



JaCarta Management System v3.7

Руководство пользователя

Версия продукта	3.7.1
Версия документа	1.00
Статус	Публичный
Дата	29 декабря 2023 г.
Листов	85

Инв. № подл.	Подп. и дата
Взам. инв. №	Инв. № дубл.
Подп. и дата	Подп. и дата

Оглавление

1.	О документе	4
1.1	Назначение документа	4
1.2	На кого ориентирован данный документ	4
1.3	Документы, рекомендуемые для предварительного прочтения (изучения)	4
1.4	Соглашения по оформлению	4
1.5	Обозначения и сокращения	5
1.6	Авторские права, товарные знаки, ограничения	6
1.7	Лицензионное соглашение	7
2.	Введение	10
2.1	Обеспечение безопасности информации при работе с клиентским ПО JMS	10
2.2	Действия после сбоев и ошибок эксплуатации клиентского ПО JMS	11
3.	Клиент JMS	11
3.1	Меню быстрого доступа клиента JMS	11
3.2	Проверка соединения с сервером JMS	12
3.3	Открытие сеанса подключения к JMS	13
3.3.1	Открытие сеанса с помощью доменной учётной записи	15
3.3.2	Открытие сеанса с помощью электронного ключа	15
3.3.3	Открытие сеанса с помощью временного пароля	16
3.3.4	Открытие сеанса на компьютере из другого домена	16
3.4	Проверка статуса клиентского агента	19
3.5	Просмотр сведений об электронных ключах	20
3.6	Операции с электронными ключами	21
3.6.1	Выпуск электронного ключа	21
3.6.2	Синхронизация электронного ключа	26
3.6.3	Отключение возможности использования электронного ключа	26
3.6.4	Разблокировка электронного ключа	27
3.6.5	Смена PIN-кода в приложении на электронном ключе	33
3.6.6	Установка PIN-кода подписи в JaCarta-2 ГОСТ	33
3.6.7	Действия в случае утери или поломки электронного ключа	34
3.6.8	Замена электронного ключа	36
3.7	Операции с ридерами смарт-карт	41
3.7.1	Назначение ридера смарт-карт пользователю	41
3.8	Биометрическая аутентификация	43
4.	Автоматическое обновление клиента JMS	45
5.	Выпуск сертификата КриптоПро в хранилище пользователя на рабочей станции	46

6. Диагностика клиента JMS	46
7. Web-портал самообслуживания пользователей	49
7.1 Аутентификация на внутреннем портале самообслуживания	49
7.1.1 Обычная (одношаговая) аутентификация	50
7.1.2 Двухфакторная (двухшаговая) аутентификация	52
7.2 Первый вход в личный кабинет	53
7.2.1 Самостоятельная установка JWA	53
7.2.2 Начальная настройка контрольных вопросов для аутентификации в ЛК	58
7.3 Вход по SMS-оповещению	59
7.4 Вход по OTP-паролю	60
7.5 Вход по Messaging-паролю	62
7.6 Функции, доступные пользователю в личном кабинете портала самообслуживания	63
7.6.1 Выпуск OTP-аутентификатора	64
7.6.2 Активация программного и Push OTP-токена через e-mail	67
7.6.3 Активация программного и Push OTP-токена в личном кабинете	68
7.6.4 Управление OTP-аутентификаторами из личного кабинета	70
7.6.5 Управление электронными ключами из личного кабинета	71
7.6.6 Управление контрольными вопросами из личного кабинета	78
7.7 Аутентификация и работа на внешнем портале самообслуживания	80
7.7.1 Работа на внешнем web-портале самообслуживания	81
8. Список литературы	82
Контакты, техническая поддержка	83
Регистрация изменений	84

1. О документе

1.1 Назначение документа

Настоящий документ представляет собой руководство пользователя клиентских компонентов ПО JaCarta Management System (JMS).

1.2 На кого ориентирован данный документ

Документ предназначен для пользователей корпоративной информационной системы управления средствами аутентификации.





1.3 Документы, рекомендуемые для предварительного прочтения (изучения)

Перед использованием клиентских приложений JMS рекомендуется ознакомиться с документами «eToken PKI Client 5.1 SP1. Руководство пользователя» [1] и «Единый Клиент JaCarta. Руководство пользователя» [2].

1.4 Соглашения по оформлению

В данном документе для представления ссылок, терминов и наименований, примеров кода программ используются различные шрифты и средства оформления. Основные типы начертаний текста приведены в таблице 1.

Табл. 1 – Элементы оформления

Выделение	Используется для выделения наименований полей, кнопок, секций, вкладок экранных форм
file.exe	Используется для выделения имен файлов, каталогов, текстов программ
[1]	Ссылка на пункт в списке литературы (приведен в конце документа)
Гиперссылка	Используется для выделения внешних ссылок
Ссылка, с. 4	Используется для выделения перекрестных ссылок
	Важная информация
	Ссылка, примечание, заметка
	Совет
	Рекомендация

1.5 Обозначения и сокращения

Табл. 2 – Обозначения и сокращения

USB	Universal Serial Bus, универсальная последовательная шина
PIN-код подписи (PIN-код ЭП)	Секретная последовательность, известная только пользователю, которую необходимо предъявить для выполнения операции электронной подписи
PIN-код пользователя	Секретная последовательность, известная только пользователю, которую необходимо предъявить для аутентификации пользователя в приложении электронного ключа
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации

1.6 Авторские права, товарные знаки, ограничения

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации.

Обладателем исключительных авторских и имущественных прав является АО «Аладдин Р. Д.».

Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. При перепечатке и использовании данных материалов либо любой их части ссылки на АО «Аладдин Р. Д.» обязательны.

Владельцем зарегистрированных товарных знаков "Аладдин", Aladdin, JaCarta, JMS, JAS, Secret Disk, SecurLogon, "Крипто БД", логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является АО «Аладдин Р. Д.».

Названия прочих технологий, продуктов, компаний, упоминающиеся в данном документе, могут являться товарными знаками своих законных владельцев.

Ограничение ответственности

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены АО «Аладдин Р. Д.» без предварительного уведомления.

АО «Аладдин Р. Д.» не гарантирует ни отсутствия ошибок в данном документе, ни того, что описанное программное обеспечение (ПО) не содержит дефектов, будет работать в произвольно выбранных условиях и при этом удовлетворять всем требованиям, которые могут быть к нему предъявлены.

АО «Аладдин Р. Д.» не гарантирует работоспособность нелегально полученного программного обеспечения. Нелегальное использование

программного обеспечения и документации на него преследуется по закону.

Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе АО «Аладдин Р. Д.» не предоставляет никаких ни явных, ни подразумеваемых гарантий.

АО «Аладдин Р. Д.» 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 ИЛИ ПОБОЧНЫЕ УБЫТКИ), ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЁННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОГО КОМПОНЕНТА ОПИСАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ АО «Аладдин Р. Д.» БЫЛО ПИСЬМЕННО УВЕДОМЛЕНО О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

Государственное регулирование и экспортный контроль

Описываемый в данном документе продукт (или продукты) может являться или содержать в себе средство криптографической защиты информации (СКЗИ), являющееся предметом экспортного контроля.

Вы соглашаетесь с тем, что продукт не будет поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону образом.

Вы гарантируете, что будете соблюдать накладываемые на экспорт и резспорт продукта ограничения.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

1.7 Лицензионное соглашение

ВАЖНО:

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

ВСЕ УКАЗАНИЯ ПО ИСПОЛЬЗОВАНИЮ НАСТОЯЩЕГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (включая без ограничений библиотеки, утилиты, файлы для скачивания с Web-сайта, CD-ROM, Руководства, описания и др. документацию), далее «ПО», «Продукт»), ПРЕДОСТАВЛЯЕМЫЕ КОМПАНИЕЙ АО «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 ПРОДУКТ И/ИЛИ ЗАГРУЖАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ как определено далее по тексту) И/ИЛИ УСТАНОВЛИВАЯ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НА ВАШ КОМПЬЮТЕР И/ИЛИ ИСПОЛЬЗУЯ ДАННЫЙ ПРОДУКТ, 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 УСТАНОВЛИВАЙТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И НЕЗАМЕДЛИТЕЛЬНО (не позднее 7 дней с даты получения этого пакета) ВЕРНИТЕ ЭТОТ ПРОДУКТ В АЛАДДИН Р.Д., СОТРИТЕ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ВСЕ ЕГО ЧАСТИ В СВОЕМ КОМПЬЮТЕРЕ И НЕ ИСПОЛЬЗУЙТЕ ЕГО НИКОИМ ОБРАЗОМ.

Лицензионное соглашение на использование программного обеспечения.

Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключенным между Вами (физическим или юридическим лицом) - конечным пользователем (далее "Пользователь") и компанией АО «Аладдин Р.Д.» (далее «компания Аладдин Р.Д.», «Правообладатель») относительно предоставления неисключительного права на использование настоящего программного обеспечения - комплекса программ для ЭВМ, и документации (печатные материалы, носители и файлы с информацией), являющихся неотъемлемой частью ПО, включая все дальнейшие усовершенствования.

Лицензионный договор считается заключенным с момента начала использования Вами ПО любым способом или с момента, когда Вы примете все условия настоящего Лицензионного договора в процессе установки ПО. Лицензионный договор сохраняет свою силу в течение всего срока действия исключительного права на ПО, если только иное не оговорено в Лицензионном договоре или в отдельном письменном договоре между Вами и компанией Аладдин Р.Д. Срок действия Лицензионного договора также может зависеть от объема Вашей Лицензии, описанного в данном Лицензионном договоре.

Права на ПО охраняются действующими законодательством и международными соглашениями. Вы подтверждаете свое согласие с тем, что Лицензионный договор имеет такую же юридическую силу, как и любой другой письменный договор, заключенный Вами. В случае нарушения Лицензионного договора Вы можете быть привлечены в качестве ответчика.

1. Предмет Соглашения

- 1.1. Предметом настоящего Соглашения является передача Правообладателем конечному Пользователю неисключительного права на использование ПО. ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ. Все условия, оговоренные далее, относятся как к ПО в целом, так и ко всем его компонентам в отдельности. Данное соглашение не передает Вам права на Программное обеспечение, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничего в данном Соглашении не подтверждает отказ компании Аладдин Р.Д. от прав на интеллектуальную собственность по какому бы то ни было законодательству.
- 1.2. Компания Аладдин Р.Д. сохраняет за собой все права, явным образом не предоставленные Вам настоящим Лицензионным договором. Настоящий Лицензионный договор не предоставляет Вам никаких прав на товарные знаки Компании Аладдин Р.Д..

- 1.3. В случае, если Вы являетесь физическим лицом, то территория, на которой допускается использование ПО, включает в себя весь мир. В случае, если Вы являетесь юридическим лицом (обособленным подразделением юридического лица), то территория на которой допускается приобретение ПО, ограничена страной регистрации юридического лица (обособленного подразделения юридического лица), если только иное не оговорено в отдельном письменном договоре между Вами и Компанией Аладдин Р.Д.

2. Имущественные права

- 2.1. 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"), и связанная с ним документация предназначается НЕ ДЛЯ ПРОДАЖИ и является и остается исключительной собственностью компании Аладдин Р.Д.
- 2.2. 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 руководству, данные, содержащиеся в нем, а также все права на ПО являются и будут являться собственностью исключительно компании Аладдин Р.Д.
- 2.3. Вам, конечному Пользователю, предоставляется неисключительное право на использование ПО в указанных в документации целях и при соблюдении приведенных ниже условий.

3. Условия использования

- 3.1. ПО может быть использовано только в строгом соответствии с документами, инструкциями и рекомендациями Правообладателя, относящимися к данному ПО.
- 3.2. ПО может предоставляться на нескольких носителях, в том числе с помощью сети интернет. Независимо от количества носителей, на которых Вы получили ПО, Вы имеете право использовать ПО только в объеме предоставленной Вам Лицензии.
- 3.3. После уплаты Вами соответствующего вознаграждения компания Аладдин Р.Д. настоящим предоставляет Вам, а Вы получаете индивидуальное, неисключительное и ограниченное право на использование данного Программного обеспечения только в форме исполняемого кода, как описано в прилагаемой к Программному обеспечению документации и только в соответствии с условиями данного Соглашения:
 - ▶ Вы можете установить Программное обеспечение и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей документации компании Аладдин Р.Д.
 - ▶ Вы можете добавить/присоединить Программное обеспечение к программам Вашего компьютера с единственной целью, описанной в данном Соглашении.
 Продукт должен использоваться и обслуживаться строго в соответствии с описаниями и инструкциями компании Аладдин Р.Д., приведенными в данном и других документах компании Аладдин Р.Д.
- 3.4. За исключением указанных выше разрешений, Вы обязуетесь:
 - 3.4.1. Не использовать и не выдавать сублицензии на данное Программное обеспечение и любую другую Продукцию компании Аладдин Р.Д., за исключением явных разрешений в данном Соглашении и в Руководстве по интеграции.
 - 3.4.2. Не продавать, не выдавать лицензий или сублицензий, не сдавать в аренду или в прокат, не передавать, не переводить на другие языки, не закладывать, не разделять Ваши права в рамках данного Соглашения с кем-либо или кому-либо еще.
 - 3.4.3. Не модифицировать (в том числе не вносить в ПО изменения в целях его функционирования на технических средствах Конечного пользователя), не демонтировать, не декомпилировать или дизассемблировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения.

- 3.4.4. Не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть.
- 3.4.5. Не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому-либо еще использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.
- 3.4.6. Не пытаться обойти технические ограничения в Программе;
- 3.4.7. Не использовать Программу для оказания услуг на платной и бесплатной основе;
- 3.4.8. Не создавать условия для использования ПО лицами, не имеющими прав на использование ПО, в том числе работающими с Вами в одной многопользовательской системе или сети Интернет.
- 3.4.9. Вы не вправе удалять, изменять или делать малозаметными любые уведомления об авторских правах, правах на товарные знаки или патенты, которые указаны на/в ПО.
- 3.4.10. Вы обязуетесь соблюдать права третьих лиц, в том числе авторские права на объекты интеллектуальной собственности.
- 3.5. Компания Аладдин Р.Д. не несет обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов данного Программного обеспечения.
- Нелегальное использование, распространение и воспроизведение (копирование) программного обеспечения является нарушением действующего законодательства и преследуется по Закону.
- В случае нарушения настоящего Соглашения Правообладатель лишает Пользователя права на использование ПО. При этом Правообладатель полностью отказывается от своих гарантийных обязательств.

4. Ограниченная гарантия

Компания Аладдин Р.Д. гарантирует, что:

Данное Программное обеспечение с момента поставки его Вам в течение двенадцати (12) месяцев будет функционировать в полном соответствии с Руководством Пользователя (Администратора), при условии, что оно будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

Правообладатель гарантирует соответствие компонентов ПО спецификациям, а также работоспособность ПО при выполнении Пользователем условий, оговоренных в документации на ПО. ПО поставляется "таким, какое оно есть". Правообладатель не гарантирует, что ПО соответствует вашим требованиям, и что все действия ПО будут выполняться безошибочно. Правообладатель не гарантирует корректную совместную работу ПО с программным обеспечением или оборудованием других производителей.

5. Отказ от гарантии

- 5.1. КОМПАНИЯ АЛАДДИН Р.Д. НЕ ГАРАНТИРУЕТ, ЧТО ЛЮБОЙ ИЗ ЕГО ПРОДУКТОВ БУДЕТ СООТВЕТСТВОВАТЬ ВАШИМ ТРЕБОВАНИЯМ, ИЛИ ЧТО ЕГО РАБОТА БУДЕТ БЕСПЕРЕБОЙНОЙ ИЛИ БЕЗОШИБОЧНОЙ. В ОБЪЕМЕ, ПРЕДУСМОТРЕННОМ ЗАКОНОДАТЕЛЬСТВОМ РФ, КОМПАНИЯ АЛАДДИН Р.Д. ОТКРЫТО ОТКАЗЫВАЕТСЯ ОТ ВСЕХ ГАРАНТИЙ, НЕ ОГОВОРЕННЫХ ЗДЕСЬ, ОТ ВСЕХ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ ГАРАНТИЮ ТОВАРНОГО ВИДА И ПРИГОДНОСТИ ИСПОЛЬЗОВАНИЯ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ.
- НИ ОДИН ИЗ ДИЛЕРОВ, ДИСТРИБЬЮТОРОВ, ПРОДАВЦОВ, АГЕНТОВ ИЛИ СОТРУДНИКОВ КОМПАНИИ АЛАДДИН Р.Д. НЕ УПОЛНОМОЧЕН ПРОИЗВОДИТЬ МОДИФИКАЦИИ, РАСШИРЕНИЯ ИЛИ ДОПОЛНЕНИЯ К ДАННОЙ ГАРАНТИИ.
- 5.2. Если Вы произвели какие-либо модификации Программного обеспечения или любой из частей данного Продукта во время гарантийного периода, то гарантия, упомянутая выше, будет немедленно прекращена.
- 5.3. Гарантия недействительна, если Продукт используется на или в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в документации, или используется на компьютере с любым установленным нелегальным программным обеспечением.
- 5.4. ПО и обновления предоставляются такими, каковы они есть, и Компания Аладдин Р.Д. не предоставляет на них никаких гарантий.

Компания Аладдин Р.Д. не гарантирует и не может гарантировать работоспособность ПО и результаты, которые Вы можете получить, используя ПО.

- 5.5. За исключением гарантий и условий, которые не могут быть исключены или ограничены в соответствии с применимым законодательством, Компания Аладдин Р.Д. не предоставляет Вам никаких гарантий (в том числе явно выраженных или подразумеваемых в статутном или общем праве или обычаями делового оборота) ни на что, включая, без ограничения, гарантии о не нарушении прав третьих лиц, товарной пригодности, интегрируемости, удовлетворительного качества и годности к использованию ПО. Все риски, связанные с качеством работы и работоспособностью ПО, возлагаются на Вас.
- 5.6. Компания Аладдин Р.Д. не предоставляет никаких гарантий относительно программами для ЭВМ других производителей, которые могут предоставляться в составе ПО.

6. Исключение косвенных убытков

Стороны признают, что Продукт по сути своей сложный и не может быть полностью лишен ошибок. КОМПАНИЯ АЛАДДИН Р.Д. НЕ НЕСЕТ 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 ПРОДУКТА, ДАЖЕ ЕСЛИ АЛАДДИН Р.Д. ПИСЬМЕННО УВЕДОМЛЕН О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

7. Ограничение ответственности

В СЛУЧАЕ ЕСЛИ, НЕСМОТЯ НА УСЛОВИЯ ДАННОГО СОГЛАШЕНИЯ, КОМПАНИЯ АЛАДДИН Р.Д. ПРИЗНАНА ОТВЕТСТВЕННОЙ ЗА УБЫТКИ НА ОСНОВАНИИ КАКИХ-ЛИБО ДЕФЕКТОВ ИЛИ НЕСООТВЕТСТВИЯ ЕГО ПРОДУКТОВ, ПОЛНАЯ ОТВЕТСТВЕННОСТЬ ЗА КАЖДУЮ ЕДИНИЦУ ДЕФЕКТНЫХ ПРОДУКТОВ НЕ БУДЕТ ПРЕВЫШАТЬ СУММУ, ВЫПЛАЧЕННУЮ КОМПАНИИ АЛАДДИН Р.Д. ЗА ЭТИ ДЕФЕКТНЫЕ ПРОДУКТЫ.

Компания Аладдин Р.Д. ни при каких обстоятельствах не несет перед Вами никакой ответственности за убытки, вынужденные перерывы в деловой активности, потерю деловых либо иных данных или информации, претензии или расходы, реальный ущерб, а также упущенную выгоду и утраченные сбережения, вызванные использованием или связанными с использованием ПО, а также за убытки, вызванные возможными ошибками и опечатками в ПО и/или в документации, даже если Компании Аладдин Р.Д. стало известно о возможности таких убытков, потерь, претензий или расходов, равно как и за любые претензии со стороны третьих лиц. Вышеперечисленные ограничения и исключения действуют в той степени, насколько это разрешено применимым законодательством. Единственная ответственность Компании Аладдин Р.Д. по настоящему Лицензионному договору ограничивается суммой, которую Вы уплатили за ПО.

8. Прекращение действия

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

После прекращения действия данного Лицензионного соглашения:

- (i) 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;
- (ii) Вы незамедлительно вернете в компанию Аладдин Р.Д. все имущество, в котором используются права Аладдин Р.Д. на интеллектуальную собственность и все копии такового и/или сотрете/удалите любую информацию, содержащуюся в них в электронном виде. Разделы 1, 3, 6-11 будут продолжать действовать даже в случае прекращения действия настоящего Соглашения.

9. Срок действия Договора

- 9.1. Если иное не оговорено в настоящем Лицензионном договоре либо в отдельном письменном договоре между Вами и Компанией Аладдин Р.Д., настоящий Лицензионный договор действует в течение всего срока действия исключительного права на ПО.
- 9.2. В случае нарушения вами условий настоящего Соглашения или неспособности далее выполнять его условия вы обязуетесь уничтожить все копии ПО (включая архивные, файлы с информацией, носители, печатные материалы) или вернуть все относящиеся к ПО материалы организации, в которой вы приобрели ПО. После этого Соглашение прекращает свое действие.
- 9.3. Без ущерба для каких-либо других прав Компания Аладдин Р.Д. имеет право в одностороннем порядке расторгнуть настоящий Лицензионный договор при несоблюдении Вами его условий и ограничений. При прекращении действия настоящего Лицензионного договора Вы обязаны уничтожить все имеющиеся у Вас копии ПО (включая архивные, файлы с информацией, носители, печатные материалы), все компоненты ПО, а также удалить ПО и вернуть все относящиеся к ПО материалы организации, в которой вы приобрели ПО.
- 9.4. Вы можете расторгнуть настоящий Лицензионный договор удалив ПО и уничтожив все копии ПО, все компоненты ПО и сопровождающую его документацию. Такое расторжение не освобождает Вас от обязательств оплатить ПО.

10. Применимое законодательство

Данное Соглашение должно быть истолковано и определено в соответствии с законами Российской Федерации (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Применение Конвенции Организации Объединенных Наций о Договорах международной купли-продажи товаров (the United Nations Convention of Contracts for the International Sale of Goods) однозначно исключается. 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.

11. Государственное регулирование и экспортный контроль

Приобретая и/или начиная использовать Продукт, Вы обязуетесь соблюдать все применимые международные и национальные законы, которые распространяются на продукты, подлежащие экспортному контролю. Настоящее ПО не должно экспортироваться или реэкспортироваться в нарушение экспортных ограничений, имеющихся в законодательстве страны, в которой приобретено или получено ПО. Вы также подтверждаете, что применимое законодательство не запрещает Вам приобретать или получать ПО.

12. Программное обеспечение третьих сторон

Если Продукт 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 Аладдин Р.Д. и Продукт соответственно.

13. Разное

- 13.1. 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.

