Аладдин РД
www.aladdin-rd.ru

# Использование JaCarta для биометрической аутентификации в среде Windows

Версия 1.0

Москва, 2013

# Аннотация

Настоящий документ содержит сведения по настройке биометрической аутентификации с использованием электронных ключей JaCarta в среде Windows. Мы постарались сделать документ удобным для практического применения. Если 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**

Лицензионное соглашение ..... 4
Введение ..... 8
Общие сведения о биометрической аутентификации ..... 8
Поддержка двух биометрических технологий ..... 8
Сведения о считывателях и сканерах отпечатков ..... 9
Дополнительная документация ..... 10
Жизненный цикл электронных ключей JaCarta ..... 10
Порядок действий ..... 12
Системные требования ..... 13
Поддерживаемые сканеры отпечатков пальцев ..... 13
Установка необходимого ПО ..... 14
Необходимые параметры командной строки ..... 15
Установка JC-Client с помощью программы-мастера ..... 16
Установка драйвера сканера отпечатков ..... 20
Настройка профиля персонализации ..... 21
Вкладка Общее ..... 23
Вкладка Пароль пользователя ..... 24
Вкладка Пароль администратора ..... 27
Персонализация с биометрическими настройками ..... 28
Операции с электронными ключами JaCarta ..... 33
Разблокировка ..... 33
Сохранение отпечатков пальцев в памяти электронного ключа JaCarta ..... 39
Дальнейшие действия ..... 41
Вход в домен с использованием биометрической аутентификации ..... 42
Приложения ..... 45
Настройка качества паролей ..... 45
Смена режима поддержки сканеров отпечатков ..... 46
История изменений ..... 48

# Лицензионное соглашение

**ВАЖНАЯ ИНФОРМАЦИЯ**

ПОЖАЛУЙСТА, ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ПРЕЖДЕ ЧЕМ ОТКРЫТЬ ПАКЕТ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ И/ИЛИ ИСПОЛЬЗОВАТЬ ЕГО СОДЕРЖИМОЕ И/ИЛИ ПРЕЖДЕ, ЧЕМ ЗАГРУЖАТЬ ИЛИ УСТАНАВЛИВАТЬ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ (далее ПО).

ВСЕ УКАЗАНИЯ ПО ИСПОЛЬЗОВАНИЮ ПО, ПРЕДОСТАВЛЯЕМЫЕ КОМПАНИЕЙ ЗАО «Аладдин Р.Д.» (или любым дочерним предприятием – каждое из них упоминаемое как ”КОМПАНИЯ”), ПОДЧИНЯЮТСЯ И БУДУТ ПОДЧИНЯТЬСЯ УСЛОВИЯМ, ОГОВОРЕННЫМ В ДАННОМ СОГЛАШЕНИИ.

ОТКРЫВАЯ ПАКЕТ, СОДЕРЖАЩИЙ ПО И/ИЛИ ЗАГРУЖАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ (как определено далее по тексту) И/ИЛИ УСТАНАВЛИВАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НА ВАШ КОМПЬЮТЕР И/ИЛИ ИСПОЛЬЗУЯ ДАННОЕ ПО ИНЫМ СПОСОБОМ, ВЫ ПРИНИМАЕТЕ ДАННОЕ СОГЛАШЕНИЕ И СОГЛАШАЕТЕСЬ С ЕГО УСЛОВИЯМИ.

ЕСЛИ ВЫ НЕ СОГЛАСНЫ С ДАННЫМ СОГЛАШЕНИЕМ, НЕ ОТКРЫВАЙТЕ ЭТОТ ПАКЕТ И/ИЛИ НЕ ЗАГРУЖАЙТЕ И/ИЛИ НЕ УСТАНАВЛИВАЙТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И НЕЗАМЕДЛИТЕЛЬНО (не позднее 7 дней с даты получения этого пакета) ВЕРНИТЕ ЭТОТ ПРОДУКТ В ЗАО «Аладдин Р.Д.», СОТРИТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ВСЕ ЕГО ЧАСТИ В СВОЕМ КОМПЬЮТЕРЕ И НЕ ИСПОЛЬЗУЙТЕ ЕГО НИКОИМ ОБРАЗОМ.

## Текст соглашения

Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключенным между Вами (физическим или юридическим лицом) - конечным пользователем (далее "Пользователь") и закрытым акционерным обществом ЗАО «Аладдин Р.Д.» (далее "Компания") относительно передачи неисключительного права на использование программного обеспечения, являющегося интеллектуальной собственностью Компании.

1. **Права и Собственность**.

   ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ. Это программное обеспечение, включая все переработки, исправления, модификации, дополнения, обновления и/или усовершенствования к нему (далее по всему тексту и любой его части определяемое как "Программное обеспечение" или "ПО"), и связанная с ним техническая / эксплуатационная документация предназначается НЕ ДЛЯ ПРОДАЖИ и является и остается исключительной собственностью Компании.

   Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), подтвержденные или включенные в приложенные/ взаимосвязанные/ имеющие отношение к данному Соглашению, данные, содержащиеся в нём, а также все права на ПО и техническую / эксплуатационную документацию являются и будут являться собственностью исключительно Компании.

   Данное соглашение не передает Вам права на ПО, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничего в данном Соглашении не подтверждает отказ Компании от прав на интеллектуальную собственность по какому бы то ни было законодательству.

2. **Лицензия**.

   После уплаты соответствующего вознаграждения Компания настоящим предоставляет Вам, а Вы получаете, индивидуальное, неисключительное и отзываемое ограниченное право на использование данного ПО только в форме исполняемого кода, как описано в прилагаемой к ПО технической / эксплуатационной документации и только в соответствии с условиями данного Соглашения.

   Вы можете установить ПО и использовать его на компьютерах, расположенных в пределах Вашего предприятия или для личного пользования, как описано в соответствующей технической / эксплуатационной документации ПО.

Вы можете добавить/присоединить Программное обеспечение к программам Вашего компьютера с единственной целью, описанной в данном Соглашении.

3. **Требования к использованию**.

ПО должно использоваться и обслуживаться строго в соответствии с описаниями и инструкциями Компании, приведенными в данном и других документах Компании, в том числе в технической / эксплуатационной документации на ПО.

Принимая условия настоящего Соглашения, Вы соглашаетесь:

- Не использовать, не модифицировать, и не выдавать сублицензии на данное ПО и любое другое ПО Компании, за исключением явных разрешений в данном Соглашении.
- Не продавать, не выдавать лицензий или сублицензий, не сдавать в аренду, не передавать, не переводить на другие языки, не закладывать, не разделять Ваши права в рамках данного Соглашения с кем-либо или кому-либо ещё.
- Не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное ПО и не пытаться раскрыть (получить) исходные коды данного ПО.
- Не помещать данное ПО на сервер с возможностью доступа к нему третьих лиц через открытую сеть.
- Не использовать какие бы то ни было резервные или архивные копии данного ПО (или позволять кому-либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

4. **Обслуживание и поддержка**.

Компания не несет обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов данного ПО.

5. **Ограниченная гарантия**.

Компания гарантирует, что:

- Данное ПО с момента приобретения его Вами в течение двенадцати (12) месяцев будет функционировать в полном соответствии с его технической / эксплуатационной документацией, при условии, что оно будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

6. **Отказ от гарантии**.

КОМПАНИЯ НЕ ГАРАНТИРУЕТ, ЧТО ПО БУДЕТ СООТВЕТСТВОВАТЬ ВАШИМ ТРЕБОВАНИЯМ, ИЛИ ЧТО ЕГО РАБОТА БУДЕТ БЕСПЕРЕБОЙНОЙ ИЛИ БЕЗОШИБОЧНОЙ. В ОБЪЕМЕ, ПРЕДУСМОТРЕННОМ ЗАКОНОДАТЕЛЬСТВОМ РФ, КОМПАНИЯ ОТКРЫТО ОТКАЗЫВАЕТСЯ ОТ ВСЕХ ГАРАНТИЙ, НЕ ОГОВОРЕННЫХ ЗДЕСЬ, ОТ ВСЕХ ИНЫХ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ. НИ ОДИН ИЗ ДИЛЕРОВ, ДИСТРИБЬЮТОРОВ, ПРОДАВЦОВ, АГЕНТОВ ИЛИ СОТРУДНИКОВ КОМПАНИИ НЕ УПОЛНОМОЧЕН ПРОИЗВОДИТЬ МОДИФИКАЦИИ, РАСШИРЕНИЯ ИЛИ ДОПОЛНЕНИЯ К ДАННОЙ ГАРАНТИИ.

Если Вы произвели какие-либо модификации ПО или любой из его частей во время гарантийного периода, ПО подверглось повреждению, неосторожному или неправильному обращению, если Вы нарушили любое из условий настоящего Соглашения, то гарантия, упомянутая выше в разделе 5, будет немедленно прекращена.

Гарантия недействительна, если ПО используется на или в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в технической / эксплуатационной документации, или используется на компьютере с любым установленным нелицензионным программным обеспечением.

7. **Ограничение возмещения**.

   В случае нарушения гарантии, оговоренной выше, Компания может по собственному усмотрению:

   - Заменить ПО, если это не противоречит вышеупомянутому ограничению гарантии.
   - Возместить стоимость, выплаченную Вами за ПО. Гарантийные требования должны быть выставлены в письменном виде в течение гарантийного периода, но не позднее семи (7) дней с момента обнаружения дефекта, и содержать в себе подтверждения, удовлетворяющие Компанию. Все ПО (все экземпляры, имеющиеся у Вас) должно быть возвращено дистрибьютору, через которого была совершена покупка (если покупка состоялась не непосредственно в Компании), и отправлена возвращающей стороной с оплаченной стоимостью перевозки и, при необходимости, страховки. Экземпляры ПО должны быть отправлены с копией платежных документов и накладных.

8. **Исключение косвенных убытков**.

   Стороны признают, что ПО не может быть полностью лишено ошибок. КОМПАНИЯ НЕ НЕСЁТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ) ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ, ПОБОЧНЫЕ ИЛИ ПОТЕНЦИАЛЬНЫЕ УБЫТКИ), ВКЛЮЧАЯ, БЕЗ ОГРАНИЧЕНИЙ, ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЕННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ КАКОГО-ЛИБО ИСПОЛЬЗОВАНИЯ ДАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОЙ КОМПОНЕНТЫ ДАННОГО ПО, ДАЖЕ ЕСЛИ КОМПАНИЯ ПИСЬМЕННО УВЕДОМЛЕНА О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

9. **Ограничение ответственности**.

   В СЛУЧАЕ ЕСЛИ, НЕСМОТРЯ НА УСЛОВИЯ ДАННОГО СОГЛАШЕНИЯ, КОМПАНИЯ ПРИЗНАНА ОТВЕТСТВЕННОЙ ЗА УБЫТКИ НА ОСНОВАНИИ КАКИХ-ЛИБО ДЕФЕКТОВ ИЛИ НЕСООТВЕТСТВИЯ ПО ВАШИМ ОЖИДАНИЯМ, ПОЛНАЯ ОТВЕТСТВЕННОСТЬ ЗА КАЖДЫЙ ЭКЗЕМПЛЯР ДЕФЕКТНОГО ПО НЕ БУДЕТ ПРЕВЫШАТЬ СУММУ, ВЫПЛАЧЕННУЮ ВАМИ КОМПАНИИ ЗА ЭТИ ДЕФЕКТНЫЕ ПРОДУКТЫ.

10. **Прекращение действия Соглашения**.

    В случае невыполнения Вами условий данного Соглашения действие Вашей лицензии и настоящего Соглашения будет прекращено.

    После прекращения действия данного Лицензионного Соглашения:

    - Лицензия, предоставленная Вам данным Соглашением, прекращает свое действие, и Вы после ее прекращения не сможете продолжать дальнейшее использование данного Программного обеспечения и других лицензионных Продуктов;
    - Вы незамедлительно вернёте в Компанию все экземпляры ПО и все копии такового и/или сотрёте/удалите любую информацию, содержащуюся в электронном виде. Разделы 1, 3, 6-11 будут продолжать действовать даже в случае прекращения действия настоящего Соглашения.

11. **Применимое законодательство**.

    Данное Соглашение должно быть истолковано и определено в соответствии с законодательством Российской Федерации, и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Невозможность для любой из сторон воспользоваться любым из прав, предоставленных ей по данному Соглашению, или принять меры против другой стороны в случае любого нарушения своих обязательств по Соглашению не должно рассматриваться как отказ этой стороны от последующего понуждения к признанию своих прав или совершению последующих действий в случае дальнейших нарушений.

12. **Государственное регулирование и экспортный контроль**.

    Вы соглашаетесь с тем, что ПО не будет Вами поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону образом. ПО является предметом дополнительного экспортного контроля, относящегося к Вам или Вашей юрисдикции. Вы гарантируете, что будете соблюдать накладываемые на экспорт и реэкспорт ПО ограничения.

13. **Программное обеспечение третьих сторон**.

    Если ПО содержит в себе любое программное обеспечение, предоставленное какой-либо третьей стороной, такое программное обеспечение третьей стороны предоставляется "как есть" без какой-либо гарантии, и разделы 2, 3, 6, 8, 9-12 настоящего Соглашения применяются ко всем таким поставщикам программного обеспечения и к поставляемому ими программному обеспечению, как если бы это были Компания и ПО соответственно.

14. **Разное**.

    Настоящее Соглашение представляет собой полное соглашение, относящееся к данной лицензии, и может быть изменено только посредством письменного соглашения, подписанного обеими сторонами. Если выполнение какого-либо условия настоящего Соглашения представляется невозможным, такое условие будет скорректировано только в пределах, обеспечивающих возможность выполнения данного условия.

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ.

Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ.

ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНАВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

# Введение

Электронные ключи JaCarta в сочетании с программным обеспечением JC-Client позволяют осуществлять биометрическую аутентификацию в домене Windows (доступ по отпечатку пальца). Помимо регистрации пользователя в домене Windows и использования подключения к удаленному рабочему столу (RDP), биометрический доступ может использоваться для дополнительной защиты:

- доступа к веб-ресурсам через HTTPS (SSL);
- электронной почты.

## Общие сведения о биометрической аутентификации

Технология биометрического контроля позволяет строить надежные решения с двух- или трехфакторной аутентификацией. Биометрический метод может использоваться как вместо пароля пользователя JaCarta, так и в сочетании с ним. В качестве уникальной биометрической характеристики используются отпечатки пальцев. Для доступа к смарт-карте можно зарегистрировать до десяти отпечатков.

Эталонный цифровой образ отпечатка пальца, или шаблон отпечатка, сохраняется в защищенной памяти смарт-карты в процессе персонализации (подробнее о персонализации см. раздел "Жизненный цикл электронных ключей JaCarta").

Во время аутентификации пользователь должен вставить смарт-карту в считыватель и приложить палец к сканеру отпечатков. Если отпечаток пальца соответствует шаблону, аутентификация будет успешной. Технология Match-on-Card позволяет произвести сравнение исключительно внутри микросхемы смарт-карты, что обеспечивает защищенность процесса аутентификации.

## Поддержка двух биометрических технологий

JC-Client поддерживает работу со смарт-картами, выполненными с использованием двух различных биометрических технологий:

- технология, разработанная компанией Precise Biometrics.
- технология, соответствующая стандарту ISO 19794.

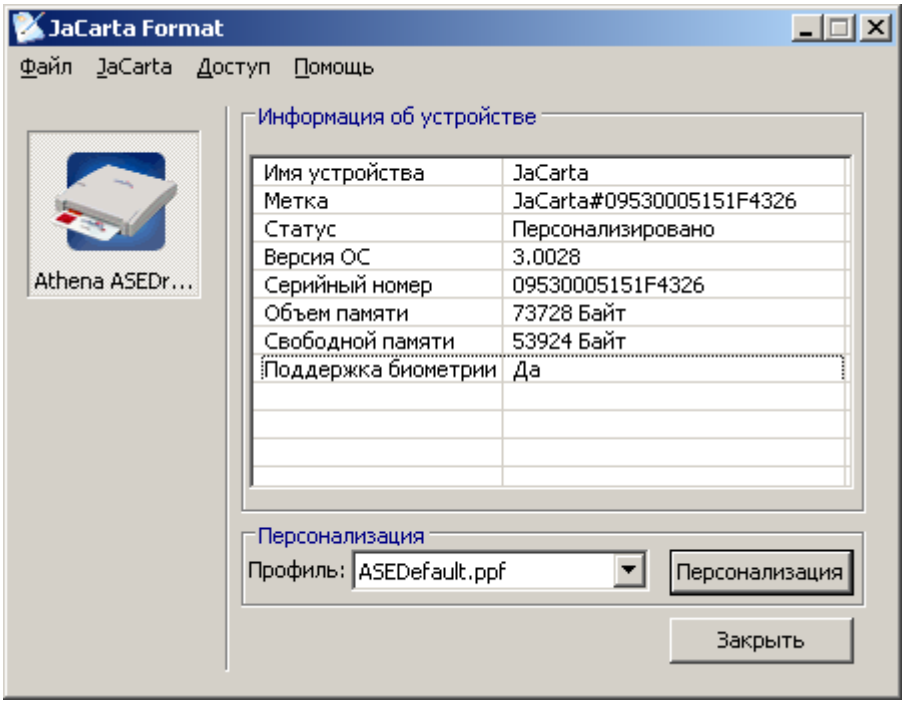
**Поддержку работы с той или иной технологией необходимо задать на этапе установки** (подробнее см. раздел "Необходимые параметры командной строки")**.**

**Примечание:**

> В настоящее время все поставляемые биометрические смарт-карты JaCarta сделаны с применением технологии Precise Biometrics. В будущем планируется выпуск смарт-карт на основе технологии ISO 19794.

