP SP2 (64-бит) • Windows Server 2003 SP2 (32/64-бит) • Windows Vista SP2 (32/64-бит) • Windows Server 2008 SP2 (32/64-бит) • Windows 7 SP1 (32/64-бит) • Windows Server 2008 R2 SP1 • Windows 8.1 Update 1 (32/64-бит) • Windows Server 2012
Поддерживаемые браузеры	• Firefox • Internet Explorer
Поддерживаемые модели электронных ключей	• USB-токен JaCarta • Смарт-карта JaCarta
Необходимые аппаратные средства	USB-порт (для аппаратных ключей JaCarta). Для смарт-карт необходимо наличие установленного считывателя смарт-карт.
Необходимые драйверы	• Если вы используете USB-токен JaCarta или считыватель смарт-карт, совместимый с CCID, необходимо, чтобы драйвер CCID был установлен в системе. Начиная с Windows Vista, этот драйвер установлен по умолчанию. На более ранних системах (Windows XP/Server 2003), если не загружались обновления, он может отсутствовать. Установить драйвер можно несколькими способами: ◆ загрузив последние обновления Windows и воспользовавшись мастером нового оборудования (для этого компьютер должен быть подключен к Интернету); ◆ драйвер также можно установить из основного пакета JC-Client - для этого необходимо использовать параметр командной строки `INSTALLCCID=1` (подробнее см. «Установка в режиме командной строки» и «Параметры командной строки»). • Если вы используете считыватель смарт-карт, несовместимый с CCID, установите драйвер производителя считывателя.
Рекомендуемое разрешение экрана	Для работы утилиты JC-Client рекомендуется установить разрешение монитора не ниже 1024x768.

Примечание:

В состав JC-Client входит компонент Minidriver, который также позволяет использовать JC-Client совместно с поставщиком услуг шифрования Microsoft Smart Card Base CSP. Microsoft Smart Card Base CSP по умолчанию установлен на ОС Vista и дальнейших версиях Windows. Чтобы установить Microsoft Smart Card Base CSP на ОС Windows XP/2003, вы можете загрузить его с сайта Microsoft вручную или воспользоваться службой обновления Windows.

Требования для подключения к удаленному рабочему столу (RDP)

JC-Client поддерживает следующие средства аутентификации при работе с подключением к удаленному рабочему столу.

Операционная система на стороне сервера	• Windows Server 2003 • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012

Состав JC-Client

В таблице ниже представлены компоненты, входящие в состав JC-Client. В процессе установки можно выбрать, какие из них будут установлены на рабочую станцию (см. «Установка и удаление JC-Client»).

Компонент	Описание
Athena CSP и **Minidriver**	**Athena CSP –** поставщик услуг шифрования, представляющий собой набор библиотек, которые обеспечивают поддержку программных интерфейсов MS Crypto API и PKCS#11. **Minidriver** – компонент, позволяющий использовать электронные ключи JaCarta с приложениями, поддерживающими стандарт Minidriver (подробные сведения представлены на сайте Microsoft http://msdn.microsoft.com/en-us/windows/hardware/gg487500.aspx - на английском языке). Minidriver также необходим, чтобы использовать в качестве поставщика услуг шифрования Microsoft Smart Card Base CSP. По умолчанию поставщик услуг шифрования Microsoft Smart Card Base CSP входит в состав Windows Vista/Server 2008/7/8.1 Update 1. На ОС Windows XP/Server 2003 Microsoft Smart Card Base CSP можно установить через службу обновлений Windows или загрузить и установить вручную. **Примечание:** на компьютер устанавливаются оба этих компонента. В процессе установки вы можете выбрать, какой из них будет использоваться по умолчанию.
Credential Provider/ GINA для биометрии	Библиотеки, заменяющие стандартные библиотеки Microsoft GINA (Windows XP/Server 2003) или Credential Provider (Windows Vista /Server 2008/7/8.1 Update 1/2012). Данный компонент позволяет: • осуществлять разблокировку электронных ключей JaCarta на экране приветствия Windows; • осуществлять вход в систему по результатам сканирования отпечатка пальца. **Примечание:** если этот компонент не установлен, для входа в систему будет использоваться стандартный механизм Windows при использовании смарт-карт.
Серверные компоненты RDP для биометрии	Набор компонентов, необходимый для поддержки доступа по отпечатку пальца при подключении к удаленному рабочему столу. Данный набор компонентов должен быть установлен на компьютер, к которому будут подключаться через удаленный доступ. **Примечание:** данный компонент используется для биометрического доступа. Описание настроек, необходимых для биометрической аутентификации с JaCarta представлено в документе *Использование JaCarta для биометрической аутентификации в среде Windows*.
Клиентские компоненты Citrix для биометрии	Набор компонентов, необходимый для поддержки работы электронных ключей JaCarta в среде Citrix. Данный набор компонентов должен быть установлен на клиентские компьютеры, которые будут подключаться к серверу Citrix. **Примечание:** данный компонент используется для биометрического доступа. Описание настроек, необходимых для биометрической аутентификации с JaCarta, представлено в документе *Использование JaCarta для биометрической аутентификации в среде Windows*.
Установить в Mozilla FireFox	Если будет отмечен данный пункт, в настройках Mozilla Firefox будет автоматически прописан путь к библиотеке, позволяющей работать с электронными ключами JaCarta через интерфейс PKCS#11. Если этот пункт не был отмечен при установке, впоследствии путь к необходимой библиотеке можно будет указать вручную.
Поддержка биометрии	Данный компонент позволяет использовать биометрические возможности JC-Client и электронных ключей JaCarta. **Примечание:** данный компонент используется для биометрического доступа. Описание настроек, необходимых для биометрической аутентификации с JaCarta представлено в документе *Использование JaCarta для биометрической аутентификации в среде Windows*.

Пользовательский интерфейс JC-Client представлен следующими утилитами (см. таблицу ниже). Эти утилиты необязательно устанавливать на компьютеры пользователей, однако в этом случае управление электронными ключами (например, разблокировка пароля пользователя) на этих компьютерах будет невозможна. При этом сохранится возможность настраивать параметры использования электронных ключей JaCarta на уровне реестра (см. «Настройка параметров реестра вручную»).

Компонент	Описание
JaCarta Monitor	Системный процесс, отвечающий за операции с хранилищем сертификатов и отображение значка  в области уведомлений. Нажатие на значок открывает меню, из которого можно запустить другие утилиты входящие в состав JC-Client.
JaCarta Manager	Утилита JaCarta Manager используется для управления сертификатами в памяти электронных ключей JaCarta. С ее помощью можно импортировать, экспортировать, просматривать и удалять сертификаты. Для подробного описания доступных функций см. в разделе «JaCarta Manager».
JaCarta PINTool	Утилита JaCarta PINTool позволяет изменять или разблокировать пароль пользователя и пароль цифровой подписи. Для разблокировки требуется участие администратора. Подробное описание доступных функций см. в разделе «JaCarta PINTool».
JaCarta BioTool	Утилита BioTool позволяет сохранять отпечатки пальцев в память электронных ключей JaCarta, если это не было сделано в процессе персонализации или если возникла необходимость повторного сохранения отпечатков. В последнем случае требуется участие администратора. Подробное описание доступных функций см. в документе *Использование JaCarta для биометрической аутентификации в среде Windows*.
JaCarta Admin PINTool	Утилита JaCarta Admin PINTool позволяет изменять пароль администратора и пароль разблокировки цифровой подписи. Подробное описание доступных функций см. в разделе «JaCarta Admin PINTool».
JaCarta Format	Утилита JaCarta Format предназначена для персонализации электронных ключей JaCarta (см. «Персонализация»). С ее помощью создаются профили персонализации, где задаются основные параметры использования электронных ключей. Подробное описание доступных функций см. в разделе «JaCarta Format».
JaCarta Options	Утилита Option позволяет настроить параметры использования электронных ключей JaCarta на уровне пользователя или на уровне рабочей станции. Подробное описание доступных функций см. в разделе «JaCarta Options».

Состав IDProtect Admin

Программное обеспечение IDProtect Admin не входит в состав JC-Client и предназначено для создания ключей администратора. Ключи администратора применяются для доступа на уровне администратора к электронным ключам JaCarta пользователей и могут быть использованы для разблокировки – как при непосредственном участии администратора, так и в удаленном режиме. (Подробнее о создании и применении ключей администратора см. раздел «Ключ администратора», а также документ *IDProtect Admin для JaCarta. Справочное руководство*.)

В состав IDProtect Admin входят следующие утилиты (см. таблицу ниже).

Компонент	Описание
Card Generator	Утилита Card Generator предназначена для создания ключей администратора. Чтобы наделить электронный ключ JaCarta функциональностью ключа администратора, этот электронный ключ необходимо сначала персонализировать, используя утилиту JaCarta Format. Подробное описание доступных функций см. в разделе «Card Generator».
HelpDesk	Утилита HelpDesk используется для разблокировки электронных ключей JaCarta в удаленном режиме. Подробное описание доступных функций см. в разделе «HelpDesk».

Памятка администратора

В качестве памятки представляем вам общий перечень задач администратора. Более подробно все эти пункты будут рассмотрены далее в руководстве.

- Установка JC-Client на каждой рабочей станции, где будут использоваться электронные ключи JaCarta. Подробную информацию см. в разделах «Установка и удаление JC-Client» и «Параметры командной строки».
- Настройка профилей персонализации в соответствии с политикой безопасности, применяемой в организации. Подробную информацию см. в разделе «Настройка профиля персонализации».
- Персонализация электронных ключей JaCarta с использованием настроенных профилей персонализации. Подробную информацию см. в разделе «Персонализация».
- В процессе работы с персонализированными электронными ключами JaCarta пользуйтесь инструкциями, представленными в разделах «Настройки, доступные после персонализации», «Операции с сертификатами в памяти электронных ключей JaCarta», «Параметры и настройки».
- Разблокировка электронных ключей JaCarta. Подробную информацию см. в разделе «Разблокировка электронного ключа JaCarta».

Установка и удаление JC-Client

Дистрибутив JC-Client включает в себя набор компонентов и утилит (см. «Описание пакетов установки»), которые предоставляют быстрый доступ к настройкам электронных ключей JaCarta.

Установка с помощью программы-мастера

Помимо возможности установки стандартного набора компонентов и утилит программа-мастер предусматривает вариант расширенной установки, где можно выбрать, какие компоненты и утилиты будут установлены на рабочую станцию.

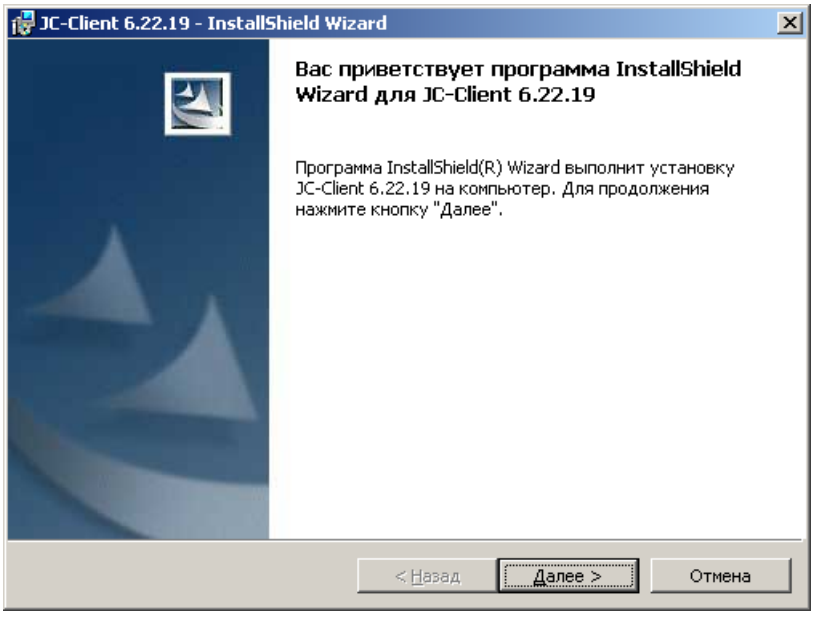
Доступны следующие варианты установки.

- **CSP:** устанавливает стандартные компоненты промежуточного слоя для JC-Client (Athena CSP и PKCS#11), а также утилиты JaCarta Format, JaCarta Manager, JaCarta Options и JaCarta PINTool. В этом режиме также устанавливается компонент Minidriver, который позволяет использовать JC-Client совместно с поставщиком услуг шифрования Microsoft Smart Card Base CSP, при этом Athena CSP помечается в качестве поставщика услуг шифрования, используемого по умолчанию.
- **Выборочная:** позволяет вручную отметить компоненты, которые будут установлены на компьютер.

Чтобы установить JC-Client с помощью программы-мастера, выполните следующие действия.

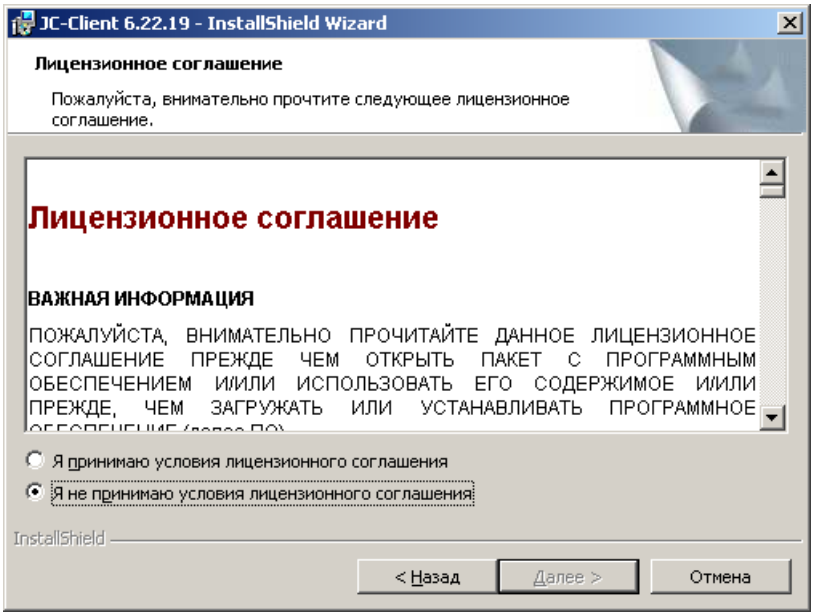
1. Войдите в систему с полномочиями администратора.
2. Закройте все приложения.
3. Запустите установочный файл:
   - `JC-Client.msi` (для 32-битных систем).
   - `JC-Clientx64.msi` (для 64-битных систем).

   Отобразится следующее окно.



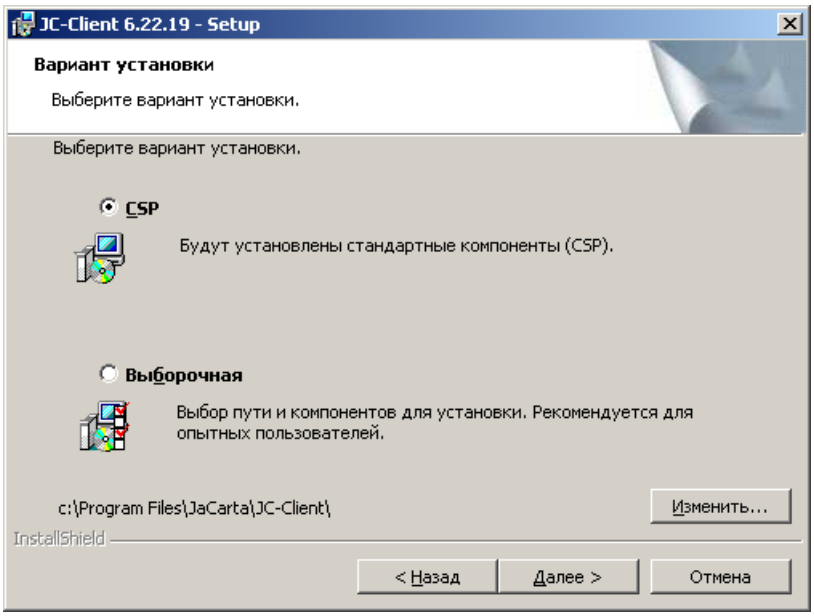
4. Нажмите **Далее**.

Появится окно лицензионного соглашения.



5. Ознакомьтесь с лицензионным соглашением и отметьте пункт **Я принимаю условия лицензионного соглашения** и нажмите **Далее**. Если вы не согласны с каким-либо из положений документа, откажитесь от установки, нажав кнопку **Отмена**.

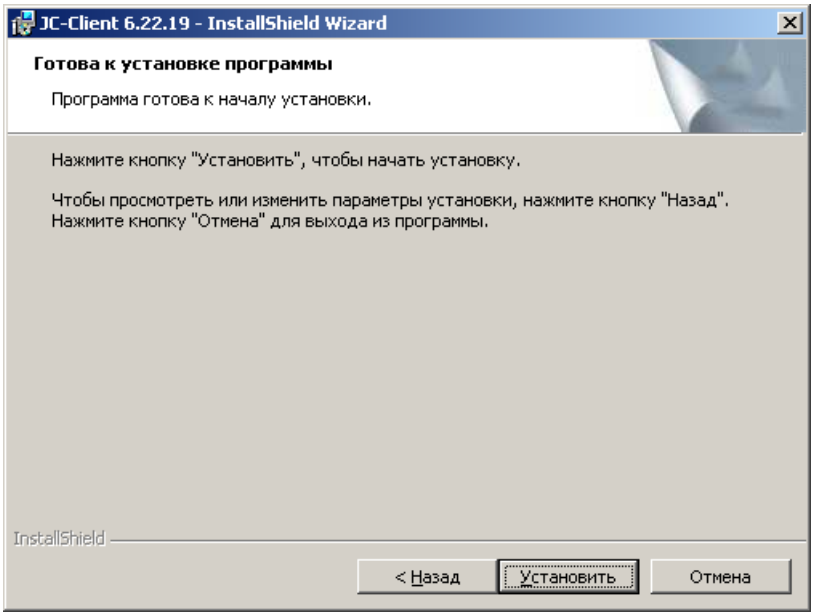
   Если вы приняли соглашение, на экране появится следующее окно.



6. Выберите вариант установки, нажмите **Далее** и продолжите процедуру в зависимости от сделанного выбора.

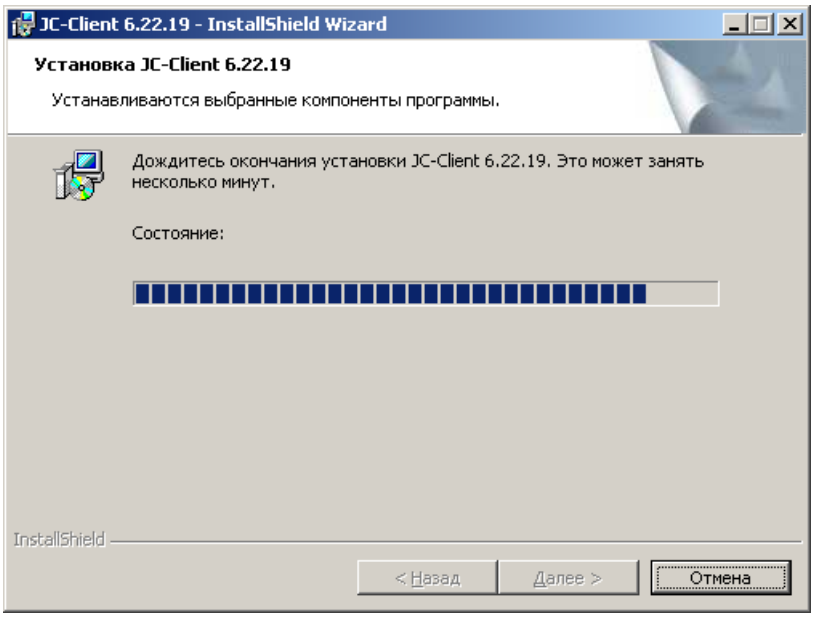
Если вы выбрали CSP

Если вы выбрали установку **CSP**, появится следующее окно.

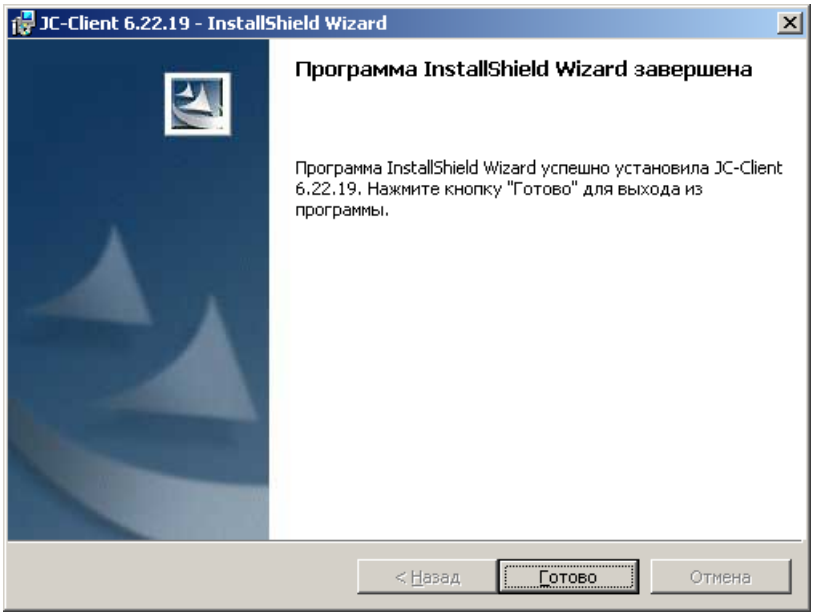


Если вы хотите изменить вариант установки, нажмите **Назад**. Чтобы запустить процесс установки нажмите **Установить**.

Установка займет некоторое время.



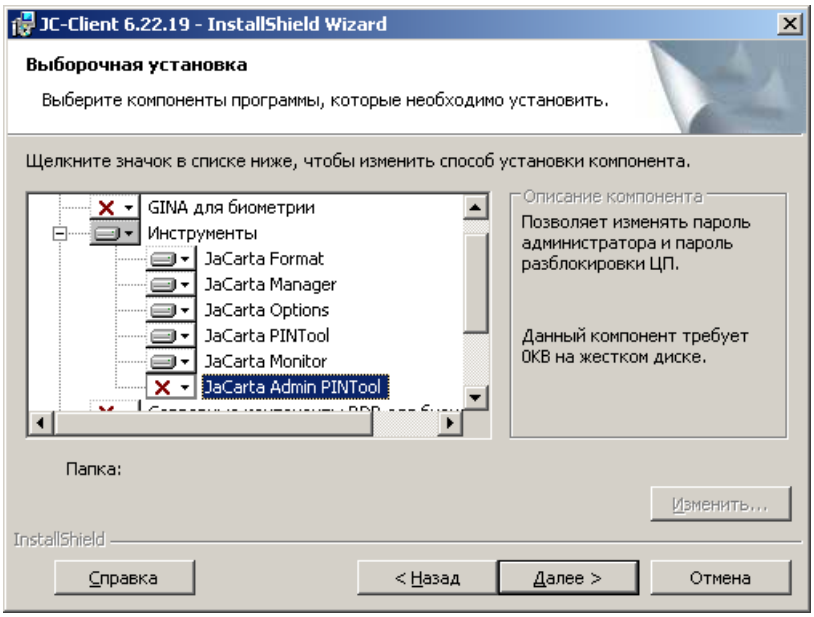
7. По завершении установки нажмите **Готово**.



При необходимости перезагрузите компьютер.

Если вы выбрали выборочную установку

Если вы выбрали вариант установки **Выборочная**, появится окно со списком компонентов установки.



1. Выберите, какой компонент будет использоваться по умолчанию
   - Athena CSP – для этого оставьте отмеченным пункт **Сделать Athena CSP стандартным поставщиком**.
   - Minidriver – для этого щелкните на пункте **Сделать Athena CSP стандартным поставщиком** и в контекстном меню выберите **Этот компонент будет недоступен**.

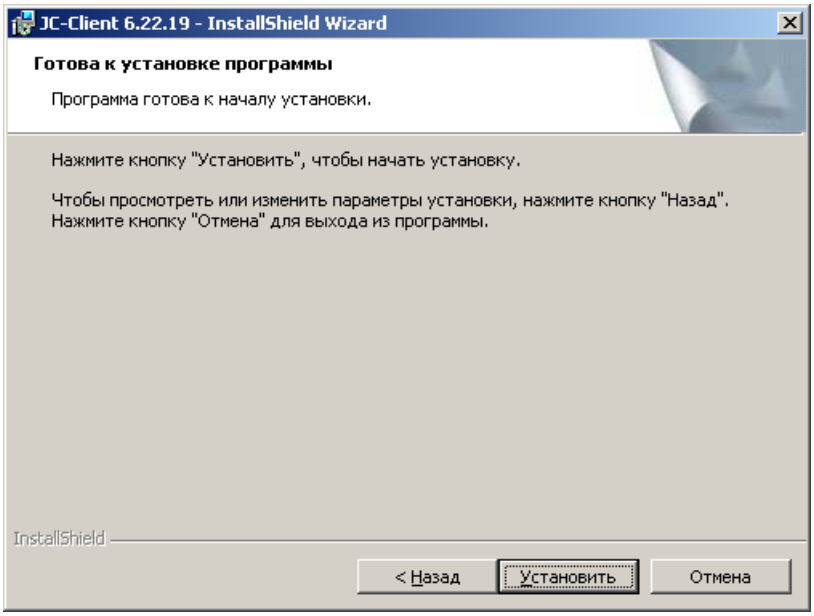
Примечание:

Независимо от выбора устанавливаются оба компонента.

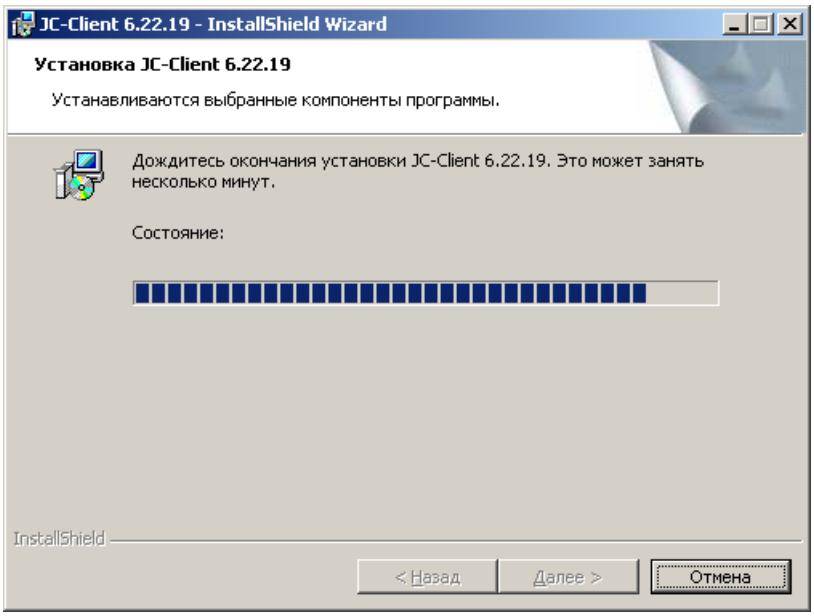
2. Выберите компоненты, которые необходимо установить, руководствуясь информацией, представленной в разделе «Состав JC-Client».

3. При необходимости выберите папку, в которую будет устанавливаться программа (если хотите устанавливать в папку, отличную от заданной по умолчанию), нажав кнопку **Изменить**.
4. Нажмите **Далее**.

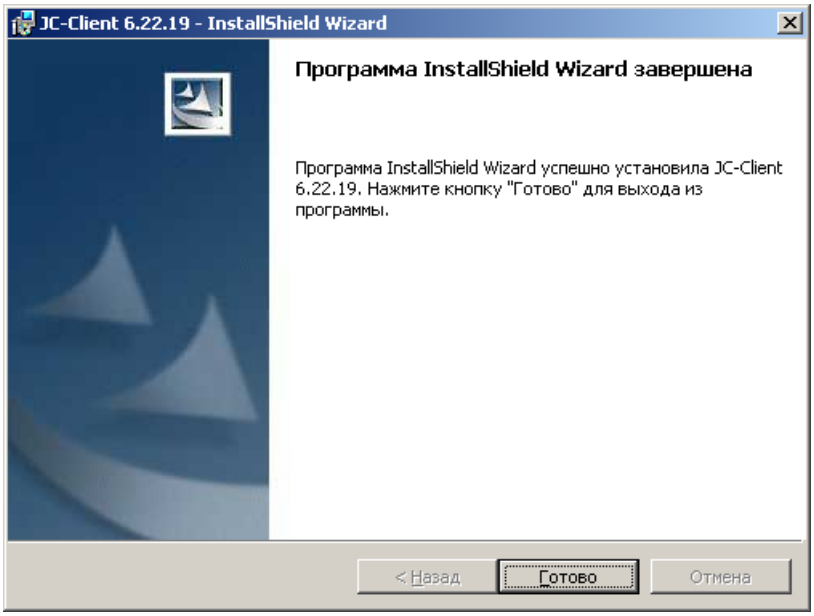
   Отобразится следующее окно.



5. Если вы хотите изменить вариант установки, нажмите **Назад**. Чтобы запустить процесс установки нажмите **Установить**. Установка займет некоторое время.



6. По завершении установки нажмите **Готово**.



При необходимости перезагрузите компьютер.

Установка в режиме командной строки

Помимо установки средствами программы-мастера также существует вариант установки из командной строки, где в качестве параметров вы можете указать необходимые для установки компоненты. В этом случае используется стандартный синтаксис Windows Installer.

```
msiexec /i JC-Client.msi
```

где, `JC-Client.msi`– это пакет установки для 32-битных платформ Windows. Для 64-битных платформ используйте файл `JC-Clientx64.msi`.

Чтобы установить JC-Client в режиме командной строки, выполните следующие действия.

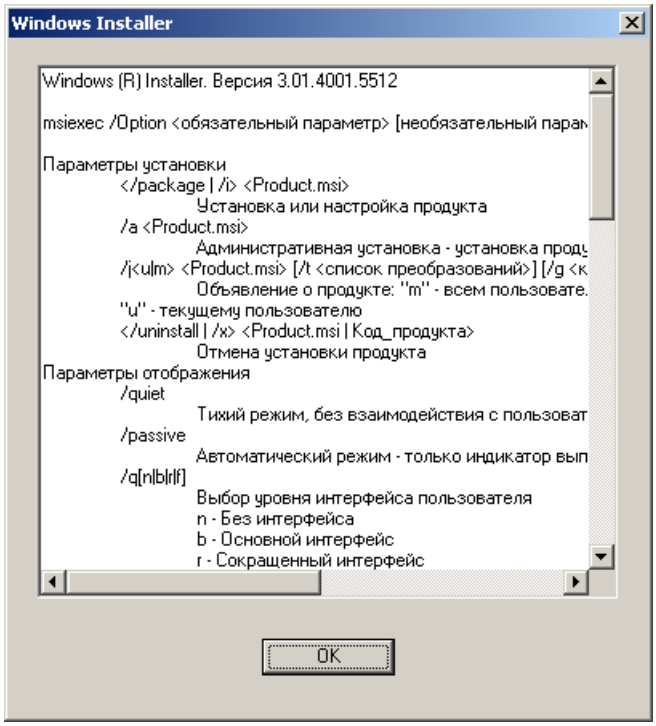
1. Войдите в систему под учетной записью с полномочиями администратора.
2. Закройте все приложения.
3. Выберите **Пуск > Все программы > Стандартные > Командная строка**.
4. Если вы выполняете установку под Windows Vista/Server 2008/7/8.1 Update 1/2012, щелкните правой кнопкой в пункте **Командная строка** и выберите **Запуск от имени Администратора**.
5. Введите в командной строке `msiexec` с необходимыми параметрами.

Справка по Windows Installer

Чтобы просмотреть полный перечень возможных параметров, которые можно использовать при установке JC-Client, обратитесь к встроенной справке Windows Installer. Для ее вызова выполните следующие действия.

1. Откройте меню **Пуск > Выполнить**.
2. В поле **Открыть** введите `msiexec` и нажмите **OK**.

На экране появится окно со списком параметров Windows Installer.



Установка параметров в режиме командной строки

При установке в режиме командной строки есть возможность задать особые параметры вместо тех, которые определены по умолчанию, и задать для таких параметров необходимые значения. Такие параметры сохраняются в реестре в следующем разделе.

```
HKEY_LOCAL_MACHINE\Software\Athena Smartcard Solutions\IDProtect Client.
```

Чтобы установить параметры установки, используйте следующий формат.

```
msiexec /i JC-Client.msi ПАРАМЕТР=ЗНАЧЕНИЕ ПАРАМЕТР=ЗНАЧЕНИЕ /qb
```

Список параметров командной строки представлен в разделе «Параметры командной строки».

Пример комбинации параметров

При установке JC-Client в режиме командной строки параметры установки можно комбинировать в одной команде, например:

```
msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLOPTIONS=0
```

(Не устанавливать утилиту JaCarta Options.)

Удаление JC-Client

Для удаления JC-Client существует три способа:

- Удаление через панель управления Windows
- Удаление с помощью программы-мастера
- Удаление из командной строки

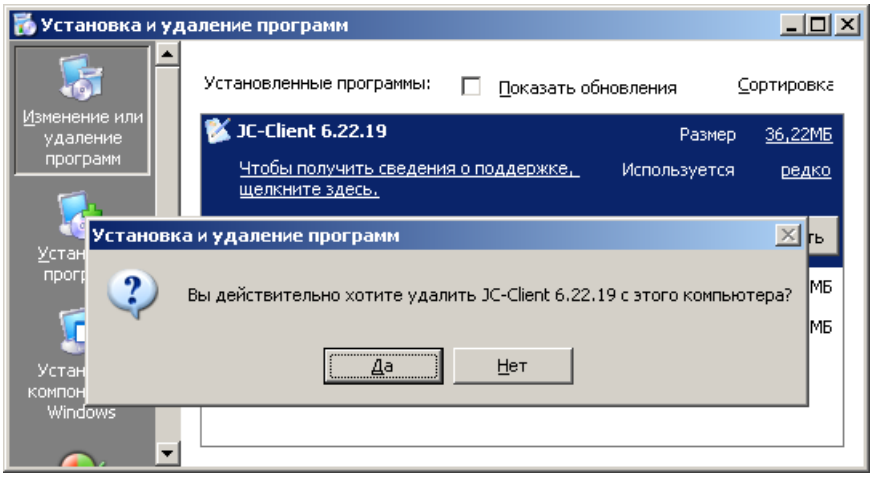
Удаление через панель управления Windows

В Windows есть стандартная схема удаления и установки программ. С ее помощью вы можете также удалить JC-Client. Для этого выполните следующие действия.