- 13.2. Все права на материалы, не содержащиеся в ПО, но доступные посредством использования ПО, принадлежат своим законным владельцам и охраняются действующим законодательством об авторском праве и международными соглашениями. Настоящий Лицензионный договор не предоставляет Вам никаких прав на использование такой интеллектуальной собственности.
- 13.3. ПО содержит коммерческую тайну и иную конфиденциальную информацию, принадлежащую Компании Аладдин Р.Д. и третьим лицам, которая охраняется действующим законодательством Российской Федерации, международными соглашениями и законодательством страны приобретения и/или использования ПО.
- 13.4. Вы соглашаетесь на добровольную передачу Компании Аладдин Р.Д. в процессе использования и регистрации ПО своих персональных данных и выражаете свое согласие на сбор, обработку, использование своих персональных данных в соответствии с применимым законодательством, на условиях обеспечения конфиденциальности. Предоставленные Вами персональные данные будут храниться и использоваться только внутри Компании Аладдин Р.Д. и ее дочерних компаний и не будут предоставлены третьим лицам, за исключением случаев, предусмотренных применимым законодательством.
- 13.5. В случае предъявления любых претензий или исков, связанных с использованием Вами ПО Вы обязуетесь сообщить Компании Аладдин Р.Д. о таких фактах в течение трех (3) дней с момента, когда Вам стало известно об их возникновении. Вы обязуетесь совершить необходимые действия для предоставления Компании Аладдин Р.Д. возможности участвовать в рассмотрении таких претензий или исков, а также предоставлять необходимую информацию для урегулирования соответствующих претензий и/или исков в течение семи (7) дней с даты получения запроса от Компании Аладдин Р.Д.
- 13.6. Вознаграждением по настоящему Лицензионному договору признается стоимость Лицензии на ПО, установленная Компанией Аладдин Р.Д. или Партнером Компании Аладдин Р.Д., которая, подлежит уплате в соответствии с определяемым Компанией Аладдин Р.Д. или Партнером Компании Аладдин Р.Д. порядком. Вознаграждение также может быть включено в стоимость приобретенного Вами оборудования или в стоимость полной версии ПО. В случае если Вы являетесь физическим лицом, настоящий Лицензионный договор может быть безвозмездным.
- 13.7. В случае если какая-либо часть настоящего Лицензионного договора будет признана утратившей юридическую силу (недействительной) и не подлежащей исполнению, остальные части Лицензионного договора сохраняют свою юридическую силу и подлежат исполнению.

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 УСТАНОВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ..

2. Введение

JaCarta Management System (JMS) - система, предназначенная для внедрения, управления и учета аппаратных средств аутентификации пользователей в масштабах предприятия.

JMS обеспечивает:

- централизованное управление средствами аутентификации в течение всего жизненного цикла (инициализация/выпуск сертификата, ввод в эксплуатацию/выдача, обслуживание, вывод из эксплуатации/блокирование);
- учет средств аутентификации, аудит их использования;
- автоматизацию типовых операций и сценариев администрирования в соответствии с политиками безопасности, принятыми в организации;
- быстрое и самостоятельное решение проблем пользователей без обращения к администраторам.

Данное руководство предназначено для пользователей клиентского ПО JMS (Клиента JMS)

2.1 Обеспечение безопасности информации при работе с клиентским ПО JMS

Безопасность информации при работе с клиентским ПО JMS (Клиентом JMS) обеспечивается в соответствии с положениями, изложенными в Табл. 3.

Табл. 3 – Обеспечение безопасности информации при работе с клиентским ПО JMS

Раздел обеспечения безопасности информации	Обеспечительные меры в ПО JMS
Режимы работы средства (клиентского ПО JMS)	Клиентское ПО JMS представляет возможность работы (открытие сеанса работы с JMS) в единственном режиме – режиме пользователя. Данный режим доступен пользователю JMS, которому назначена встроенная роль «Пользователь».
Принципы безопасной работы средства (клиентского ПО JMS)	Безопасная работа клиентского ПО JMS обеспечивается путем реализации ролевого метода управления доступом. Открытие сеанса работы с JMS предоставляется пользователю со встроенной ролью «Пользователь». (Перечень полномочий субъекта доступа со встроенной ролью «Пользователь» регламентирован в соответствии с Формуляром [3]).
Функции и интерфейсы ПО JMS, доступные встроенной роли «Пользователь»	Перечень функций и интерфейсов ПО JMS, доступных для встроенной роли «Пользователь» (в документах используется термин «пользователь»), определен в Описании архитектуры безопасности [4].
Параметры (настройки) безопасности ПО JMS, доступные встроенной роли «Пользователь», и их безопасные значения	Для встроенной роли «Пользователь» отсутствуют полномочия для определения (настроек) параметров безопасности ПО JMS. Данные настройки доступны только пользователю со встроенной ролью «Администратор ИБ» и только из консоли управления JMS.

Раздел обеспечения безопасности информации	Обеспечительные меры в ПО JMS
Типы событий безопасности, связанные с доступными пользователю функциями средства (клиентского ПО JMS)	Перечень типов событий, связанных с доступными роли «Пользователь» функциями ПО JMS в соответствии с Описанием архитектуры безопасности [4], приведен в Формуляре [3].
Действия после сбоев и ошибок эксплуатации средства (клиентского ПО JMS)	См. раздел «Действия после сбоев и ошибок эксплуатации клиентского ПО JMS», below.


2.2 Действия после сбоев и ошибок эксплуатации клиентского ПО JMS

Табл. 4 – Действия после сбоев и ошибок эксплуатации клиентского ПО JMS

Сбой/ошибка эксплуатации	Действия пользователя
Ввод неверного пароля при открытии пользовательской сессии	Ввести верный пароль. В случае исчерпания числа попыток ввода пароля (устанавливается для пользователя в соответствующей ресурсной системе) следует обратиться к администратору данной ресурсной системы для разблокировки учётной записи пользователя.

3. Клиент JMS

3.1 Меню быстрого доступа клиента JMS

Меню быстрого запуска JMS Client доступно с помощью значка  (Клиент JMS) в области уведомлений и выглядит следующим образом (см. изображение ниже).

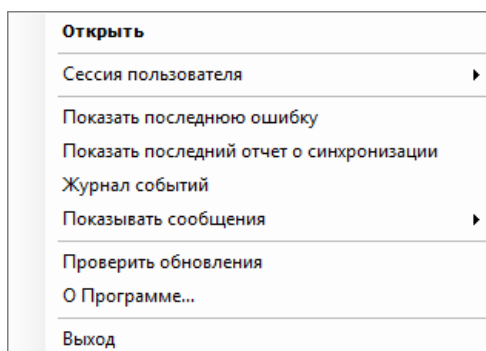


Рис. 1 – Меню быстрого запуска JMS Client

Описание пунктов меню представлено в табл. 5.


Табл. 5 – Меню быстрого запуска JMS Client

Пункт	Описание
Открыть	Открывает окно, в котором содержатся две вкладки: <ul style="list-style-type: none"> Ключевые носители – на этой вкладке отображаются сведения о подсоединённых к компьютеру электронных ключах, а также обо всех

Пункт	Описание
	<p>электронных ключах, которые были назначены или выпущены на имя пользователя (даже если они не подсоединены к компьютеру); кроме того, вкладка позволяет совершать операции с электронными ключами (см. «Просмотр сведений об электронных ключах», с. 20 и «Операции с электронными ключами», с. 21 соответственно);</p> <ul style="list-style-type: none"> • Статус – отображает сведения о состоянии соединения с сервером JMS (см. «Проверка соединения с сервером JMS», с. 12).
Сессия пользователя	Позволяет Открыть или Закрыть пользовательскую сессию с сервером JMS.
Показать последнюю ошибку	Отображает последнюю ошибку.
Показать последний отчет о синхронизации	Отображает последний отчет о синхронизации с сервером, если такой отчет был сгенерирован.
Журнал событий	Открывает окно Просмотр событий , в котором отображаются записи журнала событий, связанные с использованием JMS Client.
Показывать сообщения	<p>Позволяет отметить тип сообщений об использовании электронных ключей и JMS Client, которые будут отображаться на экране пользователя:</p> <ul style="list-style-type: none"> • Информационные; • Предупреждения; • Ошибки.
Проверить обновления	<p>Позволяет выполнить проверку наличия обновления ПО JMS Client.</p> <p>В случае если обновление уже обнаружено, в данном пункте меню будет отображаться Обновление до версии x.x.x.xxxx. Подробнее об обновлении клиента JMS см. в разделе «Автоматическое обновление клиента JMS», с. 45.</p>
О Программе	Отображает общие сведения о JMS.
Выход	Удаляет значок  (Клиент JMS) из области уведомлений, при этом клиент JMS продолжает работать. Чтобы вновь отобразить значок  (Клиент JMS) в области уведомлений, в меню Пуск выберите JaCarta Management System > Клиент JMS .

3.2 Проверка соединения с сервером JMS

Чтобы проверить статус соединения с сервером JMS, выполните следующие действия.

1. Щёлкните правой кнопкой на значке  (Клиент JMS) в области уведомлений и выберите **Открыть**.
2. В отобразившемся окне перейдите на вкладку **Статус**.

Окно примет следующий вид.

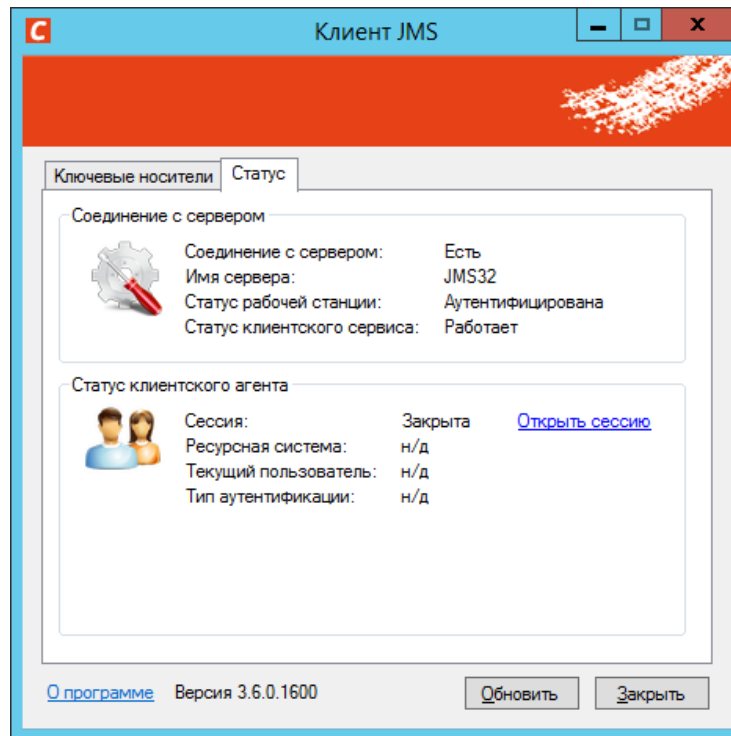




Рис. 2 – Вкладка *Статус*

3. Проверьте значение следующих полей в секции **Соединение с сервером**:
 - 3.1. в поле **Соединение с сервером** должно значиться **Есть**;
 - 3.2. в поле **Статус рабочей станции** должно значиться **Аутентифицирована**.
 - 3.3. в поле **Статус клиентского сервиса** должно значиться **Работает**;

3.3 Открытие сеанса подключения к JMS

Чтобы открыть сеанс подключения к JMS, выполните следующие действия.

 Если вы планируете открывать сеанс подключения к JMS с помощью электронного ключа, подсоедините его к компьютеру.

1. Щёлкните правой кнопкой на значке  (Клиент JMS) в области уведомлений и выберите **Открыть**.
2. В отобразившемся окне перейдите на вкладку **Статус**.

3. Если сеанс подключения к JMS не открыт, то в секции **Статус клиентского агента** в поле **Сессия** будет значиться **Закрыта** (см. рис. 3 ниже).

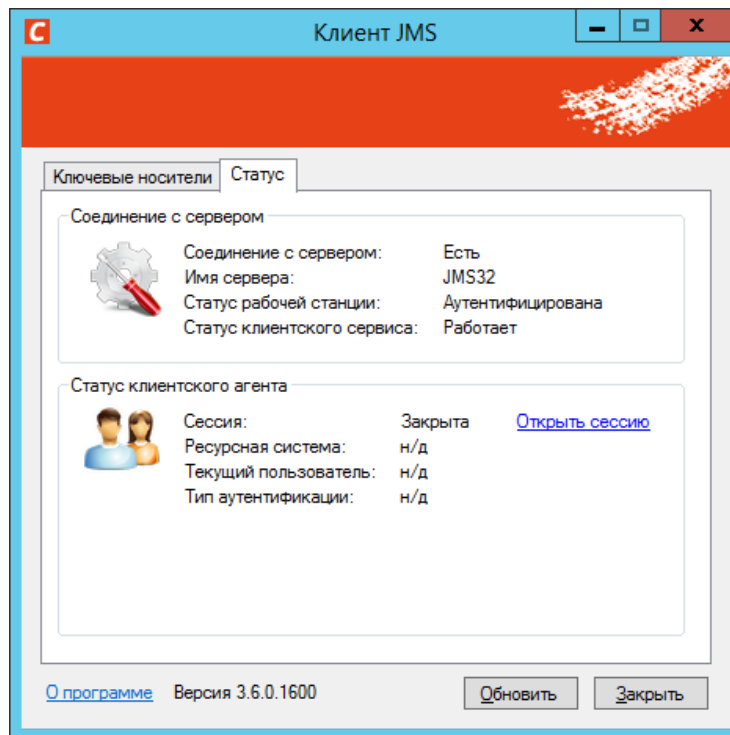


Рис. 3 – Сеанс подключения к JMS не открыт

4. Чтобы открыть сеанс подключения к JMS, щёлкните на ссылке **Открыть сессию**. Отобразится следующее окно.

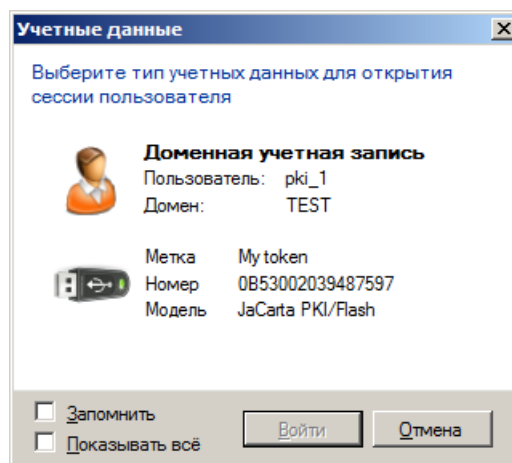



Рис. 4 – Варианты открытия сеанса подключения к JMS

5. Продолжите процедуру в зависимости от нужного типа открытия сеанса:
 - «Открытие сеанса с помощью доменной учётной записи» ниже;
 - «Открытие сеанса с помощью электронного ключа» на стр. 15;
 - «Открытие сеанса с помощью временного пароля» на стр. 16.

 В любом из вариантов вы можете установить флажок **Запомнить**, чтобы Клиент JMS при следующем входе воспроизвёл ваше прошлое решение.

3.3.1 Открытие сеанса с помощью доменной учётной записи

1. Щёлкните на пункте **Доменная учётная запись**.
Окно примет следующий вид.

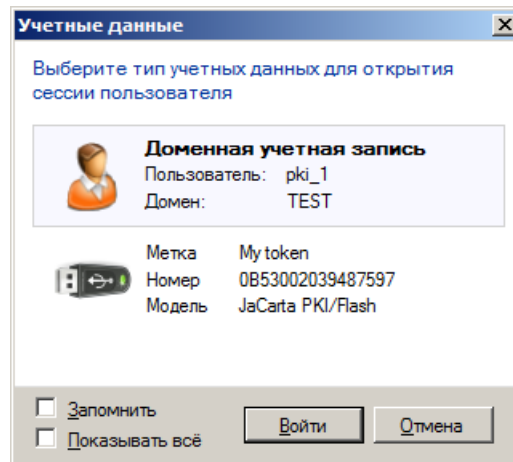


Рис. 5 – Открытие сеанса с помощью доменной учётной записи

2. Щёлкните на кнопке **Войти**.
Вход будет осуществлён автоматически.

3.3.2 Открытие сеанса с помощью электронного ключа

1. Щёлкните на значке электронного ключа.
Окно примет следующий вид.

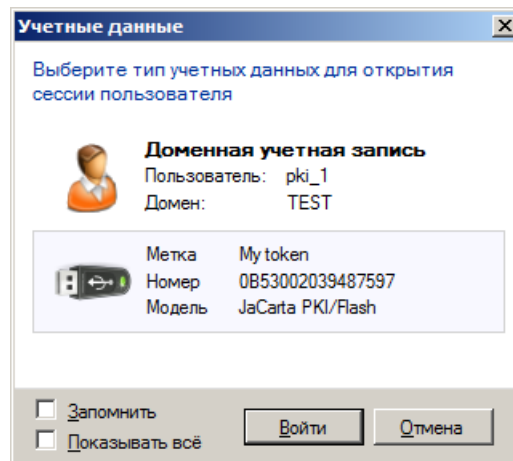


Рис. 6 – Открытие сеанса с помощью электронного ключа

2. Щёлкните на кнопке **Войти**.

3. Если отобразится окно ввода PIN-кода (см. рис. 7 ниже), введите PIN-код и нажмите **ОК**.

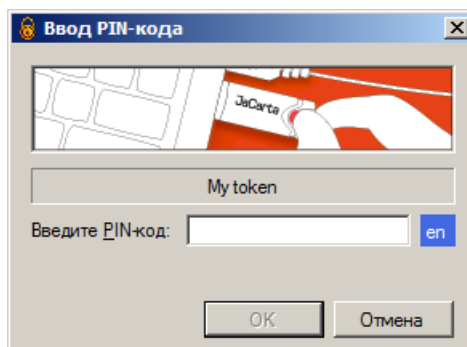


Рис. 7 – Окно ввода PIN-кода

3.3.3 Открытие сеанса с помощью временного пароля

1. Установите флажок **Показывать всё**.
Окно примет следующий вид.

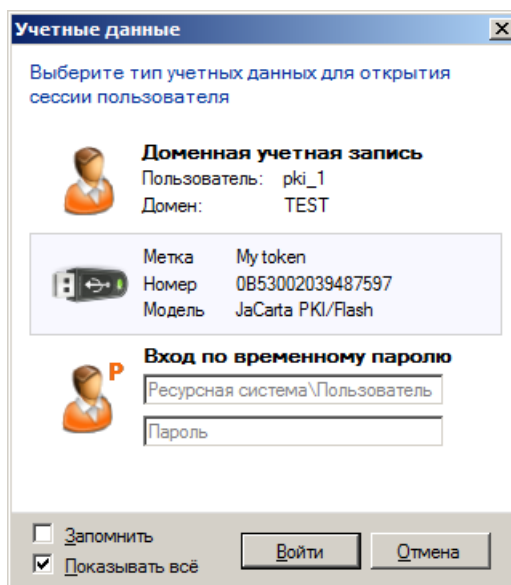


Рис. 8 – Открытие сеанса с помощью временного пароля


2. Выберите пункт **Вход по временному паролю**.
3. Введите следующие данные:
 - 3.1. в верхнем поле введите ваше имя пользователя с указанием домена, в следующем формате:
 - 3.2. **<имя ресурсной системы>\<имя пользователя>**, например, **test.com\user**;
 - 3.3. В нижнем поле введите временный пароль, сообщённый вам администратором.
4. Нажмите **Войти**.

3.3.4 Открытие сеанса на компьютере из другого домена

JMS предоставляет возможность пользователю, работающему на компьютере, не входящем в тот домен, в котором установлен JMS сервер, открывать сессию (по NTLM). При этом, пользователю для открытия сессии достаточно указать свой логин и пароль из Active Directory (AD).

Чтобы открыть сессию, необходимо выполнить следующие действия:

1. Запустите Клиент JMS и перейдите на вкладку **Статус** (см. Рис. 9).

 **Внимание!** В реестре компьютера, на котором установлен Клиент JMS должны быть прописаны настройки подключения к серверу JMS. Подробнее см. Руководство администратора JMS. Раздел Установка и первоначальная настройка компонента JMS Client.

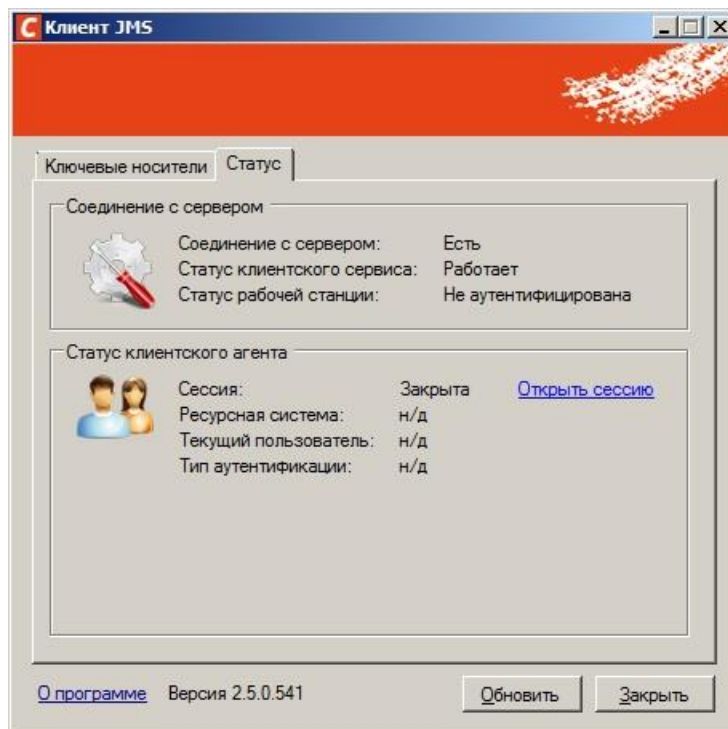


Рис. 9 – Вкладка **Статус** в окне **Клиент JMS**

2. В появившемся окне (см. рис. 10) выберите опцию **Показывать всё**

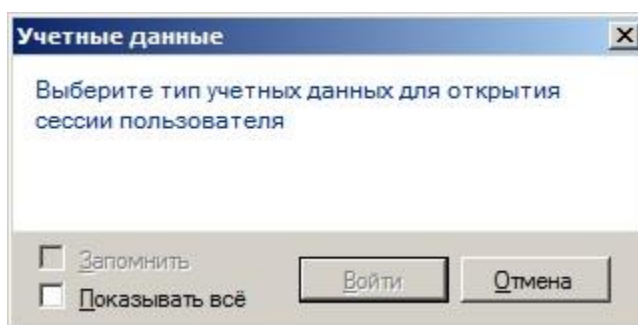


Рис. 10 – Окно выбора типа учетных данных для открытия сессии пользователя

3. В появившемся окне (см. рис. 11) в поле **Вход по доменному паролю** введите имя домена и имя пользователя AD, введите пароль и нажмите **Войти**.

 Для открытия сессии пользователя по NTLM необходимо указать логин пользователя в следующем формате: Имя домена\Имя пользователя, после чего ввести пароль.

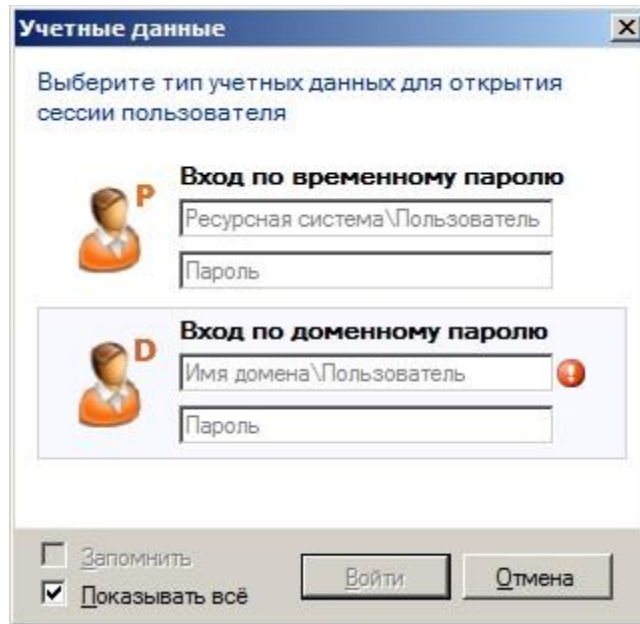


Рис. 11 – Окно ввода учетных данных для открытия сессии пользователя

В появившемся окне (см. рис. 12) после открытия сессии в секции **Статус клиентского агента** будет указана информация о текущем пользователе и ресурсной системе. Тип аутентификации: Доменный пароль.