Чтобы выяснить, какая из двух биометрических технологий была использована при производстве смарт-карты, можно воспользоваться утилитой JaCarta Format или JaCarta Manager из состава JC-Client.

Для этого подключите смарт-карту к считывателю и запустите утилиту JaCarta Format или JaCarta Manager.




В основном окне утилиты в поле **Поддержка биометрии** в зависимости от использованной технологии будет отображаться:

| Биометрическая технология | Значение в поле "Поддержка биометрии" |
|---|---|
| Precise Biometrics | **Да** |
| ISO 19794 | **ISO** |
| Биометрия не поддерживается | **Нет** |

## Сведения о считывателях и сканерах отпечатков

Комбинированные считыватели смарт-карт серии ASEDrive Bio, выпускаемые компанией Athena, представляют собой два функционально независимых устройства, объединенных в одном корпусе.

1. Считыватель ASEDrive для контактных смарт-карт (считыватель смарт-карт).
2. Сканер отпечатков пальцев Authentec/Upek. В зависимости от модели комбинированного считывателя ASEDrive Bio могут использоваться различные типы сканеров отпечатков:
   - UPEK TCS1 TouchChip sensor EIM (Authentec/Upek), тип сканера – touch, снятие отпечатка за одно прикосновение;
   - EIM Light with TCS2 (Authentec/Upek), тип сканера - touch, снятие отпечатка за одно прикосновение;
   - UPEK TCS4K TouchStrip (Authentec/Upek), тип сканера – swipe, для снятия отпечатка палец надо провести по сканеру.

Также существует возможность использовать другие сканеры отпечатков (например, если в вашей организации используются считыватели смарт-карт, не имеющие встроенного сканера, или у какого-либо пользователя уже имеется сканер отпечатков, встроенный в ноутбук) – сведения о поддерживаемых сканерах отпечатков представлены в разделе "Поддерживаемые сканеры отпечатков пальцев".

**Поддержку работы с тем или иным видом биометрического сканера необходимо задать на этапе установки.** Также, после установки существует возможность изменить режим поддержки сканеров, отредактировав параметры реестра (см. раздел "Смена режима поддержки сканеров отпечатков").

**Примечание:**

В настоящем документе подробно рассматривается вариант работы с комбинированными считывателями ASEDrive Bio.

## Дополнительная документация

В настоящем документе содержатся ссылки на дополнительную документацию, с которой также рекомендуется ознакомиться.

- *JC-Client. Руководство администратора*.
- *JC-Client. Руководство пользователя*.
- *JaCarta для Microsoft Windows. Руководство по внедрению*.
- *Технические характеристики считывателей ASEDrive Bio*.

## 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 из состава программного обеспечения JC-Client.

В процессе персонализации задаются основные параметры использования электронного ключа JaCarta, такие как качество пароля пользователя и возможность входа в систему по отпечатку пальца. Для входа пользователя в систему используется пароль пользователя и/или сканирование отпечатка пальца. Доступны следующие комбинации:

- **Пароль пользователя** – для доступа пользователь должен ввести только пароль пользователя.

**Примечание:**

В настоящем руководстве использование только пароля пользователя не рассматривается (подробнее см. документ *JC-Client. Руководство администратора.*)

- **Биометрия** – для доступа используется только сканирование отпечатка пальца.
- **Биометрия или пароль** – чтобы подтвердить доступ, пользователь должен ввести пароль пользователя или приложить палец к сканеру отпечатков. Любой из этих типов доступа будет достаточным для успешной аутентификации. В данном режиме, даже если один из типов доступа заблокирован, пользователь сможет войти в систему, используя другой тип доступа.
- **Биометрия и пароль** – чтобы получить доступ, пользователь должен ввести пароль пользователя и приложить палец к сканеру. Для успешной аутентификации необходимо выполнение обоих условий. В данном режиме, если один из типов доступа заблокирован, пользователь не сможет войти в систему без помощи администратора.

Также можно задать возможность использования дополнительного пароля цифровой подписи.

**Примечание:**

В настоящем руководстве настройка и использование пароля цифровой подписи не рассматривается (подробнее см. документ *JC-Client. Руководство администратора.*)

Процедуры настройки профиля персонализации с биометрическими параметрами и процесса персонализации описаны в разделах "Настройка профиля персонализации" и "Персонализация с биометрическими настройками" 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 (пароль пользователя или разблокировка доступа по отпечатку). Так, если в настройках электронного ключа JaCarta, был задан доступ **Биометрия или пароль**, то блокирование одного из этих типов доступа все еще позволяет пользователю войти в систему, используя другой тип доступа. Для разблокировки пароля пользователя и/или доступа по отпечатку пальца необходим пароль администратора или ключ администратора.

**Примечание:**

> Ключ администратора представляет собой электронный ключ JaCarta, предоставляющий доступ на уровне администратора к электронным ключам пользователей. Использование ключа администратора, а также описание уровней доступа к электронному ключу JaCarta представлены в документе *JC-Client. Руководство администратора* и не входит в задачи настоящего руководства.

Процедуры разблокировки представлены в разделе “Разблокировка”.

Если электронный ключ JaCarta необходимо передать другому лицу, его можно персонализировать повторно с новыми настройками (на основе того же или нового профиля персонализации). 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 этой 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.

# Порядок действий

Чтобы использовать электронные ключи JaCarta для биометрической аутентификации (аутентификации по отпечатку пальца), выполните следующие действия.

1. Ознакомьтесь с разделом “Введение”.
2. Удостоверьтесь в том, что ваша система соответствует необходимым требованиям (см. раздел “Системные требования”).
3. Установите необходимое программное обеспечение (см. раздел “Установка необходимого ПО”).
4. Настройте профиль персонализации (см. раздел “Настройка профиля персонализации”)
5. Персонализируйте электронные ключи JaCarta на основе настроенного профиля персонализации (см. раздел “Персонализация с биометрическими настройками”).
6. Ознакомьтесь с разделом “Операции с электронными ключами JaCarta”.
7. Запишите в память электронных ключей JaCarta цифровые сертификаты пользователей (см. раздел “Дальнейшие действия”).

   После выполнения необходимых действий пользователи смогут входить в домен Windows, используя биометрическую аутентификацию (см. раздел “Вход в домен с использованием биометрической аутентификации”).

# Системные требования

Убедитесь в том, что компьютеры соответствуют необходимым требованиям.

| | |
|---|---|
| **Поддерживаемые операционные системы** | • Windows XP SP3 (32-бит)<br>• Windows XP SP2 (64-бит)<br>• Windows Server 2003 SP2 (32/64-бит)<br>• Windows Vista SP2 (32/64-бит)<br>• Windows Server 2008 SP2 (32/64-бит)<br>• Windows 7 SP1 (32/64-бит)<br>• Windows Server 2008 R2 SP1<br>• Windows 8 (32/64-бит) |
| **Поддерживаемые браузеры** | • Firefox<br>• Internet Explorer |
| **Поддерживаемые модели электронных ключей** | • Смарт-карта JaCarta с поддержкой биометрии |
| **Необходимые аппаратные средства** | Наличие установленного считывателя смарт-карт и сканера отпечатков пальцев (см. также раздел "Поддерживаемые сканеры отпечатков пальцев" ниже). |
| **Необходимое ПО** | • JC-Client актуальной версии – для работы с электронными ключами JaCarta.<br>• Для обеспечения биометрической аутентификации также необходимо установить актуальный драйвер для используемой модели биометрического сканера.<br>(Установка описана в разделе "Установка необходимого ПО" далее). |
| **Рекомендуемое разрешение экрана** | Для работы ПО JC-Client рекомендуется установить разрешение монитора не ниже 1024x768. |

## Поддерживаемые сканеры отпечатков пальцев

| Производитель | Модели |
|---|---|
| Authentec/Upek | Сканеры Authentec/Upek используются в считывателях смарт-карт серии ASEDrive Bio.<br>**Примечание:** чтобы выяснить, совместима ли та или иная модель сканера с JC-Client, обратитесь в службу технической поддержки ЗАО "Аладдин Р.Д." (контактные данные указаны в аннотации к настоящему документу). |
| Nitgen | Сканеры серии Hamster. |
| Validity | • VFS5111<br>• VFS5011<br>• VFS5131<br>• VFS471<br>• VFS451<br>• Семейство сканеров VFS300<br>• VFS201<br>• VFS491 |
| Precise Biometrics | MC 200/250<br>**Примечание:** эти сканеры можно использовать только в том случае, если JC-Client установлен в режиме CSP (не Minidriver). |

**Примечание:**

В настоящем документе рассматривается вариант работы с комбинированными считывателями смарт-карт серии ASEDrive Bio со встроенным сканером отпечатков Authentec/Upek.

# Установка необходимого ПО

Установка JC-Client в режиме поддержки биометрической аутентификации возможна как из командной строки (в том числе в полуавтоматическом режиме), так и с помощью программы-мастера.

- При установке JC-Client из командной строки команда будет выглядеть следующим образом:

  `msiexec /i <файл установки> INSTALLPRECISELIBS=1 INSTBIOCOMP=1 INSTALLCP=1 /qn`

**Примечание:**

Представлено на примере команды для установки JC-Client на ОС Windows Vista/Server 2008/7/8.

где:

`<файл установки>` - путь к файлу установки, включая имя файла.

`INSTALLPRECISELIBS=1` – параметр, задающий необходимость установки JC-Client в режиме поддержки биометрической технологии Precise Biometrics, реализованной в электронных ключах JaCarta.

`INSTBIOCOMP=1` – параметр, задающий необходимость установки компонента JC-Client, позволяющего персонализировать с биометрическими настройками и использовать для биометрической аутентификации электронные ключи JaCarta.

`INSTALLCP=1` – параметр, задающий необходимость установки компонента Credential Provider, который позволяет осуществлять вход в систему по результатам сканирования отпечатка пальца. **В случае с операционными системами Windows XP/Server 2003 вместо** `INSTALLCP=1` **следует использовать** `INSTALLGINA=1`.

`/qn` – параметр, позволяющий установить JC-Client в полуавтоматическом режиме без отображения пользовательского интерфейса мастера установки.

Сведения о параметрах командной строки представлены также в разделе “Необходимые параметры командной строки” настоящего документа и в документе *JC-Client. Руководство администратора*.

- При установке JC-Client с помощью программы-мастера для запуска мастера установки также необходимо выполнить команду из командной строки. Типичная команда в этом случае будет выглядеть следующим образом.

  `msiexec /i <файл установки> INSTALLPRECISELIBS=1`

  где:

  `<файл установки>` - путь к файлу установки, включая имя файла.

  `INSTALLPRECISELIBS=1` – параметр, задающий необходимость установки JC-Client в режиме поддержки биометрической технологии Precise Biometrics, реализованной в электронных ключах JaCarta.

  После выполнения этой команды отобразится окно мастера установки, в котором можно будет отметить к установке необходимые компоненты.

  Подробные сведения об установке с помощью программы-мастера представлены в разделах “Необходимые параметры командной строки” и “Установка JC-Client с помощью программы-мастера” настоящего документа.

**Примечание:**

После установки JC-Client установите существующие пакеты обновлений. О наличии пакетов обновлений вы можете узнать в службе технической поддержки. Контактные данные службы технической поддержки указаны в аннотации к настоящему документу.

## Необходимые параметры командной строки

При установке JC-Client необходимо задать режим поддержки биометрической технологии (Precise Biometrics или ISO 19794), а также задать режим поддержки сканеров отпечатков (см. раздел "Поддерживаемые сканеры отпечатков пальцев"). Эти настройки задаются двумя параметрами.

1. `INSTALLPRECISELIBS` – данный параметр определяет режим поддержки биометрической технологи (т.е., с какими типами биометрических смарт-карт, Precise Biometrics или ISO 19794, будет взаимодействовать JC-Client).
2. `ASESENSBSPS` – данный параметр определяет режим поддержки сканера отпечатков пальцев (т.е., какие биометрические сканеры можно использовать для сканирования отпечатков).

Команда должна иметь следующий вид.

```
msiexec /i <файл установки> INSTALLPRECISELIBS=<ЗНАЧЕНИЕ> ASESENSBSPS=<ЗНАЧЕНИЕ>
```

где:

`<файл установки>` - полный путь к файлу установки, включая имя файла.

`<ЗНАЧЕНИЕ>` – нужное значение соответствующего параметра.

**Примечание:**

После выполнения команды такого вида отобразится окно мастера установки JC-Client.

Чтобы установить JC-Client в полуавтоматическом режиме, следует использовать параметр `/qn`. С помощью командной строки также можно отметить к установке другие компоненты JC-Client. Полный список параметров командной строки представлен в документе *JC-Client. Руководство администратора*.

Доступные значения параметров `INSTALLPRECISELIBS` и `ASESENSBSPS` представлены ниже.

| | |
|---|---|
| **Имя** | INSTALLPRECISELIBS |
| **Описание** | Установка библиотек, обеспечивающих взаимодействие JC-Client со смарт-картами, выполненными на основе одной из двух биометрических технологий. |
| **Значения** | 1: технология Precise Biometrics<br>2: технология ISO 19794 |
| **По умолчанию** | 2 |

| | |
|---|---|
| **Имя** | ASESENSBSPS |
| **Описание** | Установка компонентов, необходимых для взаимодействия JC-Client с различными моделями сканеров отпечатков пальцев |
| **Значения** | 1: Precise Biometrics<br>4: Validity<br>5: Precise Biometrics, Validity<br>8: Nitgen<br>9: Precise Biometrics, Nitgen<br>13: Precise Biometrics, Nitgen, Validity<br>16: Authentec/Upek<br>17: Authentec/Upek, Precise Biometrics<br>21: Authentec/Upek,Precise Biometrics, Validity<br>29: Authentec/Upek,Precise Biometrics, Validity, Nitgen<br>36: Authentec/Upek, Nitgen |
| **По умолчанию** | 16 (Authentec/Upek – сканеры, встроенные в комбинированные считыватели ASEDrive Bio) |

### Примеры

- Таким образом, чтобы установить JC-Client в режиме поддержки смарт-карт, выполненных с использованием биометрической технологии Precise Biometrics, а также задать поддержку сканеров Authentec/Upek, входящих в состав комбинированных считывателей ASEDrive Bio, необходимо выполнить следующую команду:
  - для установки с помощью программы-мастера (версия ОС не имеет значения)

    ```
    msiexec /i <файл установки> INSTALLPRECISELIBS=1
    ```

  - для установки в полуавтоматическом режиме (Windows XP/Server 2003)

    ```
    msiexec /i <файл установки> INSTALLPRECISELIBS=1 INSTBIOCOMP=1 INSTALLGINA=1 /qn
    ```

  - для установки в полуавтоматическом режиме (Windows Vista/Server 2008/7)

    ```
    msiexec /i <файл установки> INSTALLPRECISELIBS=1 INSTBIOCOMP=1 INSTALLCP=1 /qn
    ```

**Примечание:**

> В данном случае нет необходимости определять параметр `ASESENSBSPS`, т.к. значение `ASESENSBSPS=16`, соответствующее режиму поддержки сканеров Authentec/Upek, является значением по умолчанию.