1. Откройте меню **Пуск > Панель управления**.
2. Дважды щелкните на значке **Установка и удаление программ**.

3. Выберите JC-Client и нажмите кнопку **Удалить**.

   Отобразится диалоговое окно **Установка и удаление программ**.



4. Нажмите **Да**, чтобы удалить JC-Client.
5. После того как JC-Client будет удален, перезагрузите компьютер.

Удаление с помощью программы-мастера

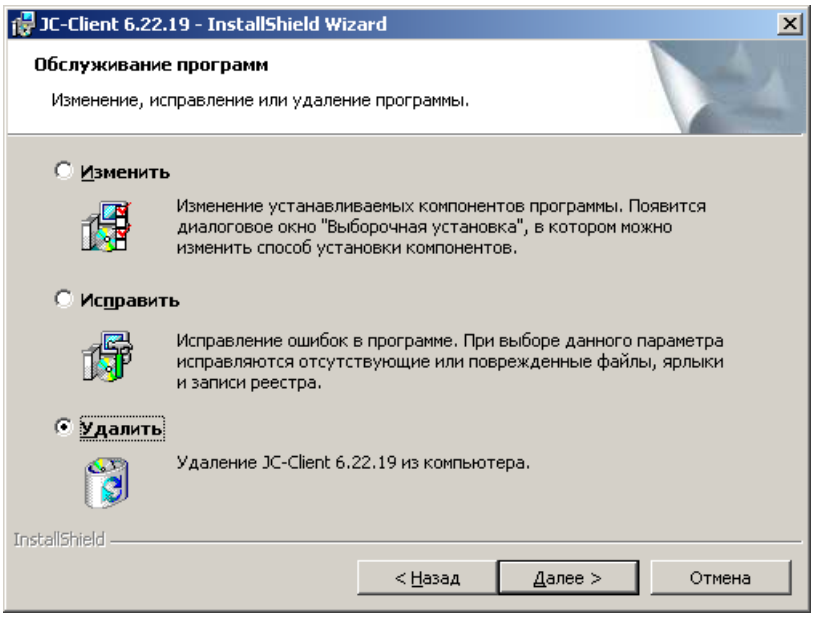
Для удаления JC-Client необходимы права администратора.

1. Запустите программу установки JC-Client

   (файл `JC-Client.msi` - для 32-битных операционных систем, `JC-Clientx64.msi` - для 64-битных ОС).

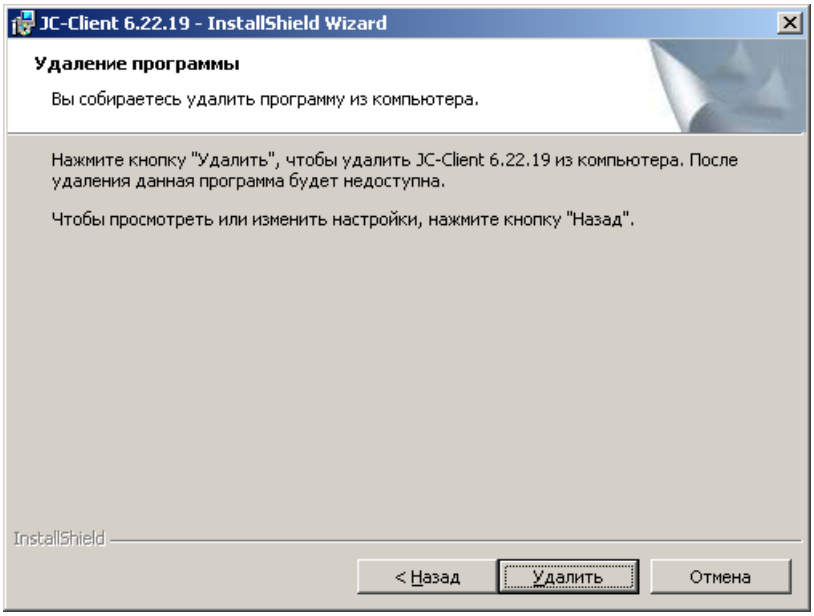
2. В окне мастера установки нажмите **Далее**.

   Появится окно выбора операции.



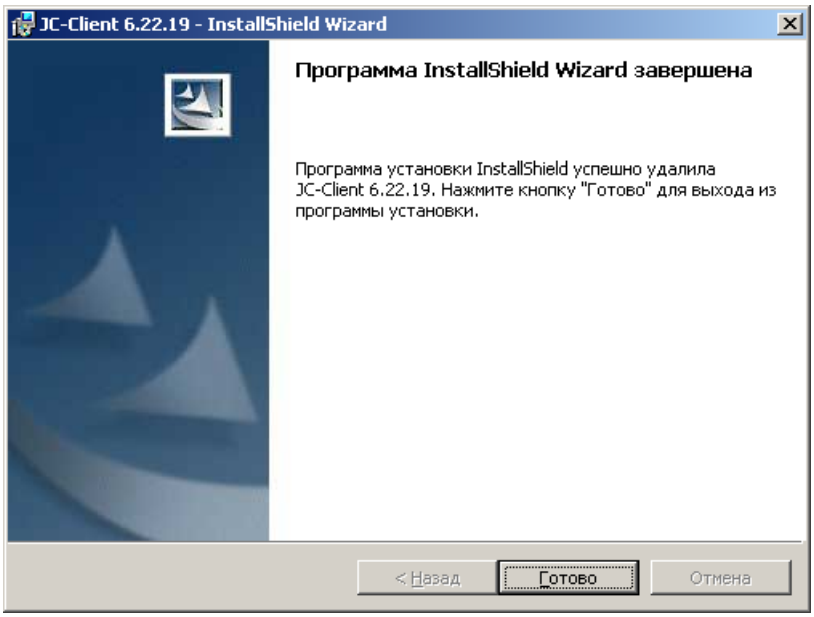
3. Выберите пункт **Удалить** и нажмите **Далее**.

Отобразится следующее окно.



4. Нажмите **Удалить**.

   По завершении процесса удаления появится окно с соответствующим сообщением.



5. Нажмите кнопку **Готово**, затем перезагрузите компьютер.

Удаление из командной строки

Чтобы удалить JC-Client из командной строки, выполните следующие действия.

1. Войдите в систему под учетной записью с правами администратора.
2. Закройте все приложения.
3. Откройте меню **Пуск > Программы > Стандартные > Командная строка**.
4. Если вы запускаете командный интерпретатор в Windows Vista/Server 2008/7/8.1 Update 1/2012, вы должны щелкнуть правой кнопкой на пункте **Командная строка**, выбрать **Запуск от имени администратора**.
5. Выполните команду msiexec в следующем формате:

   ```
   msiexec /x JC-Client.msi
   ```

   Где `JC-Client.msi` – имя установочного файла JC-Client для 32-битной платформы. Для 64-битной платформы замените это имя на `JC-Clientx64.msi`. Чтобы выполнить удаление в

полуавтоматическом режиме, то есть без необходимости подтверждения действий, добавьте в конце строки параметр `/q`.

6. После того как JC-Client будет удален, перезагрузите компьютер.

Описание JC-Client

В настоящем разделе представлена сводная информация о JC-Client и разъяснены аспекты работы с данным ПО. Настоятельно рекомендуется ознакомиться с данным разделом, прежде чем приступать к работе с JC-Client и электронными ключами JaCarta.

Основные термины

В настоящем документе применяются следующие термины (см. таблицу ниже).

Термин	Определение
Персонализация	Процесс, в результате которого задаются основные параметры использования электронных ключей JaCarta.
Профиль персонализации	Заранее настроенный профиль, который применяется для персонализации электронных ключей JaCarta (см. «Настройка профиля персонализации»).
Уровень доступа	Набор полномочий, необходимый для осуществления различных операций с электронными ключами JaCarta. Предусмотрено три уровня доступа: **гостевой доступ**; **доступ пользователя**; **доступ администратора**. (см. «Уровни доступа к устройствам JaCarta»).
Пароль пользователя	Пароль, обеспечивающий доступ на уровне пользователя.
Пароль администратора	Пароль, обеспечивающий доступ на уровне администратора.
Ключ администратора	Электронный ключ JaCarta, который используется для доступа к электронным ключам JaCarta пользователей на уровне администратора (см. «Ключ администратора»).
Пароль цифровой подписи	Дополнительный пароль, назначаемый во время персонализации для использования цифровой подписи (см. «Цифровая подпись»). Для персонализации электронного ключа JaCarta с поддержкой пароля цифровой подписи необходимо настроить параметры, в соответствии с которыми данный пароль будет связан с определенным типом закрытого ключа. Впоследствии при использовании данного закрытого ключа пользователь должен будет вводить пароль цифровой подписи.
Пароль разблокировки цифровой подписи	Пароль, позволяющий разблокировать пароль цифровой подписи (см. «Разблокировка пароля цифровой подписи»).
Очистка памяти	Удаление данных из памяти электронного ключа JaCarta.

Жизненный цикл электронных ключей JaCarta

Чтобы электронный ключ JaCarta можно было использовать, его необходимо персонализировать на основе заранее настроенного профиля персонализации. Для этих задач используется утилита JaCarta Format. В процессе персонализации задаются основные параметры использования электронного ключа JaCarta, такие как качество пароля пользователя.

Также можно задать возможность использования дополнительного пароля цифровой подписи (см. «Цифровая подпись»). Для настройки параметров использования цифровой подписи наряду с утилитой JaCarta Format применяется утилита JaCarta Options. Подробнее о создании пароля цифровой подписи см. «Настройки для использования цифровой подписи».

Процедуры настройки профиля персонализации и процесса персонализации описаны в разделах «Настройка профиля персонализации» и «Персонализация» соответственно.

В процессе использования электронного ключа JaCarta может возникнуть ситуация, когда устройство будет необходимо разблокировать. Говоря о разблокировке, следует понимать разблокировку одного или нескольких типов доступа пользователя. Так, если в профиле, на основе которого был персонализирован электронный ключ JaCarta, был задан пароль **пользователя** и **пароль цифровой подписи**, то блокирование одного из этих типов все еще позволяет пользователю использовать электронный ключ JaCarta, используя другой тип доступа.

Для разблокировки пароля пользователя необходим пароль администратора или ключ администратора.

Если в электронном ключе JaCarta пользователя задана поддержка пароля цифровой подписи, то блокирование цифровой подписи не будет являться препятствием для входа пользователя в систему посредством ввода пароля пользователя. Для разблокировки пароля цифровой подписи необходимо ввести пароль разблокировки цифровой подписи.

Процедуры разблокировки пароля пользователя и пароля цифровой подписи описаны в разделе «Разблокировка электронного ключа JaCarta».

Если электронный ключ JaCarta необходимо передать другому лицу, его можно персонализировать повторно с новыми настройками. При этом прежние данные, хранившиеся в памяти этого ключа, будут утеряны. Для повторной персонализации потребуется уровень доступа администратора.

В случае если электронный ключ JaCarta не планируется использовать в ближайшее время, следует удалить хранящуюся на нем информацию, выполнив процедуру очистки памяти. В результате данной процедуры из памяти электронного ключа удаляются все данные. Очистка памяти персонализированного электронного ключа JaCarta требует уровня доступа администратора. При последующей необходимости персонализировать электронный ключ уровень доступа администратора не потребуется.

Уровни доступа к устройствам JaCarta

После персонализации в электронном ключе JaCarta предусмотрено три уровня доступа.

- Гостевой уровень доступа
- Уровень доступа пользователя
- Уровень доступа администратора

Типы доступа к каждому из этих уровней зависят от параметров, заданных в процессе персонализации электронного ключа, и могут быть следующими (см. таблицу ниже).

Уровень доступа	Тип доступа
Гостевой	Не требуется
Пользователь	Пароль пользователя
Администратор	1. Пароль администратора 2. Ключ администратора

Для уровня доступа пользователя и администратора в процессе персонализации устанавливается допустимое количество последовательных неудачных попыток доступа, по достижении которого доступ на этом уровне блокируется. Если электронный ключ JaCarta заблокирован на уровне доступа пользователя, администратор может его разблокировать. В случае блокировки электронного ключа на уровне доступа администратора данный ключ все еще можно использовать на уровне доступа пользователя (при условии, что доступ пользователя не заблокирован), однако осуществление функций администратора на данном электронном ключе будет невозможно.

Внимание!

Блокировка пароля администратора на электронном ключе JaCarta, который был персонализирован со стандартными настройками JC-Client, означает также, что последующая очистка памяти и повторная персонализация такого электронного ключа JaCarta невозможны. Однако существует возможность персонализировать электронный ключ JaCarta таким образом, чтобы даже в случае блокировки пароля администратора оставалась возможность очистки памяти и повторной персонализации электронного ключа JaCarta (подробнее см. приложение «Настройка JC-Client, позволяющая повторную персонализацию в случае блокировки пароля администратора»).

В таблице ниже представлены действия, доступные с использованием ПО JC-Client и указанием необходимого уровня доступа.

Действие	Необходимый уровень доступа
Просмотр информации о подсоединенном электронном ключе	Гостевой
Аутентификация в системе с использованием электронного ключа JaCarta	Пользователь
Изменение пароля пользователя	Пользователь
Просмотр статуса блокировки	Гостевой
Разблокировка пароля пользователя	Администратор
Изменение пароля администратора	Администратор
Первичная персонализация электронного ключа JaCarta	Гостевой
Персонализация электронного ключа, который уже был персонализирован	Администратор
Отчистка памяти электронного ключа JaCarta	Администратор
Изменение метки (переименование) электронного ключа JaCarta	Пользователь/Администратор
Операции с сертификатами в памяти электронного ключа JaCarta	Пользователь
Определение времени, по истечении которого пользователь должен будет подтвердить свой уровень доступа	Администратор
Определение времени, по истечении которого пользователь должен сменить пароль	Администратор
Установка настройки, в соответствии с которой пользователь должен будет сменить пароль во время следующего сеанса работы с электронным ключом JaCarta	Пользователь/Администратор
Установка настройки, в соответствии с которой пользователь должен будет сменить пароль после разблокировки электронного ключа JaCarta	Администратор
Создание ключа администратора	Пользователь

Гостевой уровень доступа

Гостевой уровень доступа позволяет просматривать информацию о подсоединенном электронном ключе JaCarta. Эта информация отображается в основном окне утилит JaCarta Format и JaCarta Manager и включает сведения о статусе электронного ключа (персонализирован или не персонализирован), а также сведения о версии операционной системы, серийном номере и состоянии памяти подсоединенного электронного ключа. (Подробнее см. «JaCarta Manager» и «JaCarta Format».)

Помимо просмотра основной информации о подсоединенном электронном ключе, гостевой доступ позволяет проверить статус его блокировки (см. «JaCarta PINTool»).

Если электронный ключ JaCarta еще не был персонализирован или его память была предварительно очищена, гостевой уровень доступа позволяет персонализировать данный электронный ключ (см. разделы «Настройка профиля персонализации» и «Персонализация»). В дальнейшем в случае необходимости вновь персонализировать электронный ключ или выполнить процедуру очистки памяти потребуется уровень доступа администратора.

Уровень доступа пользователя

Уровень доступа пользователя позволяет пользователю аутентифицироваться в системе и выполнять базовые операции с электронным ключом JaCarta.

Пароль пользователя

Начальное значение пароля пользователя задается на этапе персонализации и может принимать следующие значения.

- **Вводимый** – пароль задается в процессе персонализации в соответствующем окне.
- **Стандартный** – пароль принимает стандартное значение, введенное в настройках профиля персонализации.

- **Случайный** – случайный пароль отображается на экране в процессе персонализации.

При любом значении пароля пользователя администратор может определить срок его действия, после которого пользователь должен будет его сменить, иначе пользователю будут недоступны операции с электронным ключом JaCarta. Также администратор может установить флажок **Пользователь должен сменить пароль** – в этом случае пользователь должен будет сменить пароль при следующем сеансе работы с электронным ключом JaCarta.

Настройки сложности пароля, как и способ формирования его первичного значения, определяются в профиле персонализации.

Изменение пароля пользователя после персонализации доступно с помощью утилиты JaCarta PINTool (см. документ *JC-Client. Руководство пользователя*).

Для разблокировки пароля пользователя используется пароль администратора или ключ администратора (подробнее о разблокировке пароля пользователя см. «Разблокировка электронного ключа JaCarta» и «Разблокировка с использованием ключа администратора»).

Уровень доступа администратора

JaCarta поддерживает доступ на уровне администратора двумя способами: **пароль администратора** или **ключ администратора**. Тип доступа определяется в настройках профиля персонализации.

Устанавливая данные настройки, необходимо быть предельно осторожным, так как блокировка пароля администратора (например, после превышения числа неудачных последовательных попыток ввода пароля администратора) сделает невозможным выполнение администраторских действий, таких как очистка памяти, персонализация или разблокировка пароля пользователя.

Пароль администратора

Начальное значение пароля администратора задается на этапе персонализации и может принимать следующие значения.

- **Вводимый** – пароль задается в процессе персонализации в соответствующем окне.
- **Стандартный** – пароль принимает стандартное значение, введенное в настройках профиля персонализации.
- **Случайный** – случайный пароль отображается на экране в процессе персонализации.

Настройки сложности пароля администратора, как и способ формирования его значения, определяются в профиле персонализации (подробнее см. «Настройка качества паролей» и «Персонализация»).

Для изменения пароля администратора используется утилита JaCarta Format (см. раздел «JaCarta Format»).

Разблокировка пароля администратора невозможна, поэтому в случае его блокировки (после превышения допустимого количества последовательных неудачных попыток ввода пароля) доступ к администраторским функциям на данном электронном ключе JaCarta будет утерян.

Ключ администратора

Ключ администратора используется для доступа на уровне администратора к электронным ключам JaCarta пользователей, которые были персонализированы с его использованием. В отличие от стандартного доступа с использованием пароля администратора, ключ администратора позволяет получить доступ к функциям администратора (таким как разблокировка электронного ключа JaCarta) в удаленном режиме.

Чтобы создать ключ администратора, необходимо сначала персонализировать обычный электронный ключ JaCarta, используя утилиту JaCarta Format, затем использовать утилиту Card Generator из состава дополнительного ПО IDProtect Admin. После этого ключ администратора можно использовать в процессе персонализации электронных ключей JaCarta пользователей и при дальнейшем выполнении административных задач с данными электронными ключами пользователей.

По сравнению с использованием пароля администратора использование ключа администратора имеет следующие преимущества:

- Разблокировка электронных ключей JaCarta пользователей в удаленном режиме.

- Ключ администратора можно разблокировать, зная пароль администратора для ключа администратора или имея другой ключ администратора, который использовался при персонализации заблокированного ключа администратора.

Подобнее о создании и использовании ключа администратора см. «Ключ администратора».

Цифровая подпись

JC-Client предусматривает возможность создания отдельного пароля для использования цифровой подписи. Такая возможность задается в процессе персонализации.

При создании отдельного пароля для цифровой подписи необходимо задать пароль разблокировки цифровой подписи, на случай если пользователь превысит допустимое значение последовательных неудачных попыток ввода данного пароля и пароль будет заблокирован. Таким образом, пароль разблокировки цифровой подписи так же соотносится с паролем цифровой подписи, как и пароль администратора с паролем пользователя.

Начальные значения пароля цифровой подписи и пароля разблокировки цифровой подписи настраиваются отдельно и могут принимать следующие значения:

- **Вводимый** – пароль задается в процессе персонализации в соответствующем окне.
- **Стандартный** – пароль принимает стандартное значение, введенное в настройках профиля персонализации.
- **Случайный** – случайный пароль отображается на экране в процессе персонализации.

Пароль цифровой подписи для удобства может быть синхронизирован с паролем пользователя. Для этого изначально оба пароля должны совпадать. Если при синхронизации также совпадает пароль разблокировки цифровой подписи и пароль администратора, они также будут синхронизированы.

Изменение и разблокировка пароля цифровой подписи доступны с помощью утилиты JaCarta PINTool (см. «JaCarta PINTool»).

Подробнее о настройках и использовании цифровой подписи см. разделы «Настройки для использования цифровой подписи» и «Персонализация с настройками цифровой подписи».

Настройка профиля персонализации

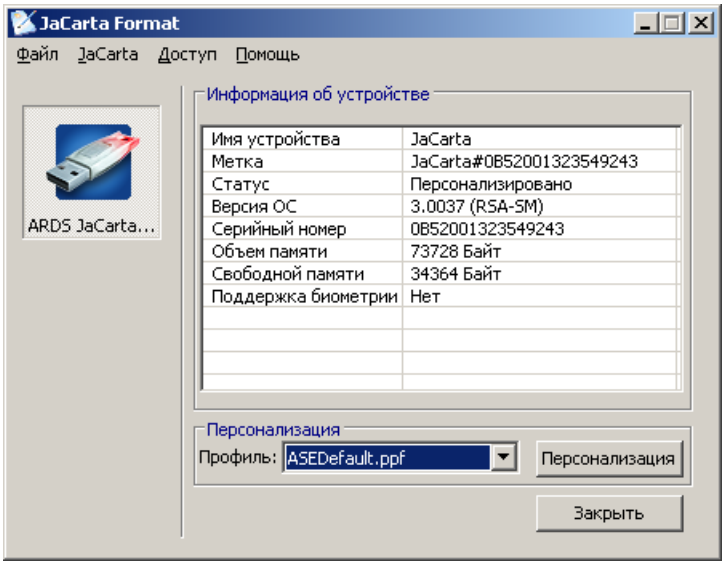
Перед использованием электронный ключ JaCarta необходимо персонализировать. Для персонализации используются заранее настраиваемые профили персонализации. Если вы не знаете, персонализирован электронный ключ JaCarta или нет, вы можете выяснить это, используя утилиты JaCarta Format или JaCarta Manager. В основном окне каждой из этих утилит содержится поле **Статус**. Данное поле может принимать два значения: **Персонализировано** и **Не персонализировано**.

После того как персонализация осуществлена, некоторые параметры можно изменить, только если персонализировать электронный ключ JaCarta повторно. Изменение других параметров не требует повторной персонализации, однако может потребоваться уровень доступа пользователя (пароль пользователя) или администратора (пароль администратора или ключ администратора).

Чтобы настроить профиль персонализации.

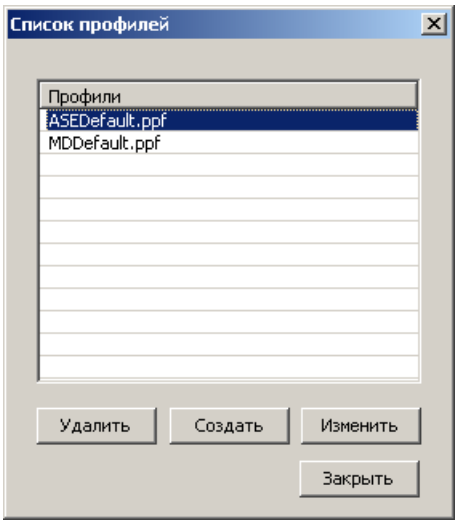
1. Выберите **Пуск > Все программы > JC-Client > JaCarta Format**.

   Отобразится окно утилиты.



2. В панели управления выберите **Файл > Управление профилями**.

   Отобразится следующее окно.



- Чтобы создать новый профиль, нажмите **Создать**.
- Чтобы изменить существующий профиль, нажмите **Изменить**.

Примечание:

> Профили **ASEDefault** и **MDDefault** являются стандартными профилями, входящими в поставку ПО JC-Client. Их нельзя изменить и удалить, однако их можно отредактировать и сохранить под другим именем.

Дальнейшее описание настроек профиля персонализации представлено в подразделах ниже.

Настройка качества паролей

JaCarta позволяет использовать четыре типа паролей.

- Пароль пользователя (см «Базовые настройки» далее)
- Пароль администратора (см «Базовые настройки» далее)
- Пароль цифровой подписи (см «Настройки для использования цифровой подписи» далее)
- Пароль разблокировки цифровой подписи (см «Настройки для использования цифровой подписи» далее)

Настройки сложности каждого из этих видов паролей в профиле персонализации устанавливаются отдельно, хотя процедура и доступные параметры сложности аналогичны. Доступ к настройкам качества каждого из видов паролей описывается в процедурах настройки профилей персонализации в настоящем разделе.

Настройка	Описание
Попыток	Определяет количество последовательных неудачных попыток ввода пароля перед блокировкой. Если данный параметр выставляется для пароля администратора или пароля разблокировки цифровой подписи, следует быть предельно осторожным, так как если эти пароли будут заблокированы, восстановить их не удастся.
Разблокировок	Максимальное количество разблокировок, которое допустимо сделать в течение эксплуатации электронного ключа JaCarta без необходимости вновь персонализировать устройство. Меню помимо числовых значений содержит два пункта. **Никогда** – после блокировки данный способ доступа больше нельзя будут использовать. **Не ограничено** – разблокировать данный способ доступа можно неограниченное количество раз. **Примечание:** при настройке пароля администратора или пароля разблокировки цифровой подписи данный параметр неактивен.
Минимум	Определяет минимальное возможное количество символов в пароле.
Максимум	Определяет максимальное возможное количество символов в пароле.
Не цифро-буквенных	Задает обязательное количество символов, не принадлежащих к алфавитно-цифровому набору, которое должно присутствовать в пароле. Если выставлено значение «0» (ноль), эти символы использовать необязательно, но их использование не запрещается.
Буквы	Задает обязательное количество букв (из набора ASCII), которое должно присутствовать в пароле. Если выставлено значение «0» (ноль), эти символы использовать необязательно, но их использование не запрещается.
Возрастание	Максимально допустимое число последовательно идущих символов, например, «1 2 3 4» или «a b c d».
Верхний регистр	Задает обязательное количество букв (из набора ASCII) в верхнем регистре, которое должно присутствовать в пароле. Если выставлено значение «0» (ноль), эти символы использовать необязательно, но их использование не запрещается.
Цифры	Задает обязательное количество десятичных цифр, которое должно присутствовать в пароле. Если выставлено значение «0» (ноль), эти символы использовать необязательно, но их использование не запрещается.
Максимум повторений	Задает дозволяемое число идущих подряд одинаковых символов в пароле.

Базовые настройки

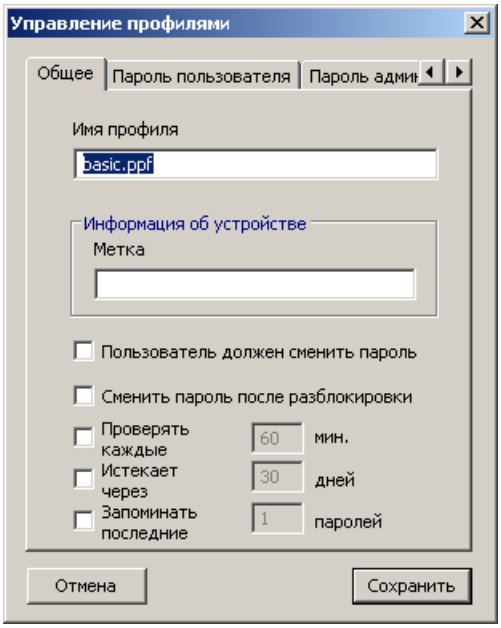
Базовая настройка профиля персонализации касается следующих параметров:

- Общие параметры использования электронного ключа JaCarta
- Качество пароля пользователя и пароля администратора
- Способ первичного формирования пароля пользователя и пароля администратора

Чтобы создать профиль персонализации с базовыми настройками.

1. Выберите **Пуск > Все программы > JC-Client > JaCarta Format**.
2. В панели управления утилиты выберите **Файл > Управление профилями**.
3. Нажмите **Создать**, чтобы создать новый профиль или **Изменить**, чтобы отредактировать существующий профиль.

   Отобразится окно настройки профиля персонализации.



4. На вкладке **Общее** настройте общие параметры использования электронного ключа JaCarta, руководствуясь приведенной ниже таблицей.

Настройка	Описание
Имя профиля	Имя профиля. В данном поле можно задать имя нового профиля или изменить имя существующего.
Метка	Данное поле используется для идентификации персонализируемых электронных ключей JaCarta. Значение данного поля не влияет на работу служб Windows, связанных с использованием смарт-карт. Его значение эквивалентно PKCS#11 Token Label. Если вы не зададите значение этого поля, оно примет значение «JaCarta#Серийный номер JaCarta».
Пользователь должен сменить пароль	Если данный флажок установлен, пользователь должен будет сменить пароль при первом использовании электронного ключа JaCarta. В противном случае все операции с данным электронным ключом, требующие пароля пользователя, будут недоступны. Пароль можно будет изменить во время входа в систему.
Сменить пароль после разблокировки	В случае разблокировки пароля пользователя новое значение пароля может задать администратор. Установка данного флажка потребует от пользователя снова сменить пароль пользователя при первом сеансе работы с электронным ключом JaCarta после разблокировки.
Проверять каждые X мин.	Если флажок установлен, значение в поле **мин.** определяет, через сколько минут после аутентификации пользователь должен будет снова подтвердить свой уровень доступа.

Настройка	Описание
Истекает через X дней	Если флажок установлен, значение в поле **дней** определяет, через сколько дней пользователь должен будет сменить пароль.
Запоминать последние X паролей	Если флажок установлен, значение в поле **паролей** определяет количество последних использованных паролей пользователя, которые не должны использоваться при назначении нового пароля.

5. Выберите вкладку **Пароль пользователя**.
6. Настройте параметры пароля пользователя, руководствуясь приведенной ниже таблицей.

Настройка	Описание
Значение пароля	Выберите из трех пунктов. **Вводимый** – пароль необходимо будет ввести в процессе персонализации вручную. **Стандартный** – электронный ключ JaCarta будет персонализирован с паролем, заданным в активном поле напротив списка. **Случайный** – случайный пароль отобразится во время персонализации. В этом случае его надо сохранить в надежном месте. В случае утери его нельзя будет восстановить.
Тип доступа	Для базовых настроек оставьте выбранным пункт **Пароль пользователя**.
Качество пароля	Нажатие на данную кнопку открывает окно настроек качества пароля. Список доступных параметров представлен выше в разделе «Настройка качества паролей».

7. Перейдите на вкладку **Пароль администратора** и настройте параметры пароля администратора, аналогично параметрам пароля пользователя на вкладке **Пароль пользователя**.

Примечание:

> Если вы хотите использовать для администраторского доступа ключ администратора, выполните действия, описанные в разделе «Настройки для персонализации с использованием ключа администратора»

8. Сохраните профиль, нажав **Сохранить**.

   Теперь профиль можно использовать для персонализации электронных ключей JaCarta (см. раздел «Персонализация с базовыми настройками»).

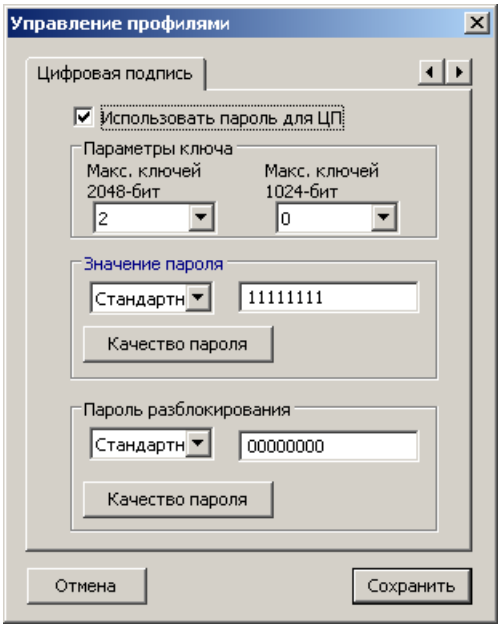
Настройки для использования цифровой подписи

Настройка профиля персонализации для использования цифровой подписи не противоречит базовой настройке. Таким образом, для настройки использования цифровой подписи также необходимо выполнить настройку базовых параметров.

Чтобы создать профиль персонализации для использования пароля цифровой подписи.

1. В панели управления выберите **Файл > Управление профилями**.
2. Нажмите **Создать**, чтобы создать новый профиль или **Изменить**, чтобы отредактировать существующий профиль.
3. Настройте базовые параметры использования электронного ключа JaCarta, руководствуясь информацией в разделе «Базовые настройки». Если вы хотите использовать для администраторского доступа ключ администратора, выполните действия, описанные в разделе «Настройки для персонализации с использованием ключа администратора».
4. Выберите вкладку **Цифровая подпись** и установите флажок **Использовать пароль для ЦП**.

Окно редактирования профиля примет следующий вид.



5. Настройте необходимые параметры, руководствуясь приведенной ниже таблицей.

Настройка	Описание
Макс. ключей 2048-бит	Максимальное количество ключей длиной 2048 бит, которые можно хранить в памяти электронного ключа JaCarta.
Макс. ключей 1024-бит	Максимальное количество ключей длиной 1024 бит, которые можно хранить в памяти электронного ключа JaCarta.
Значение пароля	Выберите из трех пунктов. **Вводимый** – пароль необходимо будет ввести в процессе персонализации вручную. **Стандартный** – электронный ключ JaCarta будет персонализирован с паролем, заданным в активном поле напротив списка. **Случайный** – случайный пароль отобразится во время персонализации. В этом случае его надо сохранить в надежном месте. В случае утери его нельзя будет восстановить.
Значение пароля > Качество пароля	Вызывает окно настроек качества пароля цифровой подписи (см. «Настройка качества паролей»).
Пароль разблокировки	Аналогично списку **Значение пароля**.
Пароль разблокировки > Качество пароля	Вызывает окно настроек качества пароля разблокировки цифровой подписи (см. «Настройка качества паролей»).

6. Нажмите **Сохранить** для сохранения профиля персонализации.

   Теперь профиль можно использовать для персонализации (см. раздел «Персонализация с настройками цифровой подписи»).