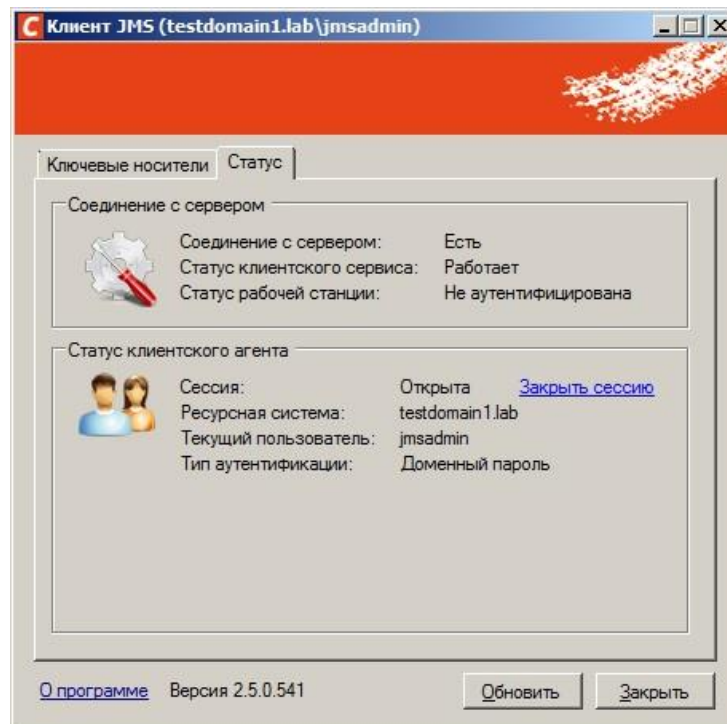


Рис. 12 – Окно с отображением статуса клиентского агента

3.4 Проверка статуса клиентского агента

После открытия соединения с сервером JMS вы можете проверить статус клиентского агента. Для этого выполните следующие действия.

1. Щёлкните правой кнопкой на значке **G** (Клиент JMS) в области уведомлений и выберите **Открыть**.
2. В образовавшемся окне перейдите на вкладку **Статус**.
Окно примет следующий вид.

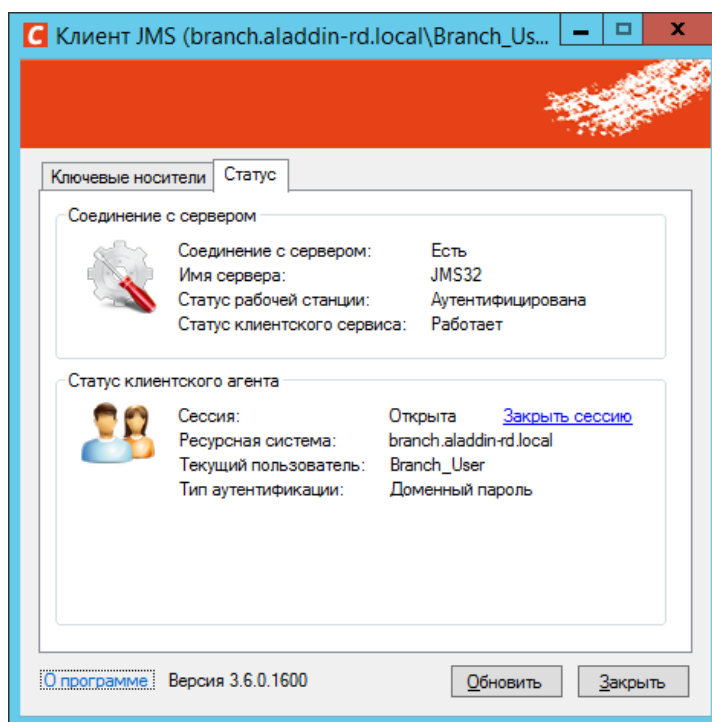


Рис. 13 – Вкладка Статус после открытия сеанса подключения к JMS


3. Проверьте значения в секции **Статус клиентского агента** (см. табл. 6 ниже).

Табл. 6 – Статус клиентского агента

Секция	Поле	Описание
Статус клиентского агента	Сессия	Показывает, Открыта или Закрыта пользовательская сессия (сеанс) подключения к серверу JMS.
	Ресурсная система	Отображает используемую ресурсную систему (например, домен Windows), если сессия соединения с сервером JMS открыта.
	Текущий пользователь	Отображает текущего пользователя, если сессия соединения с сервером JMS открыта.
	Тип аутентификации	Отображает способ аутентификации, который был использован для открытия сессии с сервером JMS – если сеанс с сервером JMS был открыт.

3.5 Просмотр сведений об электронных ключах

Чтобы просмотреть сведения о подсоединённом электронном ключе или о любом электронном ключе, который был назначен или выпущен на ваше имя, выполните следующие действия.

1. Подсоедините электронный ключ, сведения о котором вы хотите просмотреть, к компьютеру.
2. Щёлкните правой кнопкой на значке  (Клиент JMS) в области уведомлений и выберите **Открыть**.
3. В отобразившемся окне перейдите на вкладку **Ключевые носители**.
4. Сведения отобразятся в центральной части окна (см. рис. 14 и табл. 7 соответственно).

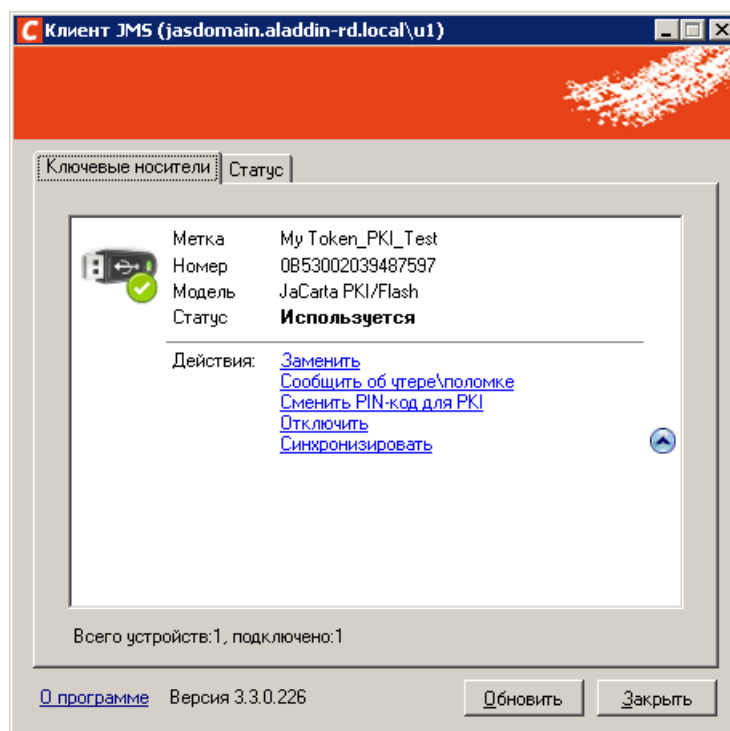


Рис. 14 – Вкладка **Ключевые носители**


Табл. 7 – Сведения на вкладке **Ключевые носители**

Поле	Описание
Метка	Метка электронного ключа.
Номер	Серийный номер электронного ключа.
Модель	Модель электронного ключа.
Статус	Текущий статус электронного ключа.
Действие	<p>Секция содержит ссылки, которые запускают операции с электронными ключами.</p> <ul style="list-style-type: none"> • Выпустить – позволяет осуществить выпуск электронного ключа (см. «Выпуск электронного ключа» на стр. 21), ссылка отображается только в том случае, если подсоединённый электронный ключ ещё не выпущен и если самостоятельный выпуск разрешён настройками JMS; • Заменить – позволяет выполнить замену электронного ключа (см. «Замена электронного ключа» на стр. 36);


Поле	Описание
	<ul style="list-style-type: none"> • Сообщить об утере\поломке – позволяет уведомить администраторов JMS об утере или поломке вашего электронного ключа (см. «Действия в случае утери или поломки электронного ключа» на стр. 34); • Сменить PIN-код для <Тип приложения> – позволяет сменить PIN-код в приложении указанного типа на электронном ключе; • Сменить PIN-код ЭП для ГОСТ 2 – позволяет сменить PIN-код подписи (ЭП) в приложении ГОСТ 2 на электронном ключе; • Установить PIN-код ЭП для ГОСТ 2 – позволяет установить PIN-код подписи (ЭП) в приложении ГОСТ 2 на электронном ключе; • Отключить – позволяет временно отключить возможность использования электронного ключа (см. «Отключение возможности использования электронного ключа» на стр. 26). • Синхронизировать – позволяет выполнить синхронизацию электронного ключа (см. «Синхронизация электронного ключа» на стр. 26); • Разблокировать <Тип приложения> – позволяет разблокировать приложение указанного типа на электронном ключе(см. «Разблокировка электронных ключей JaCarta, eToken и Рутокен», с. 27). Ссылка отображается только в том случае, если приложение указанного типа на электронном ключе заблокировано и возможность разблокировки включена в JMS. • Разблокировать PIN-код ЭП ГОСТ 2 – позволяет разблокировать PIN-код подписи (ЭП) в электронном ключе JaCarta-2 ГОСТ (ссылка отображается только в случае, если PIN-код подписи в электронном ключе заблокирован). • Разблокировать ГОСТ 2 – позволяет разблокировать PIN-код пользователя в электронном ключе JaCarta-2 ГОСТ (ссылка отображается только в случае, если PIN-код пользователя в электронном ключе заблокирован). • Назначить – действие предусмотрено только в отношении ридеров смарт-карт (см. раздел «Операции с ридерами смарт-карт», с. 41). Выполняет назначение карт-ридера пользователю, открывшему сеанс подключения к JMS..

3.6 Операции с электронными ключами

Доступность тех или иных операций с электронными ключами зависит от настроек, установленных администратором JMS. В случае возникновения вопросов относительно доступности для пользователя тех или иных действий обратитесь к администратору.


 Для выполнения операций с электронными ключами, кроме операций смены PIN-кодов, необходимо открыть сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS» на стр. 13).


3.6.1 Выпуск электронного ключа

 Для выполнения этой процедуры вы должны иметь полномочия на самостоятельный выпуск электронных ключей. В случае отсутствия таковых для выпуска электронного ключа обратитесь к администратору.

Чтобы самостоятельно выпустить электронный ключ, выполните следующие действия.

1. Подсоедините электронный ключ, который вы хотите выпустить, к компьютеру.

 В JMS может быть настроен автоматический выпуск электронного ключа. Если процедура выпуска запустилась автоматически, без инициативы с вашей стороны, выполните действие (установка метки электронного ключа), представленное в шаге 8 настоящей процедуры, и дождитесь окончания автоматического выпуска электронного ключа.

2. Щёлкните правой кнопкой на значке  (Клиент JMS) в области уведомлений и выберите **Открыть**.
3. В окне **Клиент JMS** перейдите на вкладку **Ключевые носители**.

Окно примет следующий вид.

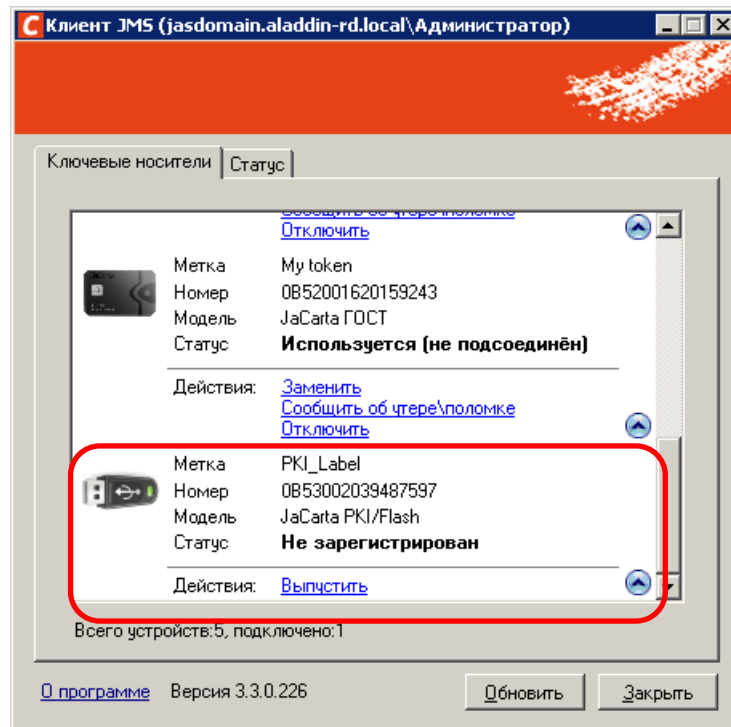



Рис. 15 – Выбор электронного ключа для выпуска

4. В центральной части окна щёлкните на ссылке **Выпустить**, расположенной ниже значка электронного ключа, который вы хотите выпустить.

 Значок электронного ключа, если он был назначен или выпущен на ваше имя, будет отображаться даже в том случае, если электронный ключ не подсоединён к компьютеру (при этом действие **Выпустить** будет недоступно). Чтобы обеспечить возможность выпуска, убедитесь в соединении электронного ключа с компьютером.

Отобразится следующее окно.

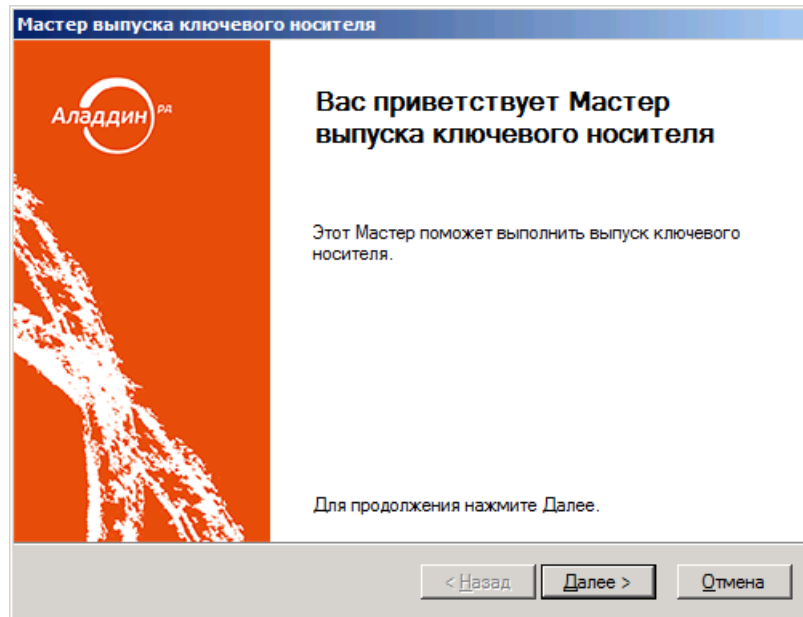


Рис. 16 – Окно приветствия мастера выпуска электронного ключа

5. Нажмите **Далее**.
Отобразится следующее окно.

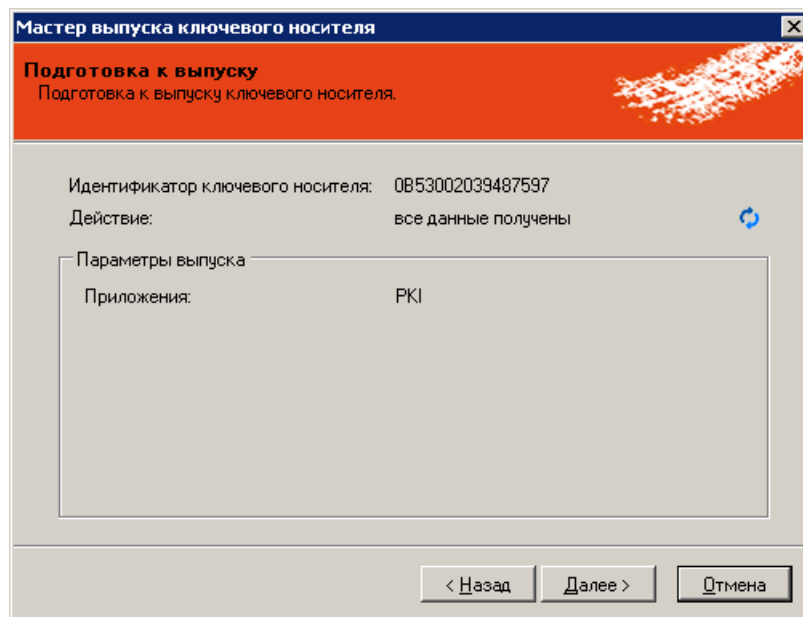


Рис. 17 – Подготовка к выпуску электронного ключа

6. Нажмите **Далее**.

Отобразится следующее окно.

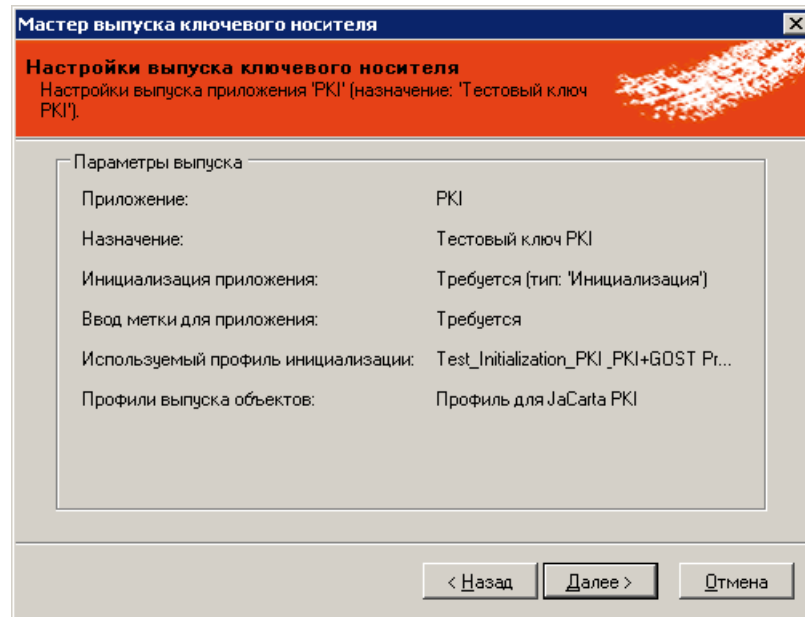


Рис. 18 – Параметры выпуска электронного ключа

7. Нажмите **Далее**.
Отобразится следующее окно.

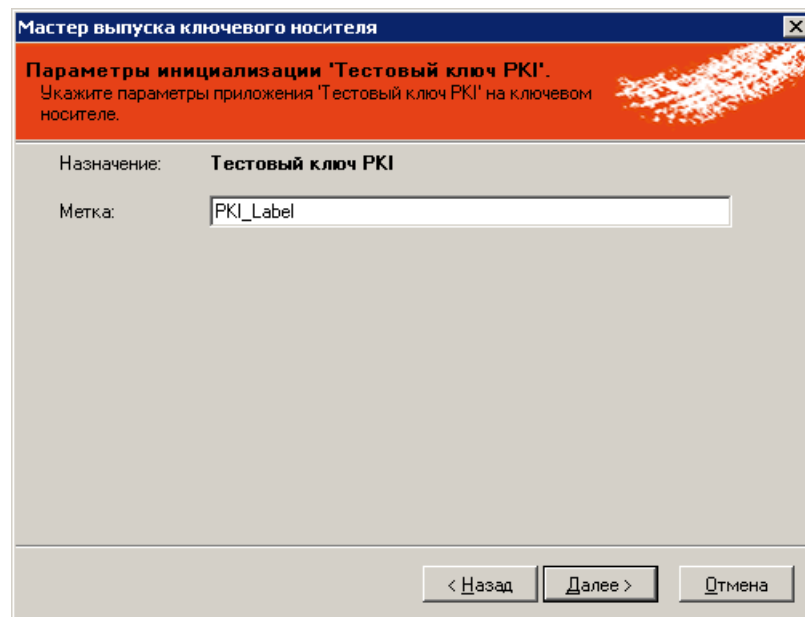


Рис. 19 – Окно задания метки электронного ключа

8. Задайте метку вашего электронного ключа (если административные настройки выпуска ключа посредством Клиента JMS допускают редактирование поля **Метка**) и нажмите **Далее**.

Отобразится следующее окно.

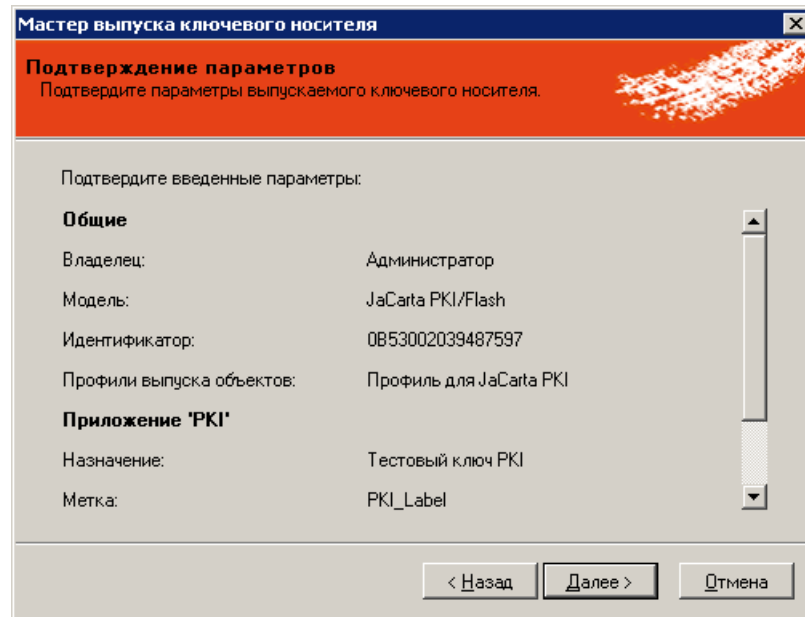



Рис. 20 – Окно подтверждения параметров выпуска

9. Нажмите **Далее**.

 Если в память электронного ключа записывается профиль SecurLogon, вам может потребоваться ввести пароль и подтверждения учётной записи Windows.

По истечении некоторого времени отобразится следующее окно.

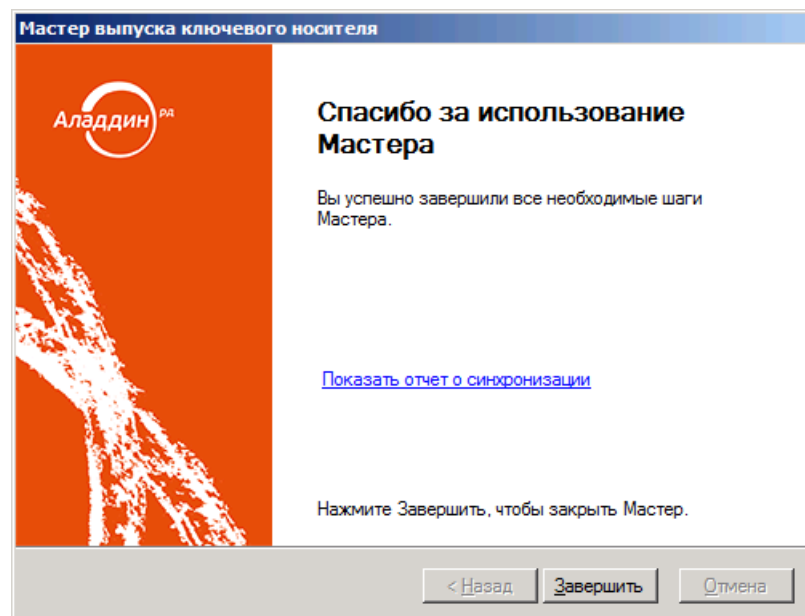


Рис. 21 – Окно завершения работы мастера выпуска электронного ключа

После выпуска электронный ключ будет иметь статус **Используется** (см. рис. 22)

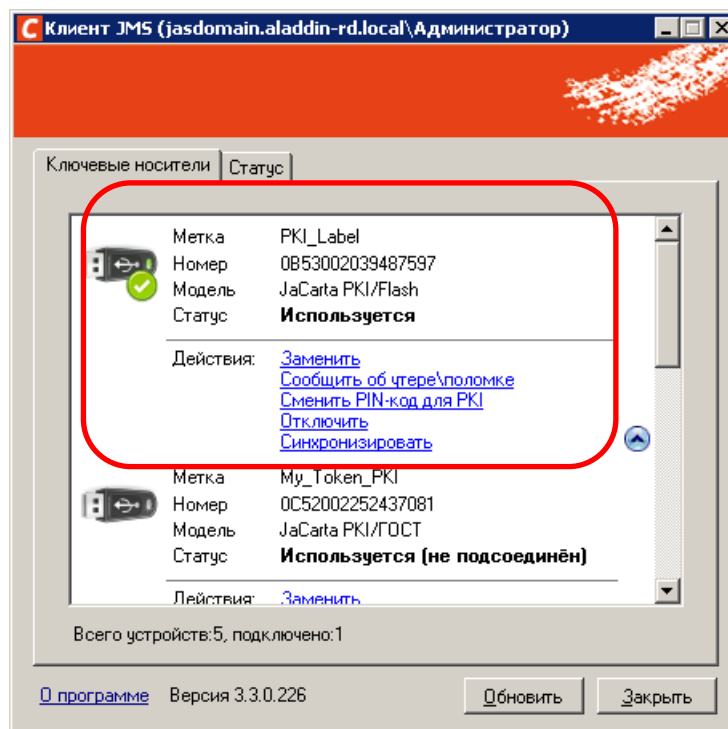


Рис. 22 – Статус выпущенного электронного ключа

3.6.2 Синхронизация электронного ключа

Чтобы синхронизировать электронный ключ, выполните следующие действия.