- Чтобы установить JC-Client в режиме поддержки смарт-карт, выполненных с использованием биометрической технологии Precise Biometrics, а также задать поддержку биометрических сканеров Validity, необходимо выполнить следующую команду.
  - для установки с помощью программы-мастера (версия ОС не имеет значения):

    ```
    msiexec /i <файл установки> INSTALLPRECISELIBS=1 ASESENSBSPS=4
    ```

  - для установки в полуавтоматическом режиме (Windows XP/Server 2003)

    ```
    msiexec /i <файл установки> INSTALLPRECISELIBS=1 ASESENSBSPS=4 INSTBIOCOMP=1
    INSTALLGINA=1 /qn
    ```

  - для установки в полуавтоматическом режиме (Windows Vista/Server 2008/7)

    ```
    msiexec /i <файл установки> INSTALLPRECISELIBS=1 ASESENSBSPS=4 INSTBIOCOMP=1
    INSTALLCP=1 /qn
    ```

## Установка JC-Client с помощью программы-мастера

1. Чтобы установить JC-Client с помощью программы-мастера, выполните из командной строки команду следующего вида.

   ```
   msiexec /i <файл установки> INSTALLPRECISELIBS=1
   ```

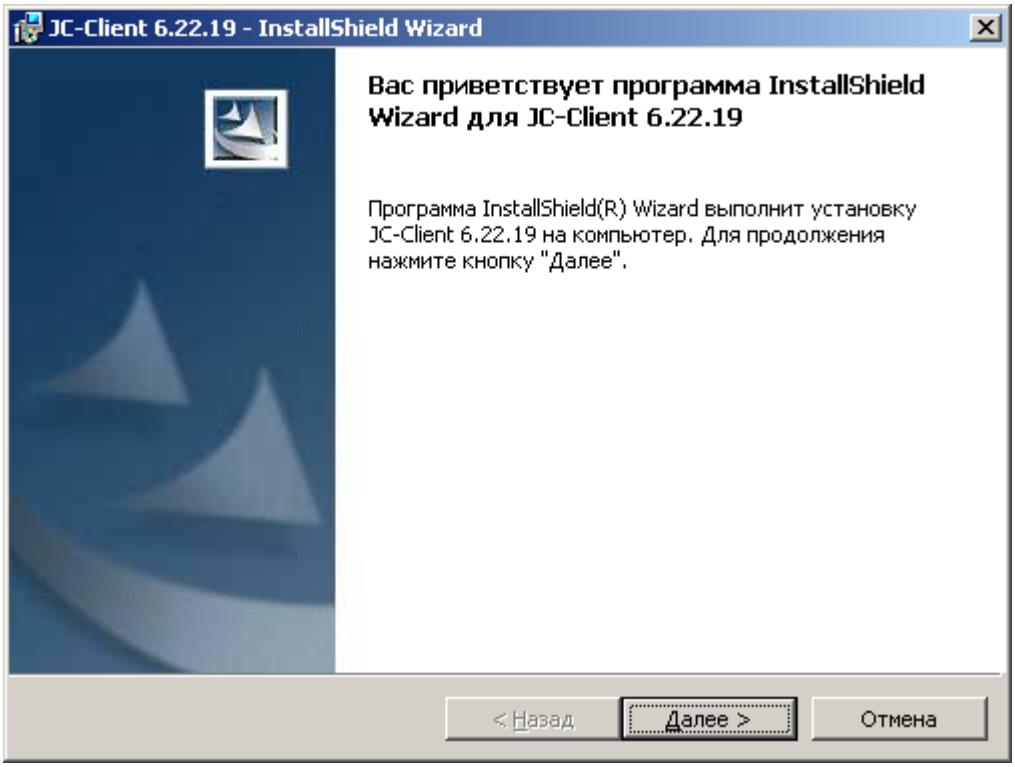
   где:

   `<файл установки>` - путь к файлу установки с указанием имени файла.

**Примечание:**

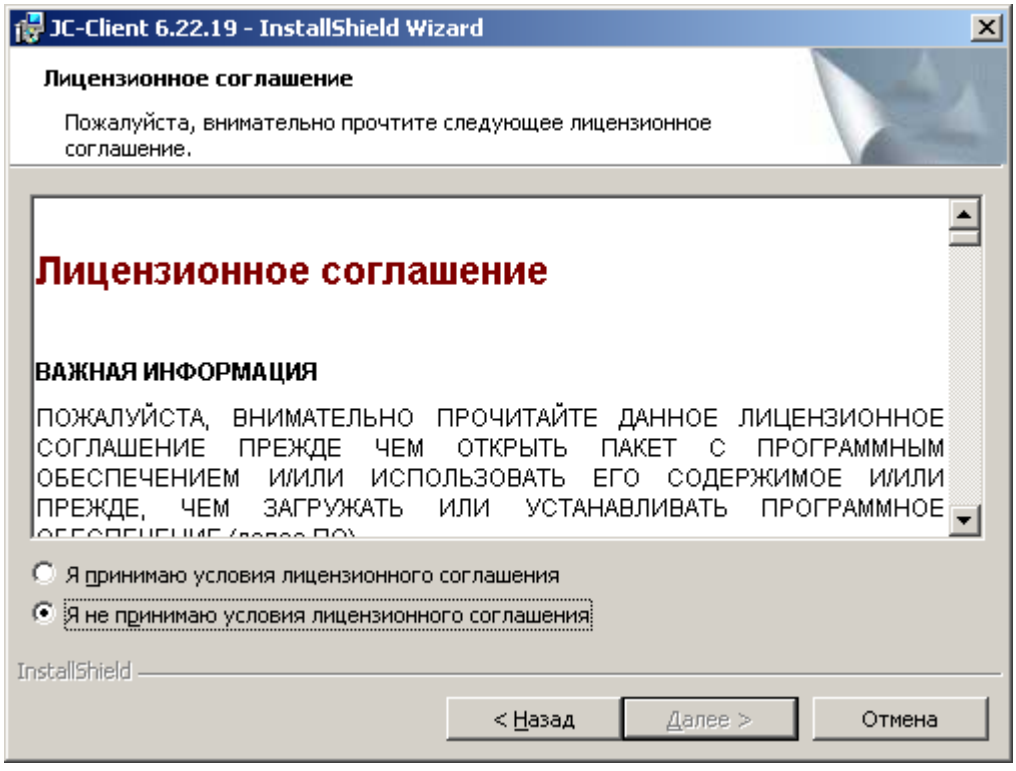
> Приведенная команда задает поддержку биометрической технологии Precise Biometrics и сканеров Authentec/Upek, входящих в состав комбинированных считывателей ASEDrive Bio.

Отобразится следующее окно.



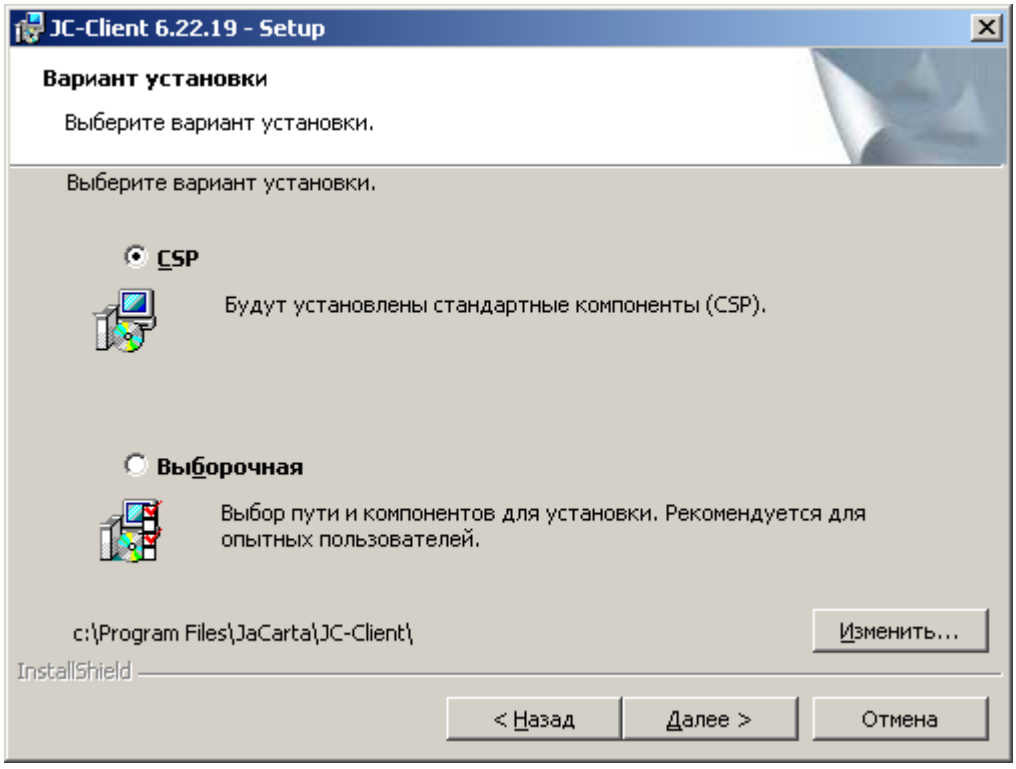

1. Нажмите **Далее**.

   Отобразится следующее окно.



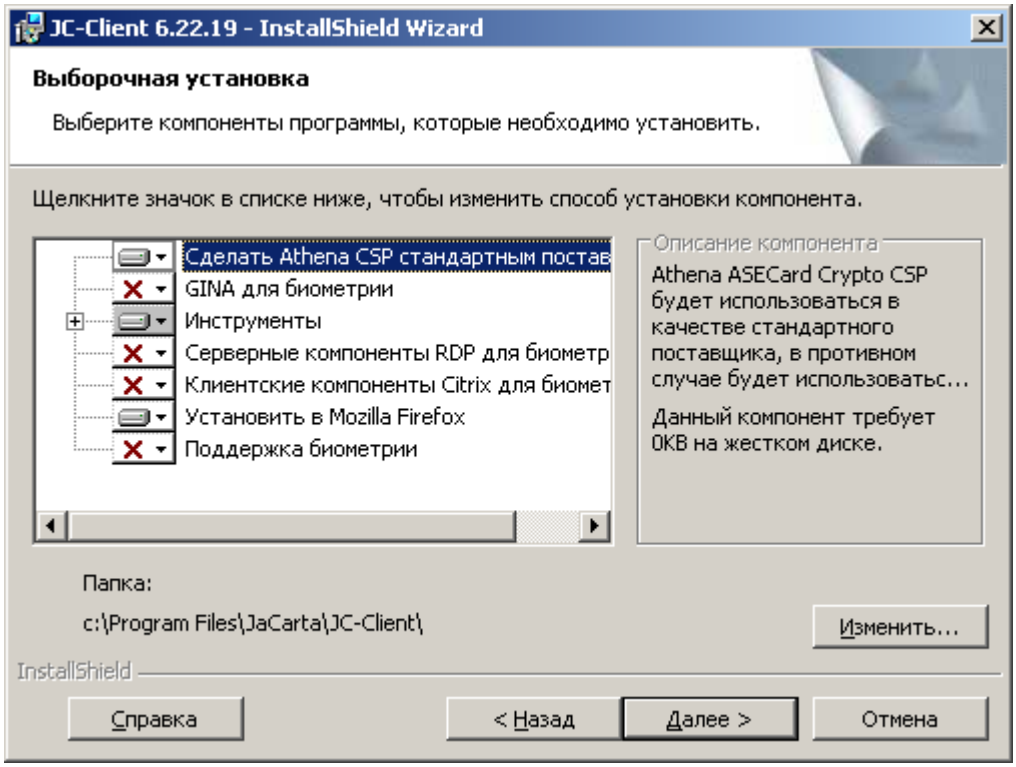

2. Внимательно прочтите лицензионное соглашение и, если вы согласны со всеми его пунктами, выберите **Я принимаю условия лицензионного соглашения**. В противном случае выберите **Я не принимаю условия лицензионного соглашения**.
3. Нажмите **Далее**.

Если вы приняли условия лицензионного соглашения, отобразится следующее окно.




4. Выберите пункт **Выборочная** и нажмите **Далее**.

   Отобразится следующее окно.



5. Выберите **CSP** или **Minidriver**, руководствуясь таблицей ниже.

| CSP | Minidriver |
|---|---|
| Данный компонент обеспечивает поддержку биометрической аутентификации на следующих системах:<br>**Windows XP**<br>**Windows Server 2003**<br>**Windows Vista**<br>**Windows Server 2008**<br>**Windows 7** | Данный компонент обеспечивает поддержку биометрической аутентификации на следующих системах:<br>**Windows Vista**<br>**Windows Server 2008**<br>**Windows 7** |

**Примечание:**

Если вы планируете использовать сканеры отпечатков компании Precise Biometrics, необходимо выбрать компонент **CSP -** подробнее см. раздел "Поддерживаемые сканеры отпечатков пальцев".

Не стоит при этом путать название компании-производителя сканеров отпечатков с названием биометрической технологии, используемой в электронных ключах JaCarta. Электронные ключи, в которых реализована поддержка биометрической технологии Precise Biometrics, могут использоваться в обоих случаях.

6. Отметьте к установке компонент **Поддержка биометрии**.
7. В зависимости от операционной системы, на которую вы устанавливаете JC-Client, отметьте следующий компонент.

| | |
|---|---|
| **Windows XP**<br>**Windows Server 2003** | **GINA для биометрии** |
| **Windows Vista**<br>**Windows Server 2008**<br>**Windows 7** | **Credential Provider** |

8. При необходимости, отметьте остальные компоненты, связанные с использованием биометрии (см. таблицу ниже).

| Компонент | Описание |
|---|---|
| **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. |
| **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. |

9. При необходимости отметьте к установке или отмените установку остальных компонентов JC-Client (подробное описание компонентов представлено в документе *JC-Client. Руководство администратора*).
10. Нажмите **Далее** и следуйте инструкциям мастера установки.

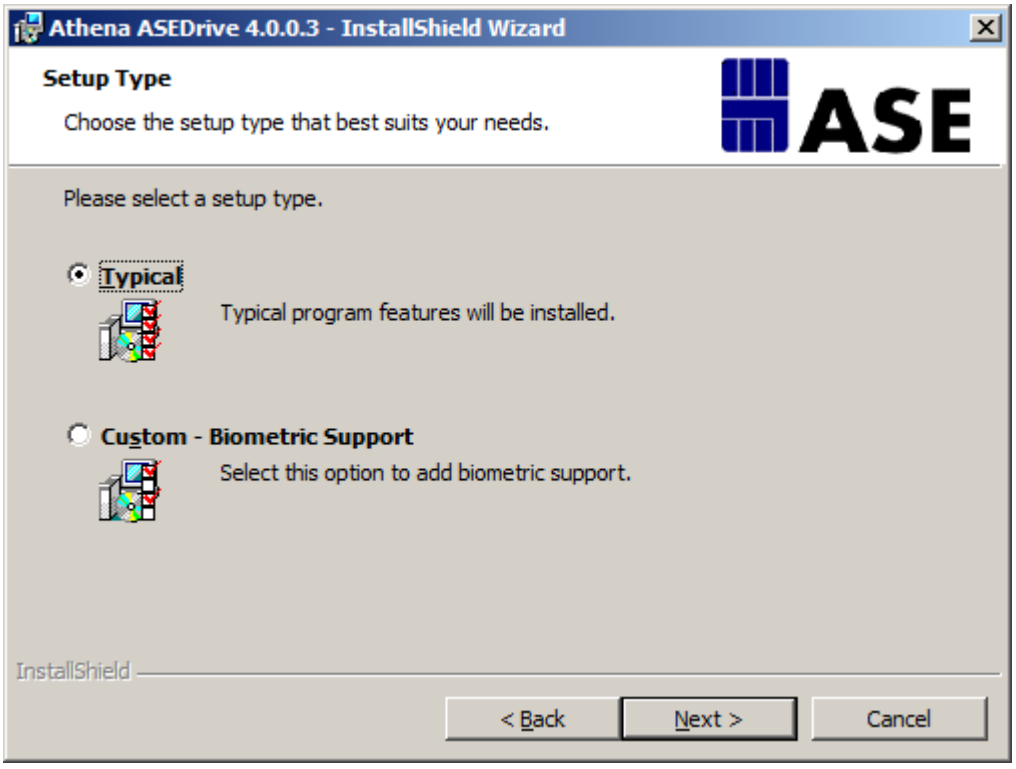
## Установка драйвера сканера отпечатков

Установка драйвера биометрического сканера нужна для обеспечения возможности записи, считывания и сверки отпечатков пальцев пользователей.

**Примечание:**

> В данном руководстве приведен пример установки драйвера для комбинированных считывателей серии ASEDrive Bio со сканером Authentec/Upek. Если вы используете сканер другого производителя, установите соответствующий драйвер.

В процессе установки драйвера отобразится следующее окно.