Настройки для персонализации с использованием ключа администратора

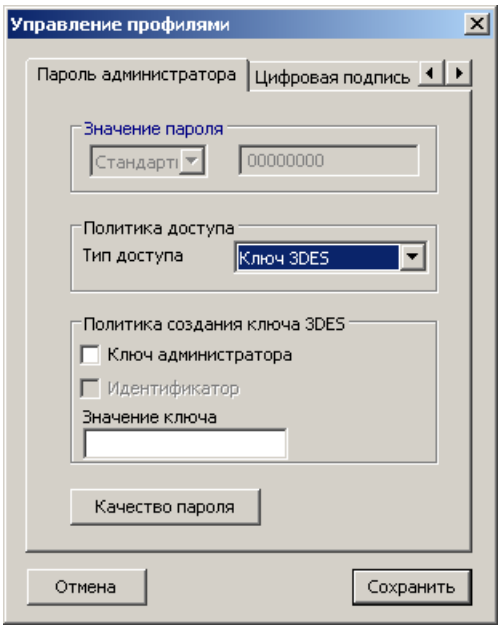
Чтобы использовать ключ администратора для доступа к другим электронным ключам JaCarta, такой ключ необходимо сначала создать. Процедура создания ключа администратора описана в разделе «Ключ администратора».

Настройки профиля для последующей персонализации с использованием ключа администратора не противоречит настройками, задающим необходимость использовать пароль цифровой подписи. Отличие от базовых настроек заключается в том, что для доступа на уровне администратора к электронному ключу JaCarta, который будет персонализирован на основе данного профиля, будет применяться не пароль администратора, а ключ администратора.

Чтобы настроить профиль для последующей персонализации с использованием ключа администратора.

1. Выберите **Пуск > Все программы > JC-Client > JaCarta Format**.
2. В панели управления выберите **Файл > Управление профилями**.
3. Нажмите **Создать**, чтобы создать новый профиль или **Изменить**, чтобы отредактировать существующий профиль.
4. Перейдите на вкладку **Пароль администратора** и в списке **Тип доступа** выберите **Ключ 3DES**.

   Окно примет следующий вид.



5. Установите флажок **Ключ администратора**.

Примечание:

> Если не устанавливать флажок **Ключ администратора**, существует возможность в поле **Значение ключа** явно задать ключ 3DES в шестнадцатеричном формате. Данная возможность предназначена для технологических партнеров компании ЗАО «Аладдин Р.Д.» и не рекомендуется к использованию в практических целях.

6. Если вы хотите исключить возможность удаленной разблокировки электронных ключей JaCarta, установите флажок **Идентификатор**.
7. Настройте пароль пользователя и, при необходимости, настройте также параметры пароля цифровой подписи, руководствуясь информацией, представленной в разделах «Базовые настройки» и «Настройки для использования цифровой подписи».
8. Нажмите **Сохранить**, чтобы сохранить профиль персонализации.

   Теперь данный профиль можно использовать для персонализации с ключом администратора (см. раздел «Персонализация с использованием ключа администратора»).

Персонализация

В процессе персонализации задаются основные параметры использования электронного ключа JaCarta, такие как качество пароля пользователя и возможность использования пароля цифровой подписи. Персонализация производится на основе заранее настроенных и сохраненных профилей. О настройке профилей персонализации см. раздел «Настройка профиля персонализации».

Внимание!

Если электронный ключ JaCarta персонализирован со стандартными настройками, блокировка пароля администратора на этом электронном ключе приведет к невозможности последующей очистки памяти и персонализации. Если вы хотите сохранить возможность очистки памяти и повторной персонализации электронного ключа JaCarta после блокировки пароля администратора, перед персонализацией выполните действия, приведенные в приложении «Настройка JC-Client, позволяющая повторную персонализацию в случае блокировки пароля администратора».

Персонализация с базовыми настройками

Процедура персонализации с базовыми настройками может отличаться в зависимости от выбранного способа первичного формирования пароля пользователя и пароля администратора. Возможны следующие комбинации (см. таблицу ниже).

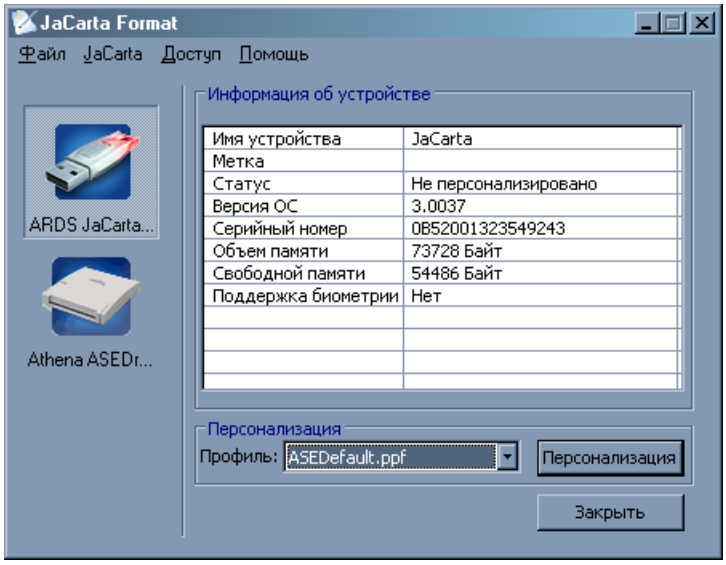
Пароль пользователя	Пароль администратора
Вводимый	**Вводимый**
Вводимый	**Стандартный**
Вводимый	**Случайный**
Стандартный	**Вводимый**
Стандартный	**Стандартный**
Стандартный	**Случайный**
Случайный	**Вводимый**
Случайный	**Стандартный**
Случайный	**Случайный**

В нашем примере мы рассмотрим комбинацию, где параметр первичного формирования пароля пользователя установлен как **Случайный**, а администратора как **Вводимый**

Чтобы персонализировать электронный ключ JaCarta, используя профиль с базовыми настройками.

1. Подключите к рабочей станции электронный ключ JaCarta, который необходимо персонализировать.
2. Выберите **Пуск > Все программы > JC-Client > JaCarta Format**.

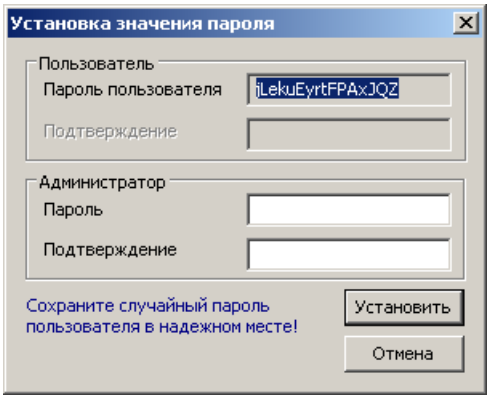
Отобразится основное окно утилиты.



Если электронный ключ JaCarta не персонализирован, поле **Статус** будет содержать значение **Не персонализировано**.

3. В списке **Профиль** выберите заранее сохраненный профиль персонализации и нажмите **Персонализация**.

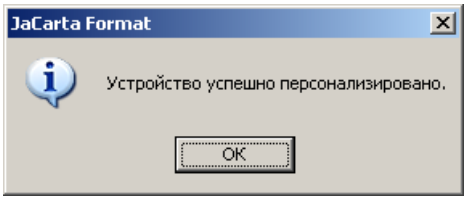
   В процессе персонализации отобразится следующее окно.



   В поле **Пароль пользователя** отображается случайный пароль пользователя. Необходимо сохранить этот пароль в надежном месте, так как в случае утери случайного пароля его будет невозможно восстановить.

4. Чтобы продолжить персонализацию в поле **Пароль** и **Подтверждение** в секции **Администратор** введите пароль администратора и подтверждение соответственно и нажмите **Установить**.

   По завершении процесса персонализации отобразится следующее сообщение.



5. Нажмите **OK**.

   Электронный ключ JaCarta персонализирован и готов к использованию.

Персонализация с настройками цифровой подписи

Процедура персонализации на основе профиля с настройками цифровой подписи является дополнительной частью процедуры персонализации с базовыми настройками и может отличаться

в зависимости от выбранного способа первичного формирования пароля цифровой подписи и пароля разблокировки цифровой подписи.

Примечание:

> Перед персонализацией необходимо настроить правила связывания пароля цифровой подписи с закрытым ключом. Для этого используется утилита JaCarta Options. Процедура настройки описана ниже в настоящем разделе.

Для пароля цифровой подписи и пароля разблокировки цифровой подписи возможны три способа первичного формирования.

- **Вводимый** – пароль задается в процессе персонализации в соответствующем окне.
- **Стандартный** – пароль принимает стандартное значение, введенное в настройках профиля персонализации.
- **Случайный** – случайный пароль отображается на экране в процессе персонализации.

Таким образом, доступны следующие комбинации (см. таблицу ниже).

Пароль цифровой подписи	Пароль разблокировки цифровой подписи
Вводимый	**Вводимый**
Вводимый	**Стандартный**
Вводимый	**Случайный**
Стандартный	**Вводимый**
Стандартный	**Стандартный**
Стандартный	**Случайный**
Случайный	**Вводимый**
Случайный	**Стандартный**
Случайный	**Случайный**

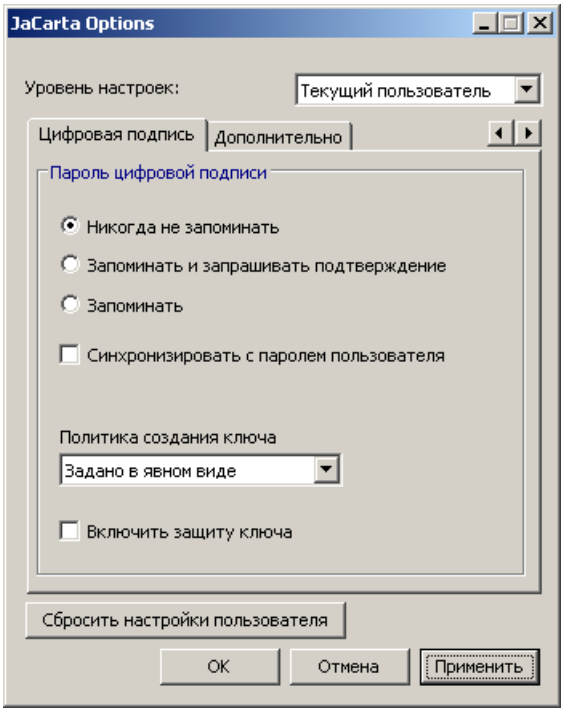
В данном примере для простоты используется профиль с настроенным типом доступа пользователя по паролю пользователя, а параметр формирования первичного значения пароля пользователя и пароля администратора установлен как **Стандартный**.

Для первичного формирования пароля цифровой подписи и пароля разблокировки цифровой подписи используется тип **Вводимый**.

Чтобы персонализировать электронный ключ JaCarta на основе профиля, настроенного для использования пароля цифровой подписи.

1. Выберите **Пуск > Все программы > JC-Client > JaCarta Options.**
2. Выберите вкладку **Цифровая подпись**.

Окно примет следующий вид.



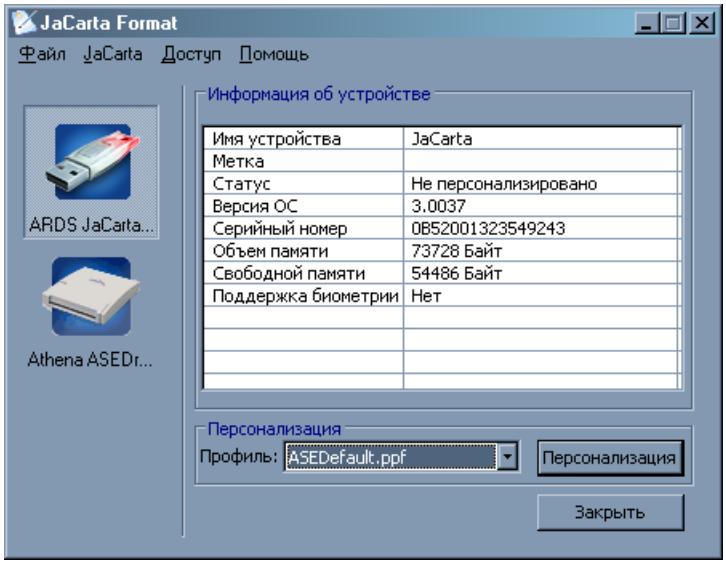
- Если вы хотите установить настройки для текущего пользователя рабочей станции, в меню **Уровень настроек** оставьте выбранным пункт **Текущий пользователь**.
- Если вы хотите установить настройки на уровне локальной машины, в меню **Уровень настроек** выберите пункт **Локальный компьютер** и установите флажок **Сбросить настройки пользователей**.

3. Определите параметры связывания пароля цифровой подписи с закрытым ключом, используя следующие настройки (см. таблицу ниже).

Настройка	Описание
Политика создания ключа	Данный список содержит три пункта: **Задано в явном виде** - если выбран этот пункт, закрытый ключ связан с паролем цифровой подписи только в том случае, если явно задан параметр PKCS#11 2.20 CKA_ALWAYS_AUTHENTICATE. **Любой ключ подписи** - если выбран этот пункт, пароль цифровой подписи будет связан с любым ключом, для которого установлен атрибут AT_SIGNATURE. **Имя контейнер начинается с** - если выбран этот пункт, существует возможность задать префикс контейнера (в появляющемся поле **Префикс**). Любой ключ цифровой подписи, имя контейнера которого начинается с заданного префикса, будет автоматически связан с паролем цифровой подписи. Для приложений, использующих PKCS#11, - если CKA_ID начинается с заданного префикса, этот ключ будет связан с паролем цифровой подписи, вне зависимости от значения параметра CKA_ALWAYS_AUTHENTICATE.
Включить защиту ключа	Если данный флажок установлен, закрытый ключ с атрибутом AT_SIGNATURE, созданный с установленным в `true` (истина) параметром CRYPT_FORCE_KEY_PROTECTION_HIGH, будет ассоциирован с паролем цифровой подписи.

4. Подключите к рабочей станции электронный ключ JaCarta, который необходимо персонализировать.
5. Выберите **Пуск > Все программы > JC-Client > JaCarta Format**.

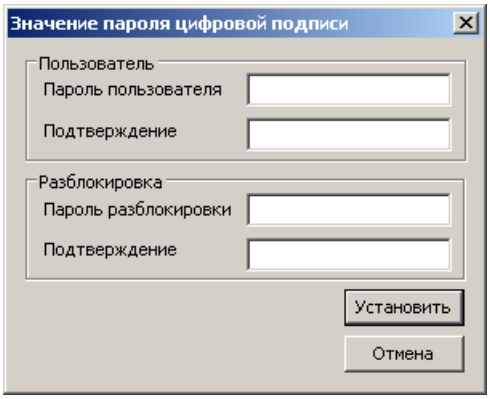
Отобразится основное окно утилиты.



Если электронный ключ JaCarta не персонализирован, поле **Статус** будет содержать значение **Не персонализировано**.

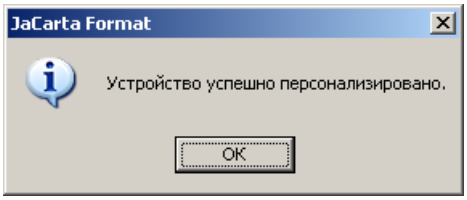
6. В списке **Профиль** выберите заранее сохраненный профиль персонализации и нажмите **Персонализация**.

   Отобразится следующее окно.



7. В секции **Пользователь**, в полях **Пароль пользователя** и **Подтверждение** введите пароль цифровой подписи и подтверждение соответственно.
8. В секции **Разблокировка**, в полях **Пароль разблокировки** и **Подтверждение** введите пароль разблокировки цифровой подписи и подтверждение соответственно.
9. Нажмите **Установить** для продолжения процедуры персонализации.

   По завершении персонализации отобразится следующее сообщение.



10. Нажмите **ОК**.

    Электронный ключ JaCarta персонализирован и готов к использованию.

Персонализация с использованием ключа администратора

Персонализация на основе профиля, настроенного для использования ключа администратора, отличается от персонализации с базовыми настройками. Отличие состоит в том, что вместо пароля администратора, который задается при базовой персонализации, используется

дополнительный электронный ключ JaCarta (ключ администратора). В остальном процедура персонализации данного типа является дополнительной частью процедуры базовой персонализации и персонализации на основе настроек цифровой подписи.

Примечание:

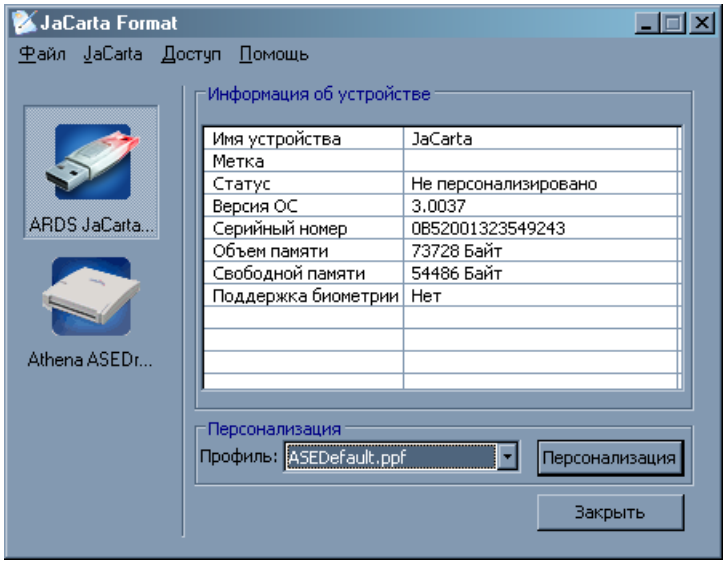
> Для персонализации с использованием ключа администратора необходимо, чтобы к рабочей станции было подключено два устройства чтения смарт-карт.

Прежде чем приступать к процедуре персонализации с использованием ключа администратора, ознакомьтесь с разделами «Ключ администратора» и «Состав IDProtect Admin».

Для того чтобы персонализировать электронный ключ JaCarta с использованием ключа администратора.

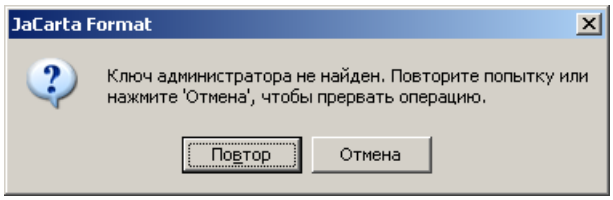
1. Подсоедините электронный ключ JaCarta, который необходимо персонализировать.
2. Выберите **Пуск > Все программы > JC-Client > JaCarta Format**.

   Отобразится основное окно утилиты.



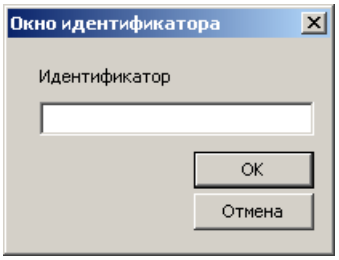
   Если электронный ключ JaCarta не персонализирован, поле **Статус** будет содержать значение **Не персонализировано**.
3. В списке **Профиль** выберите сохраненный профиль и нажмите **Персонализация**.

   Если ключ администратора не подключен, отобразится следующее сообщение.



4. Подсоедините ключ администратора и нажмите **Повтор**.
5. Введите пароль пользователя для ключа администратора и нажмите **Подтвердить**.

   Отобразится следующее окно.



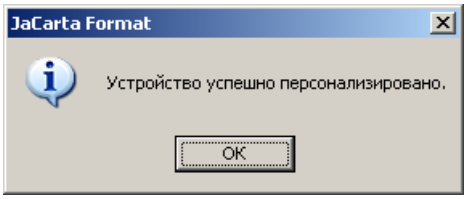
6. В поле **Идентификатор** введите значение, которое в числе прочего будет использоваться для удаленной разблокировки персонализируемого электронного ключа JaCarta. Это значение необходимо будет сообщить пользователю.

Примечание:

> Если в настройках профиля персонализации на вкладке **Пароль администратора** вы установили флажок **Идентификатор**, значение будет случайным и окно ввода идентификатора не появится. В этом случае персонализируемый электронный ключ JaCarta нельзя будет разблокировать в удаленном режиме.

7. Нажмите **OK**.

   По завершении персонализации отобразится следующее сообщение.



8. Нажмите **OK** для завершения процедуры.

   Электронный ключ JaCarta успешно персонализирован. В случае необходимости его можно будет разблокировать или повторно персонализировать с использованием ключа администратора.

Возможные сценарии персонализации

Данный раздел содержит таблицу (см. ниже), в которой представлены все возможные сценарии персонализации и приведен список необходимых действий со ссылками на соответствующие разделы.

Возможный сценарий	Необходимые действия	Ссылки на разделы
1. Доступ пользователя по паролю. 2. Доступ администратора по паролю.	1. Настройте профиль с базовыми параметрами персонализации. 2. Используйте настроенный профиль для персонализации электронного ключа JaCarta.	См. разделы: 1. Базовые настройки 2. Персонализация с базовыми настройками
1. Доступ пользователя по паролю. 2. Доступ администратора с использованием ключа администратора.	1. Создайте ключ администратора. 2. Настройте профиль для персонализации с использованием ключа администратора. 3. Используйте настроенный профиль и ключ администратора для персонализации электронного ключа JaCarta.	См. разделы: 1. Ключ администратора 2. Настройки для персонализации с использованием ключа администратора 3. Персонализация с использованием ключа администратора
1. Доступ пользователя по паролю. 2. Использование пароля цифровой подписи. 3. Доступ администратора по паролю.	1. Настройте профиль персонализации с поддержкой цифровой подписи. 2. Используйте настроенный профиль для персонализации электронного ключа JaCarta.	См. разделы: 1. Настройки для использования цифровой подписи 2. Персонализация с настройками цифровой подписи
1. Доступ пользователя по паролю. 2. Использование пароля цифровой подписи. 3. Доступ администратора с использованием ключа администратора.	1. Создайте ключ администратора. 2. Настройте профиль персонализации с поддержкой цифровой подписи и задайте в нем необходимость использования ключа администратора. 3. Используйте настроенный профиль и ключ администратора для персонализации электронного ключа JaCarta.	См. разделы: 1. Ключ администратора 2. Настройки для использования цифровой подписи 3. Настройки для персонализации с использованием ключа администратора 4. Персонализация с настройками цифровой подписи 5. Персонализация с использованием

Возможный сценарий	Необходимые действия	Ссылки на разделы
		ключа администратора

Примечание:

Сценарии с использованием биометрических настроек представлены в документе *Использование JaCarta для биометрической аутентификации в среде Windows*.

Ключ администратора

Ключ администратора представляет собой инструмент для доступа на уровне администратора к электронным ключам JaCarta пользователей. Для создания ключа администратора используется ПО IDProtect Admin, которое не входит в состав JC-Client. Описание состава ПО IDProtect Admin и обзор входящих в него утилит представлены в разделах «Состав IDProtect Admin» и «Обзор утилит в составе IDProtect Admin» соответственно.

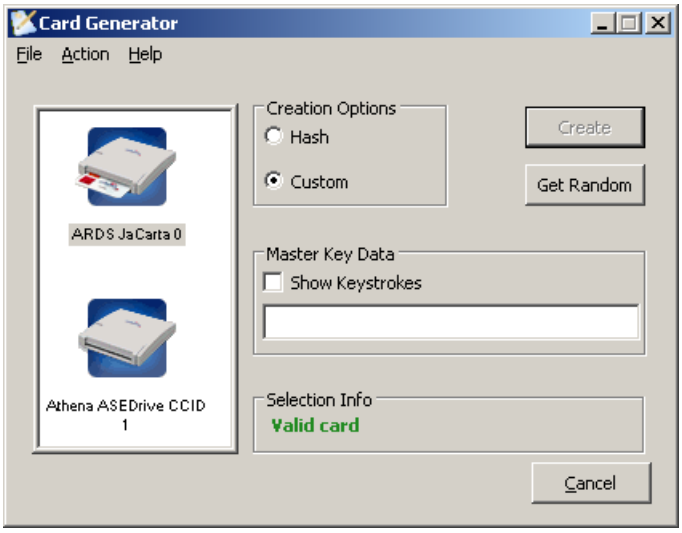
Примечание:

ПО IDProtect Admin не является необходимым для управления электронными ключами JaCarta пользователей. При любом упоминании в настоящем руководстве подразумевается, что данное ПО уже установлено на рабочей станции администратора.

Для того чтобы создать ключ администратора.

1. Персонализируйте электронный ключ JaCarta с помощью утилиты JaCarta Format (см. «Персонализация»).
2. Запустите утилиту Card Generator.
3. Подключите персонализированный электронный ключ JaCarta, который вы хотите сделать ключом администратора.

   Если электронный ключ JaCarta подходит для создания ключа администратора, в области **Selection Info** (Информация об электронном ключе) будет отображаться **Valid Card** (Подходящий электронный ключ), как на изображении ниже.

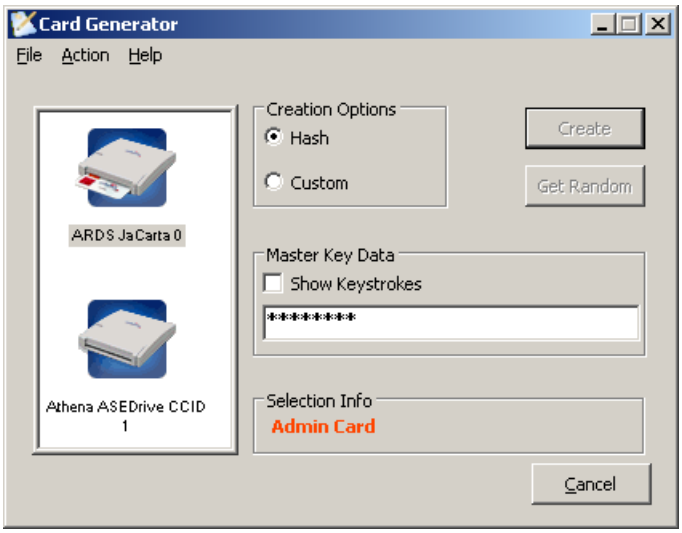


4. В области **Creation Options** (Параметры создания) выберите **Hash** (Хеш) или **Custom** (Произвольный).
   - Если вы выбрали **Hash** (Хеш), в поле **Master Key Data** (Мастер-ключ) введите значение, хеш которого будет использоваться для создания ключа администратора (это может быть любое значение).
   - Если вы выбрали **Custom** (Произвольный), в поле **Master Key Data** (Мастер-ключ) введите 16 байт данных в шестнадцатеричном формате или нажмите **Get Random** (Сгенерировать).
5. Нажмите **Create** (Создать).
6. Подтвердите уровень доступа пользователя, введя пароль пользователя JaCarta и/или приложив палец к сканеру отпечатков.

После успешного создания ключа администратора, отобразится следующее сообщение.

7. Нажмите **OK** для завершения процедуры.

   Поле **Selection Info** (Информация об электронном ключе) примет значение **Admin Card** (Ключ администратора).



Теперь ключ администратора можно использовать при персонализации электронных ключей JaCarta, а также для их разблокировки, если возникнет такая необходимость (см. «Персонализация с использованием ключа администратора» и «Разблокировка с использованием ключа администратора»).

Операции с сертификатами в памяти электронных ключей JaCarta

JC-Client поддерживает работу с сертификатами стандарта X.509. В памяти электронных ключей JaCarta можно хранить как сертификаты открытого ключа (файлы имеют расширение .cer), так и сертификаты, содержащие пару открытого и закрытого ключа (файлы имеют расширение .p12 и .pfx). В последнем случае, если сертификат защищен паролем, его необходимо будет ввести во время процедуры импортирования сертификата. Также можно задать сертификат по умолчанию (если в памяти электронного ключа JaCarta имеется несколько сертификатов) или удалить сертификат, хранящийся в памяти электронного ключа JaCarta.

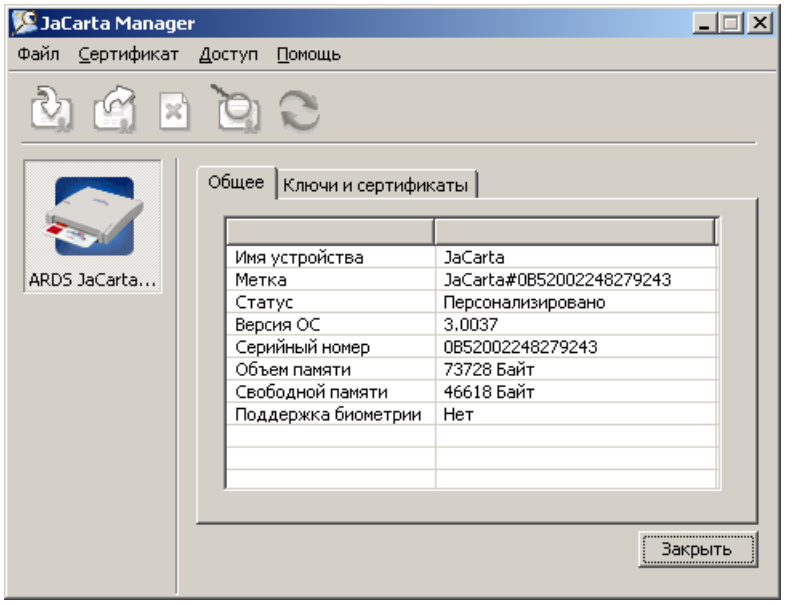
Для работы с сертификатами используется утилита JaCarta Manager. Все операции, связанные с сертификатами, требуют уровня доступа пользователя.

Просмотр сертификатов в памяти JaCarta

Чтобы просмотреть сертификат, хранящийся в памяти электронного ключа JaCarta.

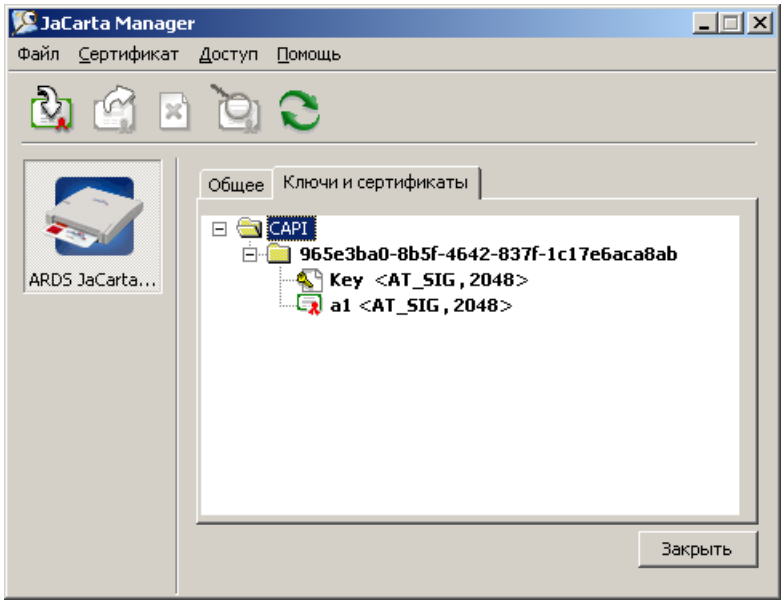
1. Выберите **Пуск > Все программы > JC-Client > JaCarta Manager**.

   Отобразится основное окно утилиты.



2. Выберите вкладку **Ключи и сертификаты**.
3. В зависимости от настроенных параметров доступа введите пароль пользователя и/или приложите палец к сканеру отпечатков.

Отобразится вкладка **Ключи и сертификаты**.



4. Выберите сертификат, информацию о котором необходимо посмотреть, и щелкните на кнопке  .

   Отобразится окно с информацией о сертификате.

Импорт сертификата в память электронного ключа

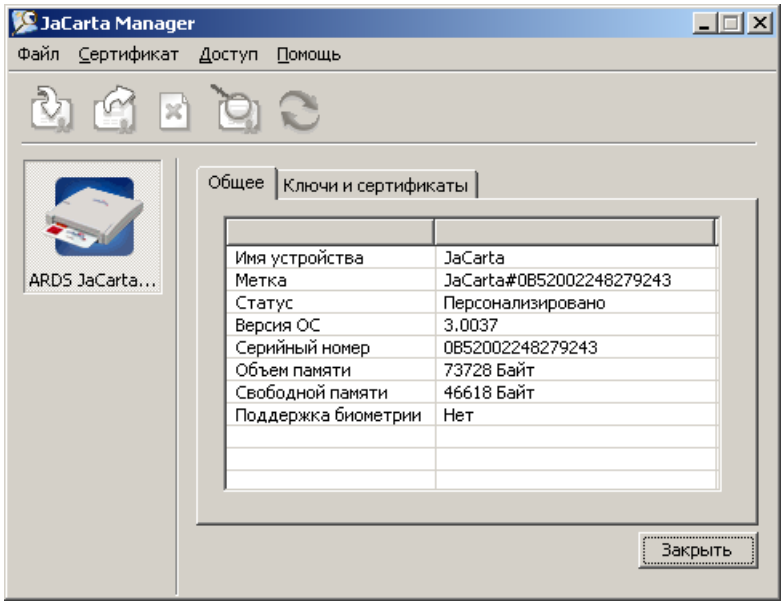
Чтобы импортировать сертификат, выполните следующие действия.

Примечание:

> Если при импорте сертификата (.cer) с помощью утилиты JC-Client Manager в памяти электронного ключа находится тот же открытый ключ, что и в файле сертификата, данный сертификат импортируется в контейнер с закрытым ключом, соответствующим совпадающему открытому ключу.

1. Выберите **Пуск > Все программы > JC-Client > JaCarta Manager**.

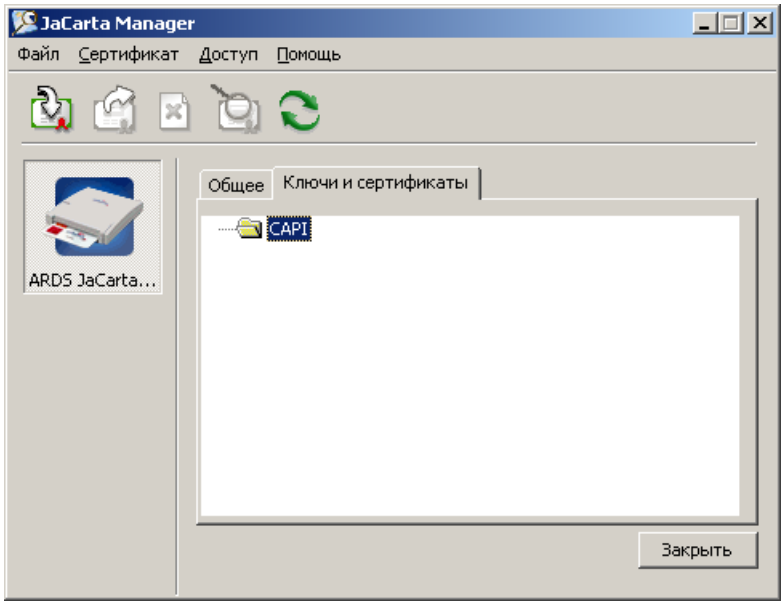
   Отобразится окно утилиты.