1. Подсоедините электронный ключ, который вы хотите синхронизировать, к компьютеру.
2. Щёлкните правой кнопкой на значке **C** (Клиент JMS) в области уведомлений и выберите **Открыть**.
3. В отобразившемся окне перейдите на вкладку **Ключевые носители**.
4. В секции **Действия** под значком вашего электронного ключа щёлкните на ссылке **Синхронизировать** и дождитесь окончания процедуры синхронизации.

3.6.3 Отключение возможности использования электронного ключа

Чтобы на время отключить возможность использования электронного ключа, выполните следующие действия.


⚠ После отключения возможности использования электронного ключа включить такую возможность может только администратор.


1. Щёлкните правой кнопкой на значке **C** (Клиент JMS) в области уведомлений и выберите **Открыть**.
2. В отобразившемся окне перейдите на вкладку **Ключевые носители**.
3. В секции **Действия** под значком вашего электронного ключа щёлкните на ссылке **Отключить**.
4. В окне предупреждающего сообщения нажмите **Да** для подтверждения процедуры.

3.6.4 Разблокировка электронного ключа

Если вы превысили допустимое число попыток ввода неверного PIN-кода приложения в электронном ключе, ваш электронный ключ заблокируется. Чтобы разблокировать его, выполните следующие действия.

3.6.4.1 Разблокировка электронных ключей JaCarta, eToken и Рутокен

1. Подсоедините электронный ключ, который вы хотите разблокировать, к компьютеру.
2. Щёлкните правой кнопкой на значке  (Клиент JMS) в области уведомлений и выберите **Открыть**.
3. В отобразившемся окне перейдите на вкладку **Ключевые носители**.
4. В центральной части окна щёлкните на **Разблокировать <Название приложения>** под значком электронного ключа.

 Если электронный ключ заблокирован, его статус будет отображён красным цветом. Отобразится следующее окно.

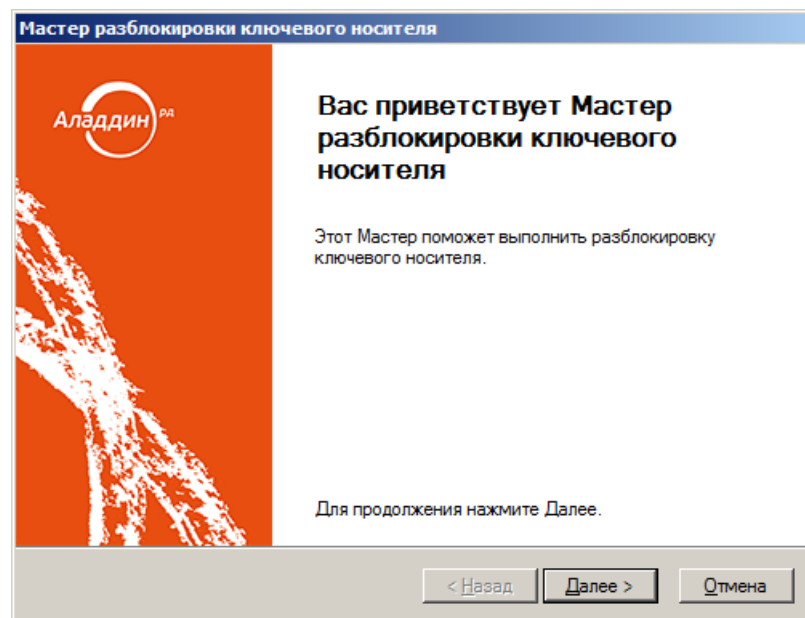


Рис. 23 – Окно приветствия мастера разблокировки электронного ключа

5. Нажмите **Далее**.

Отобразится следующее окно.

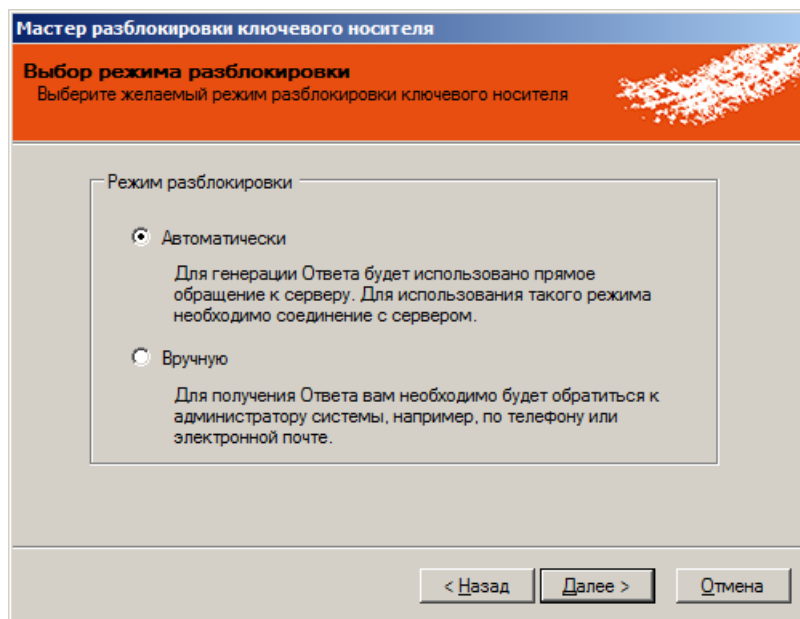



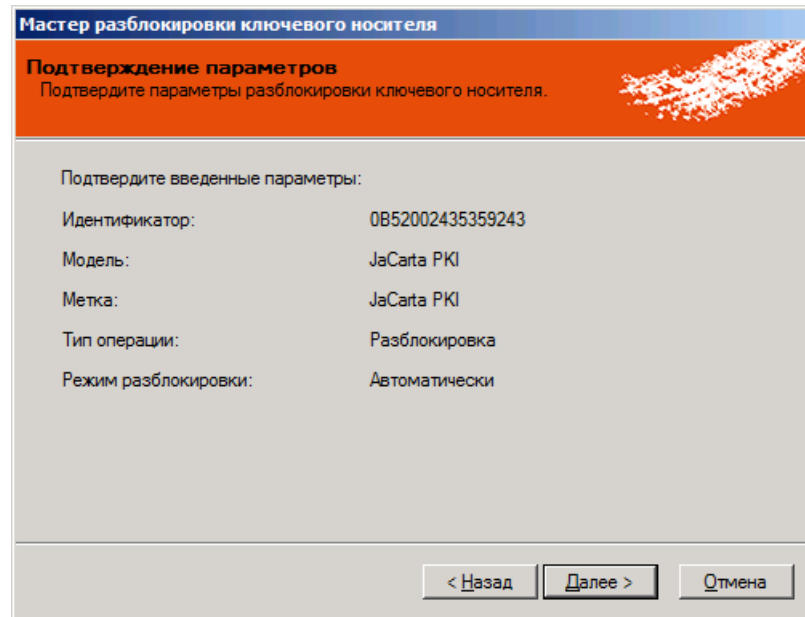
Рис. 24 – Выбор режима разблокировки

6. Выберите один из двух режимов и нажмите **Далее**.
 - **Автоматически** – разблокировка в этом режиме происходит без участия администратора;
 - **Вручную** – разблокировка в этом режиме возможна только с участием администратора (с администратором можно связаться, например, по телефону).

 Разблокировку электронных ключей JaCarta и eToken также можно произвести с помощью Единого Клиента JaCarta, например, если блокировка препятствует входу в ОС Windows с помощью электронного ключа (подробнее см. в документе «Единый Клиент JaCarta. Руководство пользователя»).

 В случае невозможности использования функции разблокировки обратитесь к администратору.

Отобразится следующее окно.



The screenshot shows a dialog box titled "Мастер разблокировки ключевого носителя" (Master of key unlocking). The main heading is "Подтверждение параметров" (Confirmation of parameters) with the instruction "Подтвердите параметры разблокировки ключевого носителя." (Confirm the key unlocking parameters). Below this, it says "Подтвердите введенные параметры:" (Confirm the entered parameters:). The parameters are listed as follows:

Идентификатор:	0B52002435359243
Модель:	JaCarta PKI
Метка:	JaCarta PKI
Тип операции:	Разблокировка
Режим разблокировки:	Автоматически

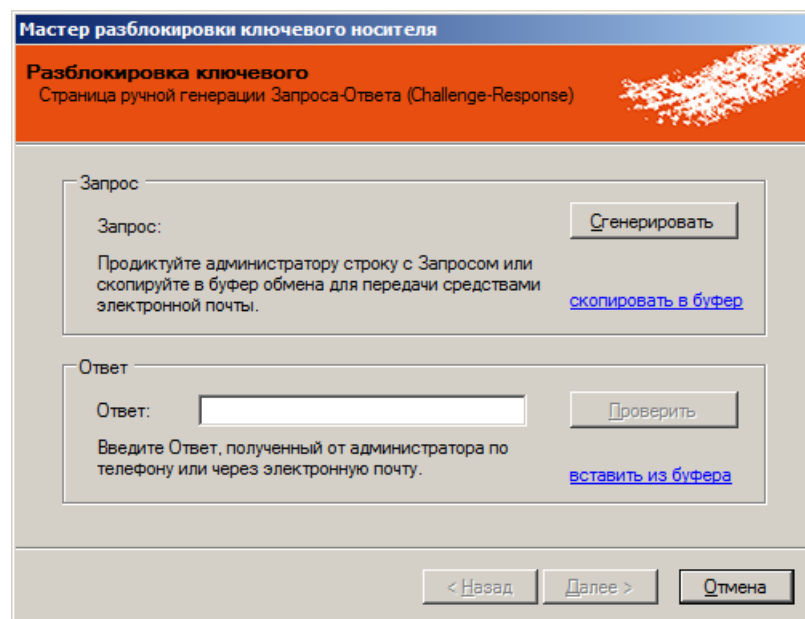
At the bottom of the dialog, there are three buttons: "< Назад" (Back), "Далее >" (Next), and "Отмена" (Cancel).

Рис. 25 – Окно подтверждения параметров

Нажмите **Далее**.

- Если вы выбрали автоматический режим разблокировки, переходите к шагу 11 настоящей процедуры.
- Если вы выбрали ручной режим разблокировки, переходите к следующему шагу настоящей процедуры.

7. Отобразится следующее окно.



The screenshot shows a dialog box titled "Мастер разблокировки ключевого носителя" (Master of key unlocking). The main heading is "Разблокировка ключевого" (Key unlocking) with the subtitle "Страница ручной генерации Запроса-Ответа (Challenge-Response)" (Manual generation page of Challenge-Response). The dialog is divided into two sections:

Запрос (Challenge): Includes a "Запрос:" label, a "Сгенерировать" (Generate) button, and instructions: "Продиктуйте администратору строку с Запросом или скопируйте в буфер обмена для передачи средствами электронной почты." (Dictate the administrator the line with the Request or copy it to the clipboard for transfer by email). A link "скопировать в буфер" (copy to clipboard) is also present.

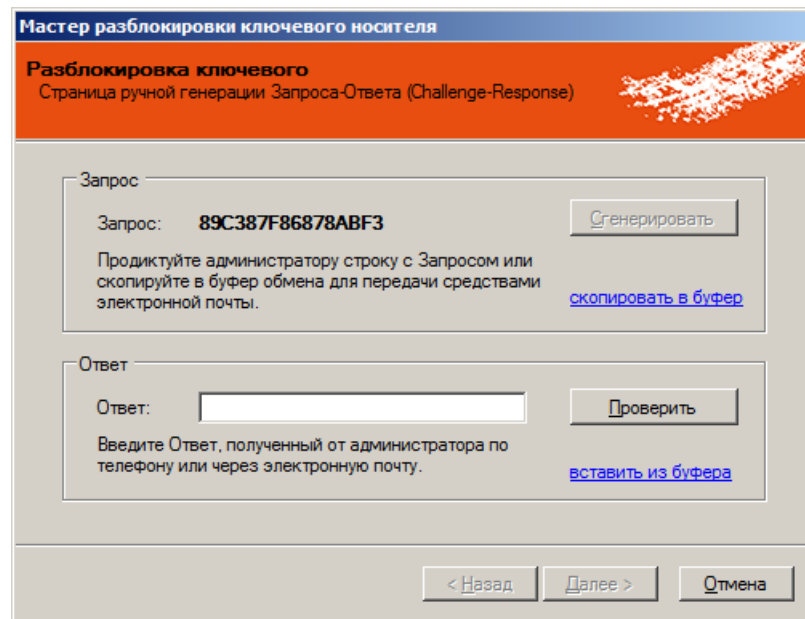
Ответ (Response): Includes an "Ответ:" label, an input field, a "Проверить" (Check) button, and instructions: "Введите Ответ, полученный от администратора по телефону или через электронную почту." (Enter the Response received from the administrator by phone or via email). A link "вставить из буфера" (paste from clipboard) is also present.

At the bottom of the dialog, there are three buttons: "< Назад" (Back), "Далее >" (Next), and "Отмена" (Cancel).

Рис. 26 – Окно разблокировки по схеме «запрос-ответ»

Нажмите **Сгенерировать**.

В окне отобразится код запроса (см. рис. 27).



The screenshot shows a software window titled "Мастер разблокировки ключевого носителя" (Master of key unlocking). The main heading is "Разблокировка ключевого" (Key unlocking) and the subtitle is "Страница ручной генерации Запроса-Ответа (Challenge-Response)" (Manual generation of Challenge-Response page). The window is divided into two main sections: "Запрос" (Challenge) and "Ответ" (Response). In the "Запрос" section, a "Запрос:" label is followed by the alphanumeric code "89C387F86878ABF3". To the right of the code is a "Сгенерировать" (Generate) button. Below the code, there is a text instruction: "Продиктуйте администратору строку с Запросом или скопируйте в буфер обмена для передачи средствами электронной почты." (Dictate the line with the Challenge to the administrator or copy it to the clipboard for transmission via email). A blue link "скопировать в буфер" (copy to clipboard) is provided. In the "Ответ" section, there is an "Ответ:" label followed by an empty text input field. To the right of the field is a "Проверить" (Check) button. Below the field, there is a text instruction: "Введите Ответ, полученный от администратора по телефону или через электронную почту." (Enter the Response received from the administrator by phone or via email). A blue link "вставить из буфера" (paste from clipboard) is provided. At the bottom of the window, there are three navigation buttons: "< Назад" (Back), "Далее >" (Next), and "Отмена" (Cancel).

Рис. 27 – Код запроса

8. Свяжитесь с администратором (например, по телефону) и сообщите ему код запроса. Администратор сообщит вам код ответа.
9. Введите код ответа в поле **Ответ** и нажмите **Проверить**. Если код ответа соответствует коду запроса, отобразится следующее сообщение.

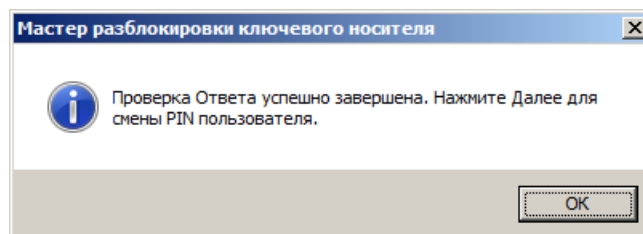


Рис. 28 – Сообщение об успешной проверке ответа

10. Нажмите **ОК**.

Отобразится следующее окно.

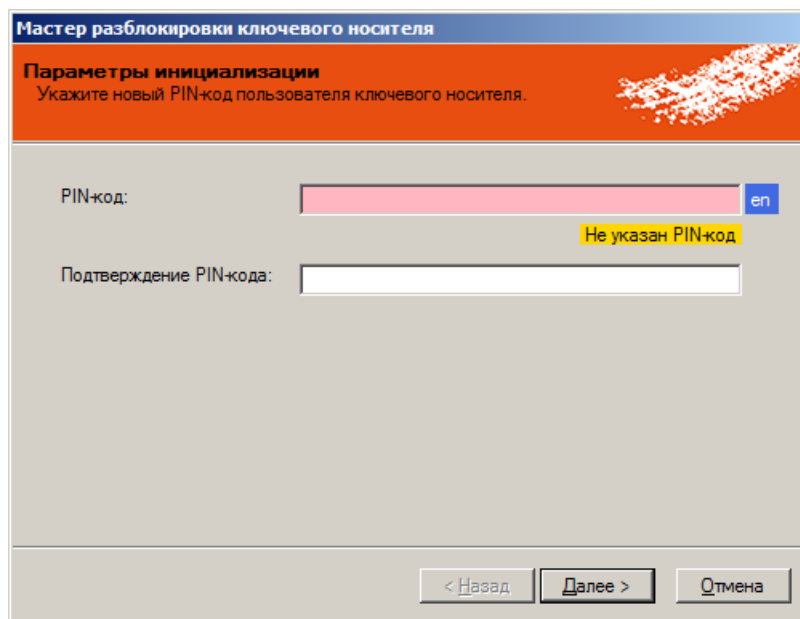


Рис. 29 – Окно ввода PIN-кода

11. В полях **PIN-код** и **Подтверждение PIN-кода** введите PIN-код пользователя и его подтверждение соответственно, после чего нажмите **Далее**.
Отобразится следующее окно.

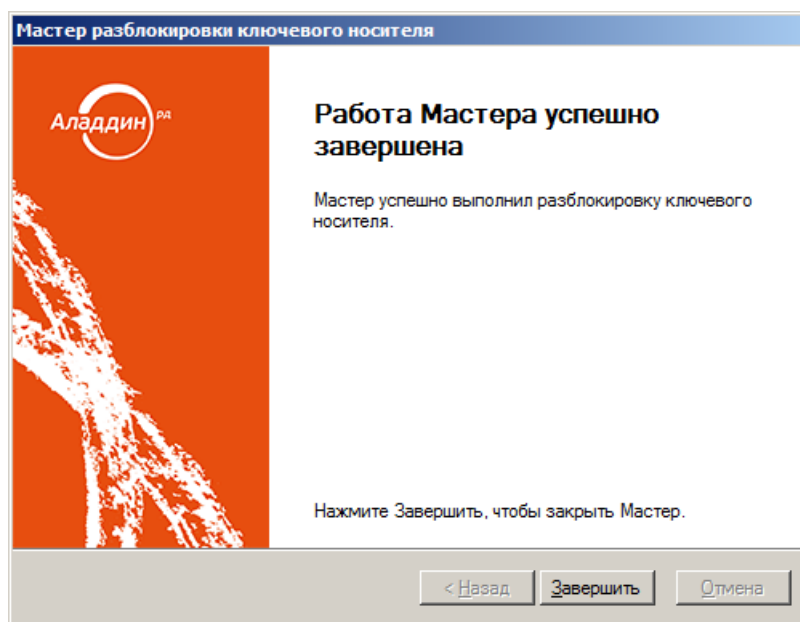


Рис. 30 – Окно завершения работы мастера разблокировки

12. Нажмите **Завершить**.

3.6.4.2 Разблокировка PIN-кодов в электронных ключах JaCarta-2 ГОСТ



Важно! Разблокировка PIN-кодов в электронном ключе JaCarta-2 ГОСТ требует наличия в нем установленного ПУК-кода. Факт установки ПУК-кода в электронном ключе можно проверить с помощью приложения *Единый клиент JaCarta* (производства компании Аладдин) версии 2.11 или более поздней, или обратившись к администратору.

В случае если PIN-код пользователя, PIN-код подписи (ЭП) или оба PIN-кода в электронном ключе JaCarta-2 ГОСТ оказались заблокированными, для их разблокирования выполните следующие действия.

1. В окне Клиента JMS (см. например, Рис. 31) на вкладке **Ключевые носители** у заблокированного электронного ключа нажмите ссылку:
 - **Разблокировать PIN-код ЭП ГОСТ 2** – для разблокировки PIN-кода подписи (ЭП);
 - **Разблокировать ГОСТ 2** – для разблокировки только PIN-кода пользователя или одновременно с ним – PIN-кода подписи (если он тоже заблокирован).

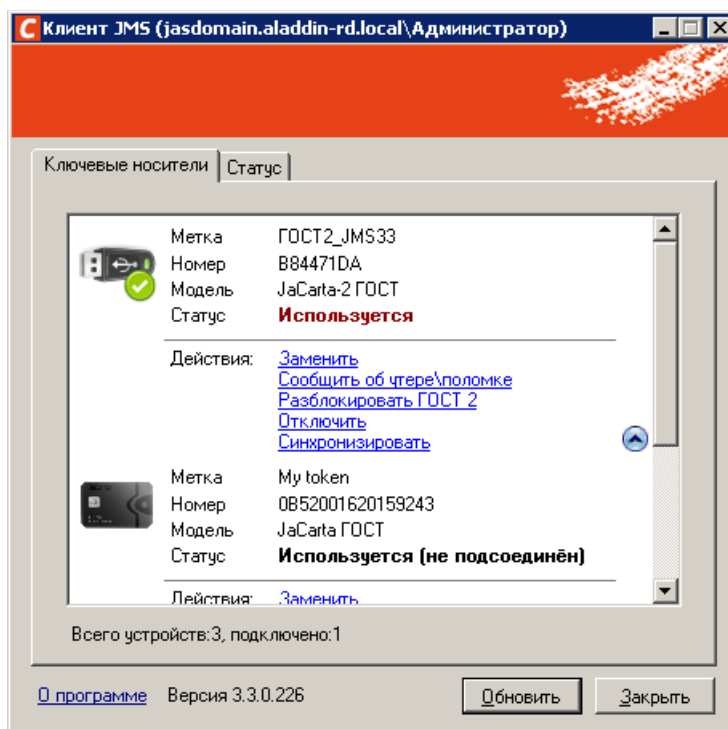


Рис. 31 – Вкладка **Ключевые носители** со ссылкой **Разблокировать ГОСТ 2**

2. Отобразится окно следующего вида:

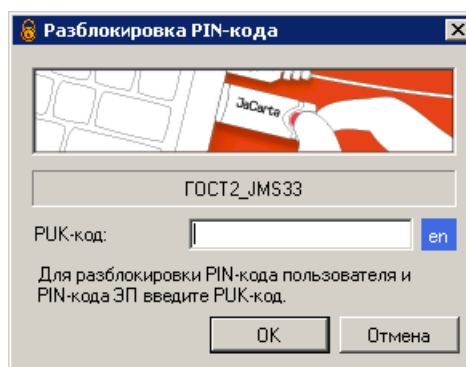




Рис. 32 – Пример окна разблокировки PIN-кодов в JaCarta-2 ГОСТ

3. Для разблокировки PIN-кодов введите **ПУК-код** и нажмите **ОК**.

 Разблокировку электронных ключей JaCarta-2 ГОСТ можно произвести также с помощью Единого Клиента JaCarta (подробнее см. в документе «Единый Клиент JaCarta. Руководство пользователя»).

3.6.5 Смена PIN-кода в приложении на электронном ключе

Чтобы сменить PIN-код в приложении на электронном ключе (в случае приложения ГОСТ 2: PIN-код пользователя и PIN-код подписи), выполните следующие действия.