Для обеспечения поддержки биометрии выберите пункт **Custom – Biometric Support** (Выборочная – поддержка биометрии) и нажмите **Next** (Далее), после чего следуйте инструкциям мастера установки.

# Настройка профиля персонализации

Чтобы подготовить электронные ключи JaCarta к использованию, их необходимо персонализировать. Персонализация происходит на основе заранее настроенного профиля персонализации. Для настройки профиля персонализации и для последующей персонализации электронных ключей JaCarta используется утилита JaCarta Format.

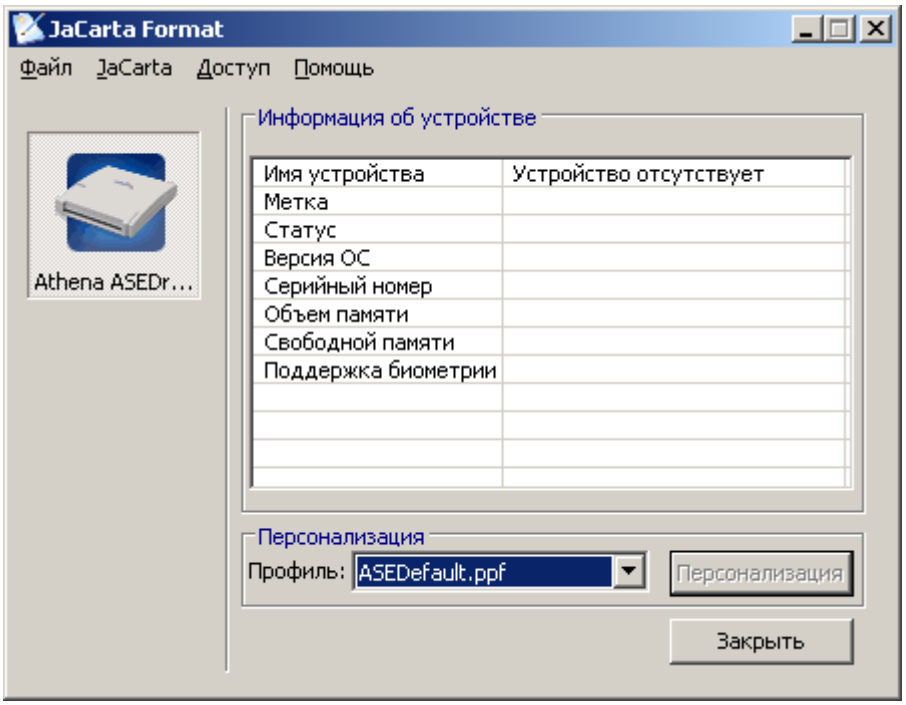
**Примечание:**

В настоящем руководстве не рассматривается настройка параметров пароля цифровой подписи. Подробные сведения о настройке и параметрах использования пароля цифровой подписи представлены в документе *JC-Client. Руководство администратора*.

Чтобы настроить профиль персонализации.

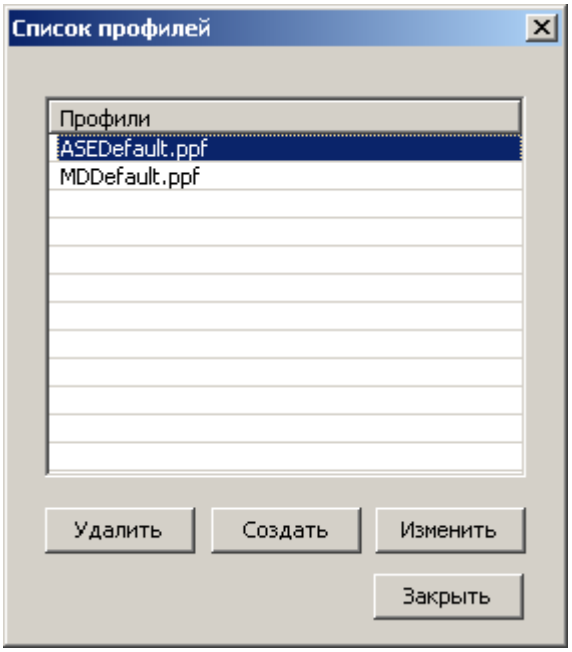
1. Выберите **Пуск > Все программы > JC-Client > JaCarta Format**.

   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**.

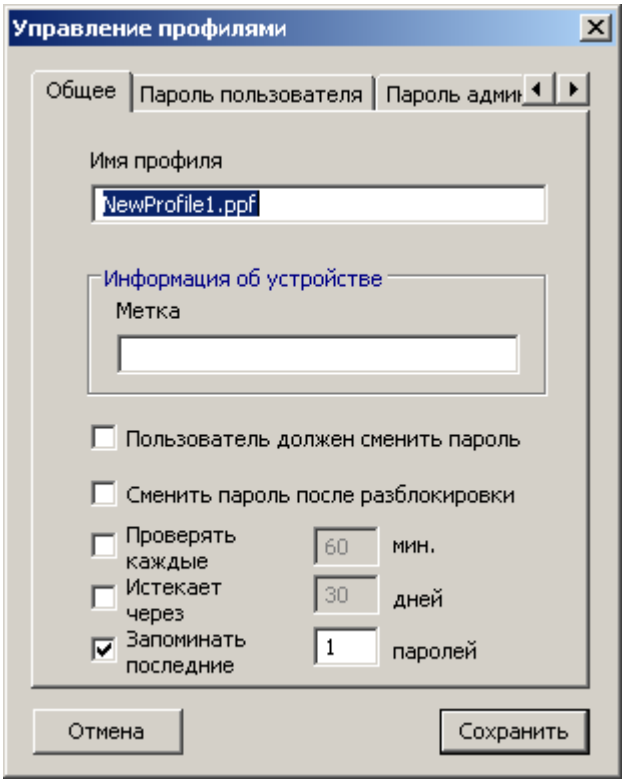
**Примечание:**

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.

3. Переходите к основным настройкам профиля (см. далее).

## Вкладка Общее

Отобразится вкладка **Общее** окна настройки профиля.




1. Сделайте необходимые настройки, руководствуясь приведенной ниже таблицей.

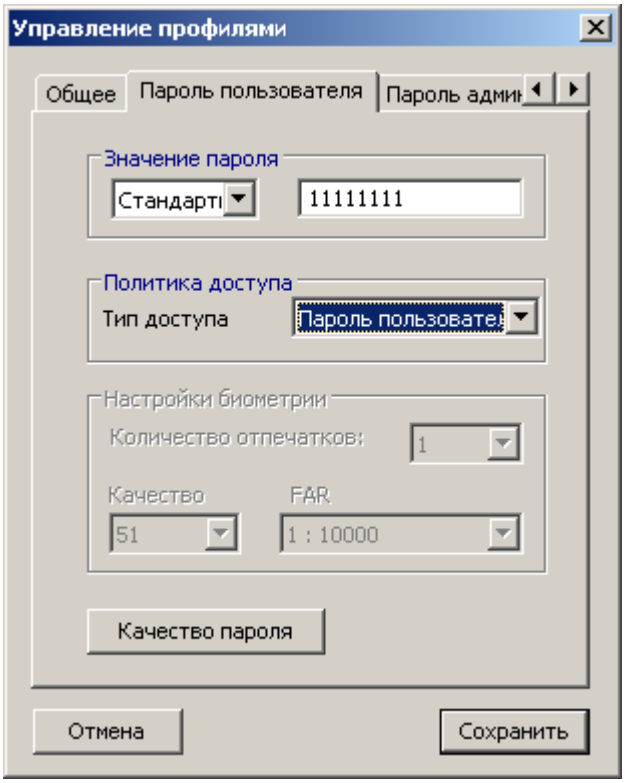
| Настройка | Описание |
|---|---|
| **Имя профиля** | Имя профиля. В данном поле можно задать имя нового профиля персонализации или изменить имя существующего. |
| **Метка** | Данное поле используется для идентификации персонализируемых электронных ключей JaCarta. Значение данного поля не влияет на 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** | **Примечание:** данная настройка нужна, только если наряду с биометрической аутентификацией будет использоваться пароль пользователя.<br>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** | **Примечание:** данная настройка нужна, только если наряду с биометрической аутентификацией будет использоваться пароль пользователя.<br>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 … мин.** | Если флажок установлен, значение в поле **мин.** определяет, через сколько минут после аутентификации пользователь должен будет снова подтвердить свой уровень доступа, введя пароль и/или приложив палец к сканеру отпечатков. |
| **Истекает через … дней** | **Примечание:** данная настройка нужна, только если наряду с биометрической аутентификацией будет использоваться пароль пользователя.<br>В случае использования пароля, если флажок установлен, значение в поле |

| Настройка | Описание |
|---|---|
| | **дней** определяет, через сколько дней пользователь должен сменить пароль. |
| **Запоминать последние … паролей** | **Примечание:** данная настройка нужна, только если наряду с биометрической аутентификацией будет использоваться пароль пользователя.<br>Если флажок установлен, значение в поле **паролей** определяет количество последних использованных паролей пользователя, которые не должны использоваться при назначении нового пароля. |

2. Чтобы настроить доступ на уровне пользователя, перейдите на вкладку **Пароль пользователя** (см. далее).

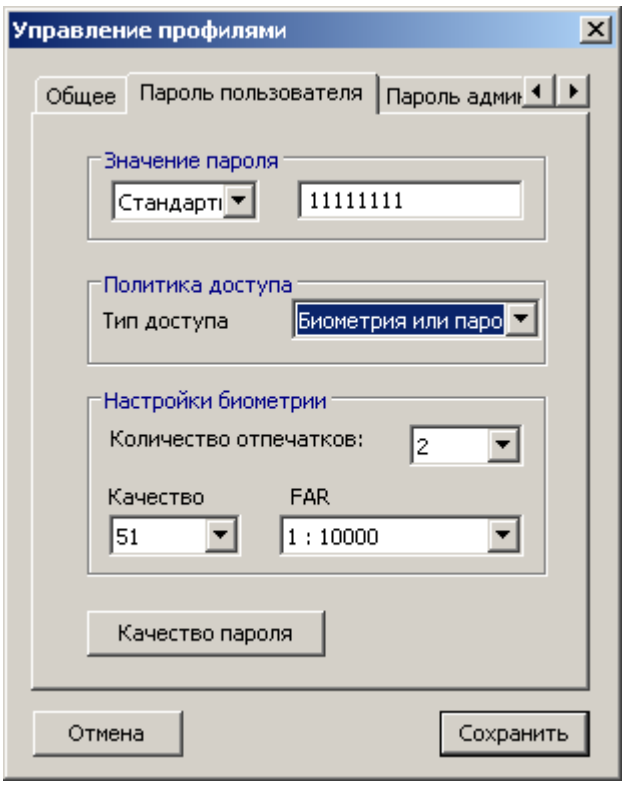
## Вкладка Пароль пользователя

Окно настройки профиля персонализации примет следующий вид.




1. Чтобы после персонализации использовать электронные ключи JaCarta с настройками биометрии, в списке **Тип доступа** выберите один из трех вариантов:
   - **Биометрия** (доступ только по отпечатку пальца)
   - **Биометрия или пароль** (доступ по отпечатку пальца или по паролю пользователя).
   - **Биометрия и пароль** (доступ по отпечатку пальца и по паролю пользователя).

Окно примет следующий вид.




2. Если в списке **Тип доступа** вы выбрали **Биометрия или пароль** или **Биометрия и пароль**, необходимо настроить параметры пароля пользователя в секции **Значение пароля**.

**Примечание:**

Описание настроек секции **Значение пароля** представлены в документе *JC-Client. Руководство администратора*.

В настоящем руководстве в качестве типа доступа рассматривается вариант **Биометрия или пароль**, при этом в секции **Значение пароля** сохранены настройки по умолчанию: стандартный пароль пользователя "11111111" (восемь единиц).

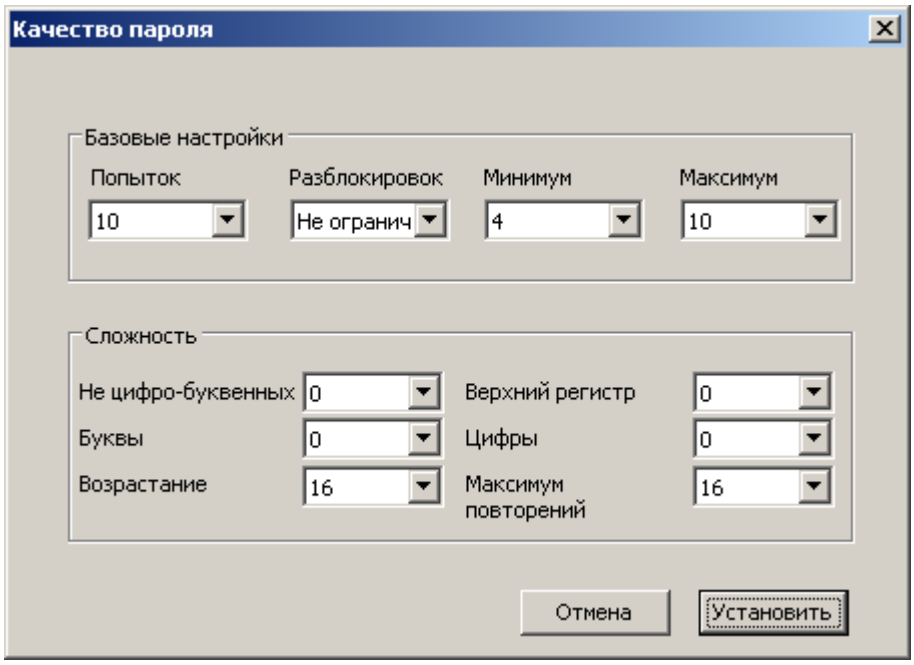
3. Настройте параметры доступа по отпечатку пальца, руководствуясь приведенной ниже таблицей.

| Настройка | Описание |
|---|---|
| **Количество отпечатков** | Определяет максимальное количество отпечатков пальцев пользователя, которое можно сохранить в памяти электронного ключа JaCarta (от 1 до 10). В каждом конкретном случае пользователь сможет выбрать, какой отпечаток использовать.<br>Минимальное рекомендуемое значение: 2.<br>Если вы выберете 1, и впоследствии доступ по отпечатку будет заблокирован, даже после разблокировки потребуется выполнение процедуры повторного сохранения отпечатков в памяти электронного ключа JaCarta (см. раздел "Сохранение отпечатков пальцев в памяти электронного ключа JaCarta").<br>Если вы выберите 2 и больше, после разблокировки доступа по отпечатку пользователь сможет получить доступ, используя отпечаток другого пальца. Повторное сохранение отпечатков в памяти электронного ключа JaCarta при этом не потребуется. |
| **Качество** | Определяет граничное значение качества изображения. Если качество изображения ниже данного значения, сохранение отпечатков пальцев пользователя не будет производиться. |
| **FAR**<br>(Вероятность ложного допуска) | Определяет вероятность ложного допуска (т.е. вероятность, с которой система считывания отпечатков ошибочно аутентифицирует пользователя). Вероятность ложного допуска определяется как |

| Настройка | Описание |
|---|---|
| | соотношение возможного количества ошибочной идентификации к числу попыток аутентификации. Соответственно, вероятность должного допуска 1:100 выше, чем вероятность ложного допуска 1:1000.<br>Рекомендуемое значение: 1:10000. |

4. Нажмите **Качество пароля**.

   Отобразится следующее окно.




5. Выполните необходимые настройки в зависимости от выбранного типа доступа.

- Если в списке **Тип доступа** вы выбрали **Биометрия**, настройте только следующие два параметра.