2. Выберите вкладку **Ключи и сертификаты**.

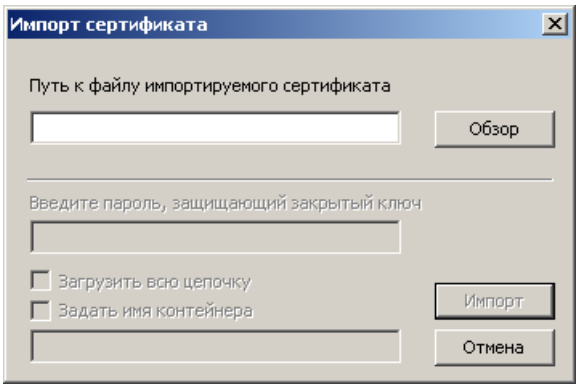
3. В зависимости от настроенных параметров доступа введите пароль пользователя и/или приложите палец к сканеру отпечатков пальцев.

   Отобразится вкладка **Ключи и сертификаты**.

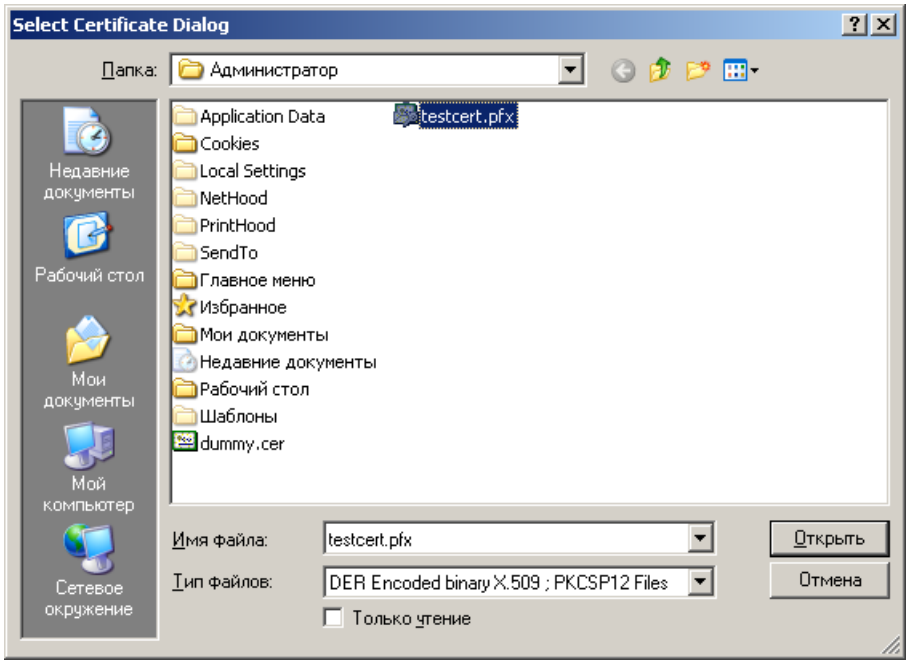


4. Выберите контейнер и щелкните на кнопке  .

   Отобразится следующее окно.

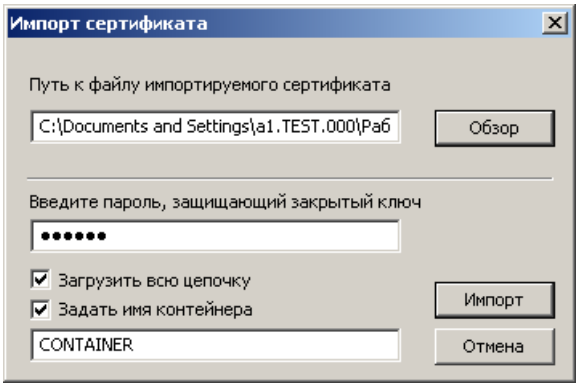


5. Нажмите **Обзор** и выберите сертификат, который вы хотите импортировать в память электронного ключа JaCarta (см. изображение ниже).



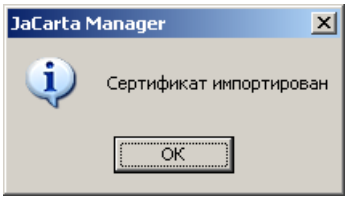
6. Нажмите **Открыть**.

   Если существует возможность загрузить цепочку сертификатов и/или если в сертификат включен закрытый ключ, окно **Импорт сертификата** примет следующий вид.



7. Введите пароль закрытого ключа сертификата в поле **Введите пароль, защищающий закрытый ключ**.
8. Если необходимо, установите флажок **Загрузить всю цепочку**.
9. Установите флажок **Задать имя контейнера** и в поле ниже введите имя контейнера сертификата и закрытого ключа (в противном случае имя будет сгенерировано автоматически).
10. Нажмите **Импорт**.
11. В зависимости от настроенных параметров доступа введите пароль пользователя и/или приложите палец к сканеру отпечатков пальцев.

    После успешного импортирования сертификата отобразится следующее сообщение.



12. Нажмите **ОК**.

    Сертификат импортирован в память электронного ключа JaCarta.

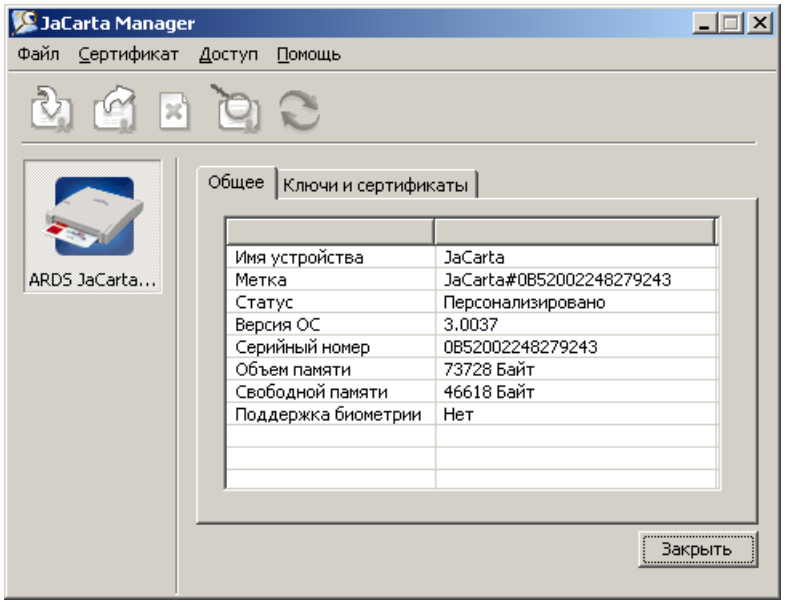
Экспорт сертификатов из памяти электронного ключа

Из памяти электронных ключей JaCarta можно экспортировать сертификаты без закрытого ключа (.cer).

Чтобы экспортировать сертификат из памяти электронного ключа JaCarta.

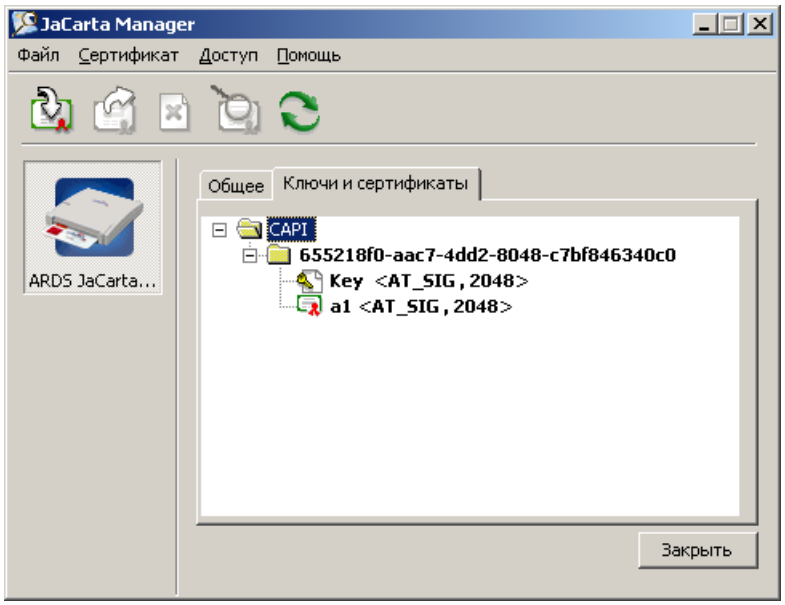
1. Выберите **Пуск > Все программы > JC-Client > JaCarta Manager**.

   Отобразится основное окно утилиты.



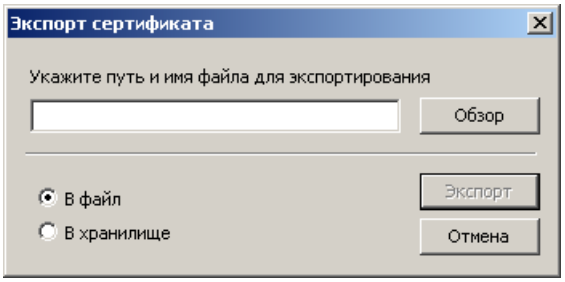
2. Выберите вкладку **Ключи и сертификаты**.
3. В зависимости от настроенных параметров доступа введите пароль пользователя и/или приложите палец к сканеру отпечатков пальцев.

   Отобразится вкладка **Ключи и сертификаты.**



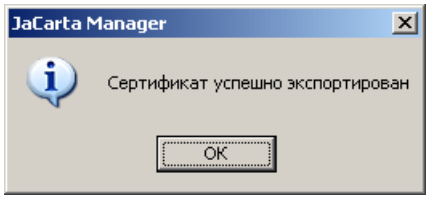
4. Выберите сертификат, который необходимо экспортировать, и щелкните на кнопке  .

Отобразится следующее окно.



5. Выберите пункт **В файл** или **В хранилище**.
   - Если вы выбрали **В файл**, введите необходимые данные в поле **Укажите путь и имя файла для экспортирования**. Для этой цели также можно воспользоваться кнопкой **Обзор**.
   - Если вы выбрали **В хранилище**, переходите к следующему шагу процедуры.
6. Нажмите **Экспорт**.

   Отобразится сообщение об успешном экспорте сертификата.



7. Нажмите **ОК** для завершения процедуры.

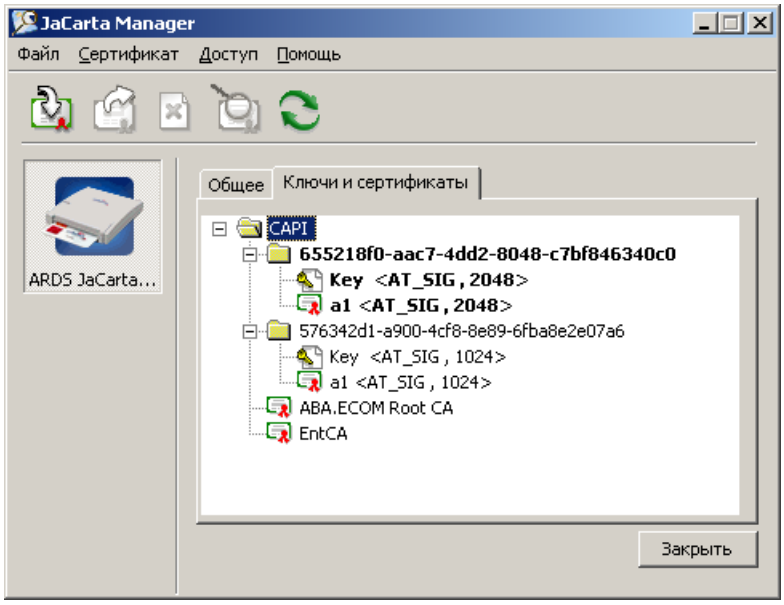
Выбор сертификата по умолчанию

Если в памяти электронного ключа JaCarta хранится несколько контейнеров (пар сертификата и закрытого ключа), для входа в Windows используется сертификат, который содержится в контейнере по умолчанию. Для назначения контейнера по умолчанию используется утилита JaCarta Manager.

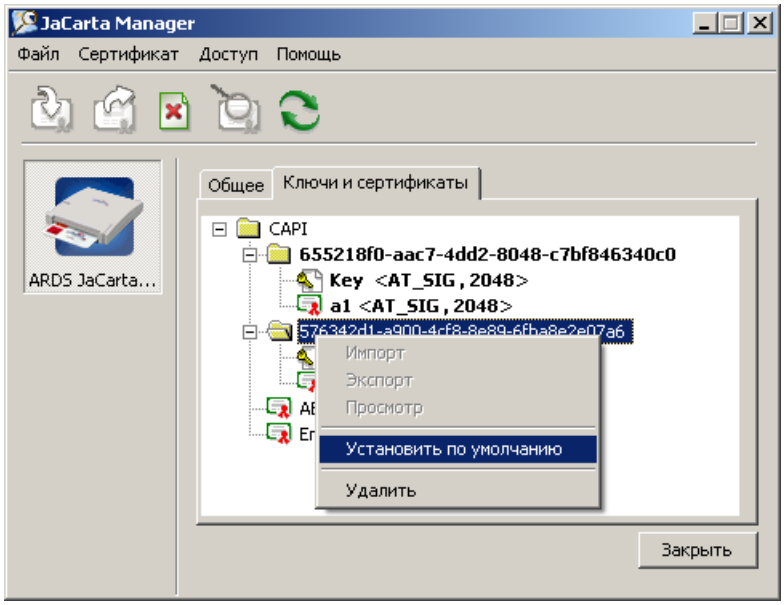
Чтобы установить контейнер в качестве контейнера по умолчанию, выполните следующие действия.

1. Выберите **Пуск > Все программы > JC-Client > JaCarta Manager**.
2. Выберите вкладку **Ключи и сертификаты**.
3. В зависимости от настроенных параметров доступа введите пароль пользователя и/или приложите палец к сканеру отпечатков пальцев.

Откроется вкладка **Ключи и сертификаты**.



4. Разверните ветвь **CAPI** и выберите контейнер, который необходимо установить в качестве контейнера по умолчанию.
5. Щелкните на выбранном контейнере правой кнопкой мыши и выберите **Установить по умолчанию**, как показано на изображении ниже.



6. В зависимости от настроенных параметров доступа введите пароль пользователя и/или приложите палец к сканеру отпечатков пальцев.

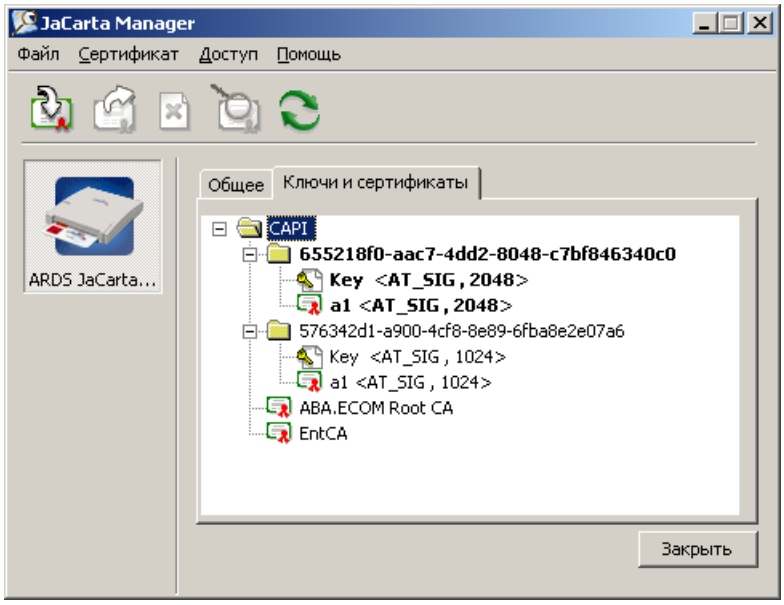
   По завершении процедуры выбранный контейнер будет помечен как контейнер по умолчанию.

Удаление сертификата из памяти электронного ключа JaCarta

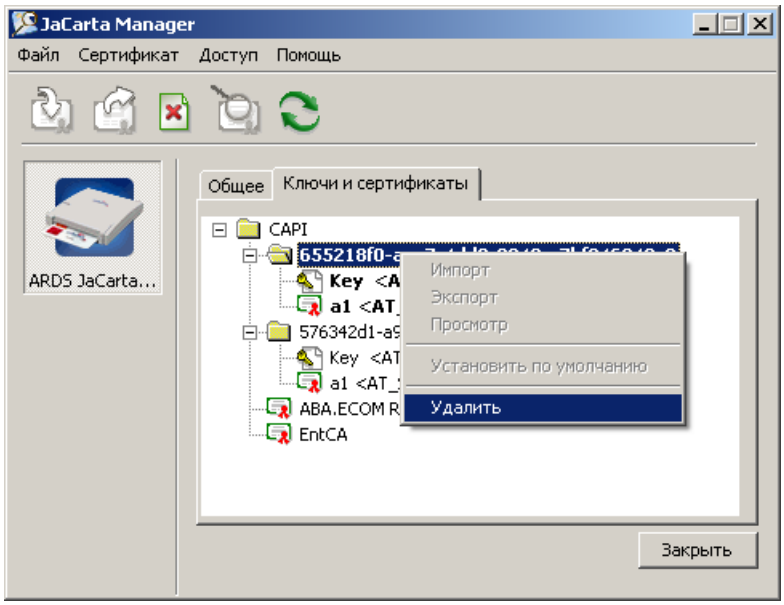
Чтобы удалить сертификат из памяти электронного ключа JaCarta, выполните следующие действия.

1. Выберите **Пуск > Все программы > JC-Client > JaCarta Manager**.
2. Выберите вкладку **Ключи и сертификаты**.
3. В зависимости от настроенных параметров доступа введите пароль пользователя и/или приложите палец к сканеру отпечатков пальцев.

Откроется вкладка **Ключи и сертификаты**.



4. Разверните ветвь **CAPI** и выберите сертификат, который необходимо удалить, как показано на рисунке ниже.

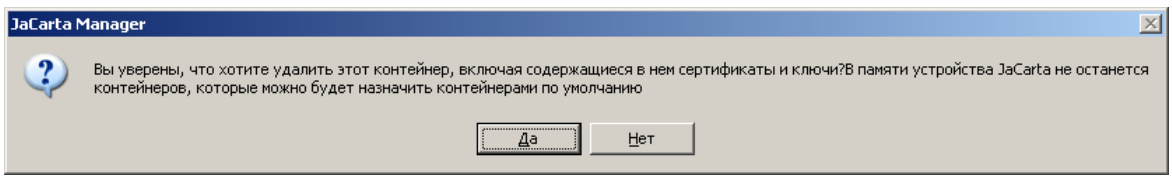


Примечание:

Если сертификат находится в контейнере, необходимо отметить этот контейнер.

5. Щелкните на выбранном сертификате или контейнере правой кнопкой мыши и выберите **Удалить**.

   Появится следующее диалоговое окно.



6. Нажмите **Да**, чтобы удалить выбранный сертификат или контейнер.
7. В зависимости от настроенных параметров доступа введите пароль пользователя и/или приложите палец к сканеру отпечатков пальцев.

По завершении процедуры выбранный сертификат или контейнер будет удален из памяти электронного ключа JaCarta.

Настройка параметров хранения сертификатов в хранилище

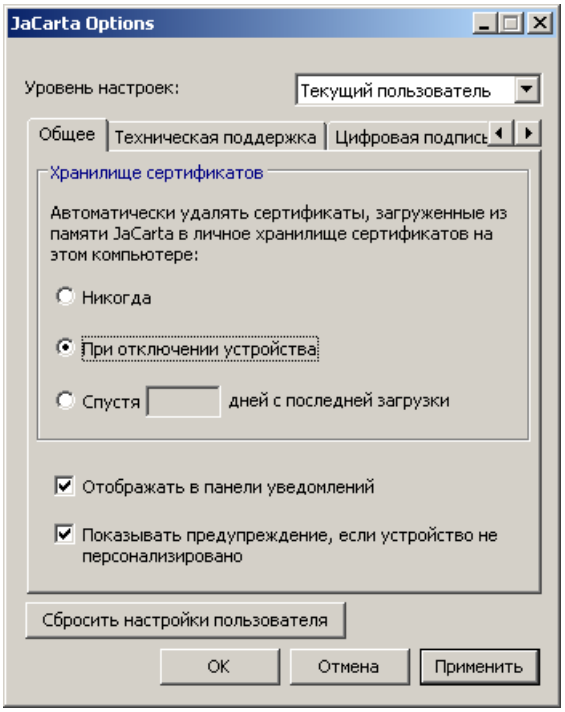
После подсоединения электронного ключа JaCarta к компьютеру, ПО JC-Client автоматически загружает сертификаты, содержащиеся в памяти устройства, в хранилище сертификатов текущего пользователя.

После того как пользователь отсоединяет электронный ключ JaCarta от компьютера, сертификаты, которые были загружены при подключении устройства, удаляются из личного хранилища сертификатов. Вы можете изменить поведение системы, используя утилиту JaCarta Options. Изменения, сделанные с помощью этой утилиты, могут применяться как на уровне текущего пользователя, так и на уровне данной рабочей станции.

Чтобы настроить параметра хранения сертификатов в личном хранилище.

1. Выберите **Пуск > Все программы > JC-Client > JaCarta Options**.

   Отобразится окно утилиты.



   - Если вы хотите сделать изменения параметров на уровне текущего пользователя.

     В списке **Уровень настроек** оставьте выбранным пункт **Текущий пользователь**.

   - Если вы хотите сделать изменения параметров на уровне данной рабочей станции.

     В списке **Уровень настроек** выберете пункт **Локальный компьютер** и установите флажок **Сбросить настройки пользователей**.

2. В области **Хранилище сертификатов** выберите один из пунктов, руководствуясь приведенной ниже таблицей.

Настройка	Описание
Никогда	Сертификаты, загруженные из памяти электронного ключа JaCarta при подключении, не удаляются после отключения устройства. Это настройка по умолчанию.
При отключении JaCarta	Сертификаты, загруженные из памяти электронного ключа JaCarta при подключении, удаляются после отключения устройства. Данная настройка применима только к сертификатам, которые загружаются в личное хранилище сертификатов.
Спустя X **дней после с**	Сертификаты, загруженные из памяти электронного ключа JaCarta при

Настройка	Описание
последней загрузки	подключении, удаляются из личного хранилища спустя X дней после отключения устройства (число дней необходимо указать в соответствующем поле).

3. Нажмите **OK**.

Более подробное описание утилиты JaCarta Options представлено в разделе «JaCarta Options».

Настройки, доступные после персонализации

Некоторые параметры использования электронных ключей JaCarta можно изменить, не прибегая к повторной персонализации (см. таблицу ниже).

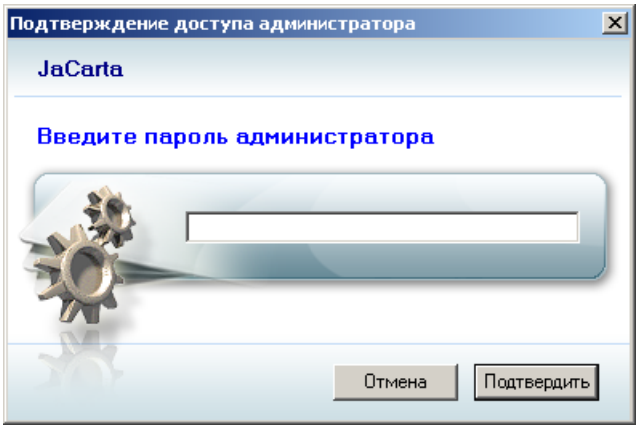
Параметр	Описание	Требуемый уровень доступа
Метка	Возможность смены метки электронного ключа JaCarta. **Используемые утилиты:** JaCarta Format JaCarta Manager	Администратор/ Пользователь
Сменить пароль во время следующего сеанса работы с электронным ключом JaCarta	Пользователь должен изменить пароль во время следующего использования электронного ключа JaCarta. Другие действия, требующие пароля пользователя, будут ему недоступны. **Используемые утилиты:** JaCarta Format	Администратор
Сменить пароль пользователя после текущего сеанса работы с электронным ключом JaCarta	Когда пользователь аутентифицируется посредством ввода пароля пользователя (или администратор после персонализации вводит первичный пароль пользователя для установки дополнительных настроек), он может установить соответствующий флажок в окне ввода пароля. В этом случае пользователь должен будет сменить пароль пользователя во время следующего сеанса работы с электронным ключом JaCarta. Другие действия, требующие пароля пользователя, будут ему недоступны. **Используемые утилиты:** JaCarta Manager	Пользователь
Сменить пароль после разблокировки	Пользователь должен изменить пароль после разблокировки электронного ключа JaCarta. Другие действия, требующие пароля пользователя, будут ему недоступны. **Используемые утилиты:** JaCarta Format	Администратор
Сохранение пароля в течение заданного количества времени	Время (минуты), через которое авторизовавшийся пользователь должен подтвердить уровень своего доступа, чтобы продолжить работу с электронным ключом JaCarta. **Используемые утилиты:** JaCarta Format	Администратор
Обязательное изменение пароля пользователя через заданное количество дней	Время (дни), через которое пользователь должен изменить пароль. По истечении данного срока любые другие действия, требующие пароля пользователя, будут ему недоступны. Отсчет дней ведется с момента установки данной настройки. **Используемые утилиты:** JaCarta Format	Администратор
Пароль пользователя	Пользователь может самостоятельно изменить свой пароль пользователя. **Используемые утилиты:** JaCarta PINTool	Пользователь
Пароль администратора	Администратор может самостоятельно сменить пароль администратора. **Используемые утилиты:** JaCarta Format JaCarta Admin PINTool	Администратор

Параметр	Описание	Требуемый уровень доступа
Пароль цифровой подписи	При условии что электронный ключ JaCarta был персонализирован с поддержкой цифровой подписи, пользователь может самостоятельно изменить пароль цифровой подписи. **Используемые утилиты:** JaCarta PINTool	Пользователь
Параметры хранения сертификатов в хранилище	Можно изменить параметры хранения сертификатов, которые загружаются в личное хранилище при подсоединении к компьютеру электронных ключей JaCarta. Данная процедура описана в разделе «Настройка параметров хранения сертификатов в хранилище». **Используемые утилиты:** JaCarta Options	Любой
Установка сертификата по умолчанию	Если в памяти электронного ключа JaCarta хранится несколько сертификатов, можно выбрать сертификат, который будет использоваться по умолчанию. **Используемые утилиты:** JaCarta Manager	Пользователь
Синхронизация пароля цифровой подписи и пароля пользователя	При условии что электронный ключ JaCarta был персонализирован с поддержкой цифровой подписи, можно синхронизировать пароль цифровой подписи с паролем пользователя, чтобы они принимали одни и те же значения. Для этого изначально пароль пользователя и пароль цифровой подписи должны совпадать. **Используемые утилиты:** JaCarta Options	Любой

Процедуры доступа и изменения настроек электронных ключей JaCarta на уровне администратора описаны далее.

Доступ с использованием пароля администратора

Если функции администратора на электронном ключе JaCarta доступны после предъявления пароля администратора, при необходимости подтверждения соответствующих прав во время разблокировки отображается следующее окно.



В этом случае вы должны ввести пароль администратора и нажать **Подтвердить**, после чего продолжить выполнение необходимой процедуры.

Доступ с использованием ключа администратора

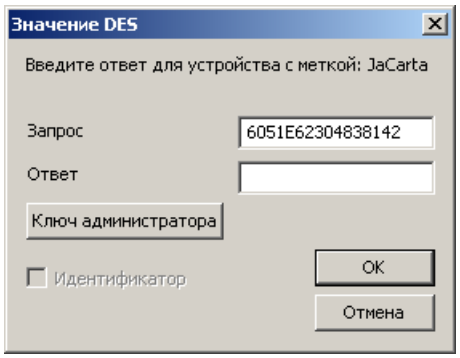
Если электронный ключ JaCarta был персонализирован с использованием ключа администратора, при необходимости осуществления действий с правами администратора возможно как при непосредственном участии администратора, так и в удаленном режиме.

Примечание:

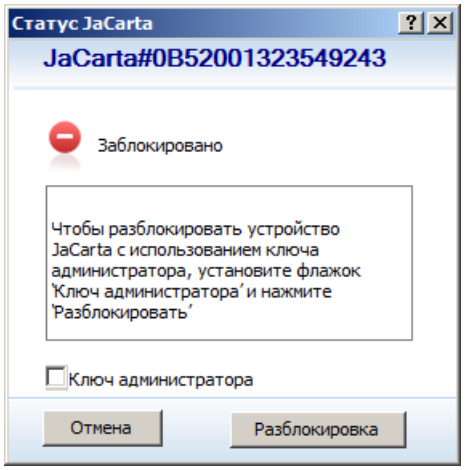
Если доступ происходит в присутствии администратора, к рабочей станции необходимо подсоединить как электронный ключ JaCarta пользователя, так и электронный ключ администратора.

При непосредственном участии администратора

Если вы пытаетесь выполнить действие, которое требует уровня доступа администратора, отобразится одно из следующих окон.



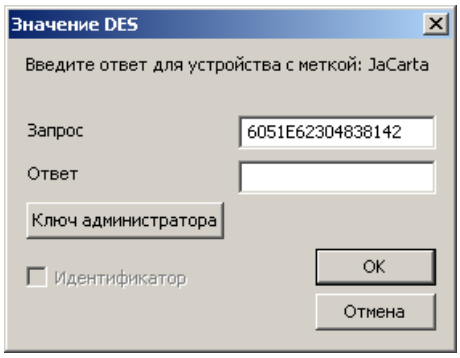
1. Подсоедините ключ администратора к компьютеру, к которому подсоединен электронный ключ пользователя.
2. Нажмите **Ключ администратора** и продолжите выполнение процедуры.



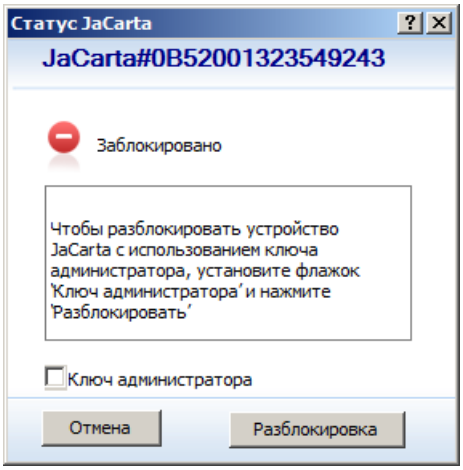
1. Подсоедините ключ администратора к рабочей станции
2. Установите флажок **Ключ администратора**.
3. Нажмите соответствующую кнопку (в данном примере **Разблокировка**) и продолжите выполнение процедуры.

В удаленном режиме

Если пользователю необходимо выполнить действие, которое требует уровня доступа администратора, на его экране отобразится одно из следующих окон.



В данном случае пользователь должен перейти к выполнению процедуры, представленной ниже.

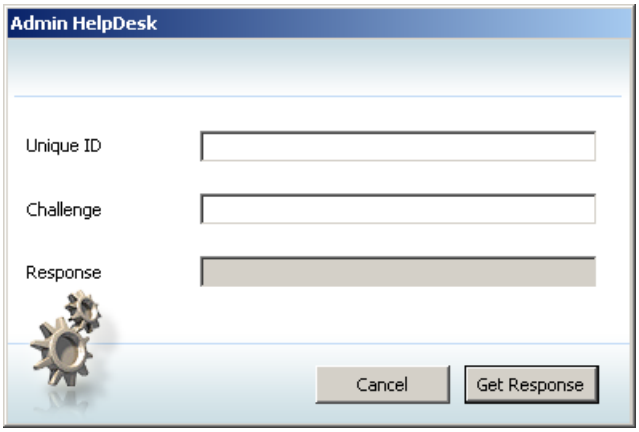


В данном случае пользователь должен оставить пункт **Ключ администратора** неотмеченным и нажать **Разблокировка.** Отобразится окно с данными запроса, после чего пользователь должен перейти к выполнению процедуры, представленной ниже.

Для того чтобы продолжить действие на уровне доступа администратора.

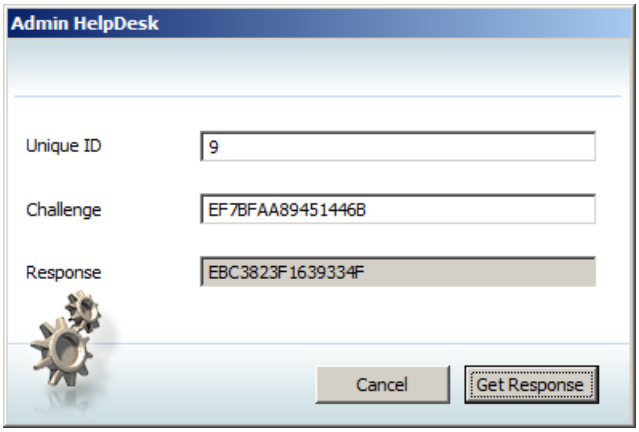
1. Пользователь должен сообщить администратору данные из поля **Запрос** и идентификатор, сообщенный ему после персонализации электронного ключа JaCarta администратором.
2. Администратор должен подсоединить ключ администратора, который применялся при персонализации электронного ключа пользователя, к своей рабочей станции и запустить утилиту Admin HelpDesk.

   На экране администратора после проверки данных доступа для ключа администратора отобразится следующее окно.

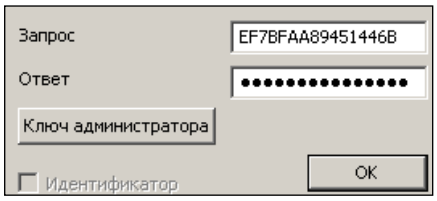


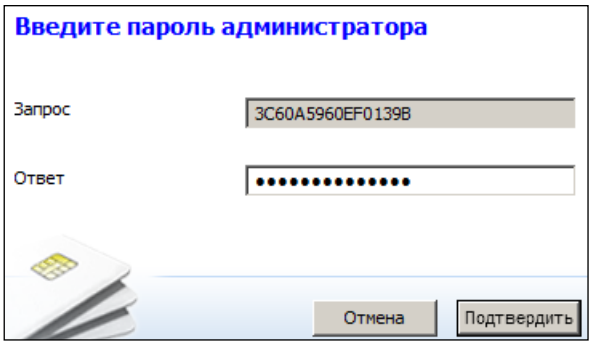
3. В поле **Unique ID** (Идентификатор) и **Challenge** (Запрос) администратор должен соответственно ввести идентификатор и запрос, сообщенные пользователем, после чего нажать кнопку **Get Response** (Получить ответ).