1. Щёлкните правой кнопкой на значке  (Клиент JMS) в области уведомлений и выберите **Открыть**.
2. В отобразившемся окне перейдите на вкладку **Ключевые носители**.
3. В секции **Действия** под значком вашего электронного ключа щёлкните на ссылке:
 - **Сменить PIN-код для PKI** – в случае смены PIN-кода в приложении PKI;
 - **Сменить PIN-код для ГОСТ** – в случае смены PIN-кода в приложении ГОСТ;
 - **Сменить PIN-код ЭП для ГОСТ 2** – в случае смены PIN-кода подписи в приложения ГОСТ 2;
 - **Сменить PIN-код для ГОСТ 2** – в случае смены PIN-кода пользователя в приложении ГОСТ 2;
 - **Сменить PIN-код для RuToken ECP** – в случае смены PIN-кода в электронных ключах Рутокен;
4. В отобразившемся окне **Смена PIN-кода** введите текущий PIN-код, новый PIN-код и его подтверждение (в случае смены PIN-кода подписи – при выполнении операции для приложения ГОСТ 2 – требуется ввести также PIN-код пользователя).
5. Для завершения операции нажмите **ОК**.



Смену PIN-кодов в электронных ключах JaCarta и eToken также можно произвести с помощью Единого Клиента JaCarta, (подробнее см. в документе «Единый Клиент JaCarta. Руководство пользователя»).

3.6.6 Установка PIN-кода подписи в JaCarta-2 ГОСТ

В случае если электронном ключе JaCarta-2 ГОСТ еще не установлен PIN-код подписи (PIN-код ЭП), это можно сделать с помощью приложения Клиент JMS. Для этого выполните следующие действия.

1. Щёлкните правой кнопкой на значке  (Клиент JMS) в области уведомлений и выберите **Открыть**.
2. В отобразившемся окне перейдите на вкладку **Ключевые носители**.
3. В секции **Действия** под значком вашего электронного ключа (Рис. 33) щёлкните на ссылке **Установить PIN-код ЭП для ГОСТ 2**.

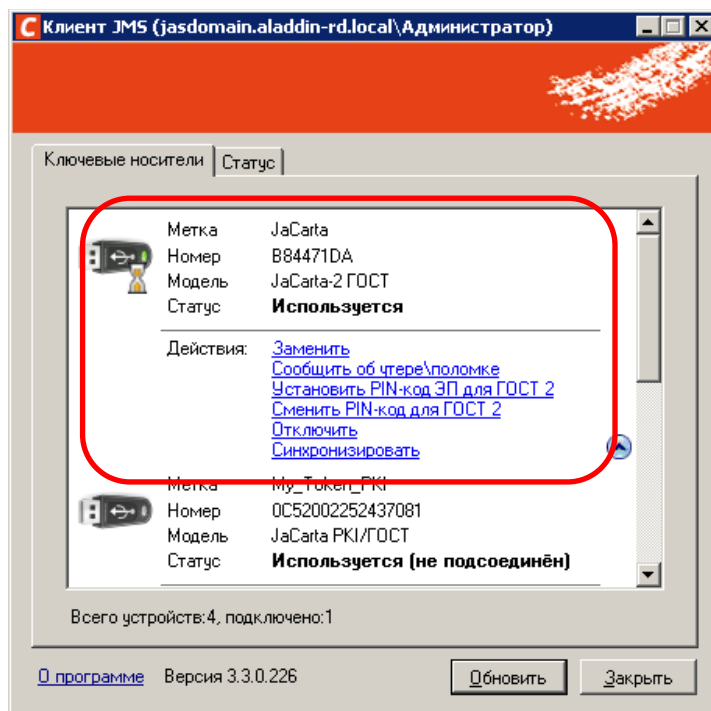


Рис. 33 – Пример окна разблокировки PIN-кодов в JaCarta-2 ГОСТ

4. В отобразившемся окне (Рис. 34) введите PIN-код пользователя, PIN-код подписи (**Новый PIN-код**) и его **Подтверждение**.

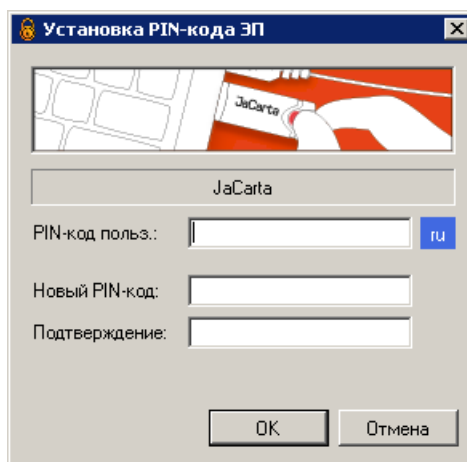




Рис. 34 – Пример окна разблокировки PIN-кодов в JaCarta-2 ГОСТ

5. Для завершения операции нажмите **ОК**.

 Установку PIN-кода подписи в электронных ключах JaCarta-2 ГОСТ также можно произвести с помощью Единого Клиента JaCarta (подробнее см. в документе «Единый Клиент JaCarta. Руководство пользователя»).

3.6.7 Действия в случае утери или поломки электронного ключа

Чтобы сообщить об утере или поломке электронного ключа, выполните следующие действия.

1. Щёлкните правой кнопкой на значке  (Клиент JMS) в области уведомлений и выберите **Открыть**.
2. В отобразившемся окне перейдите на вкладку **Ключевые носители**.
3. В центральной части окна щёлкните правой кнопкой на значке электронного ключа и в контекстном меню выберите **Сообщить об утере\поломке**.

Отобразится следующее окно.

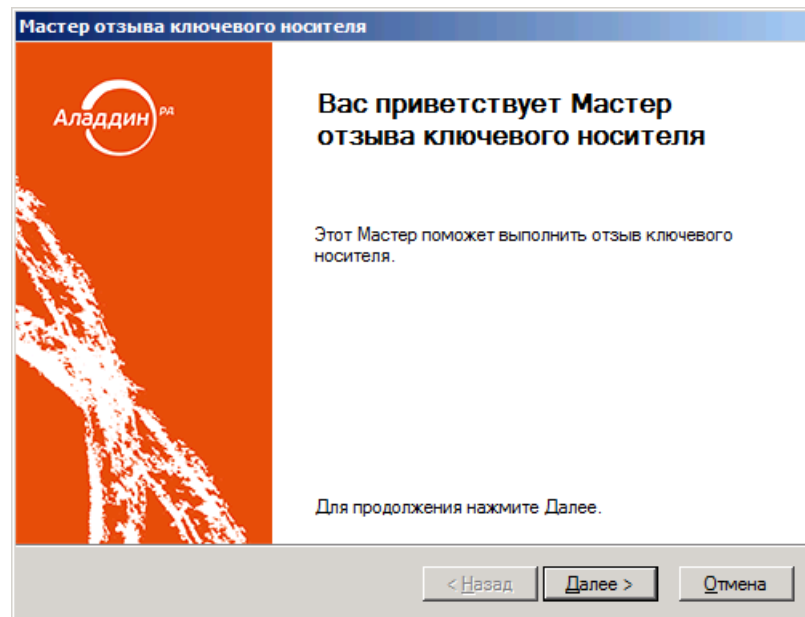


Рис. 35 - Окно приветствия мастера отзыва ключевого носителя

4. Нажмите **Далее**.
Отобразится следующее окно.

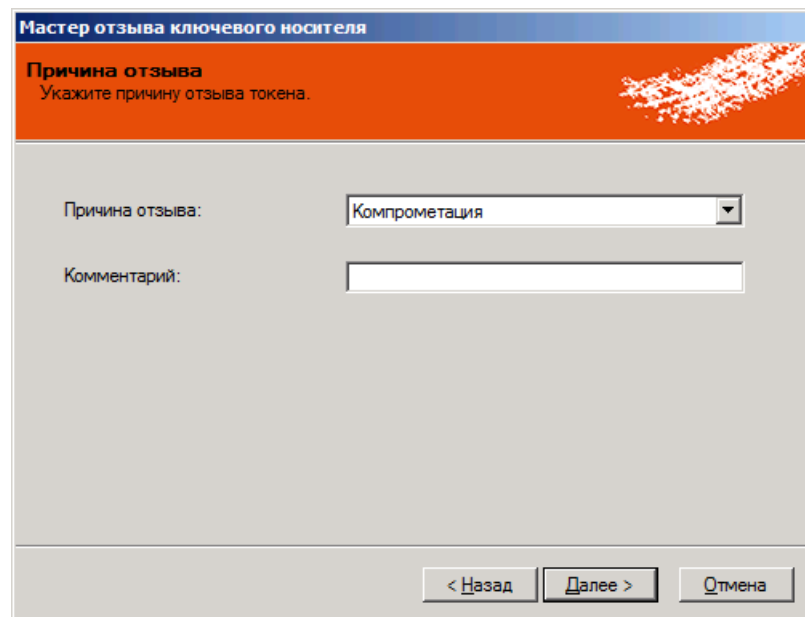


Рис. 36 – Укажите причину отзыва

5. В раскрывающемся списке **Причина отзыва** выберите причину, по которой отзывается электронный ключ, при необходимости укажите комментарий в соответствующем поле, после чего нажмите **Далее**.

Отобразится следующее окно.

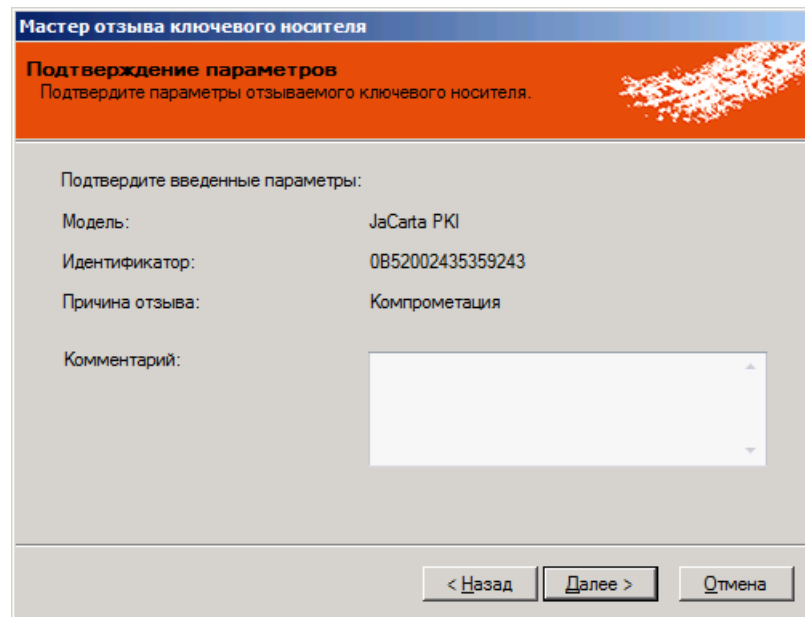


Рис. 37 – Окно подтверждения параметров отзываемого ключевого носителя

6. Нажмите **Далее**.
Отобразится следующее окно.

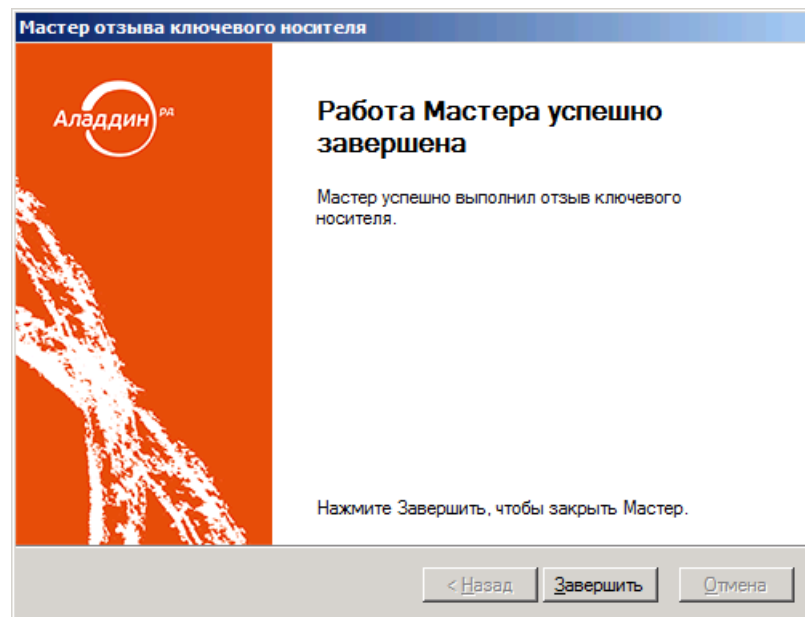


Рис. 38 – Окно завершения работы мастера отзыва ключевого носителя


7. Нажмите **Завершить**.
- 3.6.8 Замена электронного ключа

В случае необходимости замены электронного ключа и при условии, что новый ключ находится у вас на руках, вы можете самостоятельно выполнить процедуру замены.



Для выполнения этой процедуры вы должны иметь полномочия на самостоятельный выпуск электронных ключей. В случае отсутствия таковых для замены электронного ключа обратитесь к администратору.

1. Щёлкните правой кнопкой на значке **C** (Клиент JMS) в области уведомлений и выберите **Открыть**.
2. В отобразившемся окне перейдите на вкладку **Ключевые носители**.
3. В центральной части окна щёлкните на ссылке **Заменить** под значком электронного ключа, который вы хотите заменить.

 Значок электронного ключа будет отображаться даже в том случае, если электронный ключ не подсоединён к компьютеру.

Отобразится следующее окно.

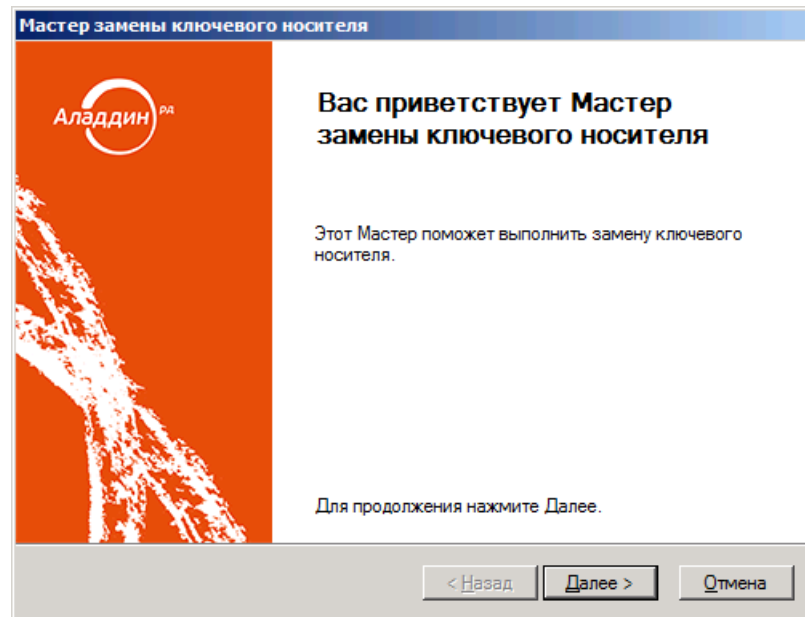


Рис. 39 – Окно приветствия мастера замены ключевого носителя

4. Нажмите **Далее**.
Отобразится следующее окно.

Рис. 40 – Укажите причину замены электронного ключа

5. В раскрывающемся списке **Причина замены** укажите причину, по которой ключ необходимо заменить, при необходимости укажите комментарий в соответствующем поле, после чего нажмите **Далее**.
Отобразится следующее окно.

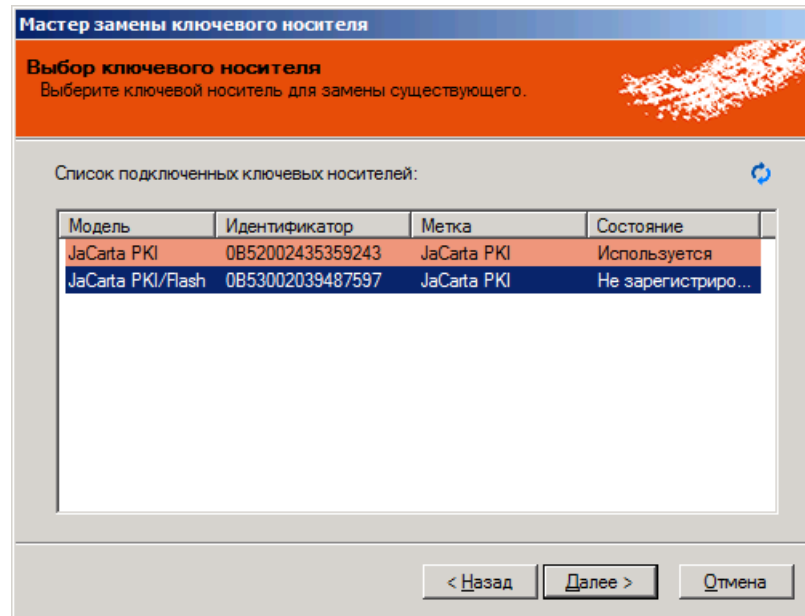


Рис. 41 – Окно выбора нового электронного ключа

6. Выберите электронный ключ, который выступит заменой старому и нажмите **Далее**.



Новый электронный ключ должен быть подсоединён к компьютеру.

Отобразится следующее окно.

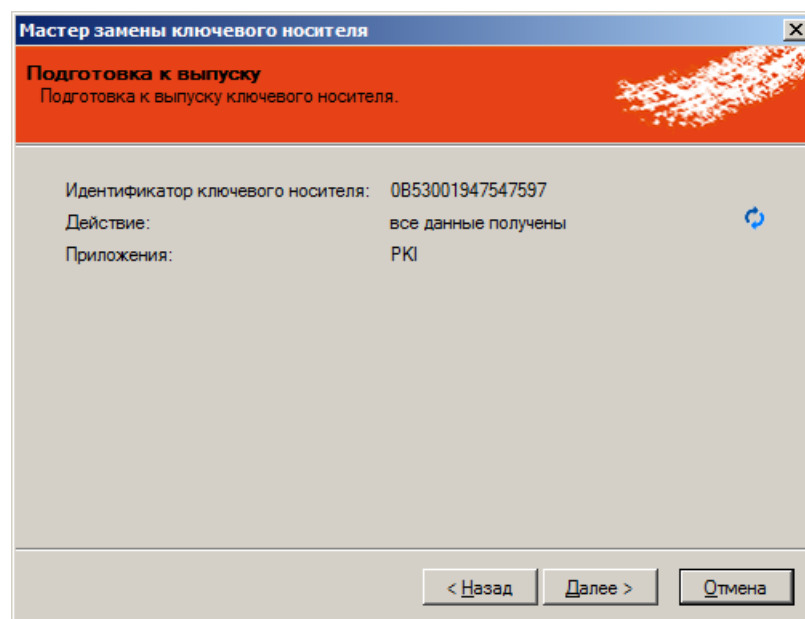


Рис. 42 – Подготовка к выпуску электронного ключа

Отобразится следующее окно.

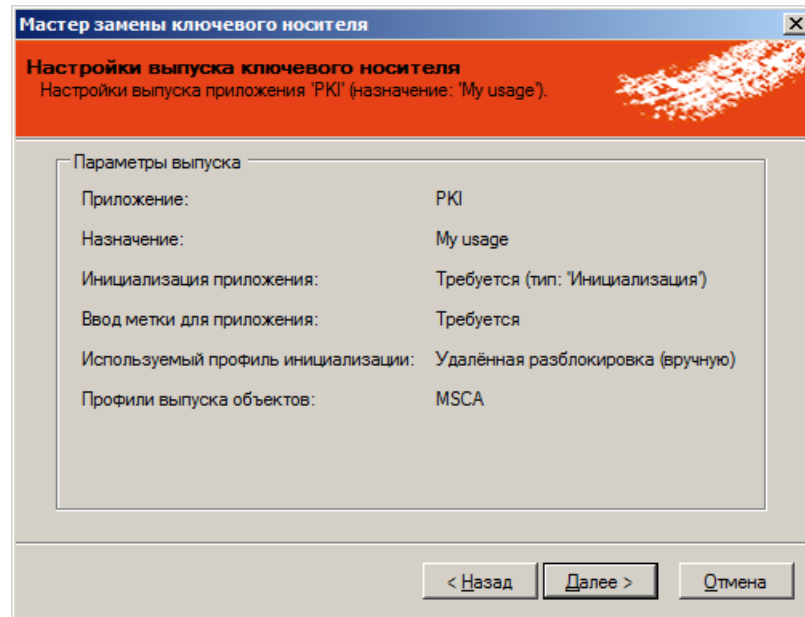


Рис. 43 – Окно подготовки к выпуску ключевого носителя

7. Нажмите **Далее**.
Отобразится следующее окно.

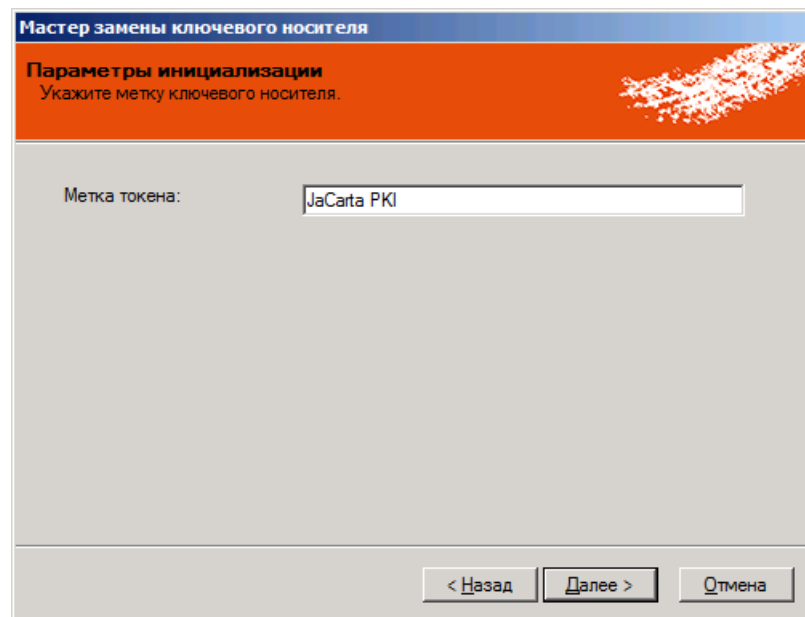


Рис. 44 – Окно задания метки ключевого носителя

8. Укажите метку ключевого носителя, после чего нажмите **Далее**.

Отобразится следующее окно.

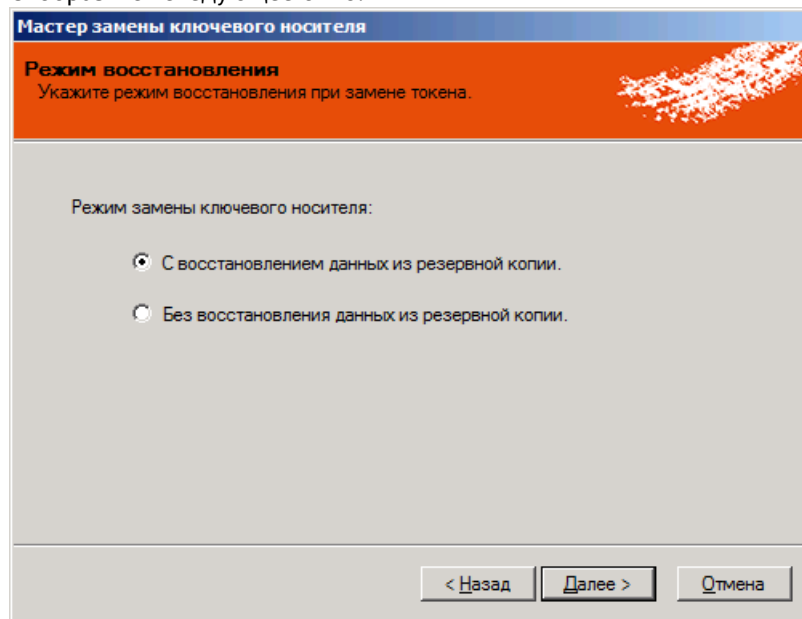



Рис. 45 – Режим восстановления при замене электронного ключа

9. Выберите нужный режим замены электронного ключа.