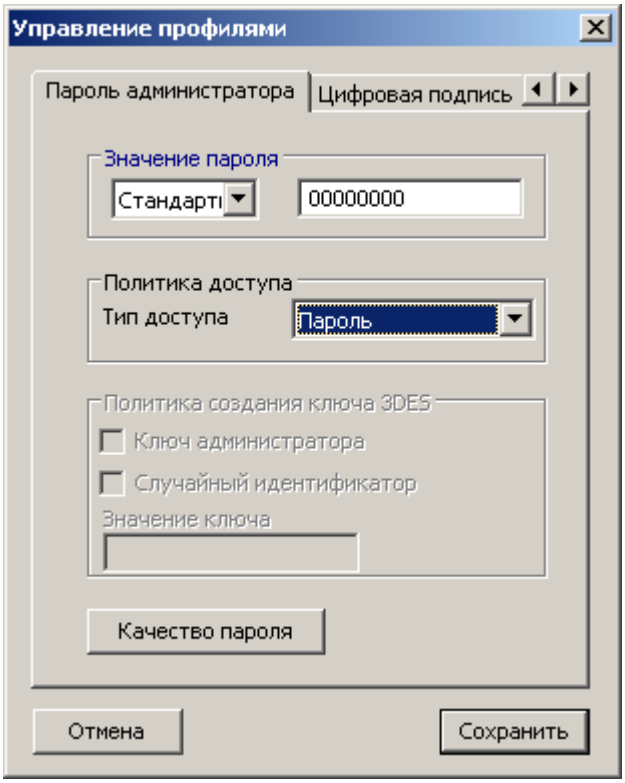
  - **Попыток** – число неудачных попыток аутентификации, после которого доступ пользователя блокируется. Для разблокировки необходим уровень доступа администратора (см. также следующий параметр: **Разблокировок**).
  - **Разблокировок** – число возможных разблокировок. Если данное значение превышено, выбранный тип доступа блокируется без возможности разблокировки. Чтобы снова использовать заблокированный тип доступа на данном электронном ключе JaCarta, его необходимо персонализировать повторно (см. раздел "Персонализация с биометрическими настройками"), при этом все данные на электронном ключе будут удалены.

- Если в списке **Тип доступа** вы выбрали **Биометрия и пароль** или **Биометрия или пароль**, выполните полную настройку, руководствуясь сведениями, представленными в приложении "Настройка качества паролей".

6. Перейдите на вкладку **Пароль администратора** (см. ниже).

## Вкладка Пароль администратора

Окно настройки профиля персонализации примет следующий вид.




1. Выполните необходимые настройки в секциях **Значение пароля**, **Политика доступа** и, при необходимости, **Политика создания ключа 3DES**.

**Примечание:**

*Данная процедура подробно описана в документе JC-Client. Руководство администратора.*

2. Нажмите **Качество пароля** и настройте параметры качества пароля администратора, руководствуясь сведениями, представленными в приложении "Настройка качества паролей".
3. Нажмите **Сохранить** для сохранения профиля персонализации.

   Теперь профиль можно использовать для персонализации электронных ключей JaCarta (см. раздел "Персонализация с биометрическими настройками").

# Персонализация с биометрическими настройками

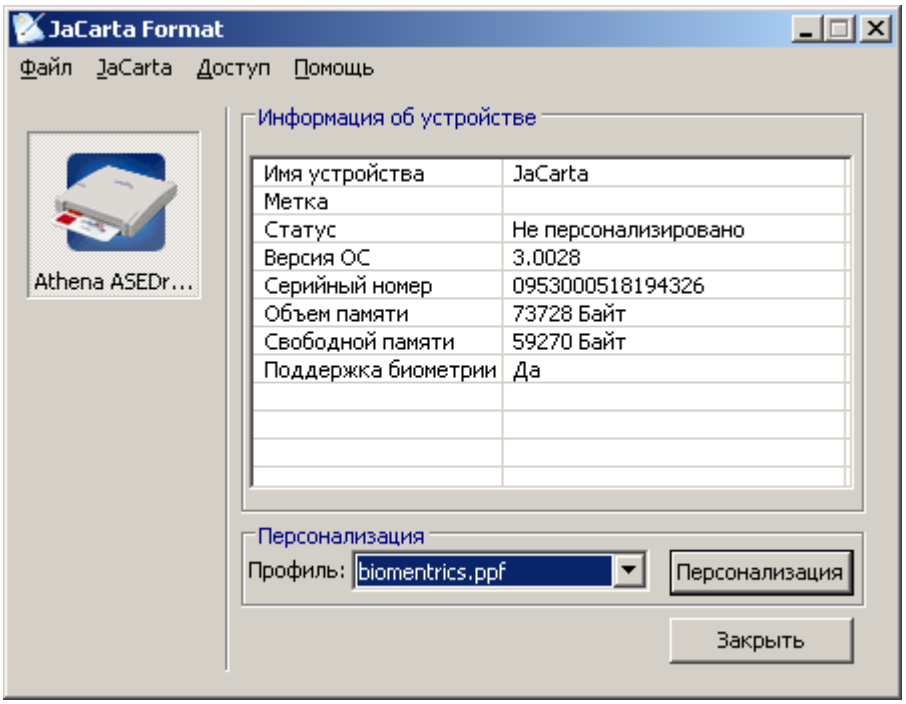
В процессе персонализации на основе профиля с биометрическими настройками пользователю будет предложено пройти процедуру считывания отпечатков пальцев. На этапе персонализации эту процедуру можно пропустить. Впоследствии, чтобы сохранить отпечатки пальцев пользователя в памяти электронного ключа JaCarta, необходимо будет воспользоваться утилитой JaCarta BioTool – для этого потребуется уровень доступа администратора.

В настоящем руководстве рассматривается персонализация на основе профиля с настроенным типом доступа пользователя **Биометрия или пароль**, а пароль пользователя и пароль администратора установлены как **Стандартный** и имеют значения по умолчанию.

**Чтобы персонализировать электронный ключ JaCarta на основе профиля с биометрическими настройками.**

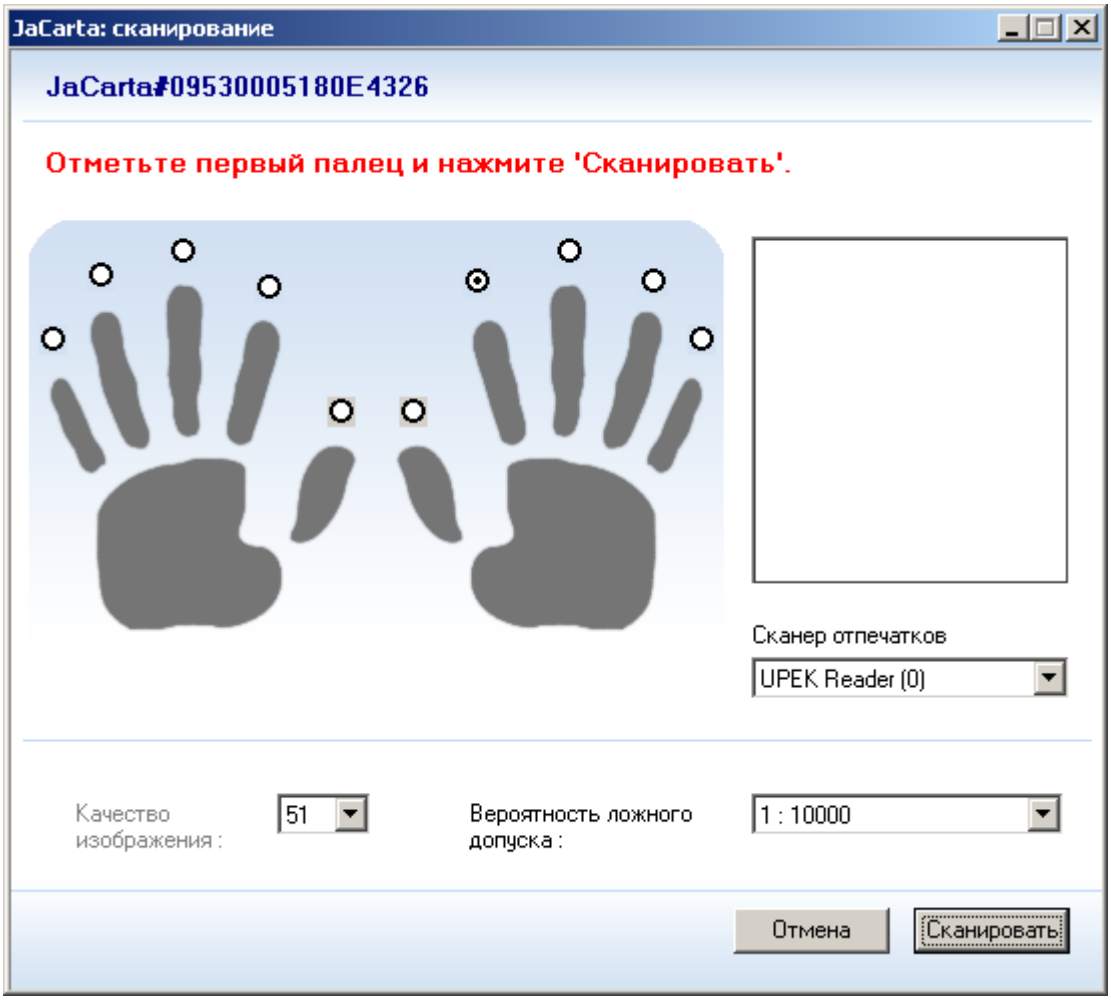
1. Подключите к рабочей станции сканер отпечатков пальцев и электронный ключ JaCarta, который необходимо персонализировать.
2. Выберите **Пуск > Все программы > JC-Client > JaCarta Format**.

   Отобразится основное окно утилиты.



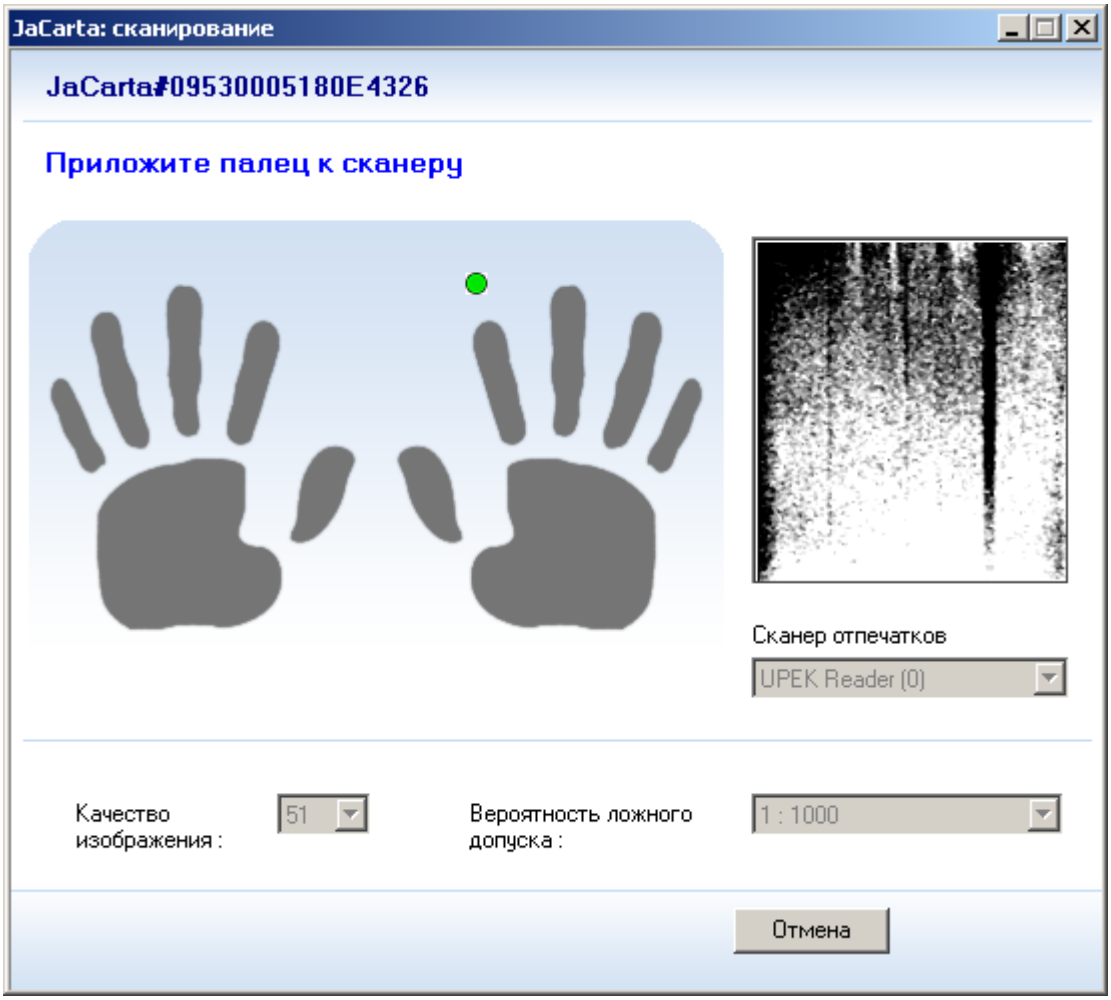

3. Если данный электронный ключ JaCarta не персонализирован, поле **Статус** будет содержать значение **Не персонализировано**, также, если электронный ключ поддерживает доступ по отпечатку пальца, поле **Поддержка биометрии** будет содержать значение **Да** (технология Precise Biometrics) или **ISO** (технология в соответствии с ISO 19794).
4. В поле **Профиль** выберите заранее сохраненный профиль персонализации и нажмите **Персонализация**.

Отобразится следующее окно.



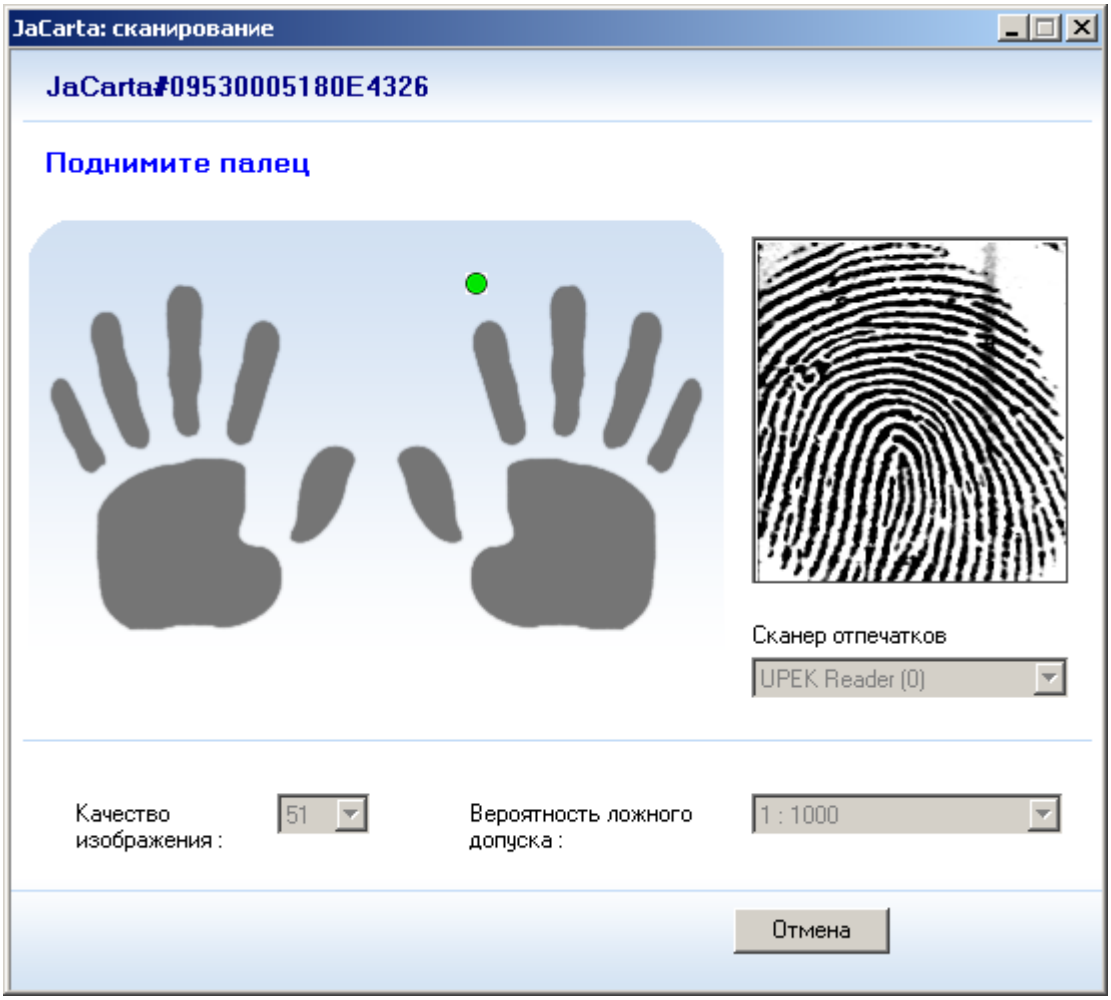

5. Используя схематическое изображение ладоней, отметьте палец, отпечаток которого будет сохранен в память электронного ключа JaCarta.
6. При необходимости измените параметры **Вероятность ложного допуска** и **Качество изображения**.
7. Нажмите **Сканировать**.

Отобразится следующее окно.