Окно утилиты Admin HelpDesk на рабочей станции администратора будет выглядеть следующим образом.



4. Администратор должен сообщить пользователю данные из поля **Response** (Ответ).
5. Пользователь на своей рабочей станции должен ввести ответ, сообщенный администратором в поле **Ответ**, как показано на изображениях ниже.

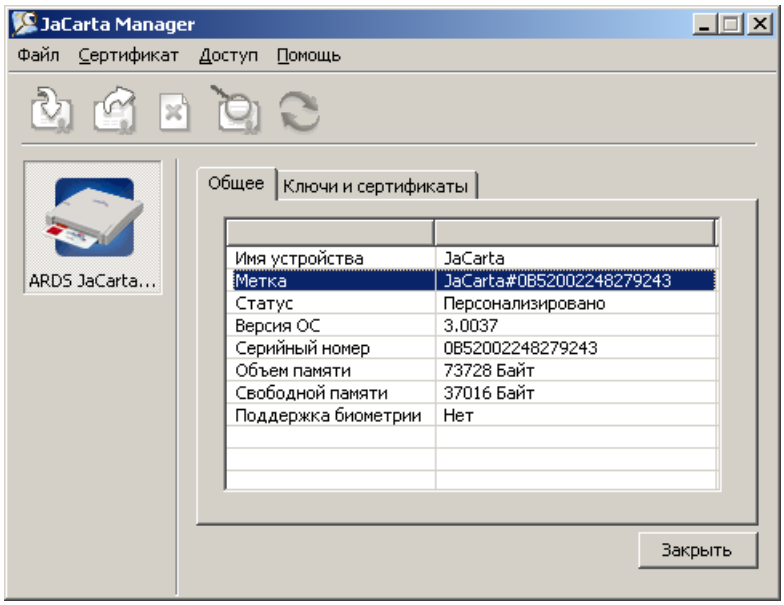




6. После того как ответ введен, пользователь должен подтвердить ввод и продолжить выполнение необходимой процедуры (например, назначить новый пароль пользователя).

Смена метки электронного ключа JaCarta

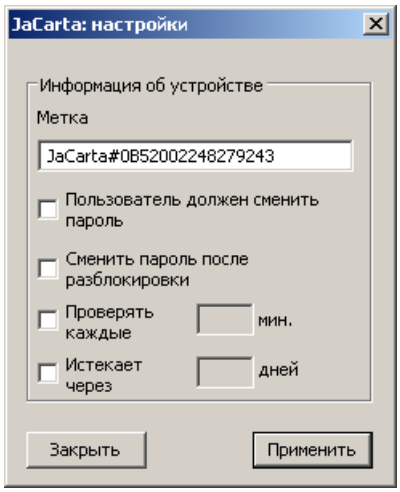
Значение **Метка** отображается в главном окне утилит JaCarta Format и JaCarta Manager. Если данное значение не установлено явно в процессе персонализации, оно принимает значение по умолчанию: «JaCarta#Серийный номер» (см. изображение ниже).



Чтобы изменить значение метки после персонализации.

1. Подсоедините к рабочей станции электронный ключ JaCarta.
2. Выберите **Пуск > Все программы > JC-Client > JaCarta Format**.
3. В панели управления выберите **Файл > Настройки администратора**.

   Отобразится следующее окно.



4. В поле **Метка устройства** введите значение новой метки и нажмите **Применить**.

Примечание

Допускается вводить только символы из набора ASCII.

5. В зависимости от настроенных параметров доступа введите пароль администратора или используйте ключ администратора.

   Метка изменена.

Настройки, связанные с использованием пароля пользователя

После персонализации электронного ключа JaCarta возможно изменить некоторые настройки, связанные с использованием пароля пользователя. Список этих параметров приведен в таблице ниже.

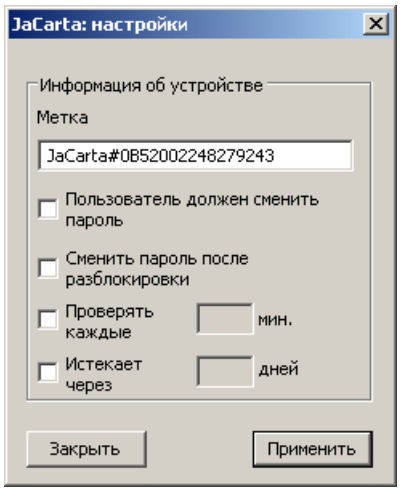
Параметр	Описание
Пользователь должен сменить пароль	Если данный флажок установлен, пользователь должен будет сменить пароль при следующем сеансе работы с электронным ключом JaCarta. В противном случае все операции с электронным ключом, требующие пользовательского пароля, будут недоступны. Пароль можно будет изменить во время входа в систему.
Сменить пароль после разблокировки	В случае разблокировки электронного ключа JaCarta администратором задается новое значение пользовательского пароля. Установка данного флажка потребует от пользователя снова сменить пользовательский пароль после разблокировки.
Проверять каждые … мин.	Если флажок установлен, значение в поле **мин.** определяет, через сколько минут после подтверждения доступа пользователь должен будет снова подтвердить свой доступ.
Истекает через … дней	Если флажок установлен, значение в поле **дней** определяет, через сколько дней пользователь должен будет сменить пароль.

Чтобы изменить параметры использования пароля пользователя.

1. Подсоедините к рабочей станции электронный ключ JaCarta.
2. Выберите **Пуск > Все программы > JC-Client > JaCarta Format**.

3. В панели управления выберите **Файл > Настройки администратора**.

   Отобразится следующее окно.



4. Внесите изменения, руководствуясь таблицей, приведенной выше в данном подразделе, и нажмите **Применить**.
5. В зависимости от настроенных параметров доступа введите пароль администратора или используйте ключ администратора.

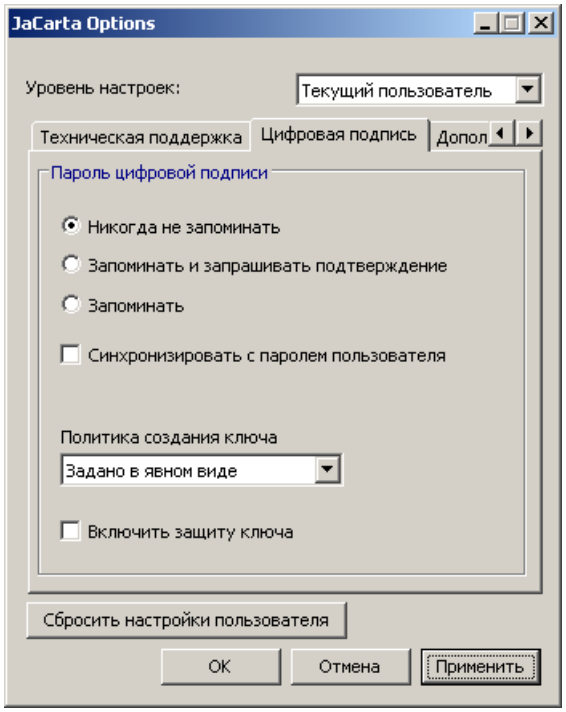
Синхронизация пароля пользователя с паролем цифровой подписи

Если в процессе персонализации электронного ключа JaCarta была задана поддержка цифровой подписи, то пароль цифровой подписи можно синхронизировать с паролем пользователя, чтобы они принимали одно и то же значение. Перед синхронизацией необходимо, чтобы пароль пользователя совпадал с паролем цифровой подписи. Если пароль администратора совпадает с паролем разблокировки цифровой подписи, эти пароли также будут синхронизированы.

Чтобы синхронизировать пароль пользователя и пароль цифровой подписи.

1. Выберите **Пуск > Все программы > JC-Client > JaCarta Options**.
2. Выберите вкладку **Цифровая подпись**.

   Окно примет следующий вид.



- Если вы хотите установить настройки для текущего пользователя рабочей станции, в меню **Уровень настроек** оставьте выбранным пункт **Текущий пользователь**.
- Если вы хотите установить настройки на уровне локальной машины, в меню **Уровень настроек** выберите пункт **Локальный компьютер** и установите флажок **Сбросить настройки пользователей**.

3. Установите флажок **Синхронизировать с паролем пользователя**. Если данный флажок установлен, не вносите никаких изменений.
4. Нажмите **ОК**.

При условии что пароль цифровой подписи и пароль пользователя изначально совпадают, изменение одного из них (например, с помощью утилиты JaCarta PINTool) приведет к изменению второго, таким образом, оба эти пароля будут принимать одно и то же значение.

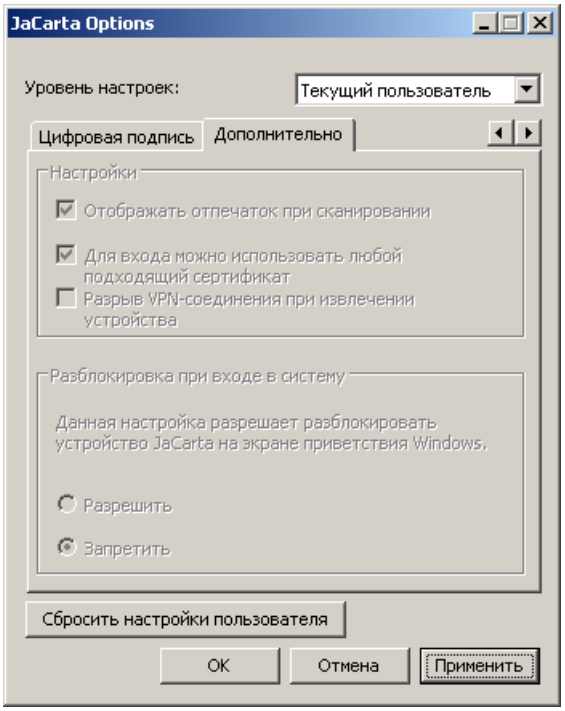
Возможность разблокировки из окна приветствия Windows

Пароль пользователя JaCarta можно разблокировать непосредственно в окне приветствия Windows.

Чтобы разрешить или запретить возможность разблокировки пароля пользователя из окна приветствия Windows.

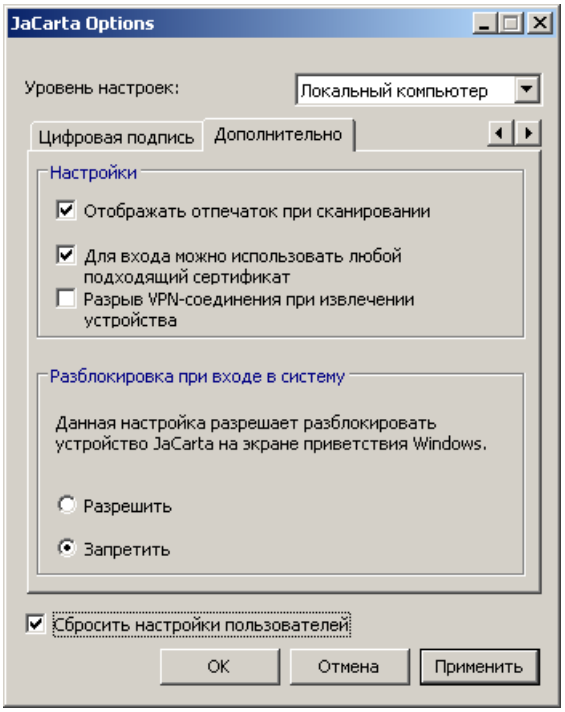
1. Выберите **Пуск > Все программы > JC-Client > JaCarta Options.**
2. Выберите вкладку **Дополнительно**.

   Окно утилиты примет следующий вид.



3. В меню **Уровень настроек** выберите пункт **Локальный компьютер** и установите флажок **Сбросить настройки пользователей**.

Окно утилиты примет следующий вид.



4. В секции **Разблокировка при входе в систему** выберите **Разрешить**, чтобы разрешить разблокировку пароля пользователя из окна приветствия Windows. Чтобы запретить такую возможность, выберите **Запретить**.

Примечание:

Если такой способ разблокировки запрещен, администратор должен будет разблокировать пароль пользователя под своей учетной записью или на другой рабочей станции.

5. Нажмите **OK**.

Более подробно о способах разблокировки см. раздел «Разблокировка электронного ключа JaCarta» ниже.

Разблокировка электронного ключа JaCarta

Для разблокировки пароля пользователя необходим пароль администратора или ключ администратора (процедура разблокировки с использованием ключа администратора описана в разделе «Разблокировка с использованием ключа администратора»). Пароль пользователя также можно разблокировать из окна приветствия Windows.

Разблокировка пароля цифровой подписи требует пароля разблокировки цифровой подписи, и это можно сделать только из активного сеанса Windows.

Возможные сценарии разблокировки представлены в таблице ниже.

Тип доступа пользователя	Тип доступа администратора	Способ разблокировки
Пароль пользователя	Пароль администратора ИЛИ Ключ администратора	Из активного сеанса Windows Из окна приветствия Windows (если установлена соответствующая настройка)
Пароль цифровой подписи	Пароль разблокировки цифровой подписи	Из активного сеанса Windows

Разблокировка пароля пользователя

Возможны два сценария стандартной процедуры разблокировки пароля пользователя:

- Из активного сеанса Windows
- Из окна приветствия Windows

В последнем случае необходимо, чтобы с помощью утилиты JaCarta Options для данной рабочей станции была установлена соответствующая настройка (см. «Возможность разблокировки из окна приветствия Windows»). Также, процедура разблокировки из окна авторизации Windows различается в зависимости от операционной системы (Windows XP/Server 2003 или Windows Vista/Server 2008/7/8.1 Update 1/2012).

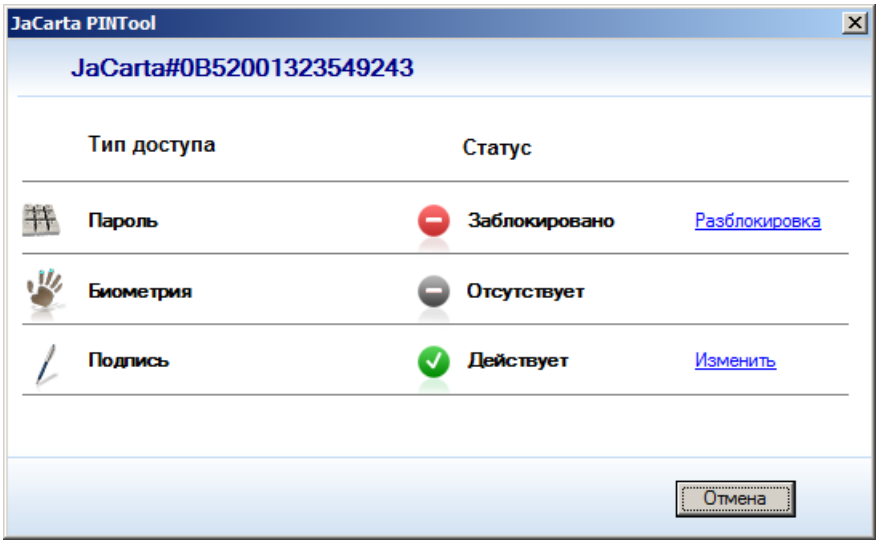
Примечание:

Сценарии разблокировки пароля пользователя с помощью ключа администратора представлены в разделе «Разблокировка с использованием ключа администратора».

Из активного сеанса Windows

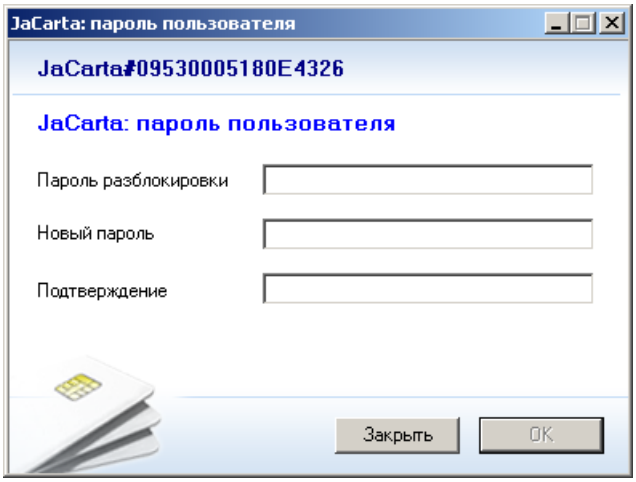
1. Подсоедините электронный ключ JaCarta с заблокированным паролем к компьютеру.
2. Выберите **Пуск > Все программы > JC-Client > JaCarta PINTool**.

Если пароль пользователя заблокирован, в поле **Статус** напротив значения **Пароль** будет значиться **Заблокировано**.



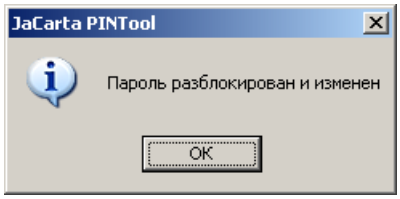
3. Щелкните на ссылке **Разблокировка**.

   Отобразится следующее окно.



4. В поле **Пароль разблокировки** введите пароль администратора.
5. В полях **Новый пароль** и **Подтверждение** пользователь должен ввести новый пароль пользователя и подтверждение соответственно.
6. Нажмите **OK**.

   Отобразится следующее сообщение.

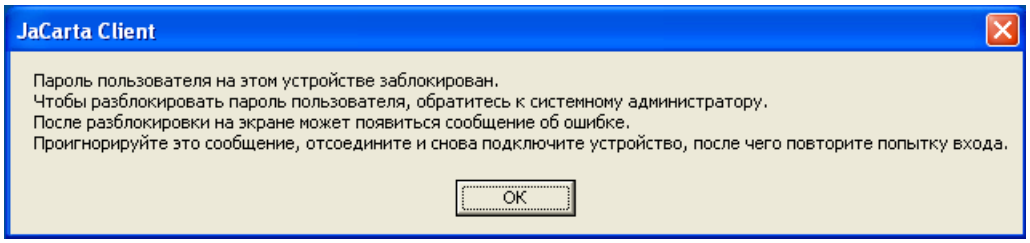


7. Нажмите **OK** для завершения процедуры.

   Если по каким-то причинам новый пароль пользователя вводил администратор, установите настройку, в соответствии с которой пользователь должен будет сменить пароль пользователя при следующем сеансе работы с электронным ключом JaCarta.

Из окна приветствия Windows XP/Server 2003

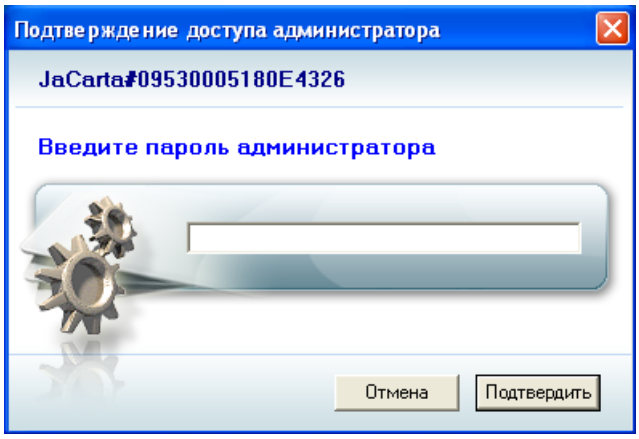
Если электронный ключ JaCarta заблокирован, в окне приветствия Windows отображается сообщение следующего вида.



Для того чтобы разблокировать пароль пользователя.

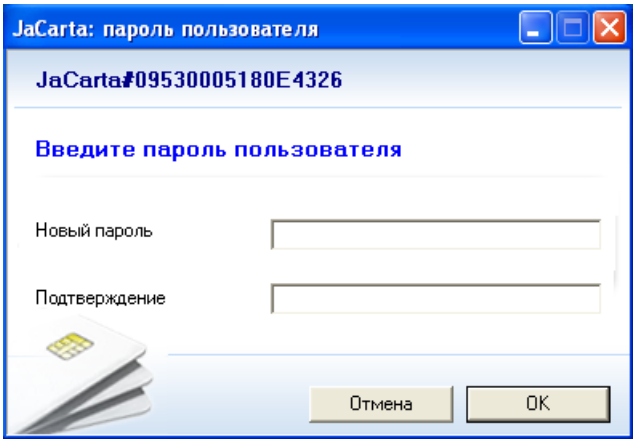
1. Нажмите **OK**.

   Отобразится окно ввода пароля администратора



2. Введите пароль администратора и нажмите **Подтвердить**.

   Отобразится следующее окно.



3. В полях **Новый пароль** и **Подтверждение** пользователь должен ввести новый пароль пользователя и подтверждение нового пароля соответственно. После этого необходимо нажать **OK**.

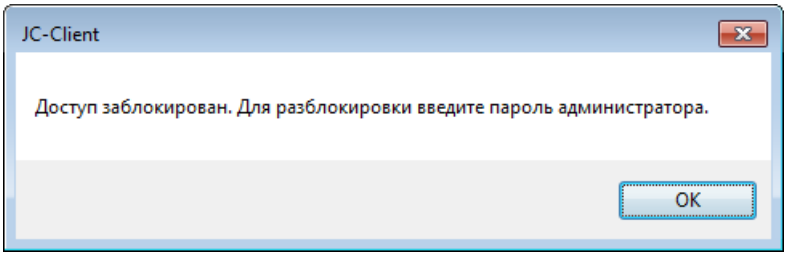
   Отобразится сообщение об ошибке.

4. Проигнорируйте сообщение и нажмите **OK**.

   Электронный ключ JaCarta разблокирован. Чтобы войти в систему отсоедините электронный JaCarta и подключите его снова.

Из окна приветствия Windows Vista/Server 2008/7/8.1 Update 1/2012

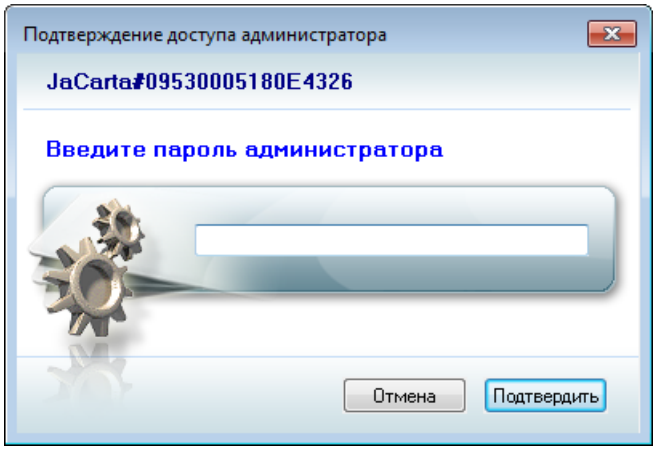
Если электронный ключ JaCarta заблокирован, на экране приветствия Windows отображается следующее сообщение.



Для того чтобы разблокировать пароль пользователя.

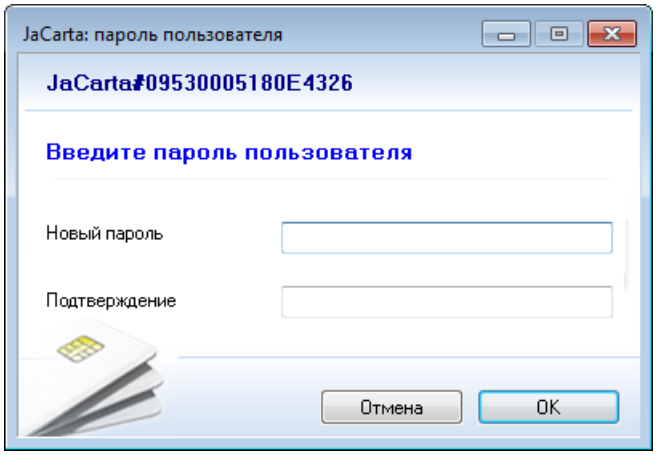
1. Нажмите **OK**.

   Отобразится окно ввода пароля администратора.



2. Введите пароль администратора и нажмите **Подтвердить**.

   Отобразится следующее окно.



3. В полях **Новый пароль** и **Подтверждение** пользователь должен ввести новый пароль пользователя и подтверждение нового пароля соответственно. После этого необходимо нажать **OK**.

   Отсоедините электронный ключ JaCarta и подключите его снова, чтобы осуществить вход в систему.

Разблокировка с использованием ключа администратора

Администратор может использовать ключ администратора, чтобы разблокировать пароль пользователя, если электронный ключ JaCarta был персонализирован с соответствующими параметрами (см. «Персонализация с использованием ключа администратора»). Если заблокированы оба способа, каждый из них надо разблокировать отдельно.

Существует два сценария разблокировки пароля пользователя использованием ключа администратора

- При непосредственном участии администратора
- В удаленном режиме

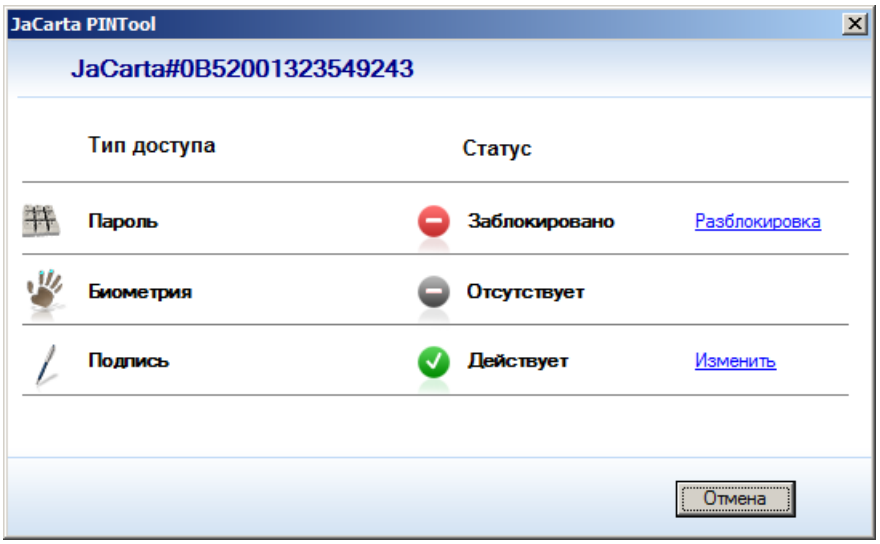
При непосредственном участии администратора

Для разблокировки с использованием ключа администратора при непосредственном участии администратора необходимо, чтобы на рабочей станции было доступно два считывателя смарт-карт.

Чтобы разблокировать пароль пользователя.

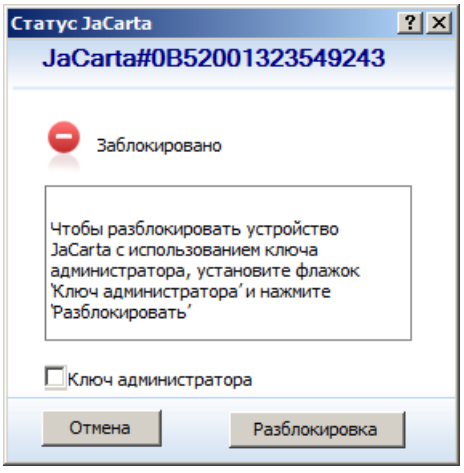
1. Подсоедините к компьютеру электронный ключ JaCarta с заблокированным паролем.
2. Запустите утилиту JaCarta PINTool.

   Если тип доступа пользователя заблокирован, в колонке **Состояние** напротив него отображается **Заблокировано**, как показано на изображении ниже.



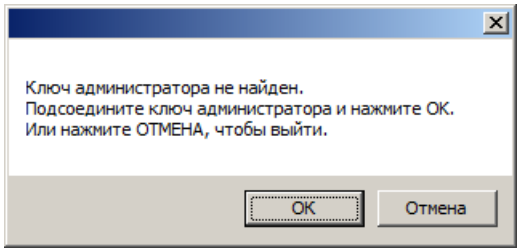
3. Для разблокировки доступа щелкните на ссылке **Разблокировка** напротив поля **Пароль**.

   Отобразится следующее окно.



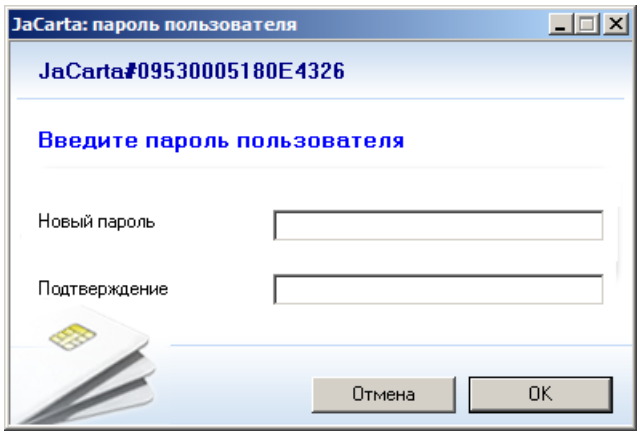
4. Установите флажок **Ключ администратора** и нажмите **Разблокировка**.

Если ключ администратора не подключен к рабочей станции, отобразится следующее окно.



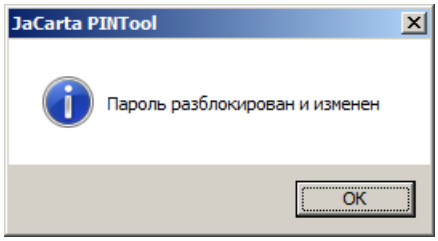
5. Подсоедините ключ администратора, нажмите **OK** и подтвердите данные доступа для подсоединенного ключа администратора.

   Отобразится следующее окно.



6. В полях **Новый пароль** и **Подтверждение** пользователь должен ввести новый пароль пользователя и подтверждение соответственно.

   Отобразится следующее сообщение.



7. Нажмите **OK** для завершения процедуры.

   Если по каким-то причинам новый пароль пользователя вводил администратор, установите настройку, в соответствии с которой пользователь должен будет сменить пароль пользователя при следующем сеансе работы с электронным ключом JaCarta.

В удаленном режиме

Если для персонализации электронного ключа JaCarta был использован ключ администратора, пароль пользователя можно разблокировать в удаленном режиме.

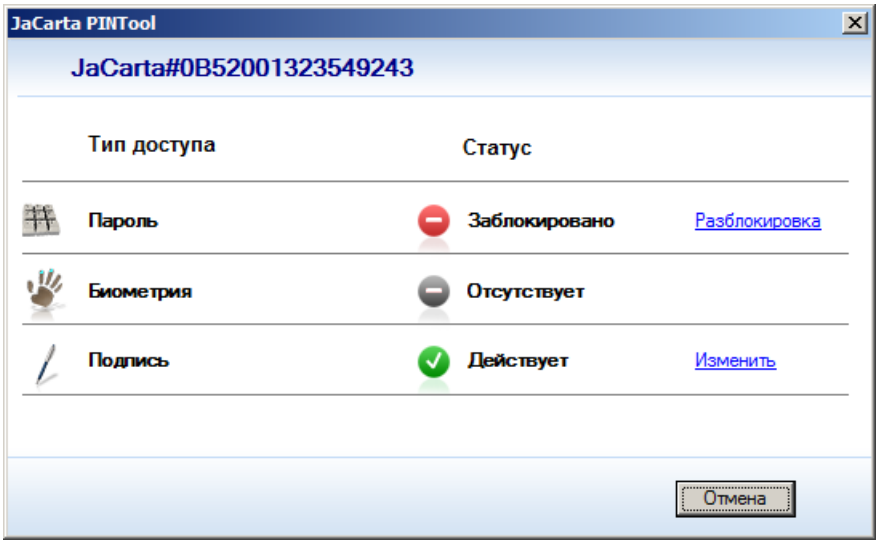
Примечание:

> Если в профиле, который использовался для персонализации электронного ключа JaCarta, на вкладке **Пароль администратора** был установлен флажок **Случайный идентификатор**, разблокировка в удаленном режиме невозможна.

Для того чтобы разблокировать электронный ключ JaCarta в удаленном режиме.

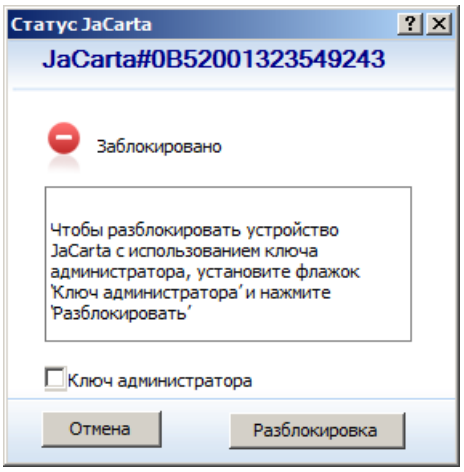
1. Пользователь должен подсоединить электронный ключ JaCarta к своему компьютеру и запустить утилиту JaCarta PINTool.

Если тип доступа заблокирован, в колонке **Статус** напротив него отображается **Заблокировано**, как показано на изображении ниже.



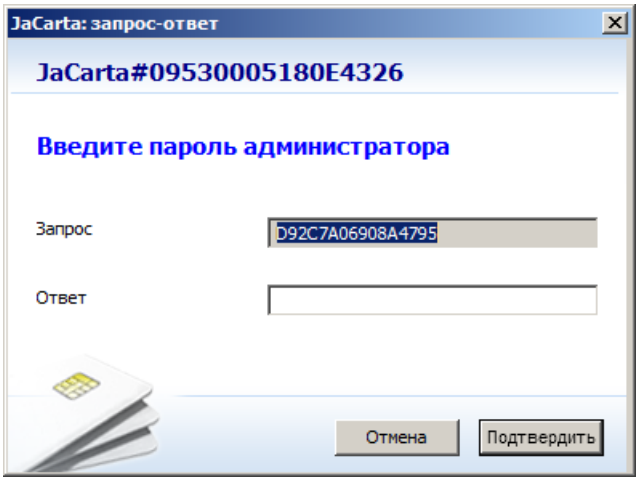
2. Для разблокировки пользователь должен щелкнуть на ссылке **Разблокировка** напротив поля **Пароль**.