 Если в настройках JMS вам запрещён выпуск электронного ключа с восстановлением данных, выпуск завершится с ошибкой. В данной ситуации следует обратиться к вашему администратору.

10. Нажмите **Далее**.
Отобразится следующее окно.

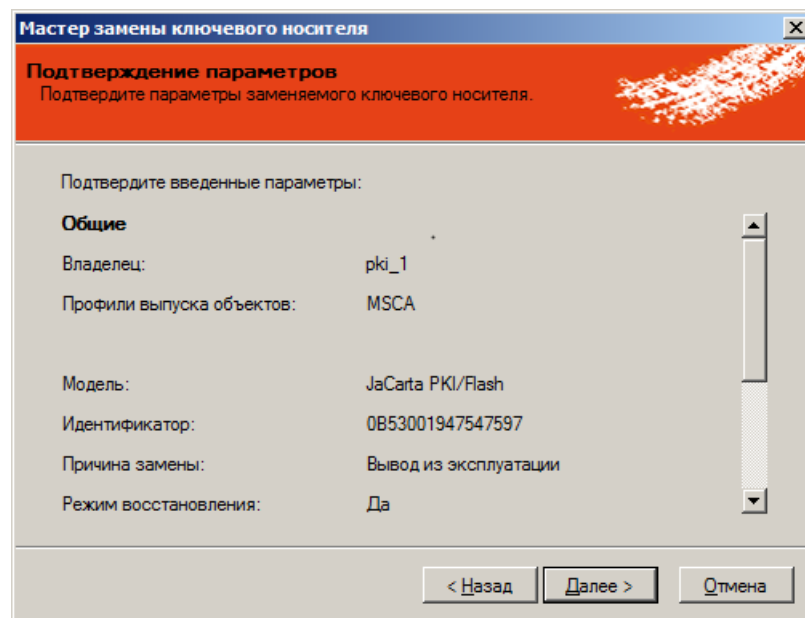


Рис. 46 – Окно подтверждения параметров заменяемого ключевого носителя

11. Нажмите **Далее**.

Отобразится следующее окно.

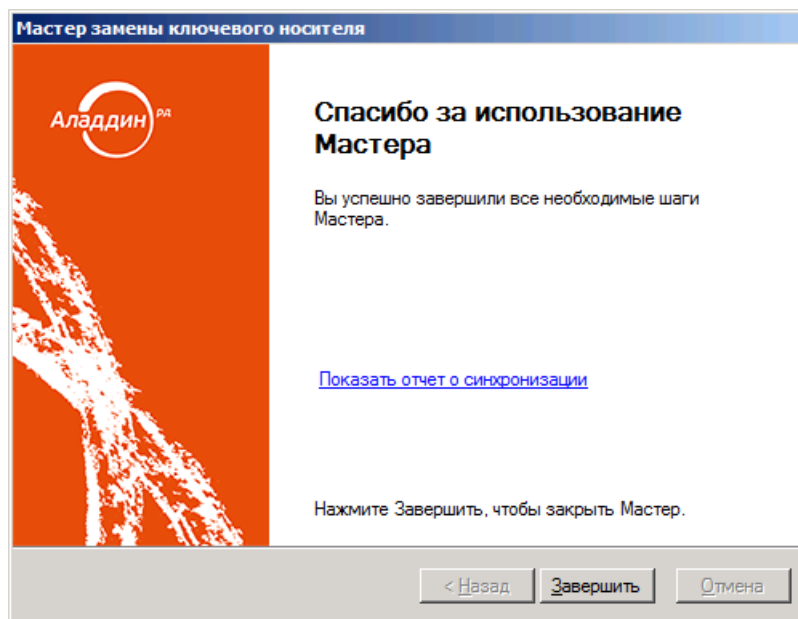



Рис. 47 – Окно завершения работы мастера замены ключевого носителя


12. Нажмите **Завершить** для завершения процедуры.

3.7 Операции с ридерами смарт-карт

Доступность тех или иных операций с ридерами смарт-карт зависит от настроек, установленных администратором JMS. В случае возникновения вопросов относительно доступности для пользователя тех или иных действий обратитесь к администратору.


 Для выполнения операций с карт-ридерами необходимо открыть сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS» на стр. 13).


3.7.1 Назначение ридера смарт-карт пользователю

 Для выполнения этой процедуры вы должны иметь полномочия на самостоятельное назначение карт-ридера. В случае отсутствия таковых для выпуска электронного ключа обратитесь к администратору.

Чтобы самостоятельно назначить карт-ридер на свое имя, выполните следующие действия.

1. Подключите карт-ридер, который вы хотите назначить на свое имя, к компьютеру.

 В JMS может быть настроено автоматическое назначение карт-ридера пользователю, открывшему сеанс подключения к JMS. В этом случае шаги 3-4 настоящей процедуры можно пропустить. Карт-ридер сразу после подключения будет иметь статус **Назначен** (см. Рис. 50).

2. Щёлкните правой кнопкой на значке  (Клиент JMS) в области уведомлений и выберите **Открыть**.
3. В окне **Клиент JMS** перейдите на вкладку **Ключевые носители**.

Окно примет следующий вид.

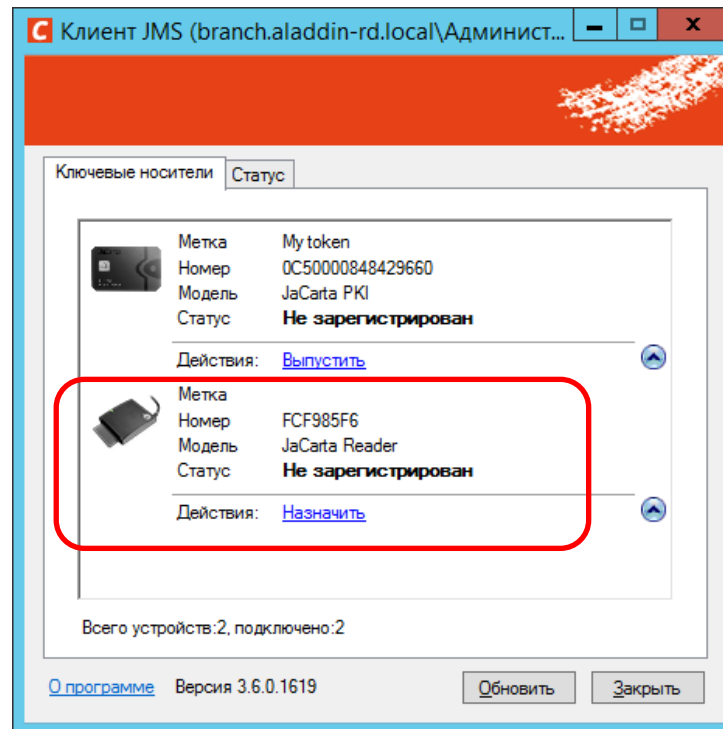


Рис. 48 – Выбор карт-ридера пользователем для назначения пользователю

4. В центральной части окна нажмите **Назначить**, расположенной ниже значка карт-ридера, который вы хотите назначить на свое имя. Отобразится следующее окно.

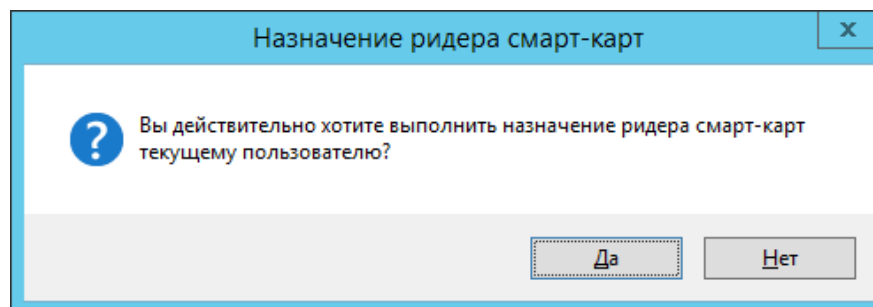


Рис. 49 – Окно подтверждения действия пользователя

5. Нажмите **Да**.

В результате операции назначения карт-ридер будет иметь статус **Назначен** (Рис. 50).

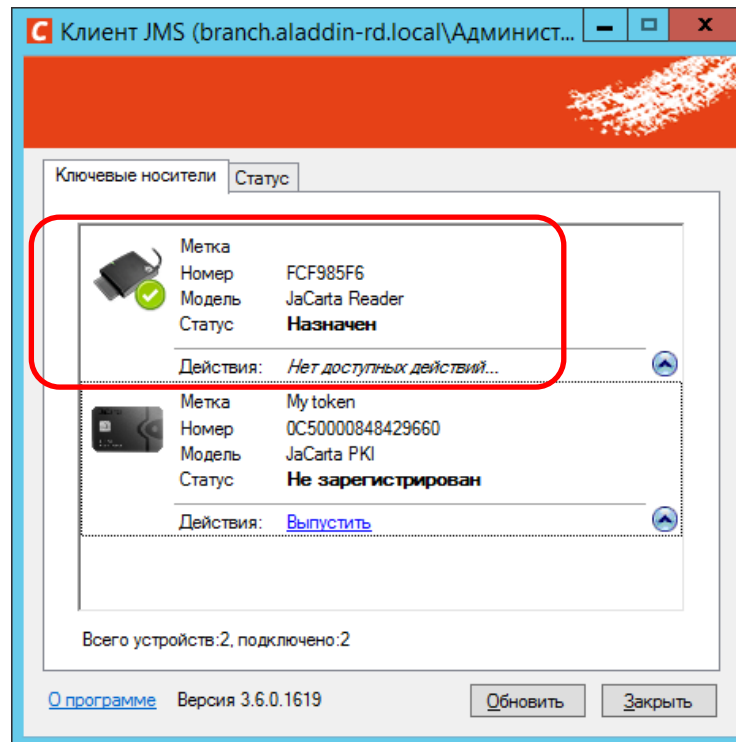


Рис. 50 – Отображение статуса назначенного карт-ридера

Примечание. После назначения карт-ридера пользователю данный ридер не может быть назначен другому пользователем без разрешения администратора JMS.

3.8 Биометрическая аутентификация

Если ваш электронный ключ поддерживает биометрическую аутентификацию, то для подтверждения доступа к защищенным ресурсам вы должны прикладывать палец к сканеру

отпечатков. Всякий раз в случае необходимости аутентифицироваться на экране будет отображаться следующее окно.

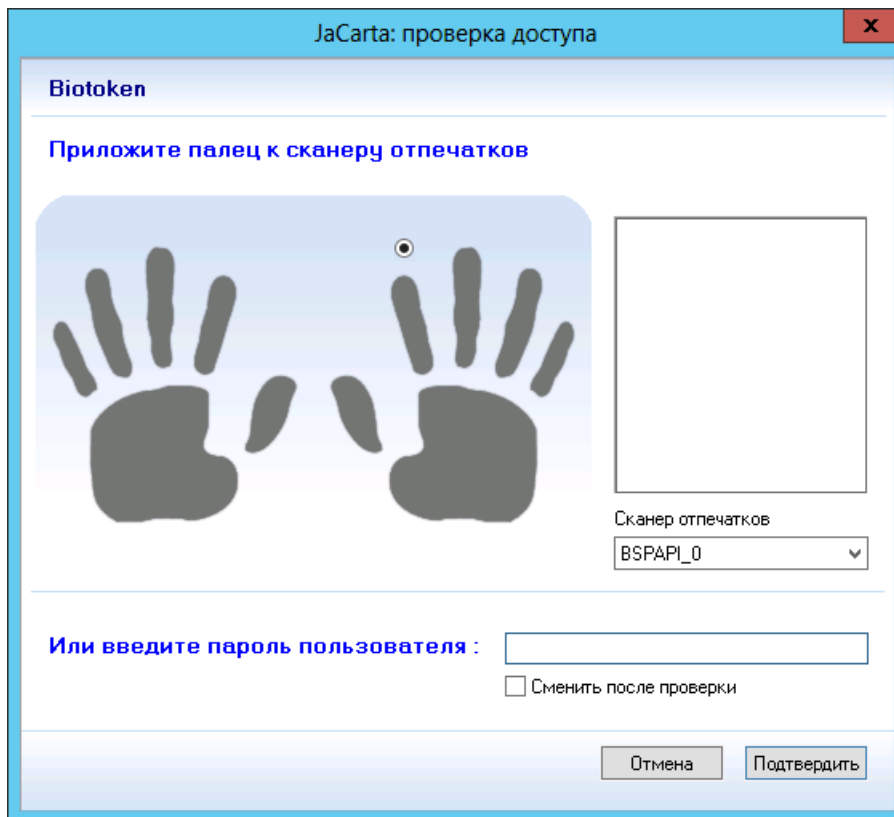



Рис. 51 – Биометрическая аутентификация

1. На схематическом изображении ладоней выберите палец, который хотите приложить к сканеру отпечатков.

 Отпечаток этого пальца должен уже быть заранее сохранён в памяти электронного ключа во время выпуска этого электронного ключа. Если у вас на данном этапе возникли затруднения, обратитесь к вашему администратору.

2. Если к компьютеру подсоединено несколько сканеров отпечатков, выберите тот, который будете использовать, в раскрывающемся списке **Сканер отпечатков**.
3. В зависимости от настроек, с которыми был выпущен ваш электронный ключ, выполните следующие действия.
 - Если для аутентификации требуется только сканирование отпечатка, – приложите палец к сканеру отпечатков.
 - Если для аутентификации требуется либо сканирование отпечатка, либо ввод PIN-кода пользователя (достаточно выполнения одного из двух условий), – введите PIN-код пользователя в поле **Или введите пароль пользователя**, после чего нажмите **Подтвердить**, или приложите палец к сканеру отпечатков.
 - Если для аутентификации требуется как сканирование отпечатка, так и ввод PIN-кода пользователя (оба условия должны быть выполнены), – сначала введите PIN-код пользователя в поле **И введите пароль пользователя**, затем приложите палец к сканеру отпечатков.

4. Автоматическое обновление клиента JMS

Система позволяет обновлять клиент JMS (ПО JMS Client) в автоматическом режиме. При обнаружении доступной версии обновления клиентская программа отобразит окно **Обновление клиента JMS** (Рис. 52).

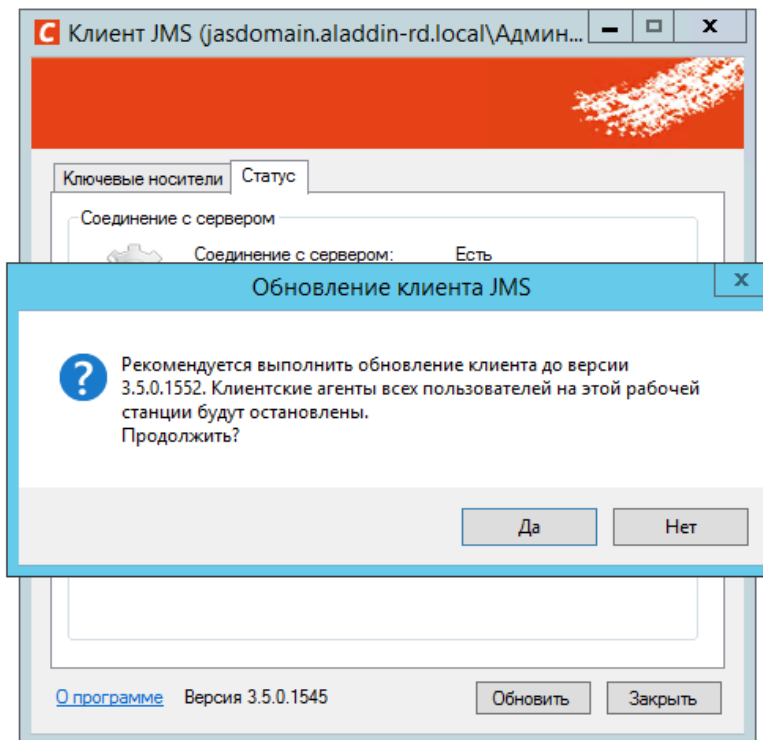


Рис. 52 – Окно приглашения к обновлению клиента JMS

Чтобы начать обновление нажмите **Да**.

Отобразится окно выполнения процесса установки обновленной версии JMS-клиента, по окончании которого отобразится окно с информацией о завершении установки (Рис. 53).

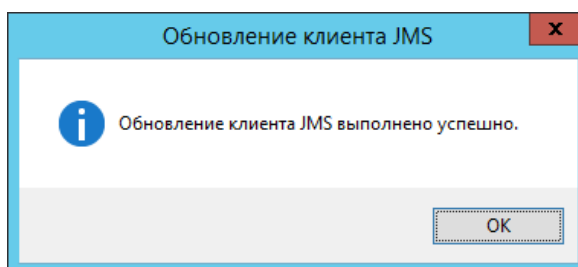


Рис. 53 – Оповещение об успешном окончании обновления

В случае отказа от обновления, предупреждение о необходимости обновить JMS-клиент будет появляться с заданной администратором периодичностью (стандартная настройка – раз в час).

Пользователю предоставляется также возможность самостоятельно проверить наличие обновления и выполнить его, выбрав пункт **Проверить обновления** или **Обновление до версии x.x.x.xxxx** в меню быстрого запуска JMS Client (Рис. 53).

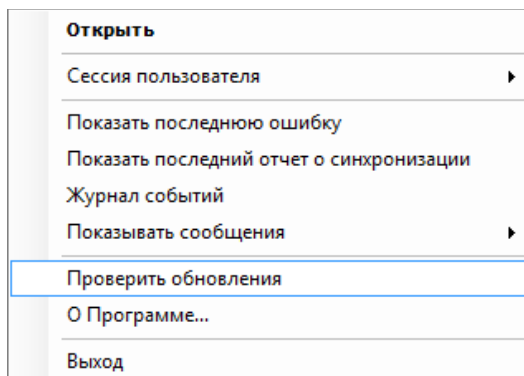


Рис. 54 – Обновление JMS-клиента из меню быстрого запуска JMS Client

5. Выпуск сертификата КриптоПро в хранилище пользователя на рабочей станции

Во время автоматического выпуска посредством Клиента JMS ключа подписи, а также ключа проверки подписи и его сертификата (сертификата ключа проверки ЭП) в личное хранилище пользователя на рабочей станции у пользователя может быть запрошен PIN-код (пароль защиты данного ключа). Для выпуска такого сертификата пользователю следует ввести и запомнить введенный PIN-код для дальнейшего использования ключа электронной подписи.

6. Диагностика клиента JMS

Администратор может попросить вас выполнить диагностику JMS-клиента на вашем компьютере. Чтобы сделать это, выполните следующие действия.

1. В меню **Пуск** выберите **Все программы > JaCarta Management System > Диагностика JMS**. Отобразится следующее окно.

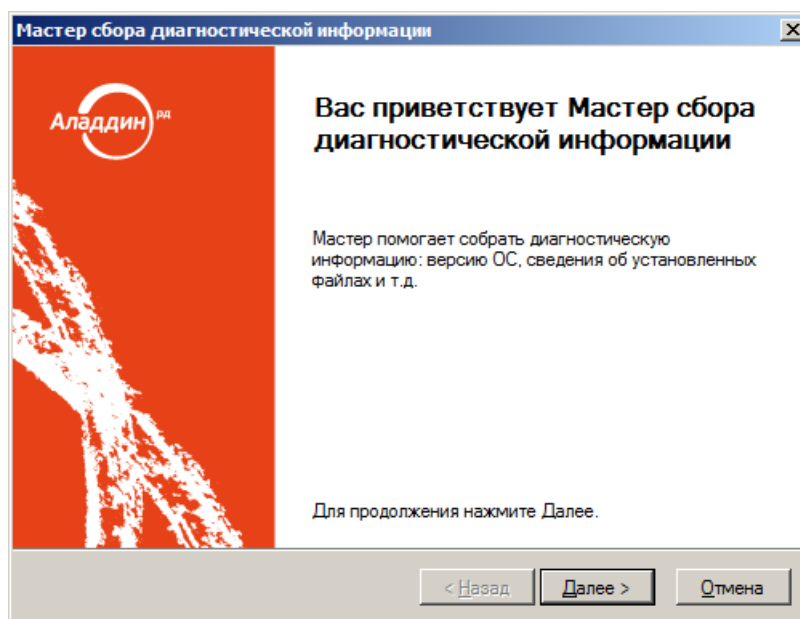


Рис. 55 – Окно приветствия мастера диагностики

2. Нажмите **Далее**.

Отобразится следующее окно.

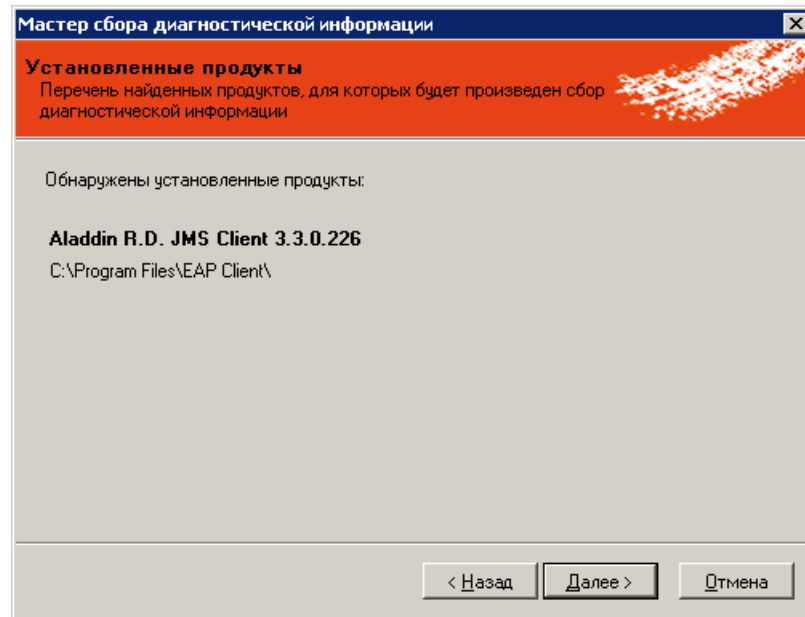


Рис. 56 – Результаты поиска установленных компонентов JMS

3. Нажмите **Далее**.
Отобразится следующее окно.