8. Если к рабочей станции подключено несколько сканеров отпечатков, выберите нужный в списке **Сканер отпечатков**.
9. После этого пользователь должен приложить палец к сканеру отпечатков (палец, который необходимо приложить, выделяется зеленой точкой).

После первичного считывания отобразится сообщение **Поднимите палец** (см. изображение ниже).




10. Пользователь должен поднять палец.

    Снова отобразится сообщение **Приложите палец к сканеру**.

11. Пользователь должен приложить палец к сканеру отпечатков для вторичного считывания.

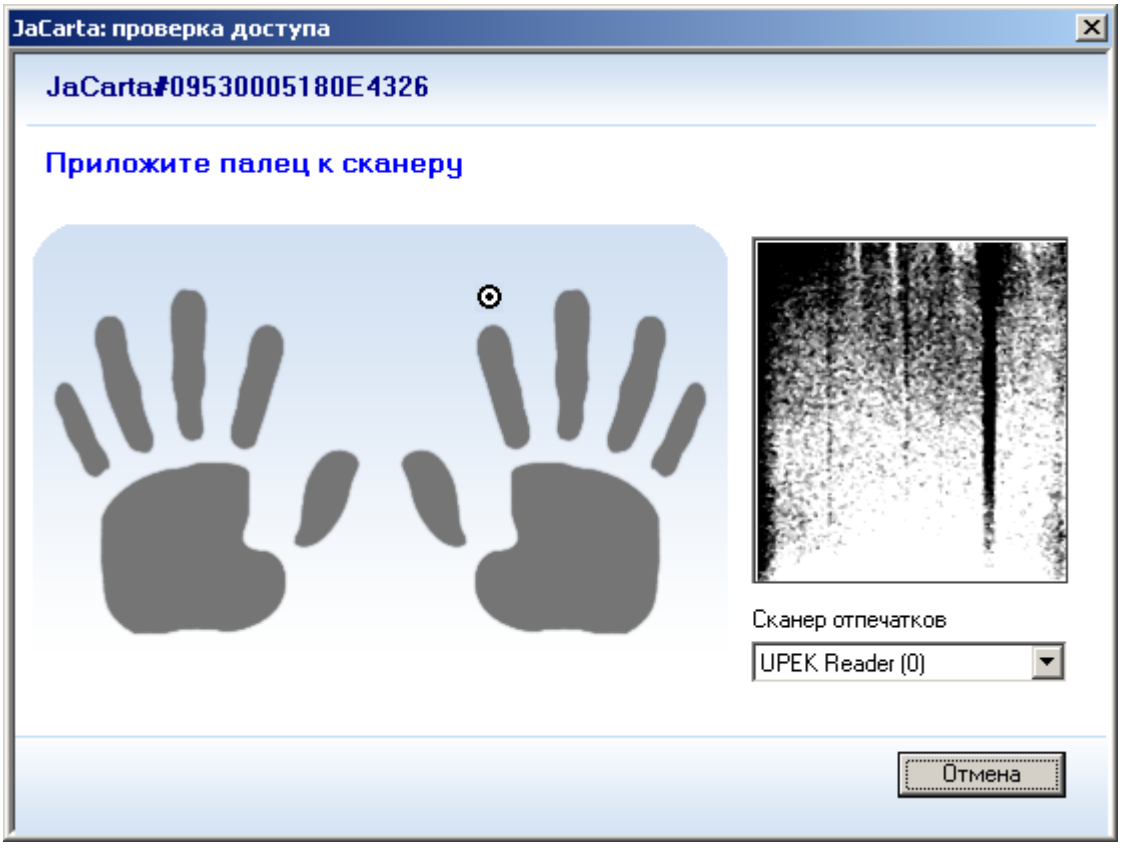
    После вторичного считывания появится сообщение **Поднимите палец**.

12. Пользователь должен снова поднять палец, после чего процесс персонализации продолжится.

**Примечание:**

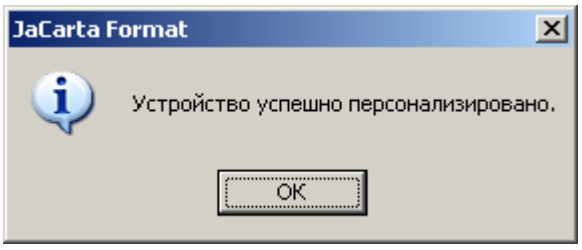
Двукратного считывания может быть недостаточно, поэтому может потребоваться прикладывать палец к сканеру для считывания больше двух раз.

Спустя некоторое время отобразится следующее окно.




13. Пользователь снова должен приложить палец к сканеру, на этот раз для проверки корректности отпечатков, сохраненных в памяти электронного ключа JaCarta.
14. Если в настройках профиля указано, что нужно сохранить несколько отпечатков, повторите необходимые шаги для каждого из них.

    По завершении процедуры персонализации отобразится следующее сообщение.




15. Нажмите **OK**.

    Электронный ключ JaCarta персонализирован и готов к использованию.

# Операции с электронными ключами JaCarta

## Разблокировка

Если превышено допустимое количество последовательных неудачных попыток доступа по отпечатку, данный тип доступа блокируется. В настоящем разделе рассматривается стандартный способ разблокировки (с использованием пароля администратора). Описание процедуры разблокировки с использованием ключа администратора представлено в разделе "Разблокировка с использованием ключа администратора".

В настоящем руководстве не рассматривается разблокировка пароля пользователя. Эта процедура подробно представлена в документе *JC-Client. Руководство администратора*.

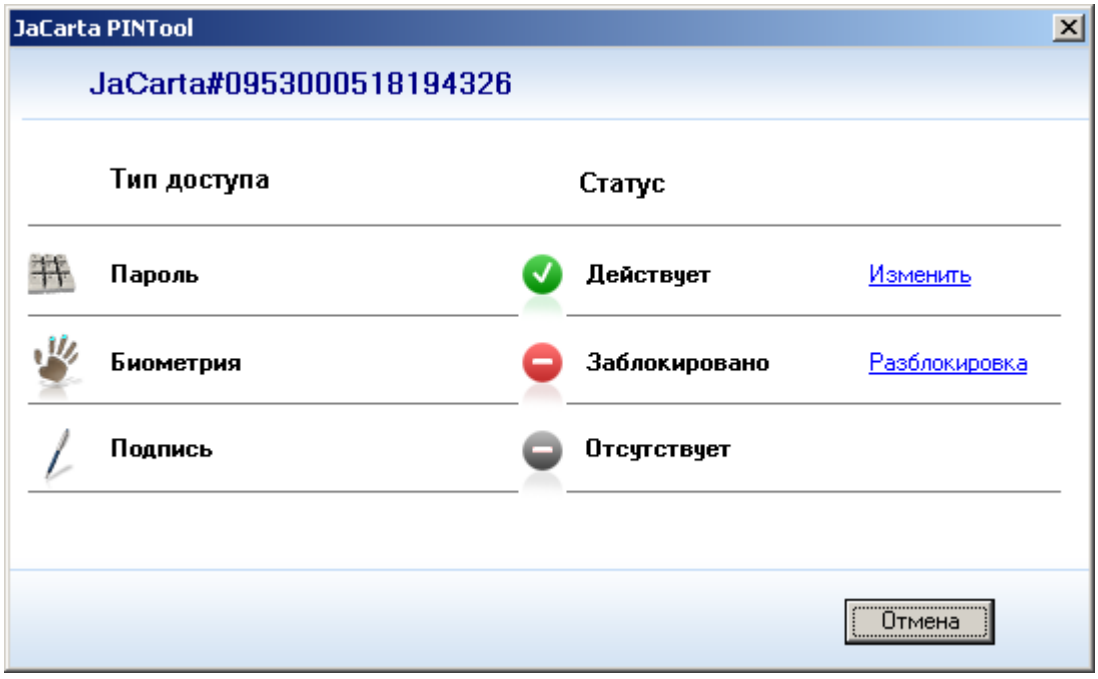
**Примечание:**

После разблокировки доступа по отпечатку пользователь не сможет использовать отпечаток, сканирование которого привело к блокированию электронного ключа JaCarta. Чтобы обеспечить такую возможность, необходимо выполнить процедуру повторного сохранения отпечатка пальца (см. раздел "Сохранение отпечатков пальцев в памяти электронного ключа JaCarta"). Таким образом, если в памяти электронного ключа JaCarta сохранена информация только об одном отпечатке, следует сразу перейти к упомянутой процедуре – по ее выполнении электронный ключ JaCarta будет автоматически разблокирован. То же относится к процедуре разблокировки с использование ключа администратора.

**Для того чтобы разблокировать доступ по отпечатку пальца.**

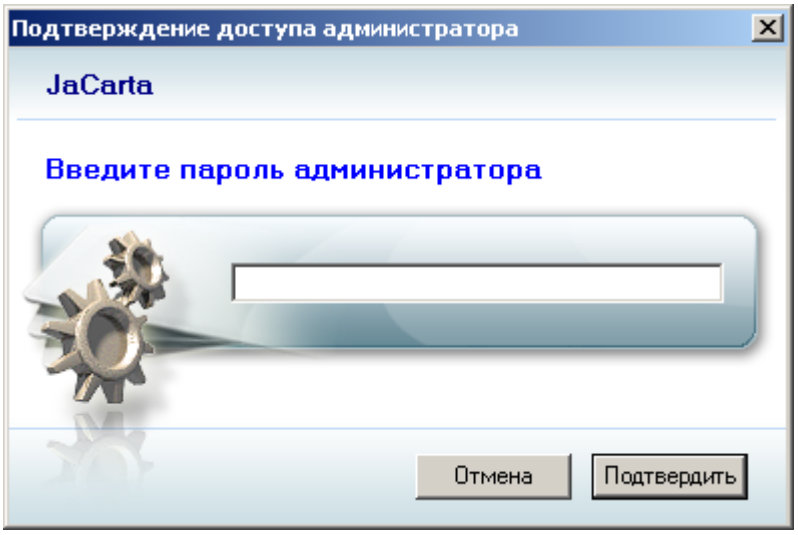
1. Выберите **Пуск > Все программы > JC-Client > JaCarta PINTool**.

   Если доступ по отпечатку заблокирован, в поле **Статус** напротив значения **Биометрия** будет значиться **Заблокировано**.



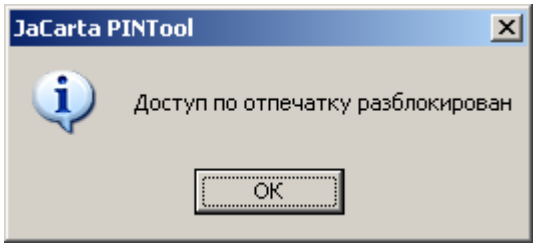

2. Щелкните на ссылке **Разблокировка**.

Отобразится следующее окно.




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

   Отобразится следующее сообщение.




4. Нажмите **OK** для завершения процедуры.

## Разблокировка с использованием ключа администратора

Администратор может использовать ключ администратора, чтобы разблокировать электронный ключ пользователя, если электронный ключ JaCarta был персонализирован с соответствующими параметрами.

**Примечание:**

Подробные сведения, касающиеся использования ключа администратора, содержатся в документе *JC-Client. Руководство администратора*.

Существует два сценария разблокировки с использованием ключа администратора.

- При непосредственном участии администратора
- В удаленном режиме

**При непосредственном участии администратора**

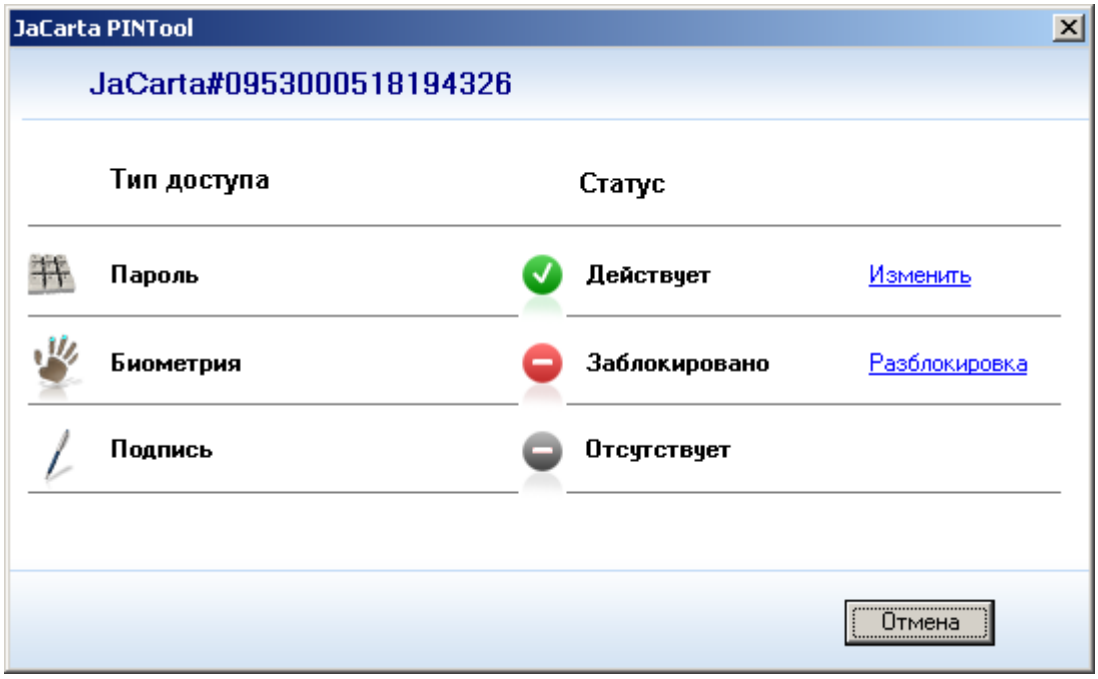
Для разблокировки с использованием ключа администратора при непосредственном участии администратора необходимо, чтобы на рабочей станции было доступно два считывателя смарт-карт.

**Чтобы выполнить разблокировку.**

1. Подсоедините к компьютеру электронный ключ JaCarta с заблокированным доступом по отпечатку.

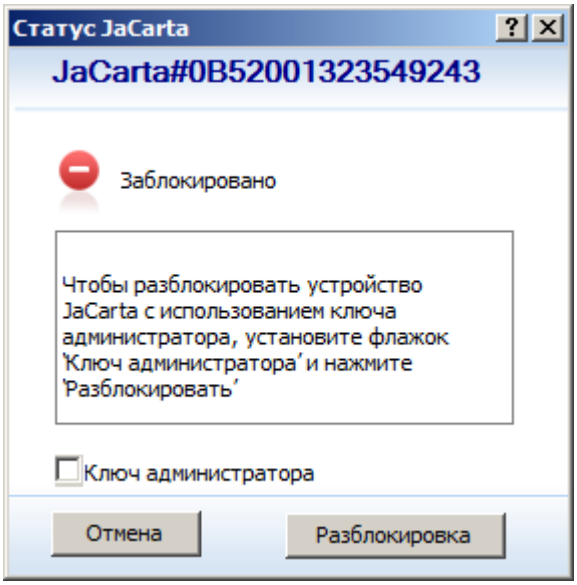
2. Запустите утилиту JaCarta PINTool.

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



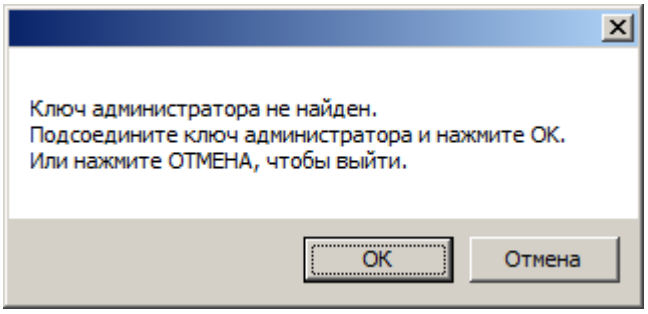

3. Для разблокировки доступа щелкните на ссылке **Разблокировка** напротив поля **Биометрия**.

   Отобразится следующее окно.



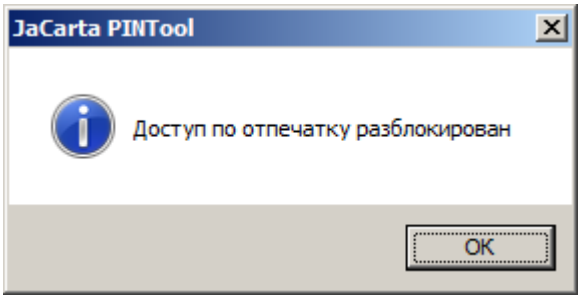

4. Установите флажок **Ключ администратора** и нажмите **Разблокировка**.