   На экране пользователя отобразится следующее окно.



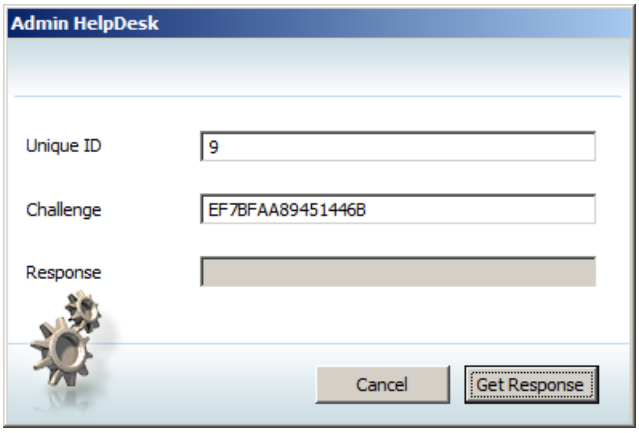
3. Пользователь должен оставить неотмеченным пункт **Ключ администратора** и нажать **Разблокировка**.

   На экране пользователя отобразится следующее окно.



4. Пользователь должен сообщить администратору идентификатор, созданный на этапе персонализации электронного ключа JaCarta (см. «Персонализация с использованием ключа администратора») и данные из поля **Запрос**.

5. Администратор на своей рабочей станции в окне утилиты HelpDesk в поля **Unique ID** (Идентификатор) и **Challenge** (Запрос) должен соответственно ввести сообщенные пользователем идентификатор и запрос, как показано на изображении ниже.

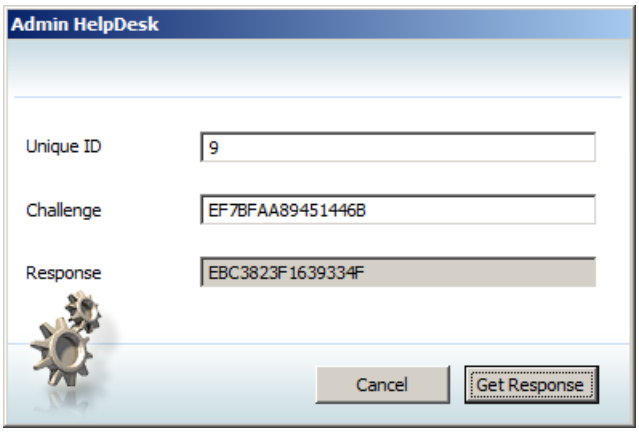


Примечание:

Ключ администратора, который применялся при персонализации электронного ключа пользователя, должен быть подключен к рабочей станции администратора. Также, для запуска утилиты JaCarta HelpDesk администратору необходимо подтвердить доступ к ключу администратора.

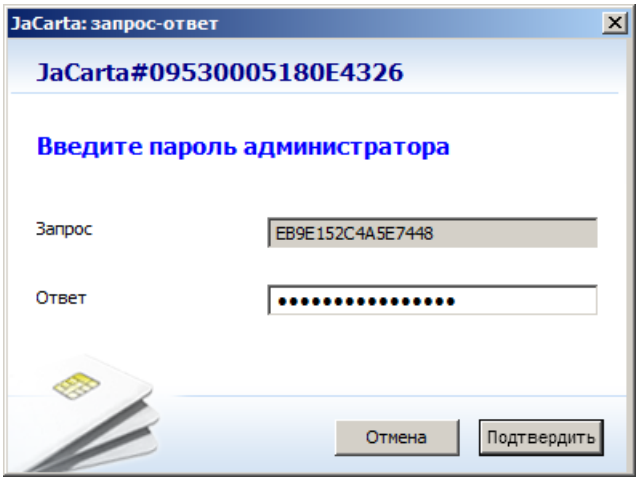
6. После того как данные введены, администратор должен нажать **Get Response** (Получить ответ).

   В поле **Response** (Ответ) утилиты HelpDesk на рабочей станции администратора отобразится ответ (см. изображение ниже).

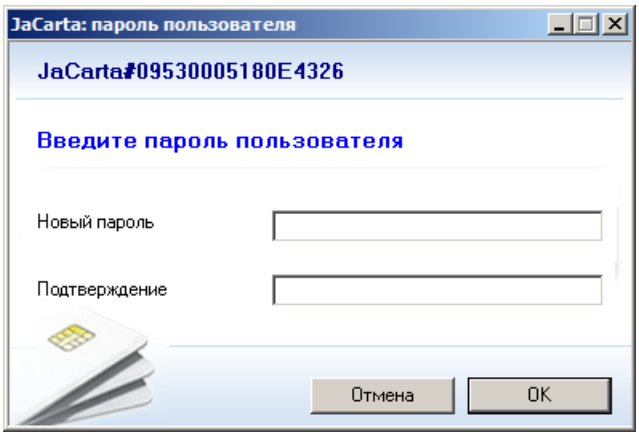


7. Администратор должен сообщить пользователю данные из поля **Response** (Ответ).

8. Пользователь на своей рабочей станции должен ввести сообщенный администратором ответ в поле **Ответ**, как показано на изображении ниже, и нажать **Подтвердить** (см. изображение ниже).

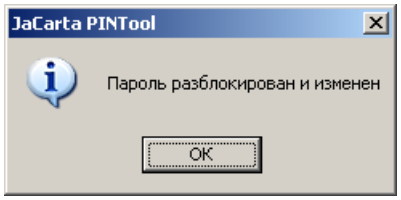


На экране пользователя отобразится следующее окно.



9. В полях **Новый пароль** и **Подтверждение** пользователь должен ввести новый пароль пользователя JaCarta и подтверждение соответственно, после чего нажать **OK**.

   На экране пользователя отобразится следующее сообщение.



10. Пользователь должен нажать **OK** для завершения процедуры.

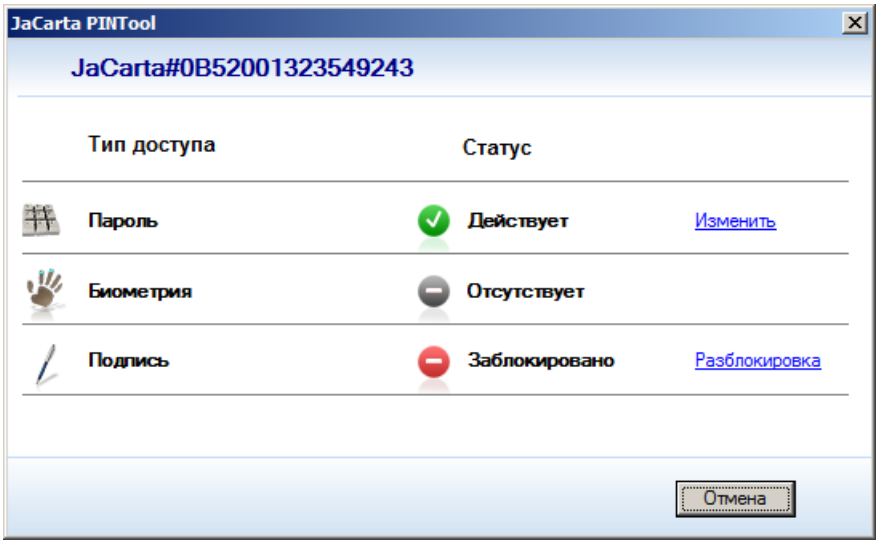
Разблокировка пароля цифровой подписи

Блокировка пароля цифровой подписи происходит, если пользователь превысил допустимое число последовательных неудачных попыток ввода данного пароля (это значение устанавливается на этапе персонализации). Для разблокировки пароля цифровой подписи используется соответствующий ему пароль разблокировки цифровой подписи.

Для того чтобы разблокировать пароль цифровой подписи.

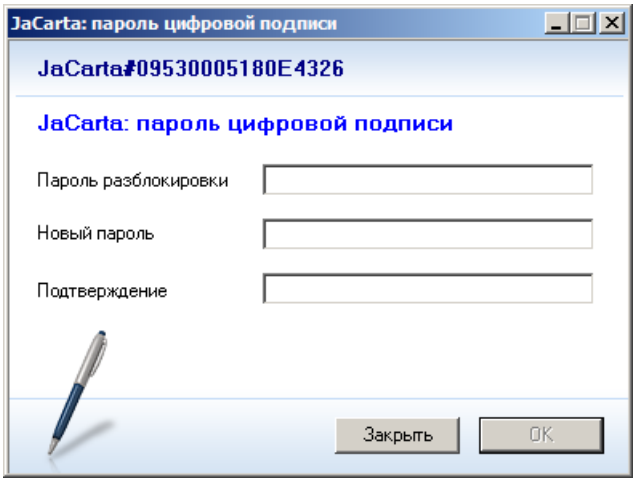
1. Выберите **Пуск > Все программы > JC-Client > JaCarta PINTool**.

Если пароль цифровой подписи заблокирован, в поле **Статус** напротив значения **Подпись** будет значиться **Заблокировано**, как показано на изображении ниже.



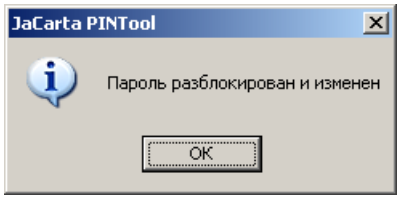
2. Щелкните на ссылке **Разблокировка** напротив поля подпись.

   Отобразится следующее окно.



3. В поле **Пароль разблокировки** введите пароль разблокировки цифровой подписи.
4. В полях **Новый пароль** и **Подтверждение** пользователь должен ввести новый пароль цифровой подписи и подтверждение соответственно.
5. Нажмите **OK**.

   Отобразится следующее сообщение.



6. Нажмите **OK** для завершения процедуры.

Параметры и настройки

Настоящий раздел посвящен описанию параметров JC-Client, хранящихся в реестре.

Краткое содержание.

Общие сведения о параметрах

Конфигурация JC-Client и связанные с ней параметры реестра определяют интерфейс JC-Client и параметры обработки различных событий. Задать значение параметров можно несколькими способами:

- **В процессе установки из командной строки** – информация об этом представлена в разделах «Установка в режиме командной строки» и «Параметры командной строки».
- **В утилите JaCarta Options** - подробное описание данной утилиты представлено в разделе «JaCarta Options».
- **Настройка параметров реестра вручную** – информация о ручной настройке параметров реестра представлена в разделе «Настройка параметров реестра вручную».

Параметры командной строки

Имя	IBOOT
Описание	Перезагрузка компьютера после установки.
Значения	0 (Ложь): После установки перезагрузка по необходимости. Например, если установлена поддержка GINA. 1 (Истина): после установки перезагрузки не будет.
По умолчанию	0 (Ложь)
Пример	(Не перезагружать после установки) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" IBOOT=1`

Имя	UBOOT
Описание	Перезагрузка после деинсталляции.
Значения	0 (Ложь): перезагрузка после деинсталляции. 1 (Истина): после деинсталляции перезагрузки не будет.
По умолчанию	0 (Ложь)
Пример	(Не перезагружать после деинсталляции) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" UBOOT=1`

Имя	INSTALLMANGEPIN
Описание	Необязательный параметр, определяющий, будет ли установлена утилита JaCarta PINTool.
Значения	0 (Ложь): не устанавливать. 1 (Истина): устанавливать.
По умолчанию	1 (Истина)
Пример	(Не устанавливать JaCarta PINTool)

	`msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLMANGEPIN=0`

Имя	INSTADMINPINTOOL
Описание	Необязательный параметр, определяющий, будет ли установлена утилита JaCarta Admin PINTool.
Значения	0 (Ложь): не устанавливать. 1 (Истина): устанавливать.
По умолчанию	0 (Ложь)
Пример	(Установить JaCarta Admin PINTool) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTADMINPINTOOL=1`

Имя	INSTALLMONITOR
Описание	Необязательный параметр, определяющий, будет ли установлена утилита JaCarta Monitor.
Значения	0 (Ложь): не устанавливать. 1 (Истина): устанавливать.
По умолчанию	1 (Истина)
Пример	(Установить JaCarta Monitor) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLMONITOR=1`

Имя	INSTALLRDPSERVER
Описание	Установка сервисов поддержки доступа через удаленный рабочий стол.
Значения	0 (Ложь): не устанавливать. 1 (Истина): устанавливать.
По умолчанию	0 (Ложь)
Пример	(Установка, не включающая поддержку доступа через удаленный рабочий стол) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLRDPSERVER=0`

Имя	INSTBIOCOMP
Описание	Необязательный параметр, позволяющий установить поддержку биометрии на данном компьютере. **Примечание:** установка только этого компонента не позволяет входить в систему по результатам сканирования отпечатка пальца, см. дополнительно INSTALLGINA и INSTALLCP.
Значения	0 (Ложь): не устанавливать компонент поддержки биометрии. 1 (Истина):установить компонент поддержки биометрии.
По умолчанию	0 (Ложь)
Пример	(Установка, включающая поддержку биометрии) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTBIOCOMP=1`

Имя	INSTALLPRECISELIBS
Описание	Установка библиотек, обеспечивающих взаимодействие JC-Client со смарт-картами, выполненными на основе одной из двух биометрических технологий. **Примечание**: подробные сведения по настройке параметров биометрической аутентификации представлены в документе *Использование JaCarta для биометрической аутентификации в среде Windows*.
Значения	1: технология Precise Biometrics 2: технология ISO

По умолчанию	2
Пример	(Установить компоненты необходимые для взаимодействия JC-Client со смарт-картами, выполненными с использованием биометрической технологии Precise Biometrics.) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLPRECISELIBS=1`

Имя	ASESENSBSPS
Описание	Установка компонентов, необходимых для взаимодействия JC-Client с различными моделями сканеров отпечатков пальцев **Примечание:** подробные сведения по настройке параметров биометрической аутентификации, а также сведения, касающиеся различных моделей сканеров отпечатков, представлены в документе *Использование JaCarta для биометрической аутентификации в среде Windows*.
Значения	1: Precise Biometrics 4: Validity 5: Precise Biometrics, Validity 8: Nitgen 9: Precise Biometrics, Nitgen 13: Precise Biometrics, Nitgen, Validity 16: Authentec/Upek 17: Authentec/Upek, Precise Biometrics 21: Authentec/Upek,Precise Biometrics, Validity 29: Authentec/Upek,Precise Biometrics, Validity, Nitgen 36: Authentec/Upek, Nitgen
По умолчанию	16 (Authentec/Upek – эти сканеры встроены в считыватели Athena)
Пример	(Установить поддержку сканеров отпечатков Authentec/Upek,Precise Biometrics, Validity и Nitgen) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" ASESENSBSPS=29`

Имя	INSTALLGINA
Описание	Установка заменяющих библиотек GINA. Позволяет осуществлять вход в систему по результатам сканирования отпечатка пальца. **Примечание:** данный компонент необходимо устанавливать с компонентом INSTBIOCOMP. INSTALLGINA следует устанавливать только на операционные системы до Windows Vista. Для Windows Vista и более поздних систем используйте параметр INSTALLCP (см. ниже).
Значения	0 (Ложь): компоненты GINA не будут установлены. 1 (Истина): установка включает компоненты GINA.
По умолчанию	1 (Истина)
Пример	(Не устанавливать компоненты GINA) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLGINA=0`

Имя	INSTALLCP
Описание	Установка компонента Credential Provider. Позволяет осуществлять вход в систему по результатам сканирования отпечатка пальца. **Примечание:** данный компонент необходимо устанавливать с компонентом INSTBIOCOMP. INSTALLCP следует устанавливать только на операционные системы, начиная с Windows Vista. Для более ранних систем используйте параметр INSTALLGINA.
Значения	0 (Ложь): компоненты Credential Provider не будут установлены. 1 (Истина): установка включает компоненты Credential Provider.
По умолчанию	0 (Ложь)
Пример	(Установить Credential Provider) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLCP=1`

Имя	INSTCITRIXCLIENT
Описание	Установка клиентских компонентов для поддержки работы электронных ключей JaCarta в среде Citrix.
Значения	0 (Ложь): не устанавливать набор клиентских компонентов Citrix. 1 (Истина): установить набор клиентских компонентов Citrix.
По умолчанию	0 (Ложь)
Пример	(установить компоненты Citrix) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTCITRIXCLIENT=1`

Имя	DELCERTSTORE
Описание	Настройка политики сохранения сертификатов при удалении сертификатов из корневого хранилища сертификатов Windows.
Значения	0 (Ложь): при удалении из хранилища сертификатов Windows, сертификат остается в памяти электронных ключей JaCarta. 1 (Истина): при удалении из хранилища сертификатов Windows, сертификат также удаляется из памяти электронных ключей JaCarta.
По умолчанию	0 (Ложь)
Пример	(Удалять сертификат из памяти электронных ключей JaCarta, если он удален из хранилища сертификатов). `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" DELCERTSTORE=1`

Имя	KEEPARCVCERT
Описание	Если данная политика включена, сертификат, помеченный в хранилище как архивный, помечается таким же образом в памяти электронного ключа JaCarta. В противном случае сертификат удаляется.
Значения	0 (Ложь): когда сертификат помечается как архивный в хранилище сертификатов Windows, он удаляется из памяти электронного ключа JaCarta. 1 (Истина): когда сертификат помечается как отправленный в архив в хранилище сертификатов Windows, он также помечается как архивный в памяти электронного ключа JaCarta.
По умолчанию	0 (Ложь)
Пример	(Сохранять сертификаты, отмеченные как архивные) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" KEEPARCVCERT=1`

Имя	DELCARDCERT
Описание	Настройка политики сохранения сертификатов в корневом хранилище Windows при удалении сертификата из памяти электронного ключа JaCarta.
Значения	0 (Ложь): при удалении сертификата из памяти электронного ключа JaCarta он остается в корневом хранилище сертификатов Windows. 1 (Истина): когда сертификат удаляется из памяти электронного ключа JaCarta, он также удаляется из корневого хранилища сертификатов Windows.
По умолчанию	0 (Ложь)
Пример	(Не удалять сертификат из корневого хранилища, даже если он удален из памяти электронного ключа JaCarta) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" DELCARDCERT=0`

Имя	LOADROOT
Описание	Настройка политики в отношении корневых сертификатов, хранящихся в памяти электронного ключа JaCarta.
Значения	0 (Ложь): корневой сертификат в памяти электронного ключа JaCarta не загружается в корневое хранилище сертификатов Windows.

	1 (Истина): корневой сертификат в памяти электронного ключа JaCarta загружается в корневое хранилище сертификатов Windows.
По умолчанию	0 (Ложь)
Пример	(Загружать сертификаты в корневое хранилище) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" LOADROOT=1`

Имя	CPSUPPORT
Описание	Определяет, будет ли установлена по умолчанию поддержка разрыва Check Point VPN-сессии при отключении электронного ключа JaCarta от рабочей станции.
Значения	0 (Ложь): не прерывать VPN-сессию при извлечении электронного ключа JaCarta. 1 (Истина): прерывать VPN-сессию при извлечении электронного ключа JaCarta.
По умолчанию	0 (Ложь)
Пример	(Задать настройку разрыва VPN-сессии при отключении электронного ключа JaCarta). `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" CPSUPPORT=1`

Имя	CERTPOLICY
Описание	Устанавливает количество дней, в течение которых сертификаты будут храниться в хранилище сертификатов, перед тем как будут удалены.
Значения	Целочисленные значения
По умолчанию	Не установлено
Пример	(Хранить сертификаты 5 дней) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" CERTPOLICY=5`

Имя	SHOWICONTRY
Описание	Определяет, будет ли отображаться значок JaCarta Monitor в области уведомлений.
Значения	0 (Ложь): значок JaCarta Monitor не отображается в панели уведомлений. 1 (Истина): значок JaCarta Monitor отображается в панели уведомлений.
По умолчанию	1 (Истина)
Пример	(Не отображать значок в области уведомлений) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" SHOWICONTRY=0`

Имя	INSTALLPERSO
Описание	Необязательный параметр, определяющий, будет ли установлена утилита JaCarta Format.
Значения	0 (Ложь): не устанавливать JaCarta Format. 1 (Истина): установить JaCarta Format.
По умолчанию	1 (Истина)
Пример	(Не устанавливать утилиту JaCarta Format) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLPERSO=0`

Имя	INSTALLMANAGER
Описание	Необязательный параметр, определяющий, будет ли установлена утилита JaCarta Manager.
Значения	0 (Ложь): не устанавливать JaCarta Manager. 1 (Истина): установить JaCarta Manager.
По умолчанию	1 (Истина)

Пример	(Не устанавливать JaCarta Manager) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLMANAGER=0`

Имя	INSTALLOPTIONS
Описание	Необязательный параметр, определяющий, будет ли установлена утилита JaCarta Options.
Значения	0 (Ложь): не устанавливать JaCarta Options. 1 (Истина): установить JaCarta Options.
По умолчанию	1 (Истина)
Пример	(Не устанавливать утилиту JaCarta Options) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLOPTIONS=0`

Имя	ORIGBIOFINGPRINT
Описание	Определяет, реальный отпечаток пальца или муляж отпечатка будет отображаться во время доступа по отпечатку пальцев.
Значения	0 (Ложь): отображать муляж отпечатка. 1 (Истина): отображать реальный отпечаток.
По умолчанию	1 (Истина)
Пример	(Отображать реальный отпечаток пальца) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" ORIGBIOFINGPRINT=1`

Имя	ALLOWUNLOCK
Описание	Определяет, допустимо ли разблокировать электронный ключ JaCarta из окна авторизации Windows.
Значения	1: не разрешать. 2: разрешить.
По умолчанию	1
Пример	(Разрешить разблокировать электронные ключи JaCarta из окна авторизации Windows) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" ALLOWUNLOCK=2`

Имя	MOZILLASUPPORT
Описание	Прописывает путь к библиотеке PKCS#11 в настройках браузера Mozilla Firefox.
Значения	0 (Ложь): не включать в установку поддержку PKCS#11 для Firefox. 1 (Истина): включить в установку поддержку PKCS#11 для Firefox.
По умолчанию	1 (Истина)
Пример	(включить поддержку PKCS#11 для Firefox) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" MOZILLASUPPORT=1`

Имя	CREATEPUKEY
Описание	Задает значение параметра реестра `enablePublicCreate`, который позволяет создавать открытый ключ в памяти электронного ключа JaCarta.
Значения	0 (Ложь): ключ создается без принудительного задания данного значения. 1 (Истина): позволить создавать открытый ключ в памяти электронного ключа JaCarta.
По умолчанию	0 (Ложь)
Пример	(Позволить создавать открытый ключ в памяти электронного ключа JaCarta) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" CREATEPUKEY=1`

Имя	ENASTROPROT
Описание	Задает значение параметра реестра enableStrongProtected.
Значения	0 (Ложь): создать без учета данного параметра. 1 (Истина): позволить, если есть поддержка цифровой подписи, в противном случае прервать операцию.
По умолчанию	0 (Ложь)
Пример	(Позволить, если есть поддержка цифровой подписи, в противном случае прервать операцию) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" ENASTROPROT=1`

Имя	VERIFPOLICY
Описание	Задает значение ключа реестра DSVerificationPolicy. Данный ключ определяет параметры кеширования пароля цифровой подписи.
Значения	0: пароль не кешируется 1: пароль кешируется, но при каждом использовании требуется подтверждение действия пользователем. 2: пароль кешируется, подтверждение пользователем при каждом действии не требуется.
По умолчанию	0
Пример	(Пароль кешируется, подтверждение каждого действия пользователем не требуется) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" VERIFPOLICY=2`

Имя	DSSYNCPOLICY
Описание	Задает значение ключе реестра DSSynchOption. Данный ключ определяет параметры синхронизации пароля пользователя и пароля цифровой подписи (см. раздел «Синхронизация пароля пользователя с паролем цифровой подписи»).
Значения	0 (Ложь): не синхронизировать пароль пользователя и пароль цифровой подписи. 1 (Истина): синхронизировать пароль пользователя и пароль цифровой подписи.
По умолчанию	0 (Ложь)
Пример	(Синхронизировать пароль пользователя и Digital signature PIN) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" DSSYNCPOLICY=1`

Имя	DNSPREFIXNAME
Описание	Задает значение ключа реестра DSNamePrefix. Данный ключ определяет префикс, с которым будет сохраняться контейнер цифровой подписи.
Значения	Буквенно-цифровые значения.
По умолчанию	Не установлено
Пример	(Префикс имени цифровой подписи) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" DNSPREFIXNAME="Prefix"`

Имя	DSCREATIONPOLICY
Описание	Задает параметр ключа реестра DSCreationPolicy.
Значения	0: закрытый ключ связан с паролем цифровой подписи только в том случае, если явно задан параметр PKCS#11 2.20 CKA_ALWAYS_AUTHENTICATE. 1: пароль цифровой подписи связан с любым ключом, для которого установлен атрибут AT_SIGNATURE. 2: существует возможность задать префикс контейнера цифровой подписи.
По умолчанию	0

Пример	(пароль цифровой подписи связан с любым ключом, для которого установлен атрибут AT_SIGNATURE) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" DSCREATIONPOLICY=1`

Имя	INSTALLMD
Описание	Установка набора компонентов Minidriver.
Значения	0 (Ложь): не устанавливать Minidriver. 1 (Истина): установить Minidriver.
По умолчанию	0 (Ложь)
Пример	(Установить Minidriver) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLMD=1`

Имя	INSTALLCSP
Описание	Установка набора компонентов CSP.
Значения	1 (Истина): устанавливать набор компонентов CSP. 0 (Ложь): не устанавливать набор компонентов CSP.
По умолчанию	1 (Истина)
Пример	(Не устанавливать CSP) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLCSP=0`

Имя	INSTMDANDCSP
Описание	Установка набора компонентов Minidriver и CSP.
Значения	0 (Ложь): не позволять устанавливать одновременно CSP и Minidriver. 1 (Истина): позволить устанавливать одновременно CSP и Minidriver.
По умолчанию	0 (Ложь)
Пример	(Позволить устанавливать одновременно CSP и Minidriver) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTMDANDCSP=1`

Имя	INSTALLBIOTOOL
Описание	Установка утилиты JaCarta BioTool. **Примечание:** данный компонент следует устанавливать вместе с компонентом INSTBIOCOMP.
Значения	0 (Ложь): не устанавливать JaCarta BioTool. 1 (Истина): установить JaCarta BioTool.
По умолчанию	1 (Истина)
Пример	(Не устанавливать JaCarta BioTool) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLBIOTOOL=0`

Имя	INSTALLCCID
Описание	Установка драйвера CCID.
Значения	0 (Ложь): не устанавливать драйвер CCID. 1 (Истина): установить драйвер CCID.
По умолчанию	0 (Ложь)
Пример	(Установить драйвер CCID) `msiexec.exe /i "<путь к файлу установки>\JC-Client.msi" INSTALLCCID=1`

Настройка параметров реестра вручную

Чтобы настроить параметры JC-Client в реестре, выполните следующие действия.

1. Откройте **Пуск > Выполнить**.
2. В поле **Открыть** введите `regedit` и нажмите **ОК**.

На экране откроется редактор реестра, и в левой части окна вы увидите древовидную структуру разделов реестра.

3. Раскройте требуемый раздел и выберите в нем тот параметр, для которого вы хотите изменить значение. Значения параметров отображаются в правой части окна.
4. Чтобы задать значение параметра в реестре, используйте имя этого параметра.

Параметр	CertRemovePolicy
Описание	Политика удаления сертификатов, которые загружаются из памяти электронного ключа JaCarta из хранилища сертификатов на рабочей станции.
Значения	0 (Ложь): не удалять сертификаты из хранилища. FF: Удалять сертификаты при отсоединении электронного ключа JaCarta Целочисленное значение: Удалять сертификаты из хранилища после указанного в данном параметре числа дней.
По умолчанию	FF

Параметр	monS
Описание	Данный параметр определяет, будет ли отображаться иконка JaCarta Monitor в панели задач.
Значения	0 (Ложь): не отображать иконку. 1 (Истина): отображать иконку.
По умолчанию	1 (Истина)

Параметр	showUnpers
Описание	Данный параметр определяет, будет ли отображаться предупреждение о том, что подсоединенный электронный ключ JaCarta не персонализирован.
Значения	0 (Ложь): не отображать предупреждение. 1 (Истина): отображать предупреждение.
По умолчанию	1 (Истина)

Параметр	TraceLogFilename
Описание	Данная настройка определяет, будет ли генерироваться файл записи событий.
Значения	Путь с указанием имени текстового файла.
По умолчанию	Не определено

Параметр	DSVerificationPolicy
Описание	Данная настройка определяет параметры кеширования пароля цифровой подписи.
Значения	0: пароль цифровой подписи не кешируется, при каждом использовании пользователю необходимо его вводить. 1: Кешировать и запрашивать подтверждение. Пользователь не должен каждый раз вводить пароль цифровой подписи, но должен подтвердить ее каждое ее использование нажатием кнопки **Подтвердить**.

	2: Пароль цифровой подписи кешируется, и пользователю нужно ввести его только при первом использовании.
По умолчанию	Не определено

Параметр	DSSynchOption
Описание	Настройка синхронизации пароля цифровой подписи и пароля пользователя.
Значения	0 (Ложь): пароль цифровой подписи не синхронизирован с паролем пользователя. 1 (Истина): пароль цифровой подписи синхронизирован с паролем пользователя.
По умолчанию	Не определено

Параметр	DSCreationPolicy
Описание	Данная настройка определяет параметры связывания пароля цифровой подписи и сертификата в памяти электронного ключа JaCarta.
Значения	0: закрытый ключ связан с паролем цифровой подписи, если явно задан параметр PKCS#11 2.20 CKA_ALWAYS_AUTHENTICATE 1: пароль цифровой подписи связан с любым ключом, для которого установлен атрибут AT_SIGNATURE. 2: существует возможность задать префикс контейнера. Любой ключ цифровой подписи, имя контейнера которого начинается с заданного префикса, будет автоматически связан с паролем цифровой подписи.
По умолчанию	0

Параметр	DSNamePrefix
Описание	Префикс контейнера, который будет связан с цифровой подписью. Данный параметр связан с параметром DSCreationPolicy.
Значения	Текстовое значение.
По умолчанию	Не определено

Параметр	enableStrongProtected
Описание	Включить защиту ключа. Закрытый ключ с атрибутом AT_SIGNATURE, созданный с установленным в true (истина) параметром CRYPT_FORCE_KEY_PROTECTION_HIGH, будет ассоциирован с паролем цифровой подписи.
Значения	0 (Ложь): включить защиту ключа. 1 (Истина): не включать защиту ключа.
По умолчанию	1 (Истина)

Параметр	ShowBMP
Описание	Определяет, будет ли отображаться на экране сканируемый отпечаток пальца вместо стандартного изображения при доступе пользователя по отпечатку. (Данный параметр действует только на уровне рабочей станции.)
Значения	0 (Ложь): отображать стандартное изображение. 1 (Истина): отображать сканируемый отпечаток пальца.
По умолчанию	1 (Истина)

Параметр	LogonCertList
Описание	Разрешить вход в систему с любым сертификатом (Данный параметр действует только на уровне рабочей станции).

Значения	0 (Ложь): Запретить вход в систему в систему с использованием сертификата, не помеченного как сертификат по умолчанию. 1 (Истина): Разрешить вход в систему с использованием любого сертификата в памяти электронного ключа JaCarta, который поддерживает такую возможность.
По умолчанию	0 (Ложь)

Параметр	Opsec
Описание	Определяет, будет ли установлена по умолчанию поддержка разрыва Check Point VPN-сессии при отсоединении электронного ключа JaCarta от компьютера.
Значения	0 (Ложь): не прерывать VPN-сессию при извлечении электронного ключа JaCarta. 1 (Истина): прерывать VPN-сессию при извлечении электронного ключа JaCarta.
По умолчанию	0 (Ложь)

Параметр	allowUnlock
Описание	Позволяет запретить или разрешить возможность разблокировки пароля пользователя из окна приветствия Windows. (Данный параметр действует только на уровне рабочей станции.)
Значения	1: не разрешать возможность разблокировки. 2: разрешить возможность разблокировки.
По умолчанию	1

Параметр	useSysDef
Описание	Заменяет настройки пользователей на настройки рабочей станции, если они отличаются (Данный параметр действует только на уровне рабочей станции.)
Значения	0 (Ложь): Не переопределять настройки пользователей. 1 (Истина): Переопределить настройки пользователей.
По умолчанию	0

Параметр	ASE_SENSOR_BSPS
Описание	Позволяет задать режим поддержки сканеров отпечатков пальцев. Приведено в следующем формате: шестнадцатеричный/десятичный
Значения	1/1: Precise Biometrics 4/4: Validity 5/5: Precise Biometrics, Validity 8/8: Nitgen 9/9: Precise Biometrics, Nitgen D/13: Precise Biometrics, Nitgen, Validity 10/16: Authentec (Upek) 11/17: Authentec (Upek), Precise Biometrics 15/21: Authentec (Upek), Precise Biometrics, Validity 1D/29: Authentec (Upek), Nitgen, Precise Biometrics, Validity 24/36: Authentec (Upek), Nitgen
По умолчанию	10/16: Authentec (Upek) – сканеры, встроенные в комбинированные считыватели ASEDrive Bio

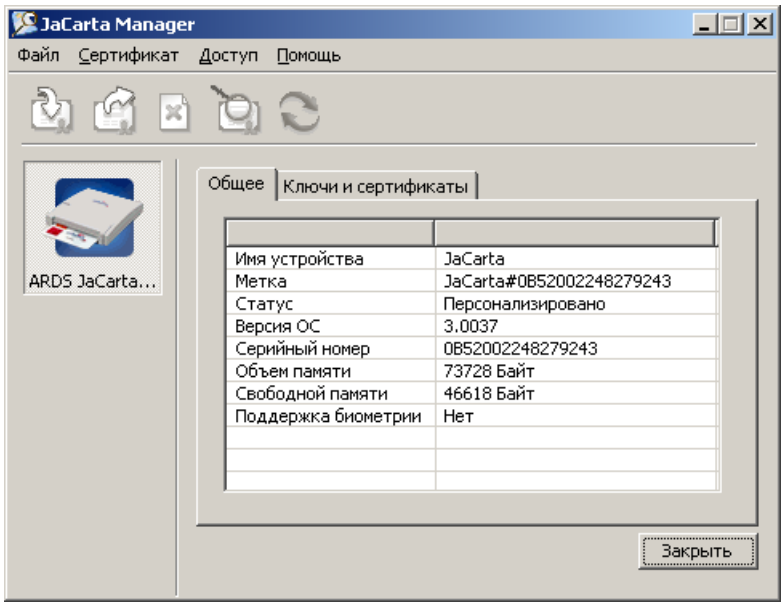
Обзор утилит в составе JC-Client

Утилиты, входящие в JC-Client перечислены в разделе «Описание пакетов установки». Ниже представлено подробное описание их интерфейса.