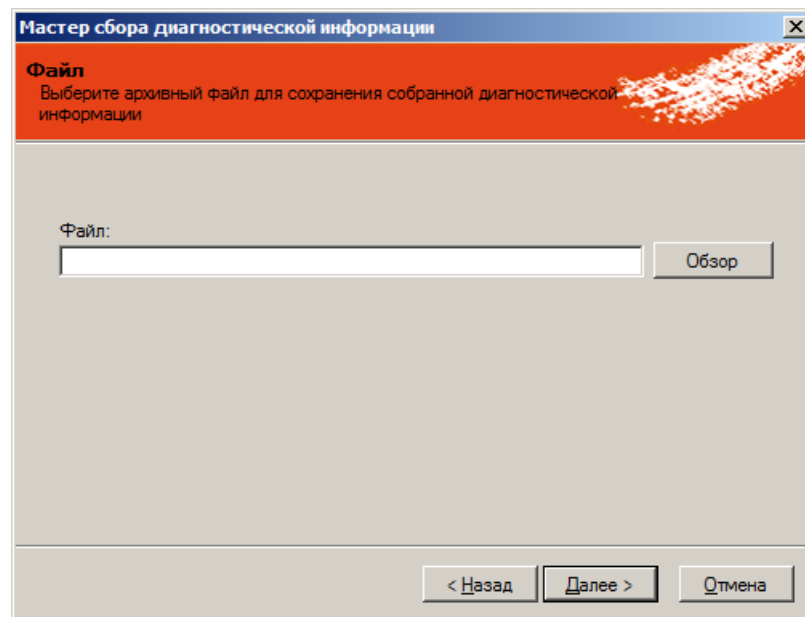
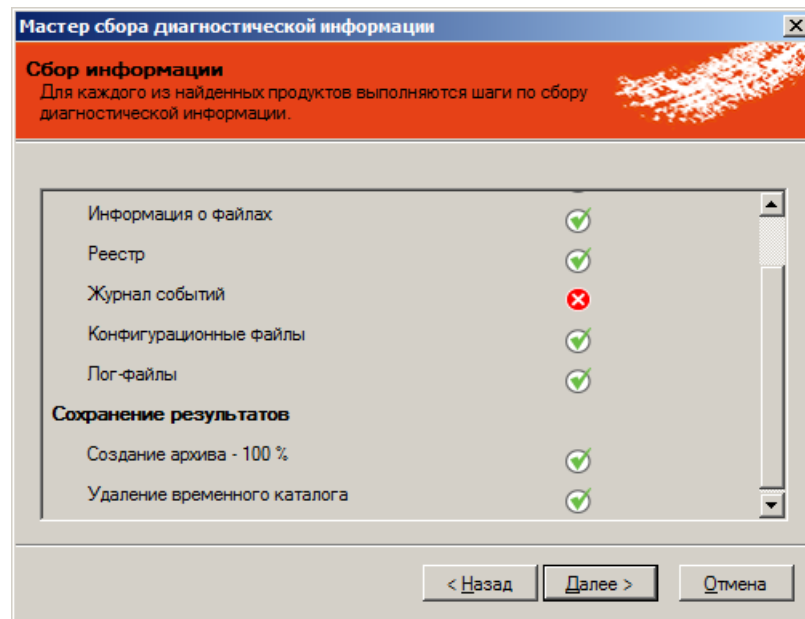


Рис. 57 – Выбор пути сохранения файла диагностики

4. Воспользуйтесь кнопкой **Обзор**, чтобы указать путь сохранения и имя файла с результатами диагностики.
Нажмите **Далее**.

Спустя некоторое время отобразится следующее окно.



5. Нажмите **Далее**.
Отобразится следующее окно.

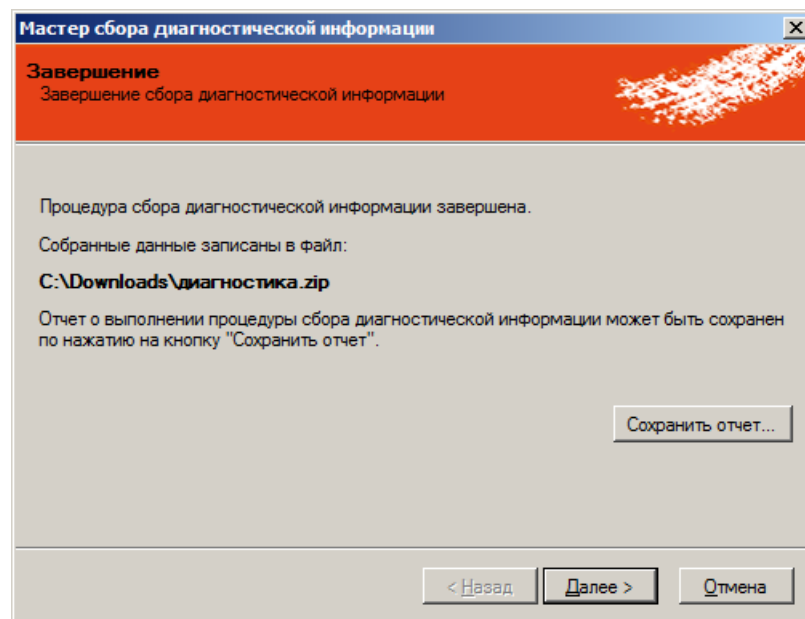


Рис. 58 – Сохранение отчёта о диагностике

6. При необходимости воспользуйтесь кнопкой **Сохранить отчёт**, чтобы сохранить журнал отчёта о процедуре диагностики, после чего в окне об успешном сохранении нажмите **ОК**.
Нажмите **Далее**.

Отобразится следующее окно.

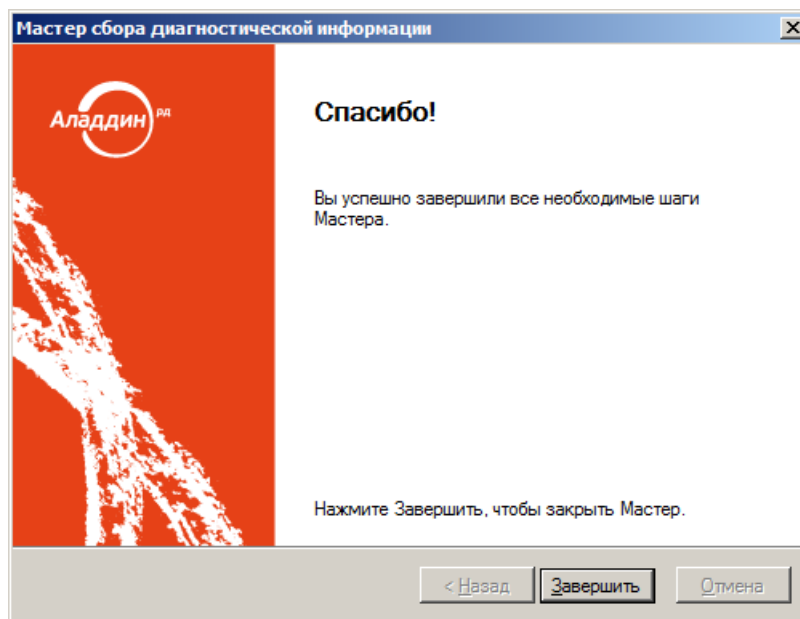



Рис. 59 – Окно завершения работы мастера диагностики


7. Нажмите **Завершить** для завершения процедуры.

7. Web-портал самообслуживания пользователей

JMS позволяет пользователю управлять своими электронными ключами с помощью web-браузера через порталы самообслуживания.

 **Примечание.** Портал самообслуживания представляет собой дополнительный (необязательный) компонент программного продукта JMS. О факте установки данного компонента следует узнать у администратора системы.

Для управления электронными ключами пользователь может подключаться к внутреннему web-порталу (из корпоративной сети) или к внешнему (из публичной сети Интернет).

 **Примечание.** Возможность подключения к внутреннему или к внешнему portalу определяется правами доступа, предоставленными пользователю администратором. Возможность подключения к внешнему portalу может также определяться самим пользователем.


7.1 Аутентификация на внутреннем портале самообслуживания

Для аутентификации на внутреннем портале самообслуживания в web-браузере откройте страницу по адресу следующего вида:

```
http://<JMS_FQDN>/JMS/private
```

где <JMS_FQDN> – полное доменное имя сервера JMS, например

```
jms31.jasdomain.aladdin-rd.local
```

 **Примечание.** Адрес внутреннего web-портала самообслуживания следует получить у администратора JMS.

В зависимости от настроек параметров аутентификации пользователя администратором, вход в личный кабинет может осуществляться:

- в один шаг (обычная или однофакторная аутентификация), см. «Обычная (одношаговая) аутентификация», с. 50;
- в два шага (двухфакторная аутентификация), см. «Двухфакторная (двухшаговая) аутентификация», с. 52.

7.1.1 Обычная (одношаговая) аутентификация

При одношаговой аутентификации после ввода http-адреса портала самообслуживания откроется страница следующего вида:

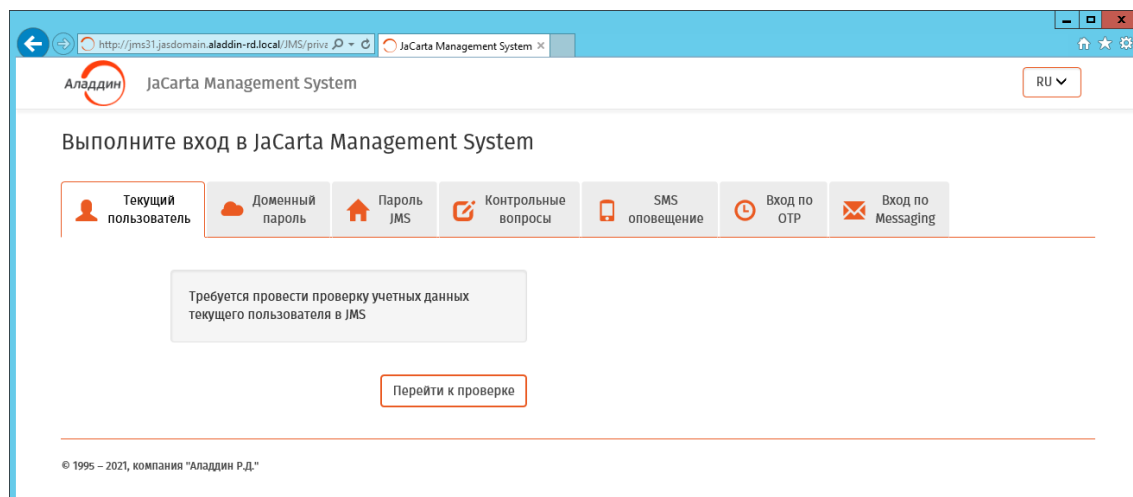


Рис. 60 – Страница аутентификации пользователя на внутреннем портале самообслуживания

Примечание. Число вкладок может варьироваться в зависимости от настроек администратора.


На странице необходимо выполнить аутентификацию одним из следующих способов:

- аутентификация с использованием проверки подлинности Windows (прозрачная аутентификация пользователя с использованием аутентификационных данных текущего сеанса работы с Windows, не требует ввода пароля);
- аутентификация по паролю службы Active Directory;
- аутентификация по паролю JMS;
- аутентификация посредством секретных вопросов;
- аутентификация посредством пароля, передаваемого по SMS;
- аутентификация посредством OTP-токена JMS;
- аутентификация посредством Messaging-токена JMS.

Чтобы выполнить аутентификацию выберите необходимую вкладку и выполните действия, руководствуясь Табл. 8.

Табл. 8 – Аутентификация пользователя на внутреннем портале самообслуживания

Название вкладки	Условия аутентификации	Действия по аутентификации
Текущий пользователь	Аутентификация с использованием проверки подлинности Windows. Пользователь, от имени которого открыт сеанс Windows или запущен web-браузер, должен быть	Для аутентификации нажмите Перейти к проверке

Название вкладки	Условия аутентификации	Действия по аутентификации
	зарегистрирован в JMS, при этом его доступ в JMS не должен быть заблокирован.	 Важно! Данный способ аутентификации недоступен при использовании web-браузера Opera.
Доменный пароль	Аутентификация по паролю службы Active Directory. Администратор должен предоставить пользователю пароль для Active Directory	Для аутентификации следует ввести Имя пользователя (в формате <Имя_домена>\<Имя_пользователя>) и Пароль службы Active Directory, после чего нажать Вход в систему
Пароль JMS	Аутентификация по паролю JMS. Администратор должен предоставить пользователю пароль доступа в JMS	Для аутентификации следует ввести Имя пользователя (в формате <имя домена или «ресурсной системы»>\<Имя_пользователя>) и Пароль JMS, после чего нажать Вход в систему
Контрольные вопросы	Для аутентификации по контрольным вопросам пользователь должен предварительно их определить (установить) в своем личном кабинете портала самообслуживания, что требует предварительной аутентификации в ЛК любым другим способом	Для аутентификации выполните следующие действия. 1. Введите Имя пользователя (в формате <полное_DNS-Имя_домена>\<Имя_пользователя>), например: jms.aladdin.ru\i_ivanov) и нажмите Перейти к вопросам 2. Заполните все поля ответов на контрольные вопросы и нажмите Отправить Аутентификация будет выполнена успешно, если все ответы будут верны
SMS-оповещение	Аутентификация путем одноразового пароля, высылаемого на телефон пользователя по SMS	см. раздел «Вход по SMS-оповещению», с. 59
Вход по OTP	Аутентификация с помощью так называемого OTP-токена (аппаратного устройства или мобильного приложения), который выдается пользователю администратором	см. раздел «Вход по OTP-паролю», с. 60
Вход по Messaging	Аутентификация с помощью виртуального OTP-токена пользователя, значение которого передается пользователю на мобильный телефон по SMS	см. раздел «Вход по Messaging-паролю», с. 62



Примечание. Время сеанса пользователя ограничивается. В случае бездействия пользователя в личном кабинете сеанс автоматически прекращается через установленное администратором время (на внутреннем портале это время обычно составляет 15 минут).

7.1.2 Двухфакторная (двухшаговая) аутентификация

При двухфакторной аутентификации пользователю предлагается сначала страница проверки первого фактора аутентификации (Рис. 61, может содержать одну или несколько вкладок для выбора типа аутентификации).

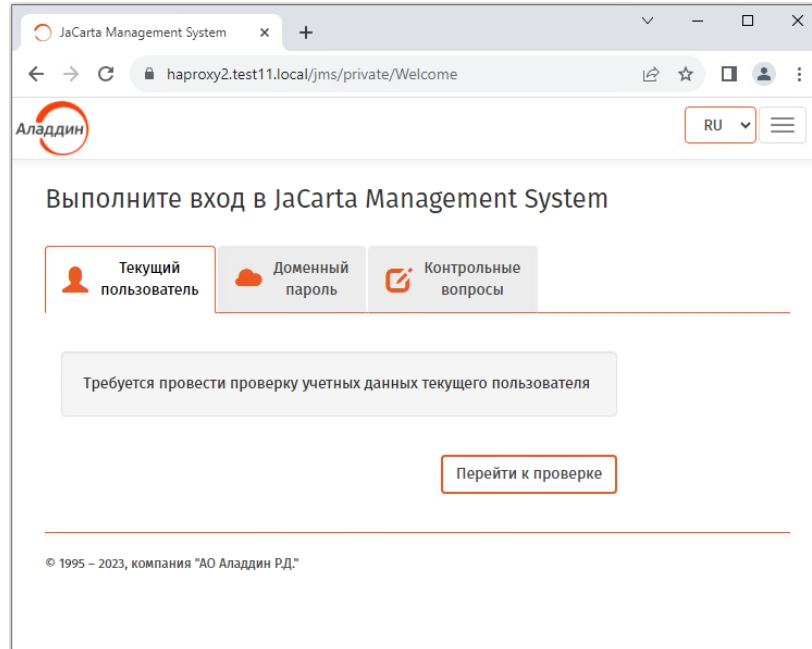


Рис. 61 – Пример страницы для первого шага двухфакторной аутентификации пользователя на внутреннем портале самообслуживания

Выполните аутентификацию на выбранной вкладке, руководствуясь Табл. 8, с. 50.

После успешной проверки первого шага отображается окно для второго шага (также могут быть предложены несколько вкладок на выбор пользователя).

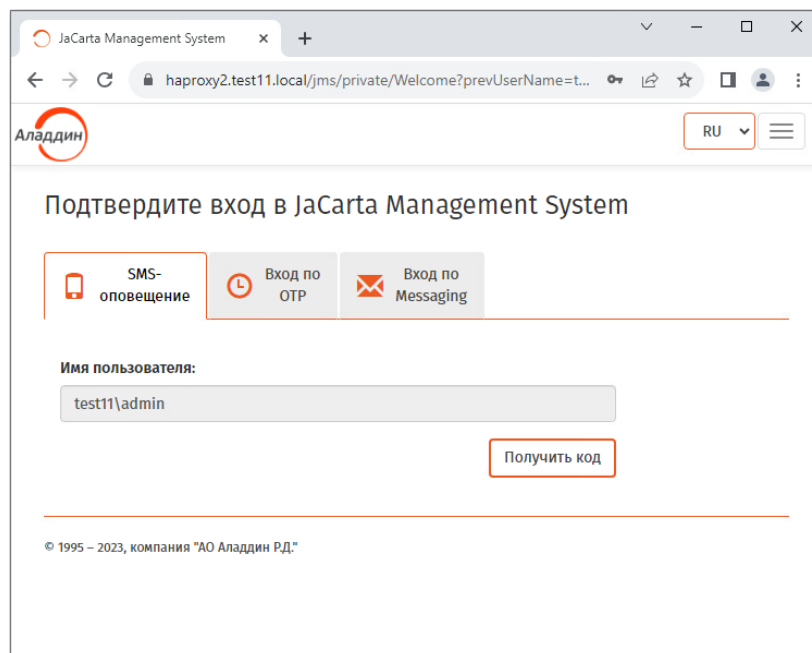


Рис. 62 – Пример страницы для второго шага двухфакторной аутентификации пользователя на внутреннем портале самообслуживания

Выполните аутентификацию на выбранной вкладке, руководствуясь Табл. 8.

После успешной проверки на втором шаге будет осуществлён вход в личный кабинет.

7.2 Первый вход в личный кабинет

При первом входе в личный кабинет пользователю может быть предложено несколько предварительных действий, описанных ниже, для обеспечения дальнейшей корректной работы web-клиента JMS, таких как:

- «Самостоятельная установка JWA», ниже;
- «Начальная настройка контрольных вопросов для аутентификации в ЛК», с. 58.

7.2.1 Самостоятельная установка JWA

Если пользователь осуществил вход в личный кабинет впервые, то в зависимости от предварительных настроек компьютера администратором, пользователю может понадобиться установить программный компонент Aladdin JMS Web Agent (JWA).

Если данный компонент не установлен (или не запущен), то отобразится страница следующего вида.

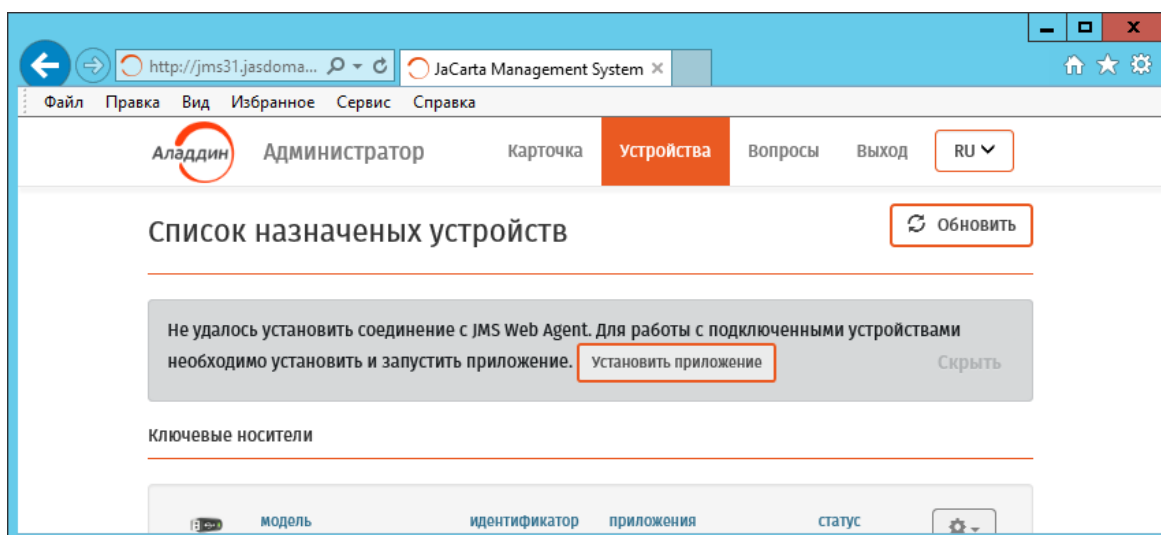


Рис. 63 – Уведомление о необходимости установки приложения JMS Web Agent (JWA)

Для установки JWA выполните следующие действия.

Примечание. Описание процесса установки приведено на примере браузера Internet Explorer. При использовании других типов браузеров порядок загрузки и запуска инсталляционного файла JWA на выполнение может незначительно отличаться.

1. Нажмите на кнопку **Установить приложение**.

Отобразится предупреждение web-браузера следующего вида.

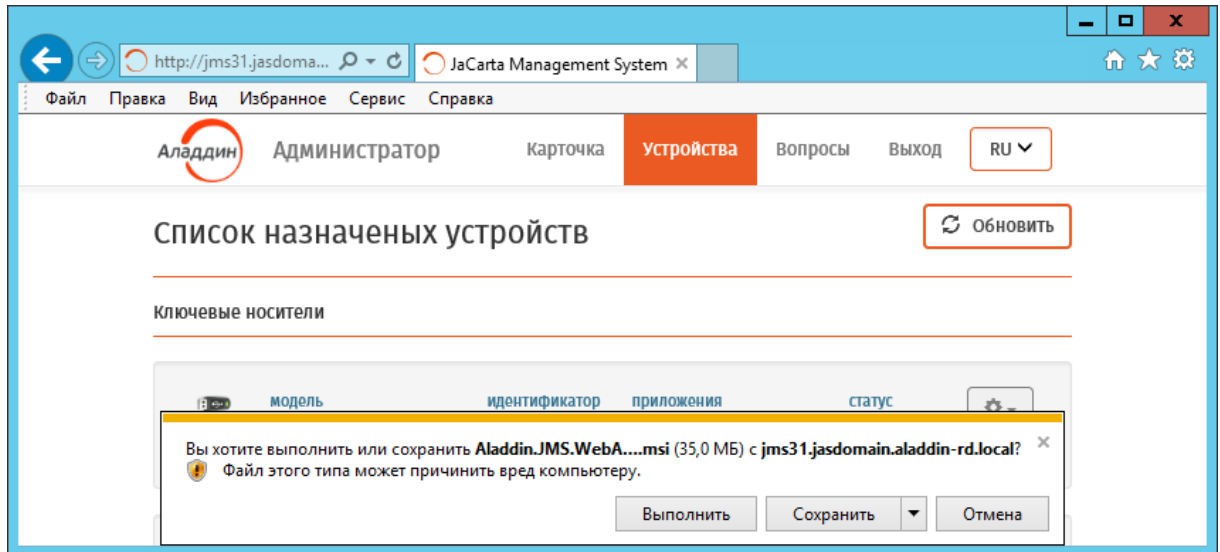


Рис. 64 – Запрос браузера на установку компонента JWA

2. Нажмите **Выполнить**.
Отобразится начальное окно мастера установки JWA.

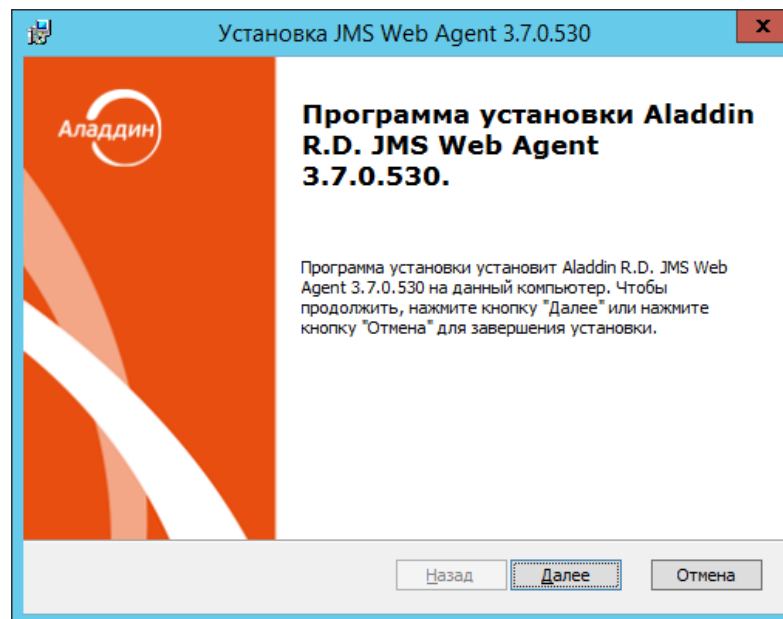


Рис. 65 – Стартовое окно мастера установки JWA

3. Нажмите **Далее**.

Отобразится следующее окно.