   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 сообщение.




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

#### В удаленном режиме

Если для персонализации электронного ключа JaCarta был использован ключ администратора, разблокировку можно осуществить в удаленном режиме.

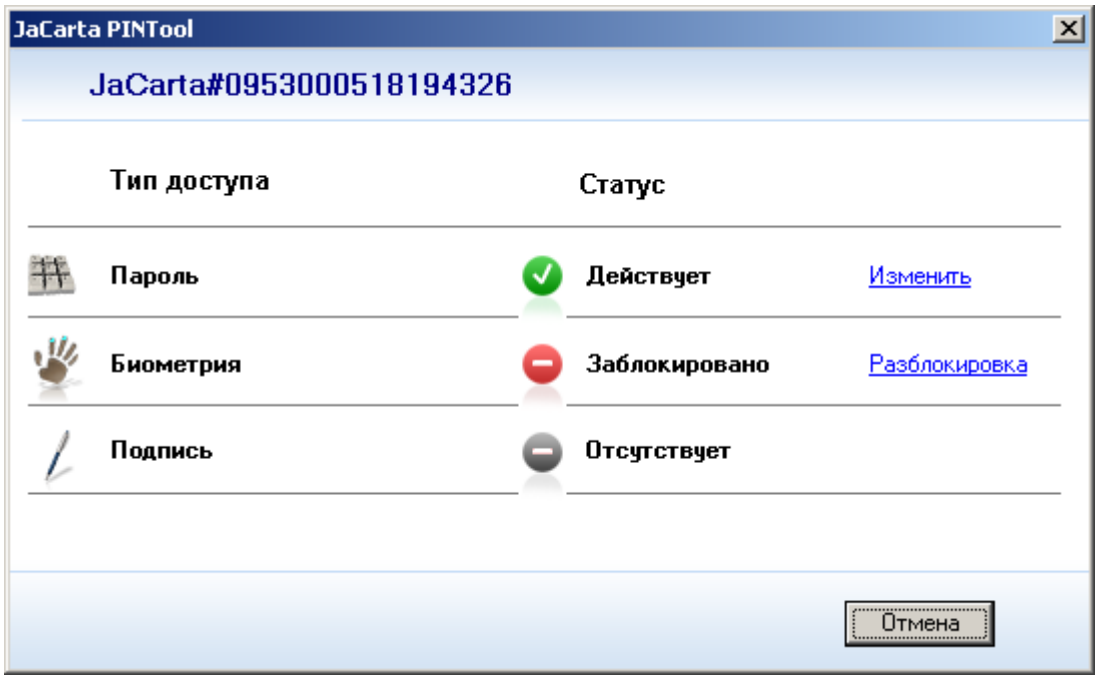
**Примечание:**

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

**Чтобы разблокировать электронный ключ JaCarta в удаленном режиме.**

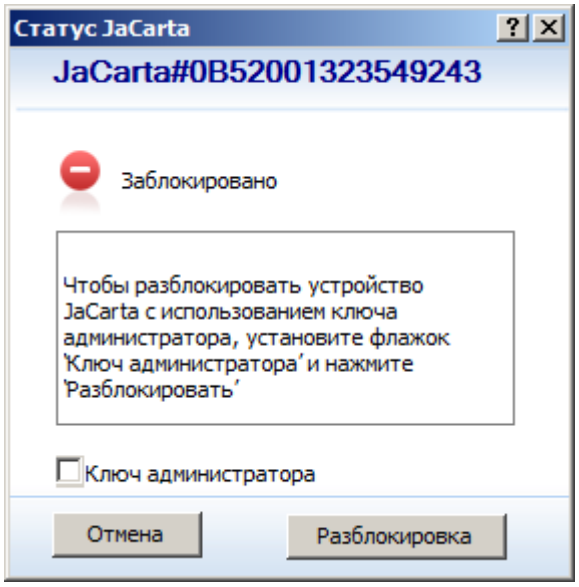
1. Пользователь должен подсоединить электронный ключ JaCarta к своему компьютеру и запустить утилиту JaCarta PINTool.

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



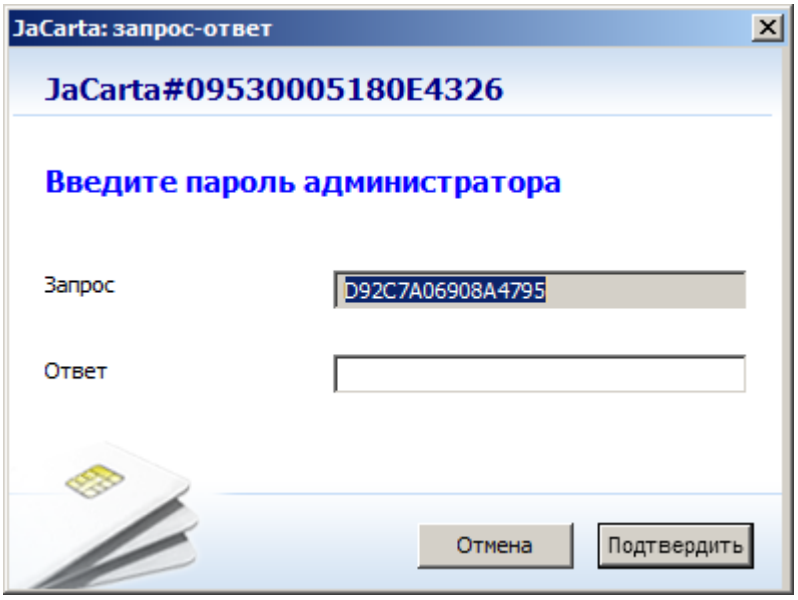

2. Для разблокировки пользователь должен щелкнуть на ссылке **Разблокировка** напротив поля **Биометрия**.

На экране пользователя отобразится следующее окно.



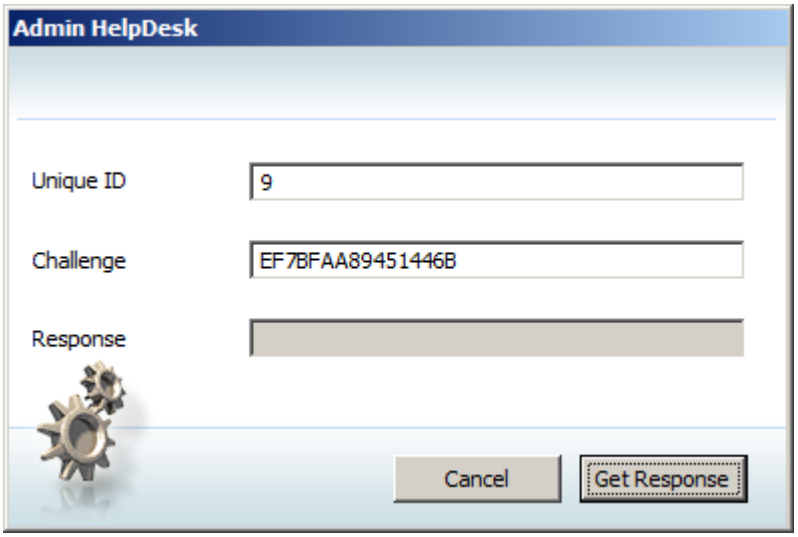

3. Пользователь должен оставить неотмеченным пункт **Ключ администратора** и нажать **Разблокировка**.

   На экране пользователя отобразится следующее окно.




4. Пользователь должен сообщить администратору идентификатор, созданный на этапе персонализации электронного ключа JaCarta, 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.

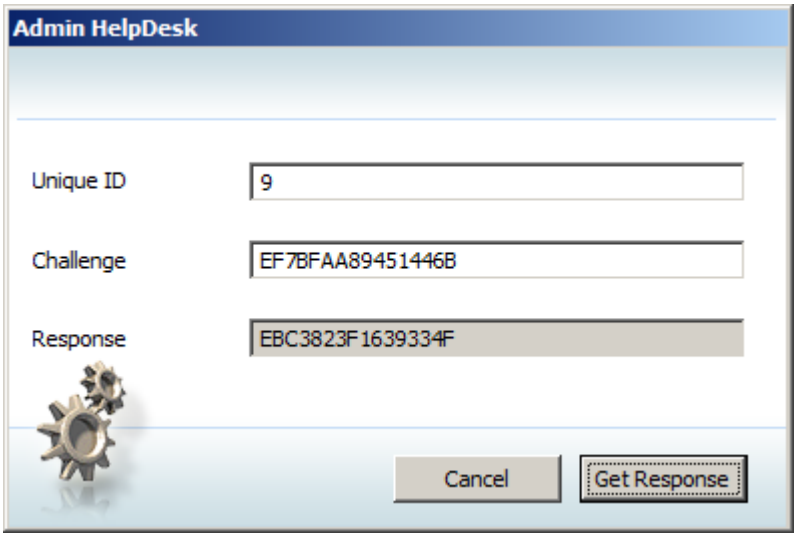



**Примечание:**

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.

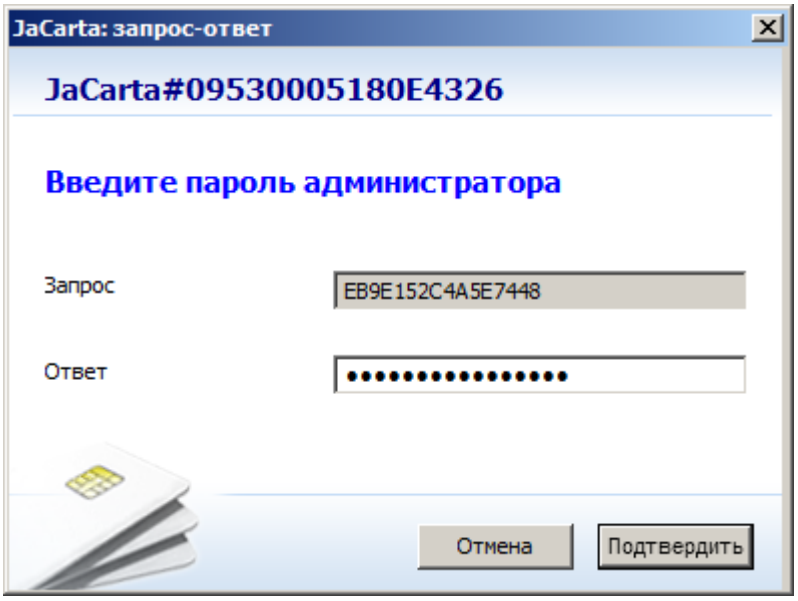
6. После того как данные введены, администратор должен нажать **Get Response** (Получить ответ).

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

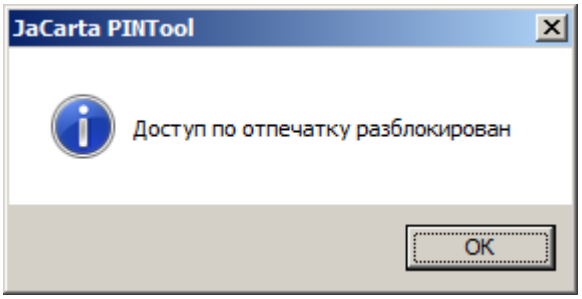



7. Администратор должен сообщить пользователю данные из поля **Response** (Ответ).

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 сообщение.




## Сохранение отпечатков пальцев в памяти электронного ключа JaCarta

Если в процессе персонализации процедура сохранения отпечатков пользователя в памяти электронного ключа JaCarta была пропущена, существует возможность выполнить эту процедуру после персонализации, используя утилиту JaCarta BioTool. Для осуществления данной процедуры необходим уровень доступа администратора (пароль администратора или ключ администратора).

**Примечание:**

> В настоящем руководстве рассматривается вариант с использованием пароля администратора. Подробные сведения об использовании ключа администратора представлены в документе *JC-Client. Руководство администратора*.

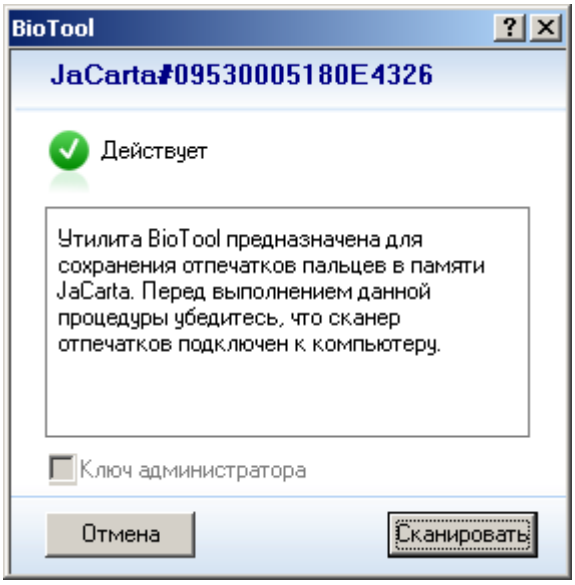
Выполнение процедуры сохранения отпечатков пальцев также необходимо, если доступ по отпечатку на электронном ключе JaCarta заблокирован и в памяти электронного ключа сохранен только один отпечаток пользователя. В этом случае выполнять процедуру разблокировки необязательно (т.к. сама по себе разблокировка не позволит использовать для доступа отпечаток, сканирование которого привело к блокировке) – можно сразу перейти к процедуре сохранения отпечатков пальцев.

Если доступ по отпечатку пальца на электронном ключе JaCarta заблокирован, однако в памяти электронного ключа сохранено более одного отпечатка, можно разблокировать доступ по отпечатку (см. раздел “Разблокировка”), однако пользователь не сможет использовать для доступа отпечаток, сканирование которого привело к блокировке – необходимо будет использовать другие отпечатки, сохраненные в памяти электронного ключа JaCarta.

**Чтобы сохранить отпечатки пальцев в памяти электронного ключа JaCarta.**

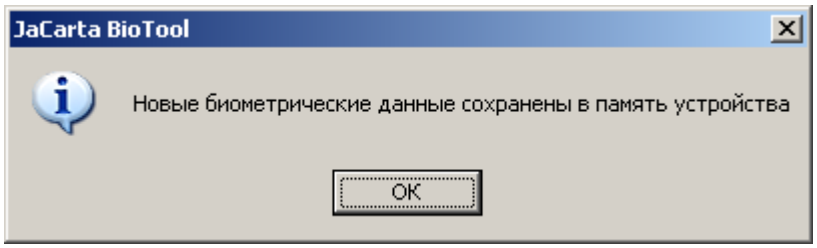
1. Выберите **Пуск > Все программы > JC-Client > JaCarta BioTool**.

   Отобразится окно следующего вида.




2. Нажмите **Сканировать**.
3. В отобразившемся окне введите пароль администратора и нажмите **Подтвердить**.
4. Выполните необходимые шаги процедуры, описанной в разделе "Персонализация с биометрическими настройками".

   По завершении процедуры отобразится следующее окно.




5. Нажмите **OK**.

   Отпечатки сохранены в памяти электронного ключа JaCarta.

# Дальнейшие действия

Чтобы обеспечить пользователям вход в домен Windows с использованием биометрической аутентификации, выполните следующие действия.

1. Настройте центр сертификации и соответствующий шаблон сертификата (например, шаблон **Пользователь со смарт-картой**). Для этого в настройках шаблона сертификата в качестве поставщика служб криптографии укажите одного из следующих поставщиков.
   - **Athena ASECard Crypto CSP** – если при установке JC-Client был выбран компонент **CSP**.
   - **Microsoft Base Smart Card Crypto Provider** – если при установке JC-Client был выбран компонент **Minidriver**.
2. Выполните необходимые настройки безопасности сертификата и опубликуйте шаблон в качестве выдаваемого.

**Примечание:**

Подробная информация о настройке центра сертификации и выдаваемого шаблона сертификата представлена в документе *JaCarta для Microsoft Windows. Руководство по внедрению*.