JaCarta Manager

Утилита JaCarta Manager предназначена для настройки параметров хранения сертификатов и закрытых ключей, хранящихся в памяти электронных ключей JaCarta. Из интерфейса JaCarta Manager также можно вызвать утилиту настройки JaCarta Options (см. «JaCarta Options») и утилиту для управления паролями (см. «JaCarta PINTool»).

При запуске окно утилиты JaCarta Manager выглядит следующим образом.



В левой части окна утилиты отображаются подключенные устройства. В правой части находятся две вкладки.

- **Общее**
- **Ключи и сертификаты**

Вкладка Общее

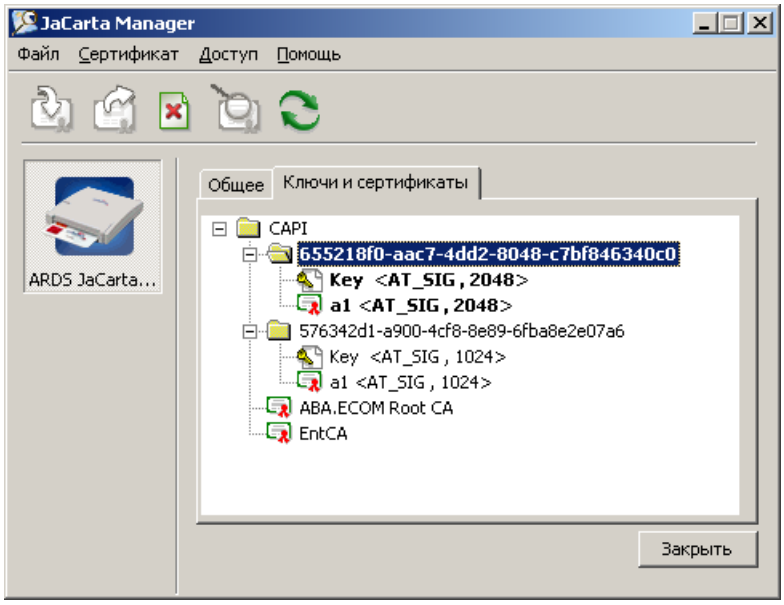
На данной вкладке отображается информация о подсоединенном электронном ключе JaCarta (см. таблицу ниже).

Поле	Описание
Имя устройства	Имя электронного ключа JaCarta (неизменяемый параметр).
Метка	По умолчанию поле принимает значение: «JaCarta#Серийный номер JaCarta».
Статус	Статус электронного ключа JaCarta, может принимать два значения. **Персонализировано** **Не персонализировано**
Версия ОС	Версия операционной системы электронного ключа JaCarta.
Серийный номер	Серийный номер электронного ключа JaCarta.
Объем памяти	Общий объем памяти электронного ключа JaCarta.
Свободной памяти	Объем свободной памяти электронного ключа JaCarta.
Поддержка биометрии	Значение поля указывает, выполнен ли подсоединенный электронный ключ с использованием биометрических технологий. Поле может принимать

Поле	Описание
	следующие значения. **Да** – электронный ключ выполнен с использованием биометрической технологии Precise Biometrics. **ISO** – электронный ключ выполнен с использованием биометрической технологии по стандарту ISO 19794. **Нет** – сохранение отпечатков не поддерживается. **Примечание:** сведения, касающиеся использования электронных ключей JaCarta с настройками биометрии, представлены в документе *Использование JaCarta для биометрической аутентификации в среде Windows*.

Ключи и сертификаты

Данная вкладка после ввода пароля пользователя и/или проверки отпечатков пальцев отображает информацию о сертификатах и закрытых ключах, хранящихся в памяти электронного ключа JaCarta.



При открытии вкладки **Ключи и сертификаты** становятся активными кнопки управления сертификатами.

Кнопка	Описание
Импорт сертификата	Позволяет импортировать сертификат в память электронного ключа JaCarta.
Экспорт сертификат	Позволяет экспортировать сертификаты, хранящиеся в памяти электронного ключа JaCarta.
Удалить	Удаляет выбранный объект из памяти электронного ключа JaCarta, если данный объект не является частью контейнера CAPI по умолчанию.
Просмотр сертификата	Отображает информацию о выбранном сертификате.
Обновить	Обновляет информацию о сертификатах, хранящихся в памяти электронного ключа JaCarta.

Большая часть приведенных выше функций также доступна из панели управления JaCarta Manager (см. следующий подраздел).

Панель управления JaCarta Manager

Панель управления утилиты JaCarta Manager содержит следующие меню (см. таблицу ниже).

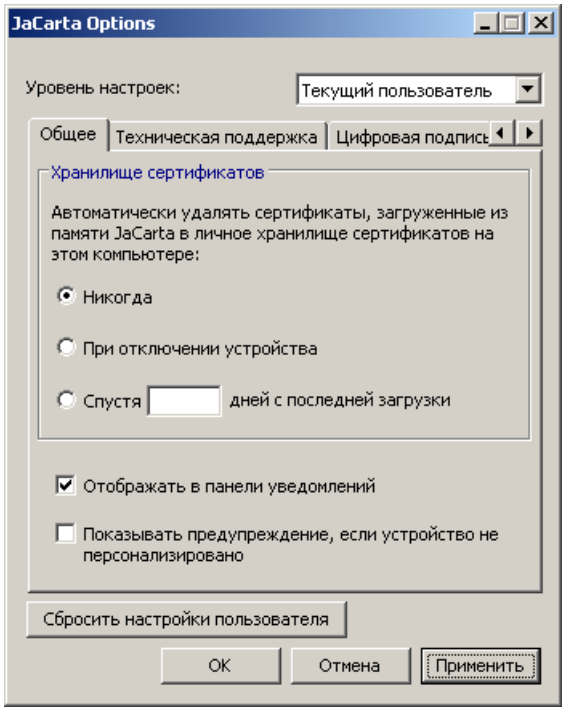
Название меню	Список пунктов	Описание
Файл	**Удалить**	Удаляет выбранный объект из памяти электронного

Название меню	Список пунктов	Описание
		ключа JaCarta, если он не является частью контейнера CAPI по умолчанию, вкладка **Ключи и сертификаты**.
	Изменить метку	Позволяет изменить метку электронного ключа JaCarta, вкладка **Общее**.
	Настройки	Запускает утилиту JaCarta Options (см. «JaCarta Options»).
	Выход	Выход из приложения.
Сертификат	**Импорт**	Позволяет импортировать сертификат в память электронного ключа JaCarta, вкладка **Ключи и сертификаты**.
	Экспорт	Позволяет экспортировать сертификаты, хранящиеся в памяти электронного ключа JaCarta, вкладка **Ключи и сертификаты**.
	Просмотр	Отображает информацию о выбранном сертификате, вкладка **Ключи и сертификаты**.
	Установить по умолчанию	Устанавливает выбранный контейнер в качестве контейнера по умолчанию, вкладка **Ключи и сертификаты**.
Доступ	**PINTool**	Запускает утилиту JaCarta PINTool (см. «JaCarta PINTool»).
	BioTool	Сведения об использовании данной утилиты представлены в документе *Использование JaCarta для биометрической аутентификации в среде Windows*.
Помощь	**О программе**	Отображает информацию об утилите JaCarta Manager.

JaCarta Options

Утилита JaCarta Options предназначена для настройки параметров использования электронных ключей JaCarta. Настройки, сделанные с помощью этой утилиты, могут применяться как для текущего пользователя, так и для всех пользователей данной рабочей станции.

При запуске окно JaCarta Options выглядит следующим образом.



В верхней части окна утилиты находится выпадающий список **Уровень настроек**. Данный список содержит два пункта.

- **Текущий пользователь –** позволяет изменять параметры использования электронных ключей JaCarta для текущего пользователя. Если выбран данный пункт, внизу окна отображается кнопка **Сбросить настройки пользователя**. Нажатие на эту кнопку изменяет настройки текущего пользователя на настройки рабочей станции.
- **Локальный компьютер –** позволяет изменять параметры использования электронных ключей JaCarta для всех пользователей рабочей станции. Если выбран данный пункт, внизу окна отображается флажок **Сбросить настройки пользователей**. Если флажок установлен, при сохранении настроек все сделанные изменения переопределяют настройки пользователей данной рабочей станции.

Также окно утилиты JaCarta Options содержит 4 вкладки:

- **Общее**
- **Техническая поддержка**
- **Цифровая подпись**
- **Дополнительно**

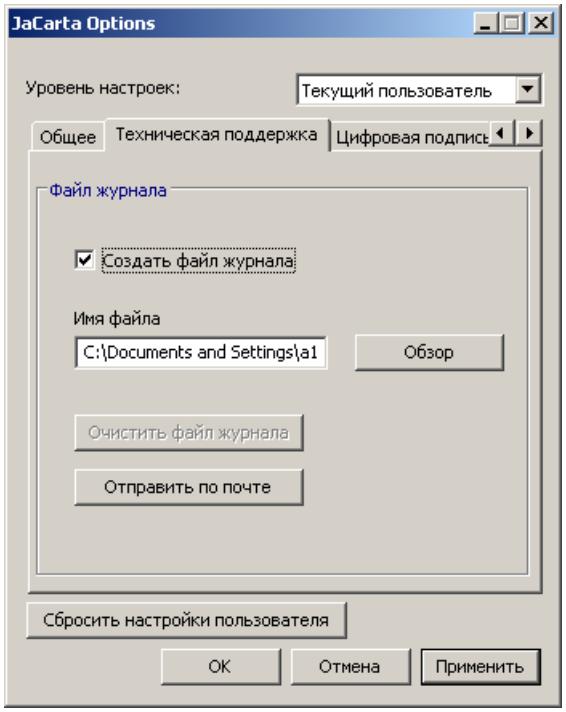
Вкладка Общее

Вкладка **Общее** позволяет настроить параметры сохранения сертификатов и параметры отображения JaCarta Monitor для текущего пользователя или для всех пользователей данной рабочей станции.

Настройка	Пояснение
Кнопка-переключатель **Никогда**	Сертификаты, загруженные в хранилище сертификатов Windows из памяти электронного ключа JaCarta, не удаляются после отключения устройства.
Кнопка-переключатель **При отключении устройства**	Сертификаты, загруженные в хранилище сертификатов Windows из памяти электронного ключа JaCarta, удаляются из хранилища после отключения устройства. Данная настройка применима только к сертификатам, которые загружаются в личное хранилище сертификатов.
Кнопка-переключатель **Спустя** X **дней с последней загрузки**	Сертификаты, загруженные в хранилище сертификатов Windows из памяти электронного ключа JaCarta, удаляются из личного хранилища сертификатов спустя **X** дней после отключения устройства (число дней необходимо ввести в соответствующем поле).
Флажок **Отображать в панели уведомлений**	Если флажок не установлен, значок  не будет отображаться в области уведомлений.
Флажок **Показывать предупреждение, если устройство не персонализировано**	Если флажок установлен, при подключении не персонализированного электронного ключа JaCarta к компьютеру, на экране будет отображаться предупреждающее сообщение.

Вкладка Техническая поддержка

Данная вкладка позволяет создать файл записи системных событий.



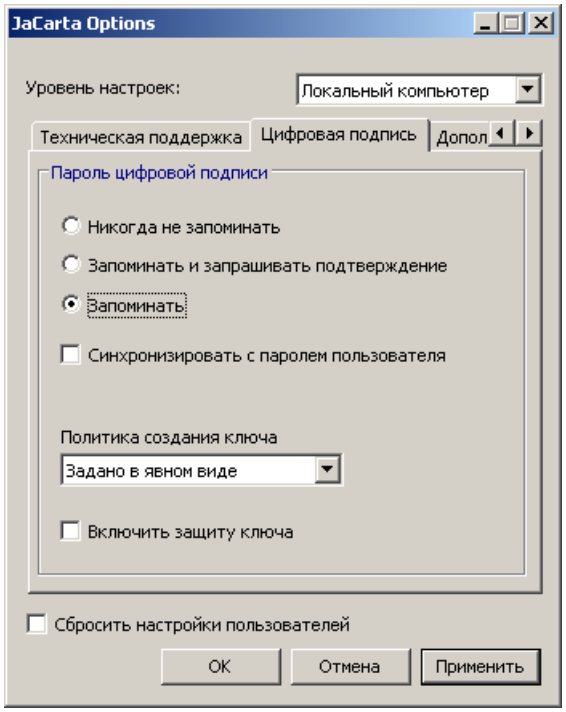
Настройка	Пояснение
Флажок **Создать файл журнала**	Если флажок установлен, системные события, связанные с использованием JC-Client, будут записываться в файл, указанный в поле **Имя файла**.
Поле **Имя файла**	Путь к файлу журнала.
Кнопка **Очистить файл журнала**	Позволяет очистить содержимое файла журнала, если он существует.
Кнопка **Обзор**	Открывает окно проводника Windows, чтобы указать путь к файлу журнала.
Кнопка **Отправить по почте**	При нажатии запускается почтовый клиент по умолчанию. Файл журнала находится во вложении нового сообщения, чтобы его можно было отправить в техническую поддержку ЗАО «Аладдин Р.Д.»

Примечание:

Файлы журнала следует создавать только в случае, если есть соответствующая инструкция представителя технической поддержки. После создания файла журнала снимите флажок **Создать файл журнала**.

Вкладка Цифровая подпись

Данная вкладка позволяет настроить параметры, связанные с использованием цифровой подписи, для текущего пользователя или для всех пользователей данной рабочей станции.



Вкладка **Цифровая подпись** содержит следующие элементы управления.

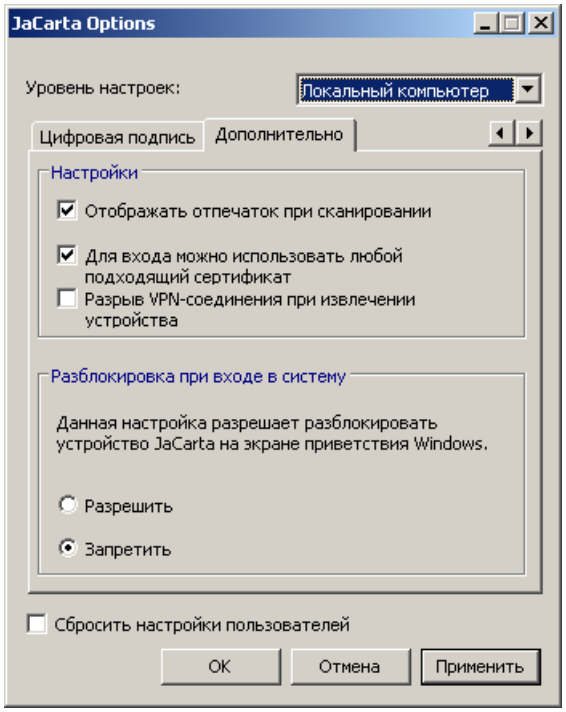
Настройка	Пояснение
Кнопка-переключатель **Никогда не запоминать**	Выбор этой настройки отключает кеширование пароля цифровой подписи.
Кнопка-переключатель **Запоминать и запрашивать подтверждение**	Выбор этой настройки включает кеширование пароля цифровой подписи. Пользователь должен ввести пароль только один раз, однако он должен подтверждать каждое последующее использование цифровой подписи в появляющемся диалоговом окне нажатием на кнопку **Подтвердить**.
Кнопка-переключатель **Запоминать**	Если выбрана эта настройка, пользователь должен будет ввести пароль цифровой подписи только один раз.
Выпадающее меню **Политика создания ключа**	Содержит три пункта: **Задано в явном виде** - если выбран этот пункт, закрытый ключ связан с паролем цифровой подписи только в том случае, если приложения явно задают параметр PKCS#11 2.20 CKA_ALWAYS_AUTHENTICATE. **Любой ключ подписи** - если выбран этот пункт, закрытый ключ связан с любым ключом, для которого установлен атрибут AT_SIGNATURE. **Имя контейнера начинается с** - если выбран этот пункт, существует возможность задать префикс контейнера (в появляющемся поле **Префикс**). Любой ключ цифровой подписи, имя контейнера которого начинается с заданного префикса, будет автоматически связан с паролем цифровой подписи. Для приложений, использующих PKCS#11, если CKA_ID начинается с заданного префикса, этот ключ будет связан с паролем цифровой подписи, вне зависимости от значения параметра CKA_ALWAYS_AUTHENTICATE.
Флажок **Синхронизировать с паролем пользователя**	Если флажок установлен, пароль цифровой подписи синхронизируется с паролем пользователя. Для этого изначально оба пароля должны совпадать.
Флажок **Включить защиту ключа**	Если данный флажок установлен, для защиты контейнера используется криптостойкий ключ (параметр CRYPT_FORCE_KEY_PROTECTION_HIGH). Используемый ключ является ключом с атрибутом AT_SIGNATURE, связанным с паролем пользователя.

Примечание:

> Если выбрана настройка, позволяющая кеширование пароля цифровой подписи - **Запоминать и запрашивать подтверждение** или **Запоминать**, пароль кешируется в контексте каждого конкретного приложения и только когда электронный ключ JaCarta подсоединен к компьютеру. Если электронный ключ отсоединен и затем подсоединен вновь или если приложение, требующее использования электронного ключа, перезапущено, пользователь должен снова ввести пароль цифровой подписи.

Вкладка Дополнительно

Данная вкладка позволяет настроить дополнительные параметры использования электронных ключей JaCarta. Редактировать параметры на данной вкладке можно только в том случае, если в выпадающем списке **Уровень настроек** выбрать **Локальный компьютер**. Таким образом, изменения настроек, сделанные на данной вкладке, коснутся всех пользователей данной рабочей станции.



Описание элементов интерфейса представлено в таблице ниже.

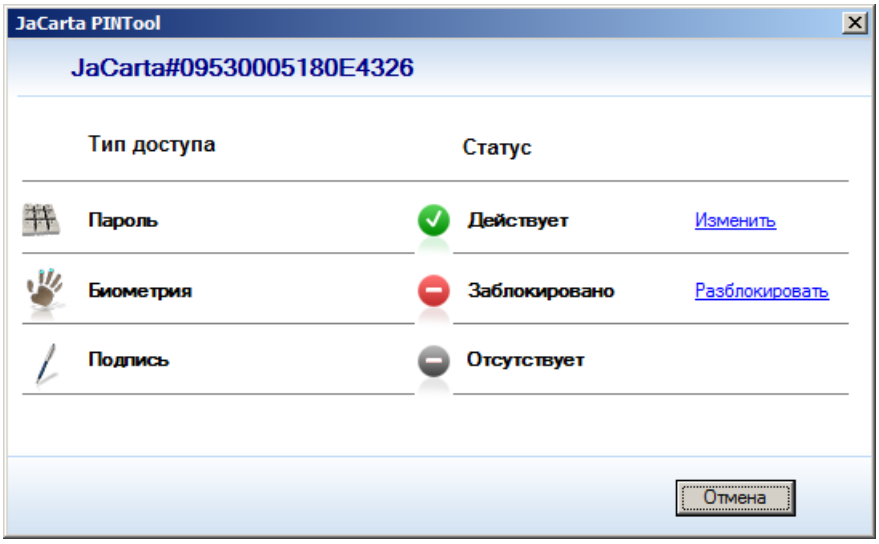
Настройка	Пояснение
Флажок **Отображать отпечаток при сканировании**	Если флажок установлен, в процессе доступа по отпечатку пальца отображается сканируемый отпечаток пальца. В противном случае отображается стандартное изображение. **Примечание:** данная настройка относится к биометрии. Процедуры использования электронного ключа JaCarta с биометрическими настройками представлены в документе *Использование JaCarta для биометрической аутентификации в среде Windows*.
Флажок **Для входа можно использовать любой подходящий сертификат**	Если данный флажок установлен, вход в систему возможен с любым сертификатом в памяти электронного ключа JaCarta, при условии что сертификат поддерживает такую возможность. В противном случае для входа в систему используется сертификат, выбранный в качестве сертификата по умолчанию.
Флажок **Разрыв VPN-соединения при извлечении устройства**	Если флажок установлен, VPN-соединение (Check Point) прерывается при отсоединении электронного ключа JaCarta от компьютера.
Кнопка-переключатель **Разрешить**	Если выбран этот пункт, заблокированный электронный ключ JaCarta можно разблокировать из окна авторизации Windows (см. раздел «Возможность разблокировки из окна приветствия Windows»).
Кнопка-переключатель	Если выбран этот пункт, заблокированный электронный ключ JaCarta

Настройка	Пояснение
Запретить	нельзя разблокировать из окна авторизации Windows.

JaCarta PINTool

Утилита JaCarta PINTool используется для просмотра информации о состоянии электронного ключа JaCarta (заблокирован или разблокирован), а также для операций смены пароля пользователя, пароля цифровой подписи и разблокировки.

При запуске утилита JaCarta PINTool выглядит следующим образом.



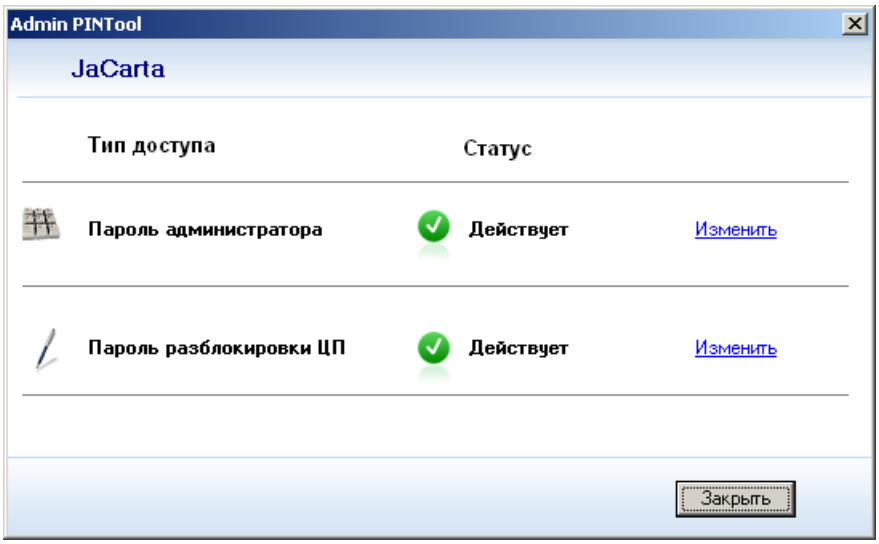
Интерфейс утилиты содержит следующие настройки.

Настройка	Пояснение
Колонка **Тип доступа**	Содержит названия типов доступа. **Пароль** – пароль пользователя. **Биометрия** – доступ по отпечатку пальца. **Подпись** – пароль цифровой подписи.
Колонка **Статус**	В данной колонке напротив каждого из типов доступа отображается статус. Возможны три состояния. **Действует** – данный тип доступа можно использовать для работы с электронным ключом JaCarta. **Заблокировано** – тип доступа заблокирован. **Отсутствует** – тип доступа не используется на данном электронном ключе JaCarta.
Ссылка **Изменить**	Данная ссылка появляется напротив типа доступа со статусом **Действующий**. Нажатие на ссылку открывает окно смены пароля пользователя (см. документ *JC-Client. Руководство пользователя*).
Ссылка **Разблокировка**	Данная ссылка появляется напротив типа доступа со статусом **Заблокировано**. Нажатие на ссылку открывает окно разблокировки (см. раздел «Разблокировка электронного ключа JaCarta»).

JaCarta Admin PINTool

Утилита JaCarta Admin PINTool позволяет изменять пароль администратора и пароль разблокирования цифровой подписи.

При запуске окно утилиты выглядит следующим образом.



Интерфейс утилиты содержит следующие элементы управления.

Настройка	Пояснение
Колонка **Тип доступа**	Содержит названия типов доступа: **Пароль администратора** **Пароль разблокировки ЦП**
Колонка **Статус**	В данной колонке напротив каждого из типов доступа отображается статус. Возможны три состояния: **Действует** – данный тип доступа можно использовать для работы с электронным ключом JaCarta. **Заблокировано** – данный тип доступа на подсоединенном электронном ключе JaCarta заблокирован. **Отсутствует** – данный тип доступа отсутствует на подсоединенном электронном ключе JaCarta.
Ссылка **Изменить**	Данная ссылка появляется напротив типа доступа со статусом **Действует**. Нажатие на ссылку открывает окно смены пароля администратора и/или пароля разблокировки цифровой подписи.

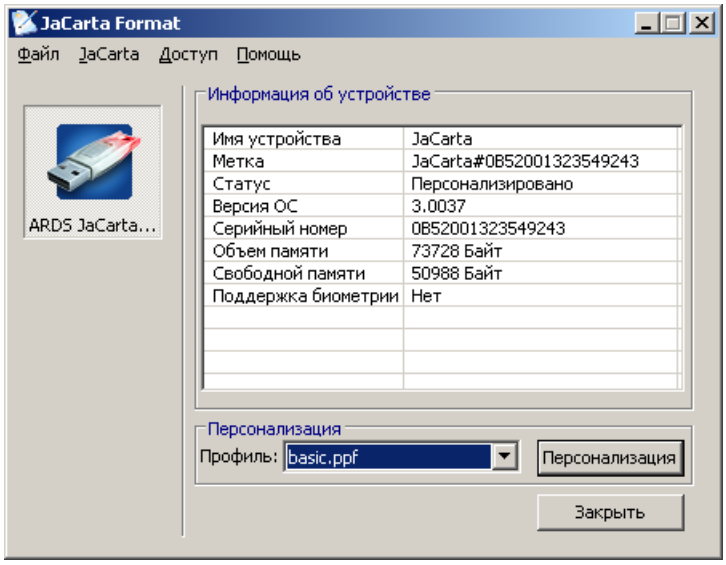
JaCarta Format

Утилита JaCarta Format предназначена для персонализации электронных ключей JaCarta (см. «Персонализация»), создания и редактирования профилей персонализации (см. «Настройка профиля персонализации»), а также для настройки различных параметров использования электронных ключей.

Утилита используется для следующих задач.

- Просмотр информации об электронных ключах JaCarta, такой как серийный номер, объем свободной памяти и т.д.
- Настройка параметров пароля пользователя и пароля администратора. Данные изменения не влияют на целостность аутентификационных данных, хранящихся в памяти электронного ключа JaCarta.
- Настройка параметров пароля цифровой подписи и пароля разблокировки цифровой подписи.
- Просмотр, редактирование и создание новых профилей персонализации.
- Персонализация и повторная персонализация электронных ключей JaCarta.
- Удаление всех данных из памяти электронных ключей JaCarta.

При запуске окно утилиты выглядит следующим образом.



В левой части окна отображаются все электронные ключ JaCarta, подключенные к компьютеру. Для выполнения операций с электронным ключом необходимо щелчком мыши выбрать нужный электронный ключ. В правой части окна отображается информация об активном электронном ключе JaCarta. В таблице ниже представлены описания отображаемых полей.

Поле	Описание
Имя устройства	Имя электронного ключа JaCarta (неизменяемый параметр).
Метка	Метка электронного ключа JaCarta, по умолчанию поле принимает значение: «JaCarta#Серийный номер JaCarta».
Статус	Статус может принимать два значения: **Персонализировано** **Не персонализировано**
Версия ОС	Версия операционной системы электронного ключа JaCarta.
Серийный номер	Серийный номер электронного ключа JaCarta.
Объем памяти	Общий объем памяти электронного ключа JaCarta.
Свободной памяти	Объем свободной памяти электронного ключа JaCarta.
Поддержка биометрии	Значение поля указывает, выполнен ли подсоединенный электронный ключ с использованием биометрических технологий. Поле может принимать следующие значения. **Да** – электронный ключ выполнен с использованием биометрической технологии Precise Biometrics. **ISO** – электронный ключ выполнен с использованием биометрической технологии по стандарту ISO 19794. **Нет** – сохранение отпечатков не поддерживается. **Примечание:** сведения об использовании электронных ключей JaCarta с настройками биометрии представлены в документе *Использование JaCarta для биометрической аутентификации в среде Windows*.

Под таблицей, содержащей информацию об электронном ключе JaCarta, находятся следующие элементы управления.

- Выпадающий список **Профиль** – данный список содержит список сохраненных профилей персонализации.
- Кнопка **Персонализация** – нажатие на данную кнопку запускает процесс персонализации на основе профиля персонализации, выбранного в списке **Профиль**, подробнее о персонализации см. «Персонализация».

Панель управления JaCarta Format

Панель управления JaCarta Format содержит следующие меню (см. таблицу ниже).

Название меню	Список пунктов	Описание
Файл	**Настройки администратора**	Вызывает окно, позволяющее изменить некоторые параметры использования выбранного электронного ключа JaCarta, который уже был персонализирован.
	Управление профилями	Вызывает окно, позволяющее добавлять, изменять и удалять профили персонализации (см. «Настройка профиля персонализации»).
	Выход	Выход из приложения.
JaCarta	**Смена метки**	Позволяет изменить метку электронного ключа JaCarta.
	Персонализация	Запускает процесс персонализации (если электронный ключ персонализируется не впервые, требуется уровень доступа администратора). (См. «Персонализация».)
	Очистка памяти	Удаляет всю информацию из памяти электронного ключа JaCarta (требуется уровень доступа администратора). По завершении данной процедуры значение поля **Статус** принимает значение **Не персонализировано.**
Доступ	**PINTool**	Открывает окно утилиты JaCarta PINTool (см. «JaCarta PINTool»).
	BioTool	Открывает окно утилиты JaCarta BioTool. Данная утилита относится к биометрии. Сведения об использовании электронных ключей JaCarta с настройками биометрии представлены в документе *Использование JaCarta для биометрической аутентификации в среде Windows*.
	Смена пароля администратора	Позволяет сменить пароль администратора.
Помощь	**О программе**	Отображает информацию об утилите JaCarta Format.

Обзор утилит в составе IDProtect Admin

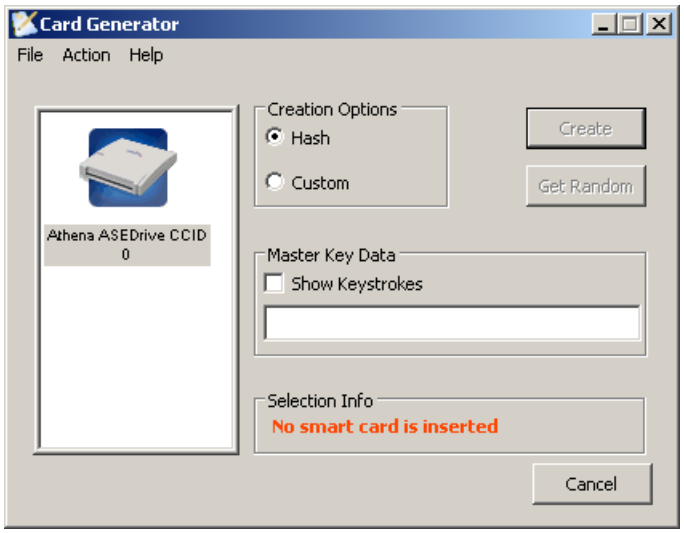
ПО IDProtect Admin предназначено для создания ключей администратора (см. «Ключ администратора») и для удаленной разблокировки электронных ключей JaCarta. В состав данного ПО входят следующие утилиты.

- Card Generator
- HelpDesk

Ниже представлено подробное описание каждой из этих утилит.

Card Generator

При запуске утилита Card Generator выглядит следующим образом.



В левой части интерфейса отображаются подключенные устройства чтения смарт-карт.

Интерфейс утилиты Card Generator содержит следующие элементы (см. таблицу ниже).

Настройка	Описание
Кнопка-переключатель **Creation Options** (Параметры создания)	Определяет способ создания мастер-ключа, который будет храниться в ключе администратора, и содержит два пункта: **Hash** (Хеш) – если выбран данный пункт, для создания мастер-ключа будет использоваться хеш значения, введенного в поле **Master Key Data** (Мастер-ключ). **Custom** (Произвольный) – если выбран данный пункт, для создания мастер-ключа будет использоваться шестнадцатеричное значение, введенное в поле в поле **Master Key Data** (Мастер-ключ).
Поле **Master Key Data** (Мастер-ключ)	Если выбран пункт **Hash** (Хеш), в данное поле необходимо ввести произвольное значение, хеш которого будет использоваться в качестве мастер-ключа. Если выбран пункт **Custom** (Произвольный), в данное поле необходимо ввести 16 байт данных в шестнадцатеричном формате либо нажать кнопку **Get Random** (Сгенерировать). В последнем случае поле заполнится автоматически.
Флажок **Show keystrokes** (Отображать символы)	Если данный флажок установлен, данные в поле **Master Key Data** (Мастер-ключ) отображаются на экране. В противном случае они отображаются в виде звездочек («*»).
Поле **Selection info** (Информация о выбранном устройстве)	В данном поле отображаются сведения о подсоединенных электронных ключах JaCarta. Поле может принимать следующие значения: **No smart card is inserted** (Устройство отсутствует) – электронный ключ JaCarta не подсоединен к считывающему устройству. **Un personalized card** (Устройство не персонализировано) – подсоединенный электронный ключ JaCarta не персонализирован и не может быть использован

Настройка	Описание
	для создания ключа администратора. **Valid card** (Подходящее устройство) – подсоединенный электронный ключ JaCarta может быть использован для создания ключа администратора. **Admin Card** (Ключ администратора) – подключенный электронный ключ JaCarta уже является ключом администратора.
Кнопка **Create** (Создать)	Нажатие на данную кнопку запускает процесс создания ключа администратора. Данная кнопка активна только в том случае, если выполнены все необходимые для создания ключа администратора условия.
Кнопка **Get Random** (Сгенерировать)	Заполняет поле **Master Key Data** (Мастер-ключ) случайными данными в шестнадцатеричном формате. Данная кнопка активна только в том случае, если выбран пункт **Custom** (Произвольный).