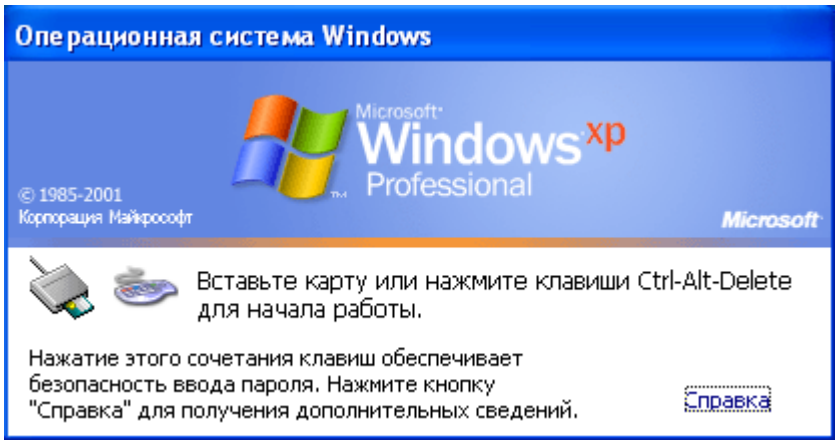
3. Настройте профиль персонализации (см. раздел “Настройка профиля персонализации”) и персонализируйте электронный ключ JaCarta с биометрическими настройками (см. раздел “Персонализация с биометрическими настройками”) Если персонализацию осуществляет администратор, считывание отпечатков пальцев пользователей можно пропустить, однако впоследствии для сохранения отпечатков пользователей в память электронных ключей JaCarta потребуется пароль администратора (или ключ администратора).
4. Запросите необходимые сертификаты от имени пользователей и запишите их в память электронных ключей JaCarta. Пользователи могут запросить сертификаты самостоятельно, если существуют соответствующие настройки безопасности центра сертификации и выдаваемого шаблона сертификата. (Подробная информация о записи цифровых сертификатов в память электронных ключей JaCarta представлена в документе *JaCarta для Microsoft Windows. Руководство по внедрению*.)

После этого электронные ключи JaCarta можно использовать для входа в домен Windows.

# Вход в домен с использованием биометрической аутентификации

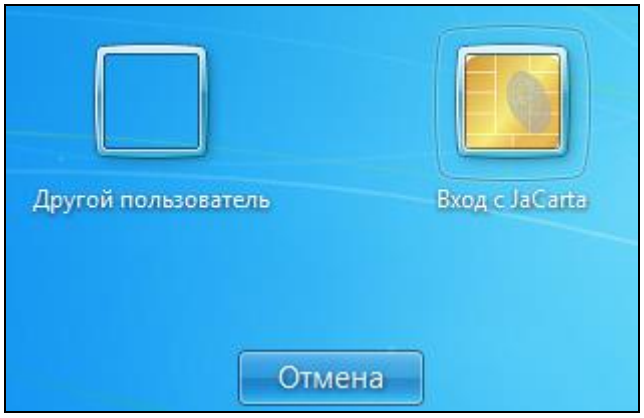
При загрузке операционной системы экран приветствия Windows выглядит следующим образом:

**Windows XP / Server 2003**




В этом случае пользователь должен перейти к первому шагу процедуры.

**Windows Vista / Server 2008 / 7**




В этом случае до подсоединения электронного ключа JaCarta к компьютеру пользователь должен щелкнуть на значке

.

1. Пользователь должен подсоединить электронный ключ JaCarta к компьютеру.
2. В зависимости от операционной системы пользователь должен выполнить следующие действия.

**Windows XP / Server 2003**

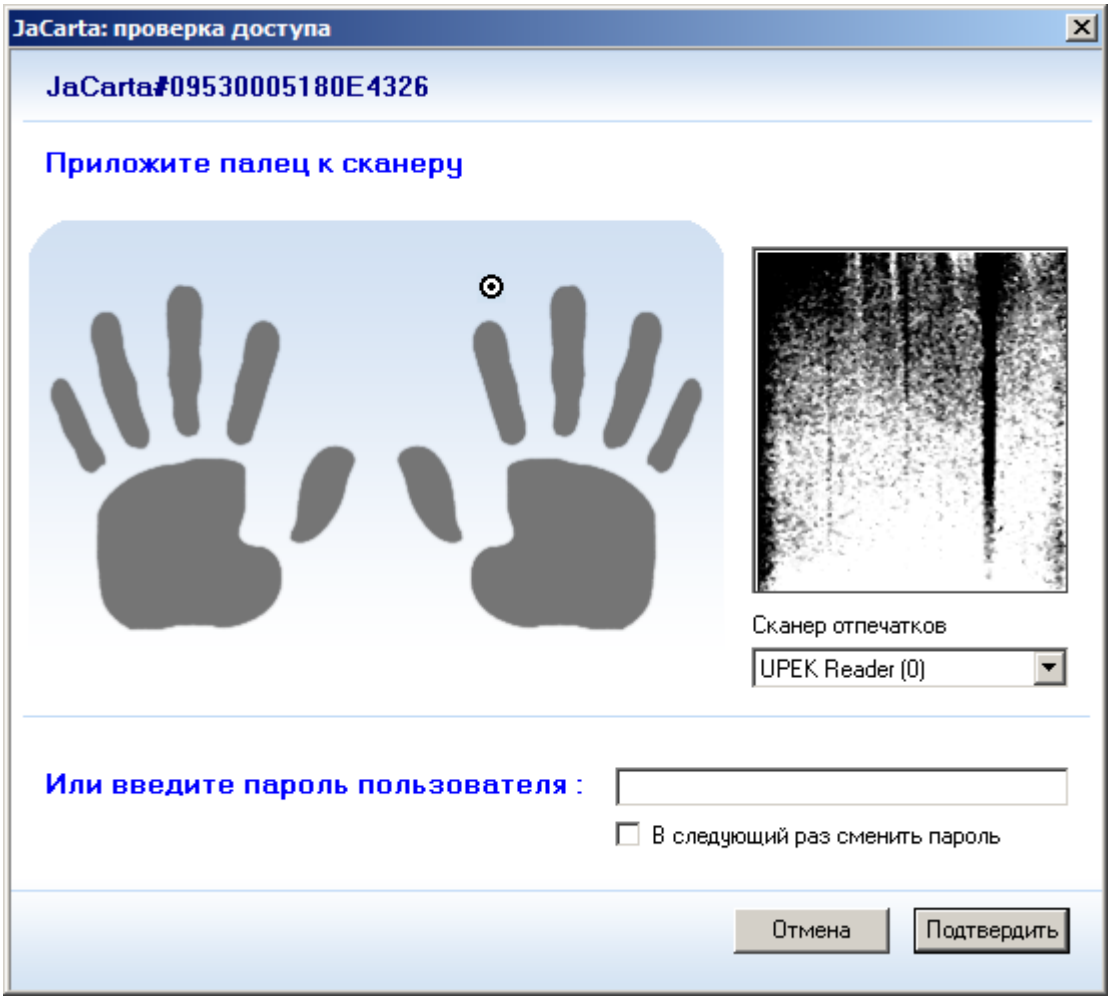
В этом случае пользователь должен перейти к следующему шагу процедуры.

**Windows Vista / Server 2008 / 7**

Отобразится следующая форма.


В этом случае пользователь должен щелкнуть на значке  и перейти к следующему шагу процедуры.

Отобразится окно следующего вида.




**Примечание:**

> Наличие или отсутствие дополнительной возможности входа с использованием пароля пользователя определяется на этапе персонализации. Подробная информация по данному вопросу представлена в документе *JC-Client. Руководство администратора*.

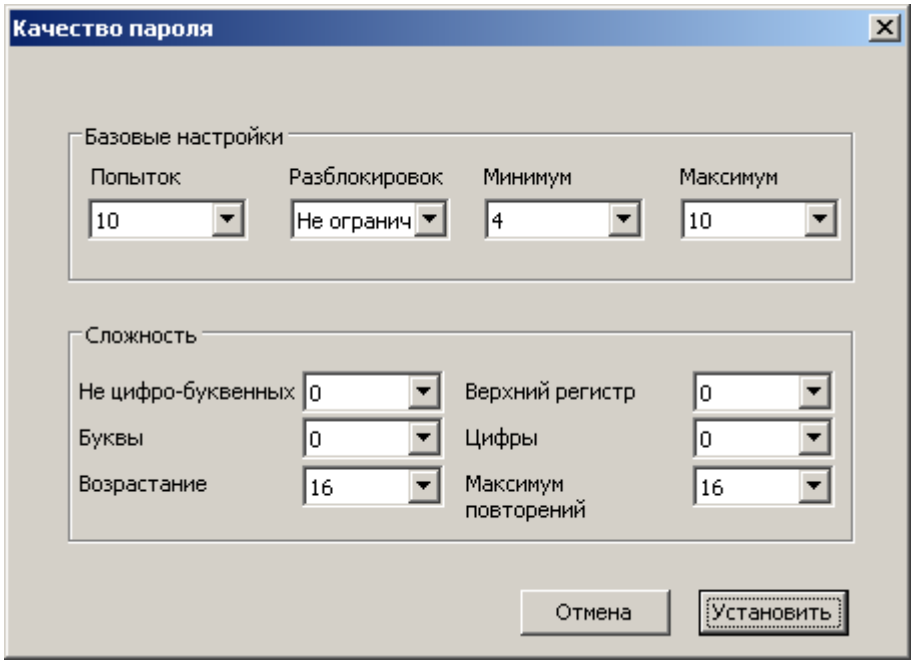
3. Пользователь, используя схематичное изображение ладоней, должен выбрать палец, который он будет использовать для аутентификации, и приложить этот палец к сканеру отпечатков.

По результату сканирования будет осуществлен вход в домен.

# Приложения

## Настройка качества паролей

Настройка качества пароля доступна после нажатия кнопки **Качество пароля** на вкладках **Пароль пользователя**, **Пароль администратора** в окне настройки профиля персонализации. Окно настройки качества пароля выглядит следующим образом.




Чтобы настроить качество пароля, задайте необходимые значения, руководствуясь таблицей, представленной ниже, и нажмите **Установить**.

| Настройка | Описание |
|---|---|
| **Попыток** | Определяет количество последовательных неудачных попыток ввода пароля перед блокировкой пароля.<br>Данный параметр также относится к доступу по отпечатку пальца. После установленного числа последовательных попыток неудачной аутентификации, доступ пользователя по отпечатку блокируется.<br>**Важно:** Если данный параметр выставляется для пароля администратора, следует быть предельно осторожным, так как пароль администратора будет заблокирован, восстановить его не удастся. |
| **Разблокировок** | Максимальное количество разблокировок, которое допустимо сделать в течение эксплуатации электронного ключа JaCarta без необходимости вновь персонализировать устройство.<br>Меню помимо числовых значений содержит два пункта:<br>**Никогда** – после блокировки данный способ доступа больше нельзя будет использовать до персонализации.<br>**Не ограничено** – разблокировать данный способ доступа можно неограниченное количество раз.<br>Данный параметр также относится к доступу по отпечатку пальца. Если число разблокировок доступа по отпечатку достигнет значения, указанного в этом параметре, после следующей блокировки такую возможность разблокировать не удастся.<br>При настройке пароля администратора или пароля разблокировки цифровой подписи данный параметр неактивен, т.к. если пароль администратора заблокирован, восстановить его невозможно.<br>**Примечание:** счетчик неудачных попыток доступа пользователя ведется отдельно для пароля пользователя и для доступа по отпечатку. Таким образом, если в настройках профиля персонализации тип доступа указан как **Биометрия или пароль**, блокировка одного из этих типов доступа позволит пользователю использовать тот тип доступа, который не заблокирован. В случае блокировки обоих типов доступа, каждый из них |

| Настройка | Описание |
|---|---|
| | также будет необходимо разблокировать отдельно. |
| **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. |

Вернуться к настройкам на вкладке **Пароль пользователя**.

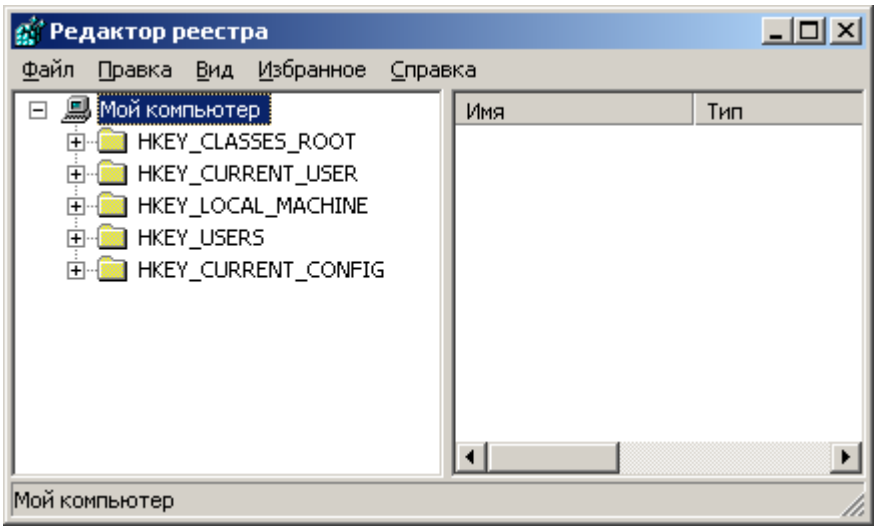
Вернуться к настройкам на вкладке **Пароль администратора**.

## Смена режима поддержки сканеров отпечатков

Существует возможность изменить режим поддержки сканеров отпечатков после установки JC-Client посредством редактирования реестра. Для этого выполните следующие действия.

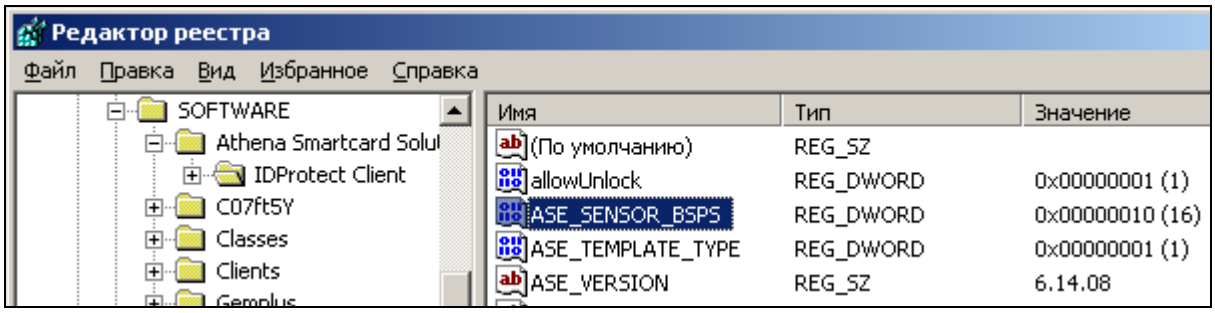
1. Из командной строки выполните команду `regedit`.

   Отобразится окно следующего вида.



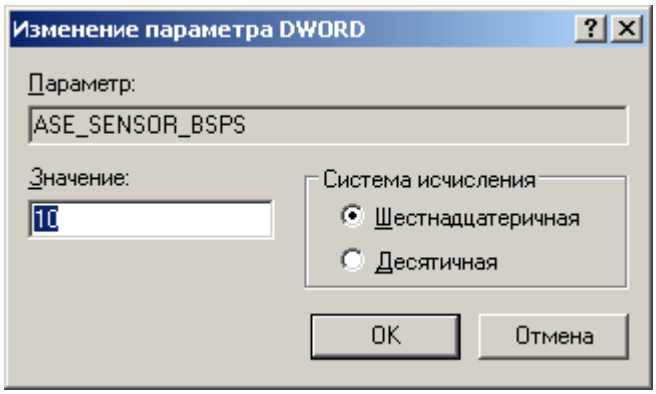
2. Параметр, отвечающий за поддержку биометрических сенсоров, расположен в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Athena Smartcard Solutions\IDProtect Client`

   и носит имя `ASE_SENSOR_BSPS` (см. изображение ниже.)




3. Чтобы отредактировать параметр, сделайте на нем двойной щелчок.

   Отобразится следующее окно.




4. Введите нужное значение в шестнадцатеричном или десятичном формате и нажмите **OK**.

   Список доступных значений представлен в таблице ниже (после изменения значения реестра необходимо перезагрузить компьютер).

| Производитель | Шестнадцатеричный | Десятичный |
|---|---|---|
| Authentec/Upek | **10** | **16** |
| Nitgen | **8** | **8** |
| Precise Biometrics | **1** | **1** |
| Validity | **4** | **4** |
| Authentec/Upek<br>Nitgen | **24** | **36** |
| Authentec/Upek<br>Precise Biometrics | **11** | **17** |
| Authentec/Upek<br>Precise Biometrics<br>Validity | **15** | **21** |
| Authentec/Upek<br>Nitgen<br>Precise Biometrics<br>Validity | **1D** | **29** |
| Precise Biometrics<br>Nitgen | **9** | **9** |
| Precise Biometrics<br>Validity | **5** | **5** |
| Precise Biometrics<br>Nitgen<br>Validity | **D** | **13** |

# История изменений

| Версия документа | Изменения |
|---|---|
| 1.0 | Исходная версия документа |

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