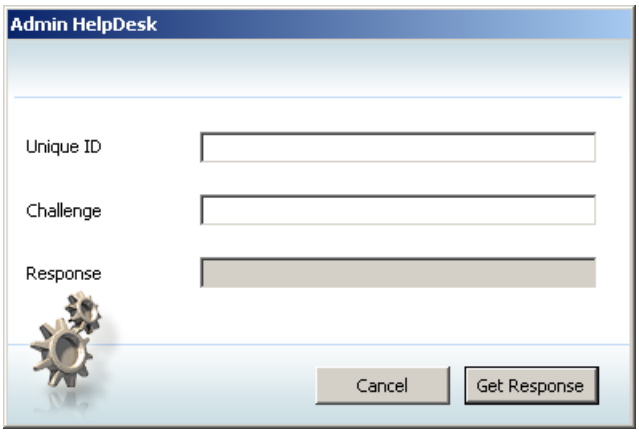
Панель управления утилиты Card Generator содержит следующие элементы (см. таблицу ниже).

Меню панели управления	Список пунктов	Описание
File (Файл)	**Exit** (Выход)	Закрывает утилиту Card Generator.
Action (Действие)	**Create Card** (Создать ключ администратора)	Запускает процесс создания ключа администратора. Данный пункт активна только в том случае, если выполнены все необходимые для создания ключа администратора условия.
	Get Random (Сгенерировать)	Заполняет поле **Master Key Data** (Мастер-ключ) случайными данными в шестнадцатеричном формате. Данная кнопка активна только в том случае, если выбран пункт **Custom** (Произвольный).
Help (Помощь)	**About** (О программе)	Отображает окно с информацией об утилите Card Generator.

HelpDesk

Утилита HelpDesk используется для разблокировки электронных ключей JaCarta в удаленном режиме с использованием схемы «запрос-ответ». При запуске утилиты необходимо, чтобы ключ администратора был подсоединен к рабочей станции. Владельцу ключа администратора также необходимо подтвердить доступ к ключу администратора.

При запуске утилита HelpDesk выглядит следующим образом.



Окно утилиты HelpDesk содержит следующие элементы (см. таблицу ниже).

Элемент интерфейса	Описание
Поле **Unique ID** (Идентификатор)	Идентификатор, задаваемый на этапе персонализации электронного ключа JaCarta пользователя с применением ключа администратора (см. «Персонализация с использованием ключа администратора»).

Элемент интерфейса	Описание
Поле **Challenge** (Запрос)	Запрос, который формируется на стороне пользователя и который пользователь сообщает владельцу ключа администратора (см. «В удаленном режиме»).
Поле **Response** (Ответ)	Ответ, генерируемый на основе запроса и идентификатора после нажатия кнопки **Get Response** (Получить ответ).
Кнопка **Get Response** (Получить ответ**)**	Нажатие на данную кнопку генерирует ответ на запрос, после чего ответ отображается в поле **Response** (Ответ).

Приложения

Настройка поведения при извлечении электронного ключа JaCarta

После аутентификации пользователя в ОС извлечение электронного ключа JaCarta вызывает событие, определенное администратором в настройках параметров безопасности Windows. В домене Windows эти параметры для всех пользовательских компьютеров можно централизованно определять в редакторе групповых политик. Также существует возможность настроить эти параметры для отдельного компьютера посредством редактирования реестра.

Доступны следующие настройки.

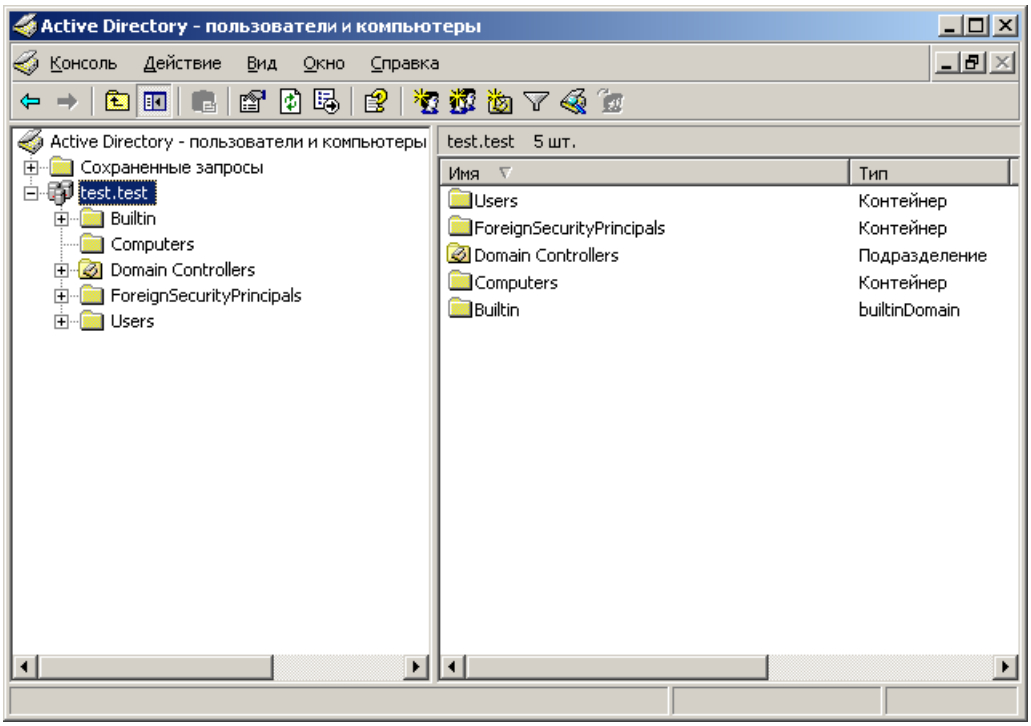
- Отсутствие действий
- Блокирование рабочей станции
- Завершение сеанса пользователя
- Завершение сеанса служб терминалов

Настройка поведения при извлечении электронного ключа JaCarta в редакторе групповых политик Windows Server 2003

Чтобы настроить поведение системы при извлечении электронного ключа JaCarta, выполните следующие действия.

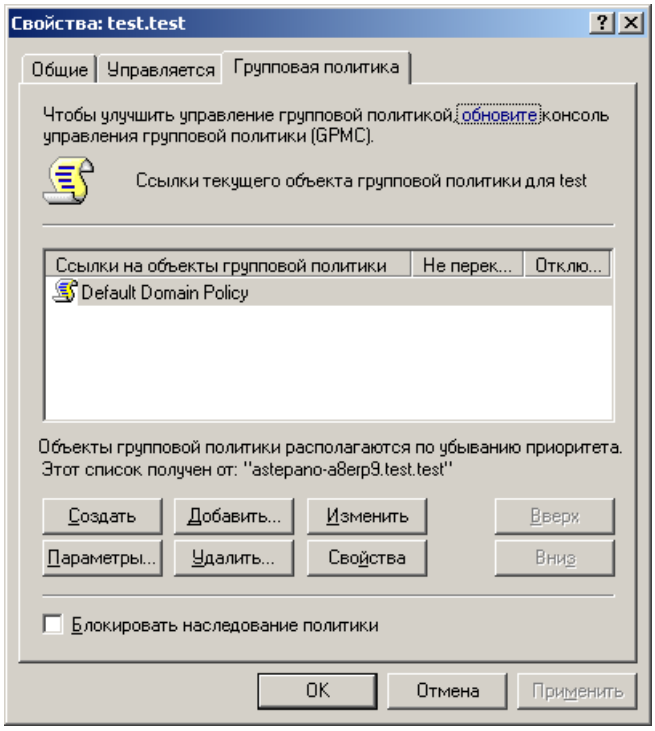
1. Выберите **Пуск > Администрирование > Active Directory - пользователи и компьютеры**.

   Откроется окно оснастки **Active Directory - пользователи и компьютеры**.



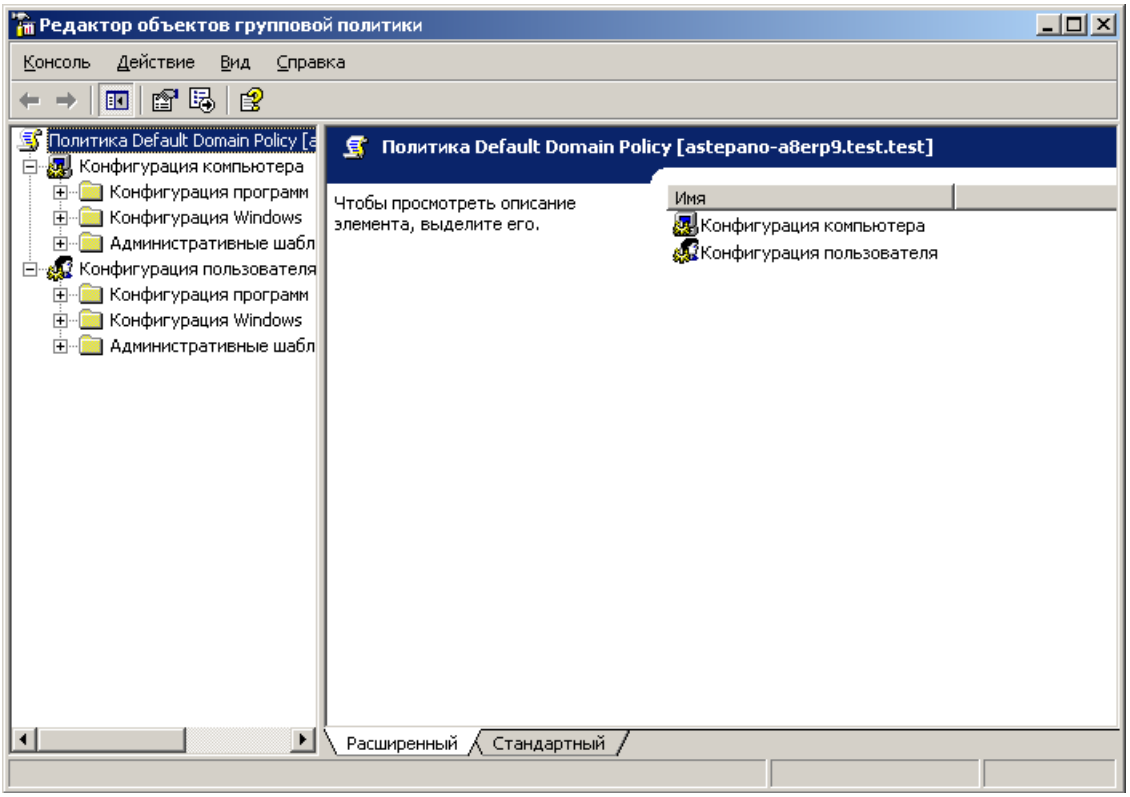
2. Щелкните правой кнопкой мыши на домене и в открывшемся контекстном меню выберите пункт **Свойства**.

3. Раскройте вкладку **Групповая политика** так, как показано на рисунке ниже.



4. Выберите в списке доступных политик пункт **Default Domain Policy** (Политика домена по умолчанию) и нажмите **Изменить**.

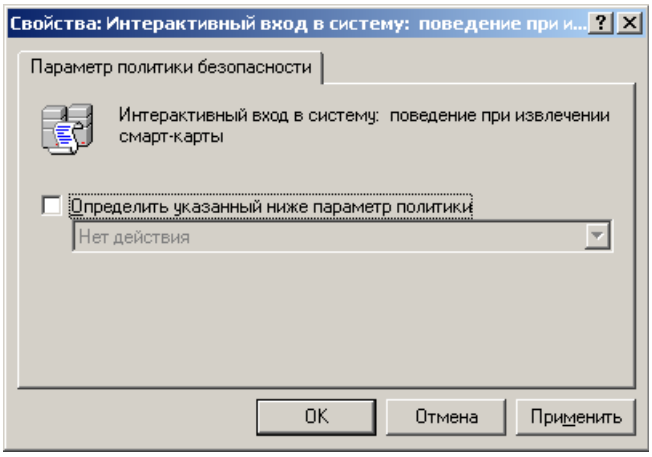
   Откроется окно редактора групповых политик.



5. Выберите **Конфигурация компьютера > Конфигурация Windows > Параметры безопасности > Локальные политики > Параметры безопасности**.

6. Щелкните правой кнопкой мыши в пункте **Интерактивный вход в систему: поведение при извлечении смарт-карты** и в открывшемся контекстном меню выберите пункт **Свойства**.

Откроется следующее окно.



7. Установите флажок в пункте **Определить указанный ниже параметр политики**.

   В поле ниже выберите из списка один из следующих пунктов:

   - **Нет действия**: при отключении не происходит никаких событий.
   - **Блокировка рабочей станции**: блокирование компьютера. Для разблокирования необходимо авторизоваться как текущий пользователь или администратор.
   - **Принудительный выход из системы**: завершение сеанса пользователя.
   - **Отключение в случае удаленного сеанса служб терминалов**: завершение сеанса службы терминалов.

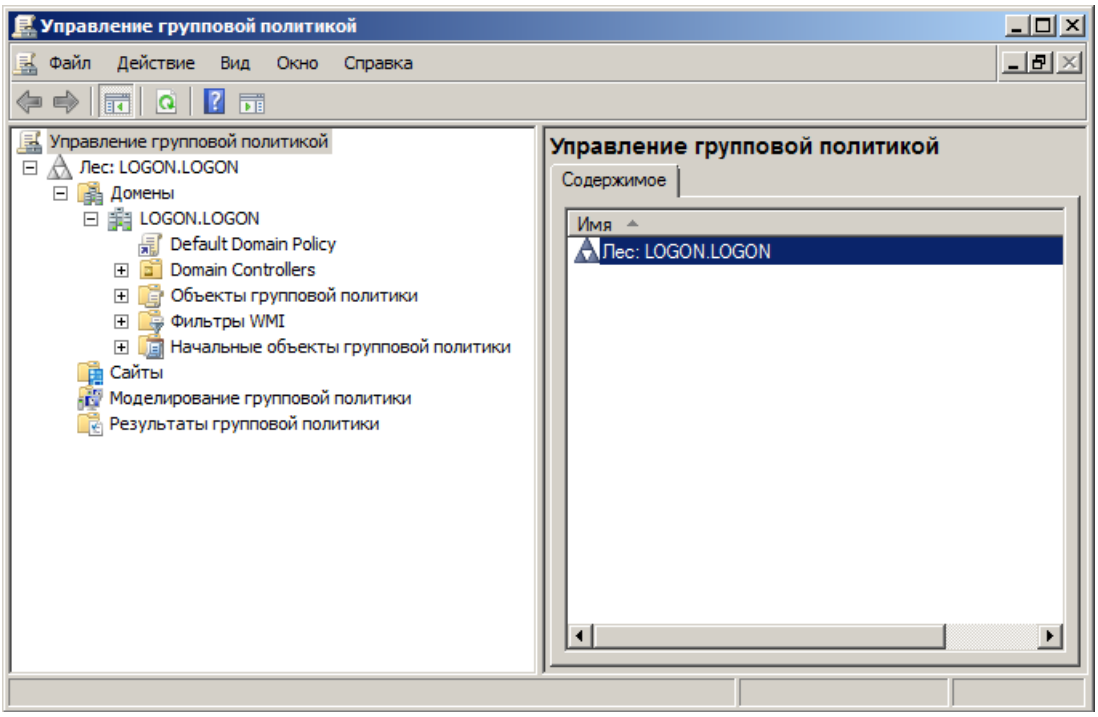
8. Нажмите кнопку **OK**.

Настройка поведения при извлечении электронного ключа JaCarta в редакторе групповых политик (Windows Server 2008/2012)

Чтобы установить в редакторе групповых политик поведение системы при извлечении электронного ключа JaCarta, выполните следующие действия.

1. Выберите **Пуск > Выполнить**, введите `gpmc.msc` и нажмите **OK**.

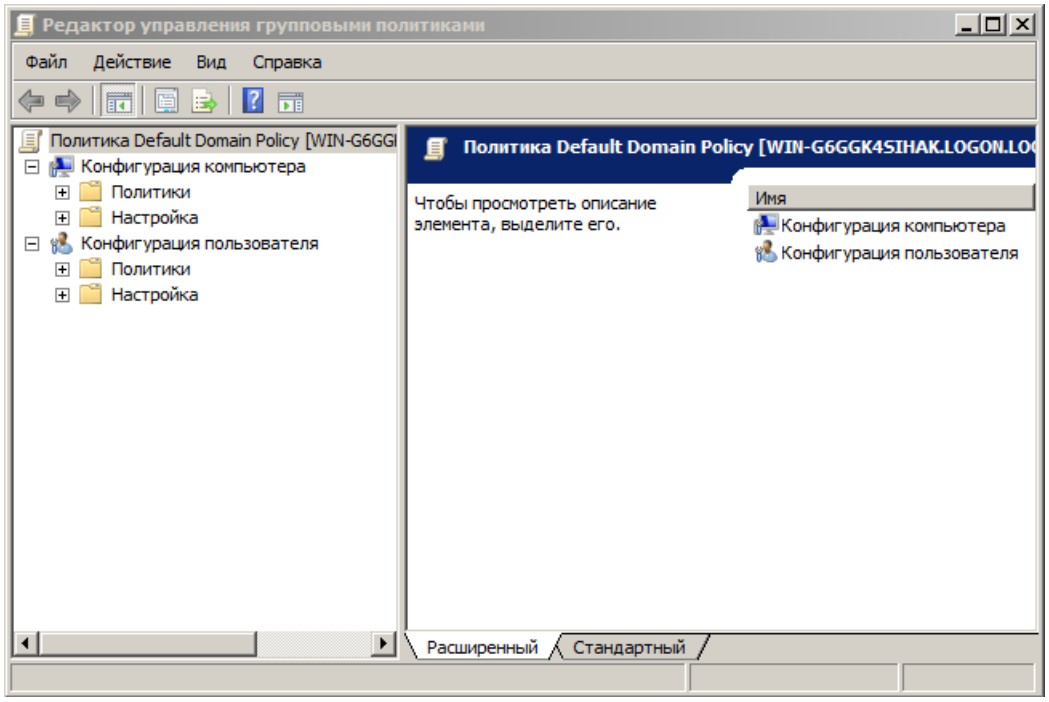
   Откроется следующее окно.



2. Выберите **Лес** и **Домен**, настройки которого необходимо изменить.

3. Щелкните правой кнопкой мыши на **Default Domain Policy** (Политика домена по умолчанию) и выберите **Изменить**.

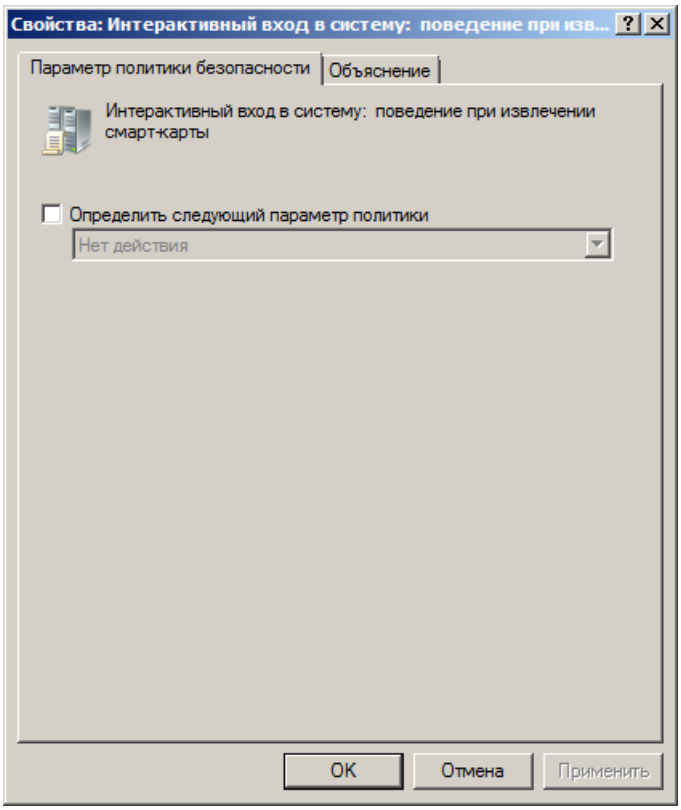
   Отобразится окно редактора групповых политик.



4. Раскройте ветвь **Конфигурация компьютера > Политики > Конфигурация Windows > Параметры безопасности > Локальные политики > Параметры безопасности**.

5. Щелкните правой кнопкой мыши в пункте **Интерактивный вход в систему: поведение при извлечении смарт-карты**.

   Отобразится следующее окно.



6. Установите флажок в пункте **Определить следующий параметр политики**.

В поле ниже выберите из списка один из следующих пунктов:

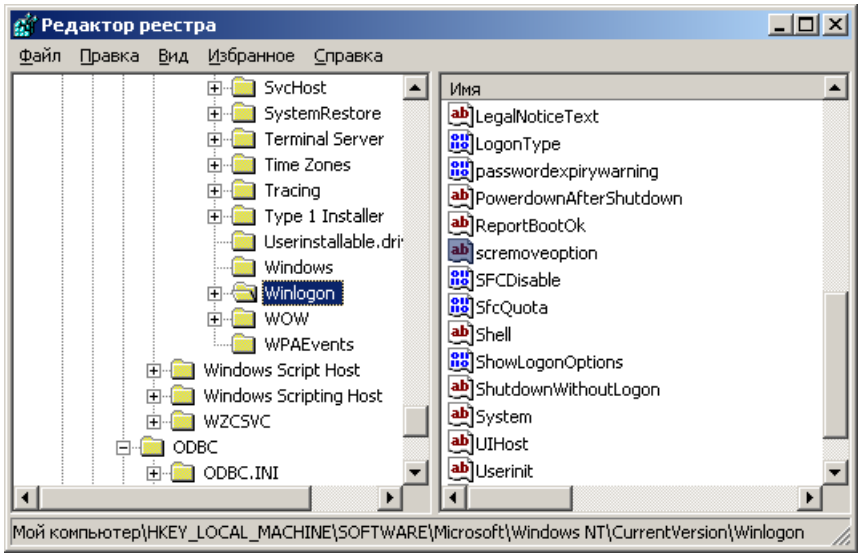
- **Нет действия**: при отключении не происходит никаких событий.
- **Блокировка рабочей станции**: блокирование компьютера (параметр устанавливается по умолчанию). Для разблокирования необходимо авторизоваться как текущий пользователь или администратор.
- **Принудительный выход из системы**: завершение текущего сеанса пользователя.
- **Отключение в случае удаленного сеанса служб удаленных рабочих столов**: завершение сеанса службы терминалов.

7. Нажмите кнопку **OK**.

Настройка поведения при извлечении электронного ключа JaCarta в редакторе реестра

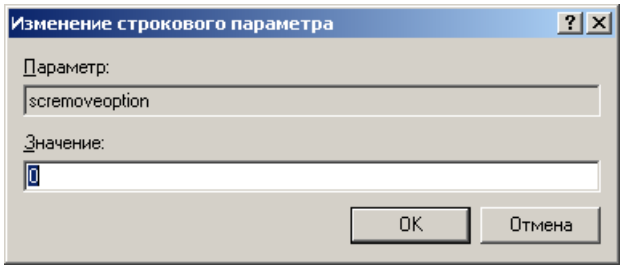
1. Запустите редактор реестра. Для этого из командной строки выполните команду `regedit`.
2. В окне редактора реестра раскройте ветвь `HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\Current Version\Winlogon`.

   (см. изображение ниже).



3. Выберите в списке параметров справа **scremoveoption** (или создайте такой параметр, если он отсутствует) и щелкните на нем дважды.

   Отобразится следующее окно.



4. Укажите необходимое значение параметра, руководствуясь приведенными данными.

Значение	Пояснение
0	При отключении не происходит никаких событий.
1	При отключении происходит блокирование компьютера. Для разблокирования необходимо авторизоваться как текущий пользователь или администратор.
2	При отключении происходит завершение сеанса пользователя.
3	При отключении происходит завершение сеанса служб

Значение	Пояснение
	терминалов (Terminal Services).

5. Нажмите **OK**.

   Новые параметры реестра вступят в силу после перезагрузки компьютера.

Стандартные профили персонализации

В поставку JC-Client входят два стандартных профиля персонализации: ASEDefault и MDDefault. В таблице ниже представлены параметры этих профилей и соответствующие этим параметрам значения.

Параметр	Значение ASEDefault	Значение MDDefault	Изменение доступно без повторной персонализации	Требуемый уровень доступа
Метка	«JaCarta#Серийный номер JaCarta»		Да	Пользователь/ Администратор
Пользователь должен сменить пароль (пароль пользователя)	Не установлено		Да	Администратор
Сменить пароль после разблокировки (пароль пользователя)	Не установлено		Да	Администратор
Проверять каждые … мин. (пароль пользователя)	Не установлено		Да	Администратор
Истекает через … дней (пароль пользователя)	Не установлено		Да	Администратор
Запоминать последние … паролей (пароль пользователя)	1	Не установлено	Нет	Не актуально
Тип доступа (пароль пользователя)	Пароль пользователя		Нет	Не актуально
Значение пароля (пароль пользователя)	11111111		Да	Пользователь
Минимум (пароль пользователя)	4 символа		Нет	Не актуально
Максимум (пароль пользователя)	10 символа		Нет	Не актуально
Попыток (неудачного ввода пароля пользователя)	10		Нет	Не актуально
Разблокировок	Не ограничено		Нет	Не актуально

Параметр	Значение ASEDefault	Значение MDDefault	Изменение доступно без повторной персонализации	Требуемый уровень доступа
(пароль пользователя)				
Количество отпечатков (пароль пользователя)	Не установлено		Нет	Не актуально
Качество (биометрия)	Не установлено		В процессе сохранения отпечатков в памяти электронного ключа JaCarta	Администратор
FAR (биометрия)	Не установлено			Администратора
Тип доступа (пароль администратора)	Пароль	Ключ 3DES	Нет	Не актуально
Значение пароля (пароль администратора)	00000000	3030303030303030	Если тип доступа – Пароль, администратор может сменить свой пароль. Если тип доступа – Ключ 3DES, изменение возможно только после очистки памяти или повторной персонализациию.	Администратор
Минимум (пароль администратора)	4 символа	Не актуально	Нет	Не актуально
Максимум (пароль администратора)	10 символов	Не актуально	Нет	Не актуально
Попыток (неудачного ввода пароля администратора)	3	3	Нет	Не актуально
Использовать пароль для ЦП	Нет		Нет	Не актуально

Настройка JC-Client, позволяющая повторную персонализацию в случае блокировки пароля администратора

При стандартных настройках JC-Client блокировка пароля администратора на электронном ключе JaCarta означает, что последующая очистка памяти и повторная персонализация такого электронного ключа JaCarta невозможны.

Чтобы сохранить возможность очистки памяти и повторной персонализации электронных ключей JaCarta, на которых заблокирован пароль администратора, необходимо выполнить следующие действия.

1. Перед персонализацией электронного ключа JaCarta установите значение ключа реестра **aseLeaveMFUnlockedAfterInit** в **1** (по умолчанию это значение установлено в **0**).

   В зависимости от разрядности операционной системы ключ расположен по следующему пути.

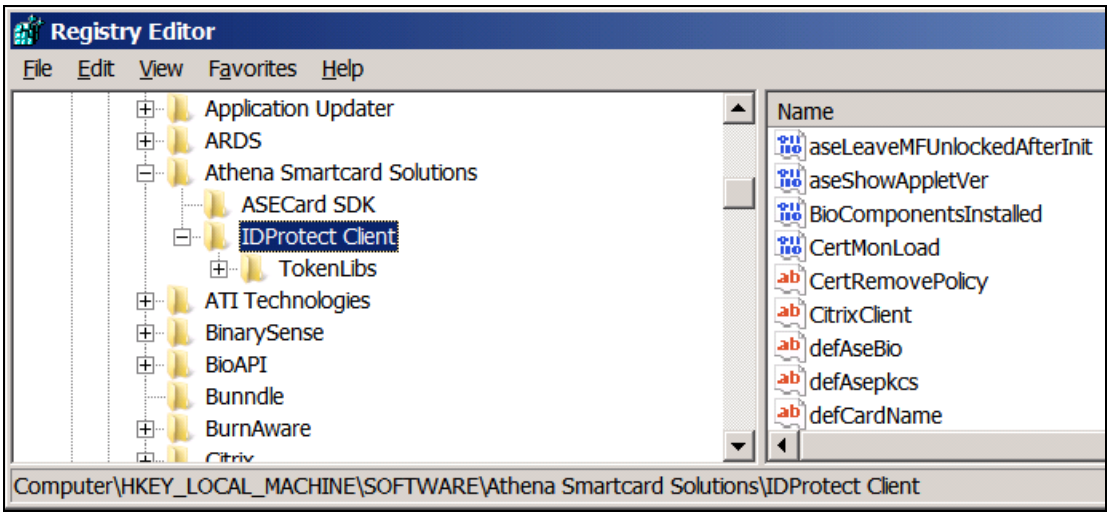
   - 32-разрядные системы:

     HKLM>Software>Athena Smartcard Solutions>IDProtect Client

   - 64-разрядные системы:

     HKLM>Software>Wow6432Node>Athena Smartcard Solutions>IDProtect Client

См. изображение ниже.



2. Персонализируйте электронный ключа JaCarta с использованием утилиты JaCarta Format (см. «Персонализация») и передайте ключ пользователю.

Если электронный ключ JaCarta был персонализирован на компьютере, на котором значение ключа реестра **aseLeaveMFUnlockedAfterInit** установлено в **1**, блокировка пароля администратора не будет препятствовать очистке памяти этого электронного ключа.

Таким образом, в случае блокировки пароля администратора на электронном ключе JaCarta выполните очистку памяти этого электронного ключа (утилита JaCarta Format, меню **JaCarta > Очистка памяти**), затем персонализируйте его на компьютере, на котором значение ключа реестра **aseLeaveMFUnlockedAfterInit** установлено в **1**.

Внимание!

Если электронный ключ JaCarta будет персонализирован на компьютере, на котором значение ключа реестра **aseLeaveMFUnlockedAfterInit** установлено в **0**, блокировка пароля администратора приведет к тому, что на этом электронном ключе невозможно будет выполнить очистку памяти и последующую персонализацию.

Известные проблемы и способы их решения

Проблема	Возможная причина и решение
Ошибки при установке программного обеспечения	
На экране появилось окно Windows Installer (Программа установки Windows) с сообщением: «Данная установка запрещена политикой, выбранной системным администратором».	**Возможная причина:** Вы не обладаете полномочиями локального администратора рабочей станции. **Решение:** 1. Нажмите **OK**. 2. Обратитесь к администратору.
Ошибки при вводе пароля администратора	
На экране появилось окно с сообщением: «Ошибка доступа! Количество попыток ввода пароля:»	**Возможная причина:** Вы неверно ввели пароль пользователя или пароль администратора электронного ключа JaCarta. **Решение:** Нажмите **OK** и повторите попытку. **Важно!** Число попыток ввода паролей пользователя и администратора электронного ключа JaCarta ограничено. Количество оставшихся попыток указано в отобразившемся сообщении.
При попытке изменить пароль пользователя или пароль администратора отображается следующее сообщение: «Неверный пароль. Возможно, он был использован раньше или не соответствует настройкам качества паролей.»	**Возможная причина:** Пароль не соответствует настройкам сложности, заданным на данном электронном ключе JaCarta. **Решение:** Нажмите **OK** и введите пароль, соответствующий существующим настройкам сложности.
На экране появилось окно с сообщением: «Пароль пользователя заблокирован».	**Возможная причина:** Пароль пользователя на данном электронном ключе JaCarta заблокирован, т.к. превышено количество попыток неправильного ввода пароля. **Решение:** Нажмите **OK** и выполните процедуру разблокировки пароля пользователя (см. «Разблокировка пароля пользователя»). **Внимание!** Не допускайте блокировки пароля администратора на электронных ключах JaCarta. Пароль администратора, в отличие от пароля пользователя, разблокировать невозможно.
Другие ошибки	
В нерусифицированной версии Windows XP и Windows Server 2003 кириллические символы в некоторых окнах JC-Client отображаются некорректно.	**Возможная причина:** Некоторые символы в интерфейсе JC-Client, не входят в набор Unicode. **Решение:** Чтобы включить поддержку соответствующих символов: 1. Выберите **Start** (Пуск) **> Control Panel** (Панель управления). 2. В отобразившемся окне двойным щелчком откройте окно **Regional and Language Options** (Язык и региональные стандарты). 3. В отобразившемся окне выберите вкладку **Advanced** (Дополнительно). 4. В списке **Select a language to match the language version of the non-Unicode programs you want to use** (Выберите язык, соответствующий языку используемых программ, которые не поддерживают Юникод) выберите **Russian** (Русский) 5. Установите флажок **Apply all settings to the current user account and to the default user profile** (Применить эти параметры для текущей учетной записи и для стандартного профиля пользователя) и нажмите **OK**, когда появится предупреждающее сообщение.

Проблема	Возможная причина и решение
	6. Нажмите **Apply** (Применить) 7. В появившемся диалоговом окне нажмите **Yes** (Да) 8. В отобразившемся окне с предложением перезагрузить компьютер нажмите **Yes** (Да) После перезагрузки компьютера символы кириллицы в соответствующих окнах будут отображаться корректно.
На ОС Windows XP / Server 2003 при первом подключении CCID-считывателя или USB-токена мастер настройки нового оборудования не может установить драйвер CCID, вследствие чего JC-Client не может увидеть подключенное устройство.	**Возможная причина:** Не установлен драйвер CCID. **Решение:** 1. Проверьте, подключен ли компьютер к Интернету и повторите попытку установки драйвера CCID с помощью мастера нового оборудования. 2. Если вам это не удалось, установите последние обновления из центра обновлений Windows и повторите попытку установки драйвера CCID с помощью мастера нового оборудования.

История изменений

Версия документа	Изменения
1.0	Исходная версия документа
1.1	Добавлены сведения, касающиеся возможности очистки памяти и повторной персонализации электронных ключей JaCarta в случае блокировки пароля администратора.

Аладдин РД

© 1995-2012, ЗАО «Аладдин Р.Д.»
Все права защищены
Тел.: +7 (495) 223-00-01
aladdin@aladdin-rd.ru
www.aladdin-rd.ru

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03 (продлены до 18.02.13)
Лицензии ФСБ России № 18229 от 13.10.10, № 9333Р от 03.09.10, № № 4205П, 4206Х от 22.06.07, № 4898П от 14.12.07
Microsoft Silver OEM Hardware Partner, Oracle Gold Partner
Все товарные знаки являются собственностью их владельцев