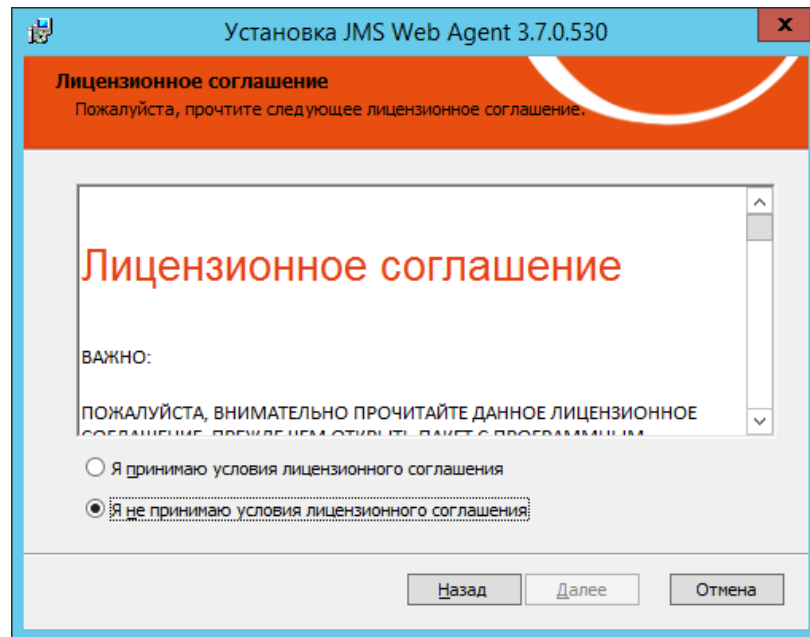


Рис. 66 – Окно лицензионного соглашения

4. Выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**. Отобразится следующее окно.

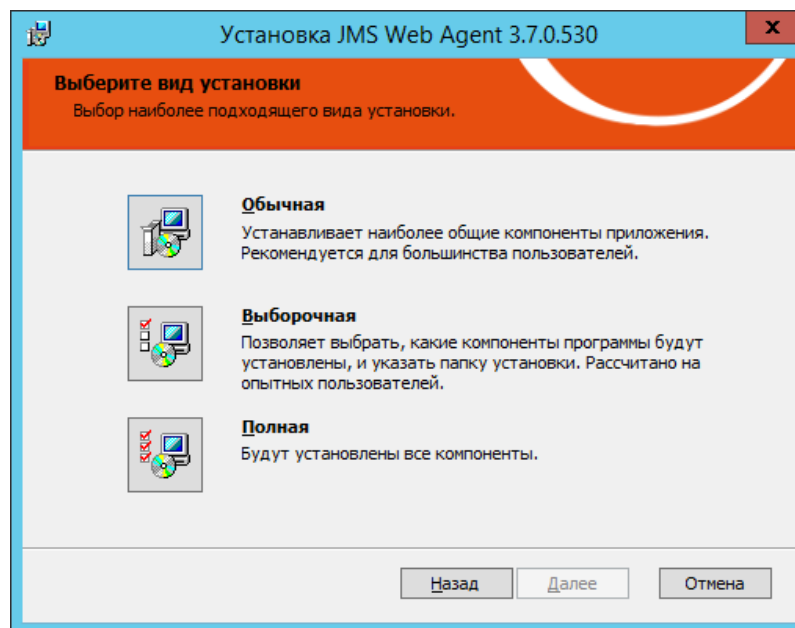


Рис. 67 – Окно выбора варианта установки.

5. Нажмите **Полная**.



Чтобы задать путь установки, отличный от пути по умолчанию, выберите вариант **Выборочная**, внесите необходимые изменения, после чего нажмите **Далее**.

Отобразится следующее окно.

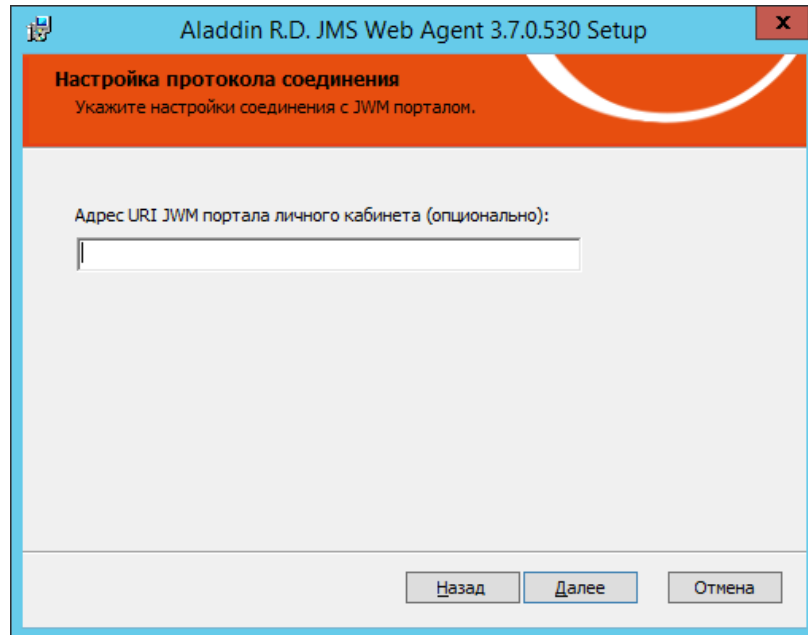


Рис. 68 – Окно ввода адреса JWM-портала

6. В поле **Адрес URI JWM портала личного кабинета (опционально)** введите адрес, указанный системным администратором, в формате `<протокол>://<FQDN-адрес web-сервера JWM>` где
 - `<протокол>` – один из протоколов `http` или `https`;
 - `<FQDN-адрес web-сервера JWM>` – полный доменный адрес web-сервера, на котором функционирует портал JWAНапример: `http://jms31.jasdomain.aladdin-rd.local`
7. **После** ввода значения поля нажмите **Далее**.

Отобразится следующее окно.

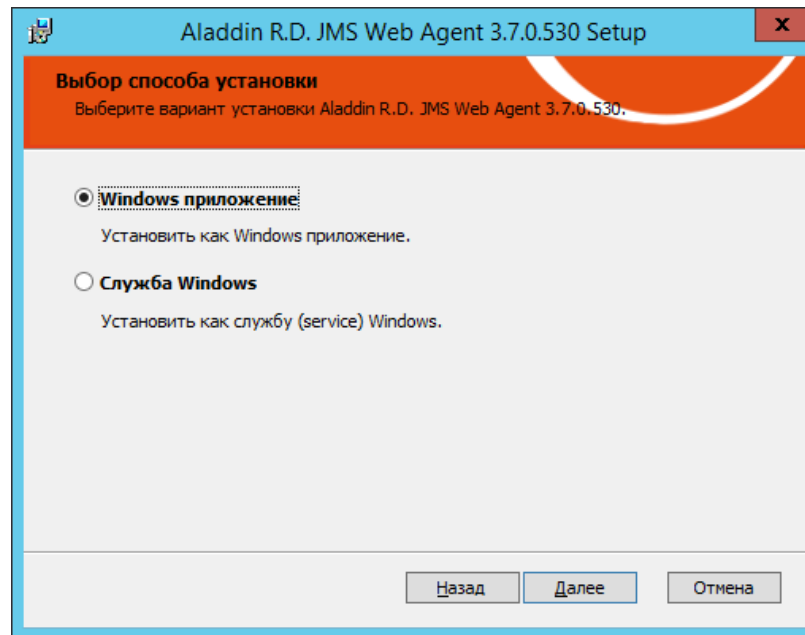


Рис. 69 – Окно выбора способа установки.

8. Выберите **Служба Windows** и нажмите **Далее**.
Отобразится следующее окно.

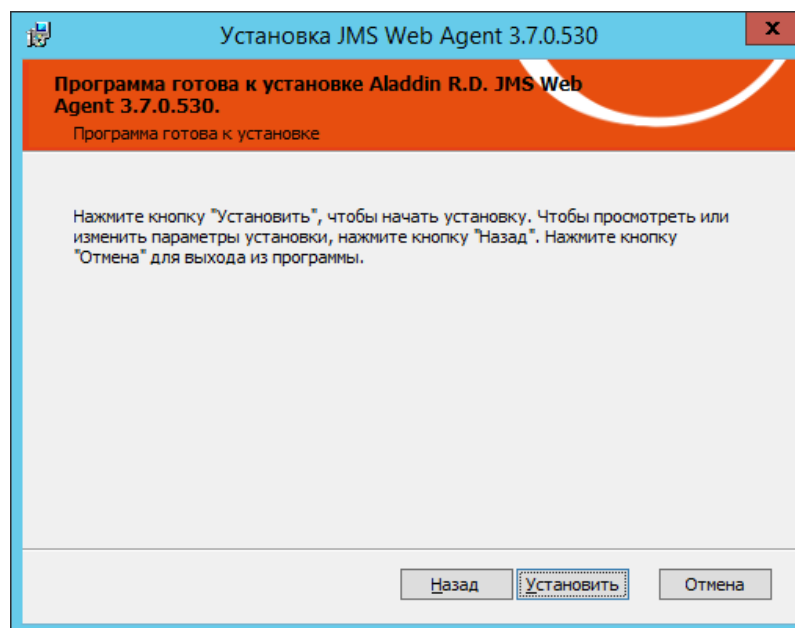


Рис. 70 – Окно готовности к установке

9. Нажмите **Установить**.

По завершении установки отобразится следующее окно.

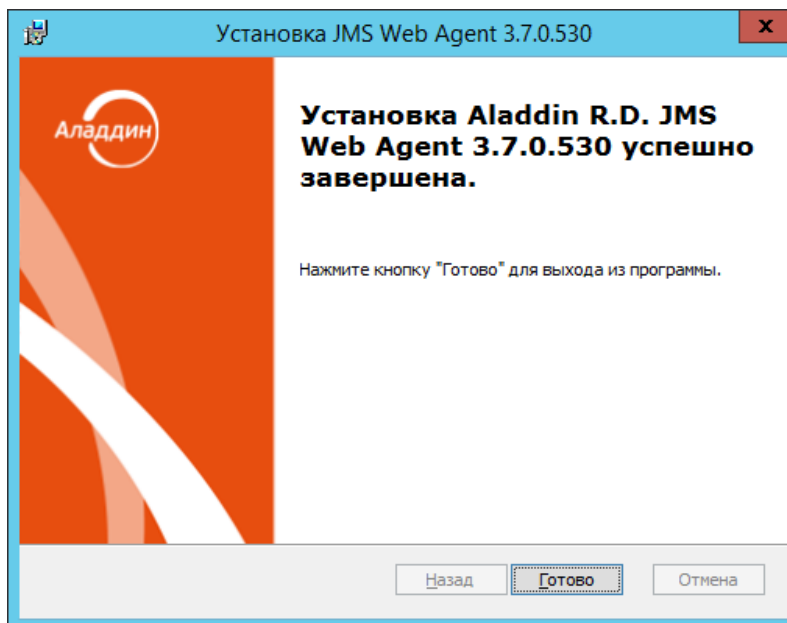



Рис. 71 – Окно завершения установки

10. Нажмите **Готово** для завершения процедуры.
Меню управления JWA будет отображаться в области уведомлений в виде значка .

7.2.2 Начальная настройка контрольных вопросов для аутентификации в ЛК

При первом входе в личный кабинет пользователю может быть рекомендовано определить (установить) требуемое число контрольных вопросов (Рис. 72). Подробнее см. раздел «Управление контрольными вопросами из личного кабинета», с. 78.

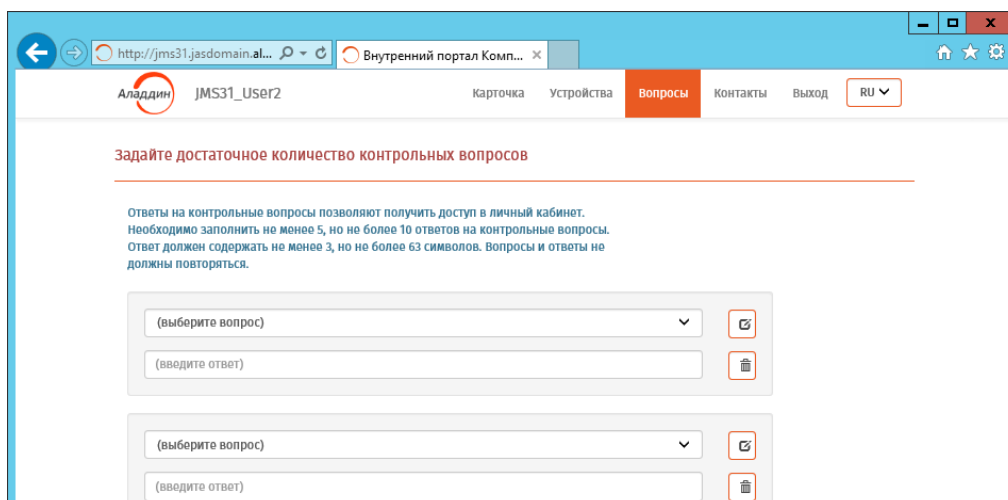


Рис. 72 – Страница определения (установки) контрольных вопросов для последующей аутентификации

7.3 Вход по SMS-оповещению



Важно! Аутентификация в личном кабинете с помощью SMS-оповещения в текущей версии продукта недоступна в браузере Internet Explorer. Для аутентификации данного типа используйте другие типы Web-браузеров.

Для входа по SMS-оповещению выполните следующие действия.

1. На странице аутентификации JWM (Рис. 60, с. 50) выберите вкладку **SMS-оповещение**. Отобразится страница следующего вида

Рис. 73 – Начальная страница входа по SMS-оповещению

2. Введите **Имя пользователя** (в формате Домен\Пользователь)
3. Ниже введите содержимое поля «капча» (символы, распознаваемые человеком) и нажмите **Получить код**.

Отобразится страница следующего вида.

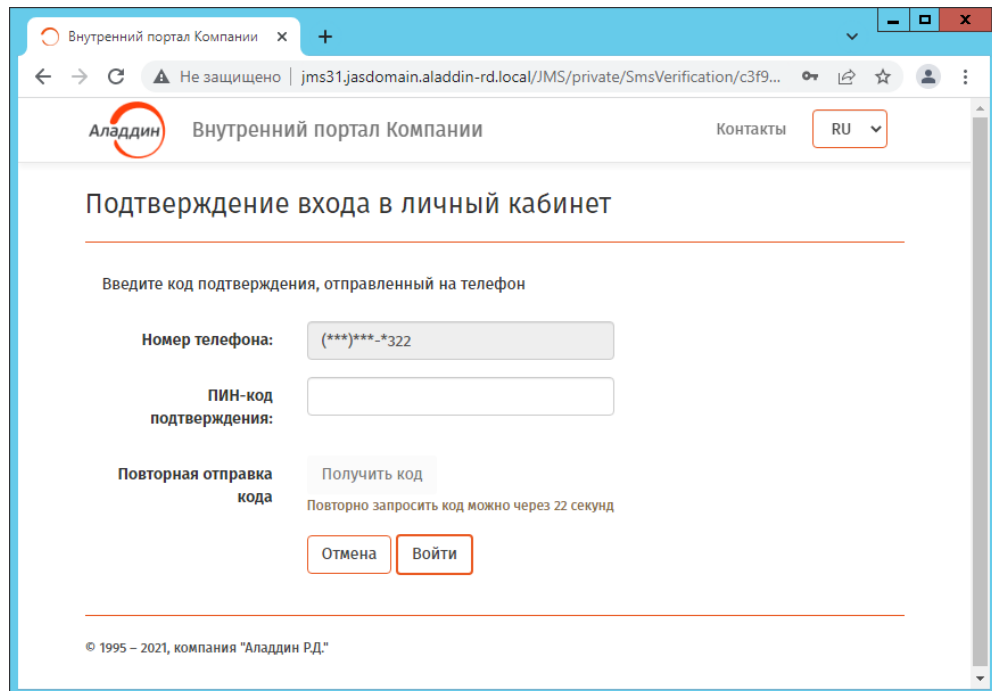


Рис. 74 – Страница ввода кода подтверждения из SMS

4. В поле **ПИН-код подтверждения** введите код, полученный в SMS на вашем мобильном телефоне.

При успешной аутентификации отобразится страница личного кабинета пользователя с вкладкой **Устройства**.

7.4 Вход по OTP-паролю

Для входа по одноразовому паролю (OTP) с помощью токена (аппаратное или программное устройство, генерирующее одноразовый цифровой пароль) выполните следующие действия.

1. На странице аутентификации JWM (Рис. 60, с. 50) выберите вкладку **Вход по OTP**.

Отобразится страница следующего вида

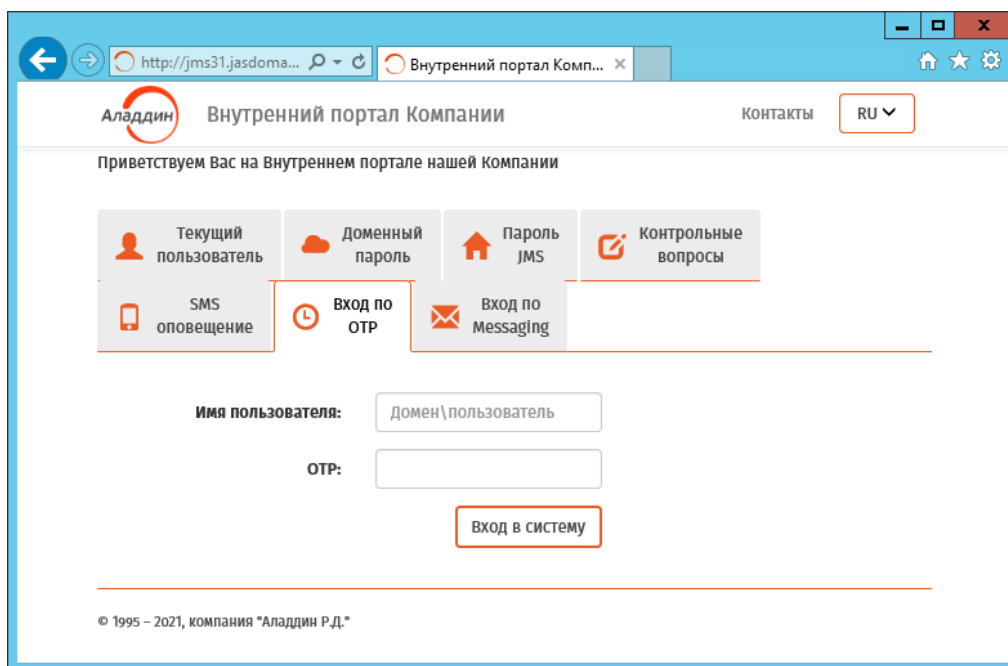


Рис. 75 – Начальная страница входа по OTP-паролю

2. Введите **Имя пользователя** (в формате Домен\Пользователь)



Примечание. При аутентификации по OTP-паролю при определённых настройках портала JWM в поле **Имя пользователя** допускается вводить только само имя, без указания домена. Способ ввода имени пользователя следует уточнить у администратора JMS.

3. Получите одноразовый пароль (цифровой код, OTP) с помощью выданного вам системным администратором OTP-токена (например, устройства JC-WebPass, производства компании Аладдин) или мобильного приложения Aladdin 2FA (или аналогичных приложений других поставщиков), активированного в JMS.
4. Введите полученный одноразовый пароль в поле **ОТР** и нажмите **Вход в систему**.

В случае успешной аутентификации отобразится страница личного кабинета пользователя JWM.

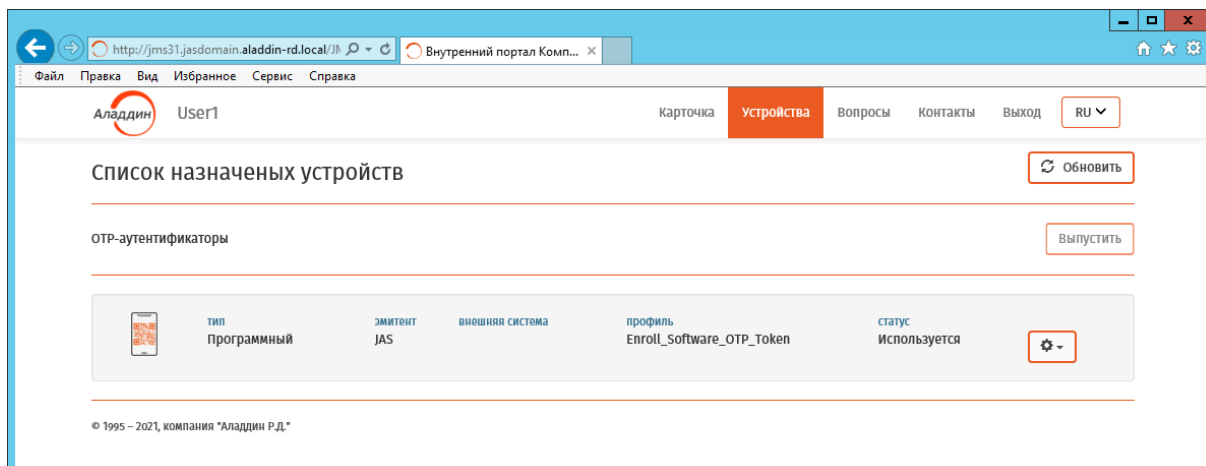


Рис. 76 – Вкладка **Устройства** личного кабинета пользователя

7.5 Вход по Messaging-паролю

Данный тип аутентификации выполняется по одноразовому паролю (OTP), передаваемому на мобильный телефон пользователя по SMS.



Важно! Аутентификация в личном кабинете по Messaging-паролю в текущей версии продукта недоступна в браузере Internet Explorer. Для аутентификации данного типа используйте другие типы Web-браузеров.



Примечание. Аутентификации данного типа доступна пользователю, если администратор JMS установил для пользователя возможность такой аутентификации. Для подключения данной возможности в JMS обратитесь к администратору.

Для входа по Messaging-паролю, выполните следующие действия.

1. На странице аутентификации JWM (Рис. 60, с. 50) выберите вкладку **Вход по Messaging**. Отобразится страница следующего вида

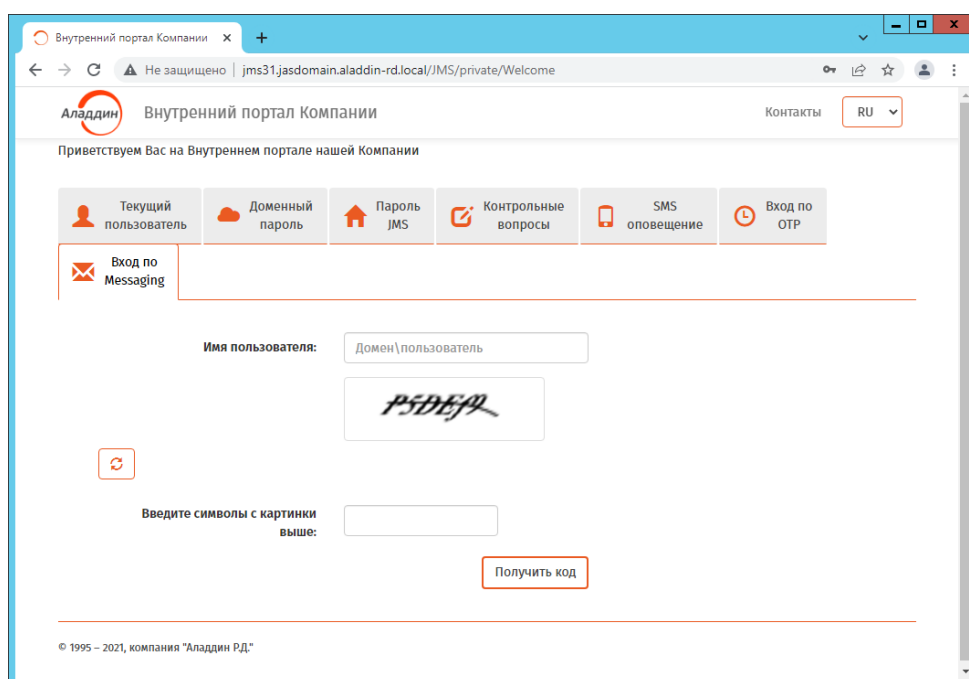


Рис. 77 – Начальная страница входа по Messaging-паролю

2. Введите **Имя пользователя** (в формате Домен\Пользователь)



Примечание. При аутентификации по Messaging-паролю при определённых настройках портала JWM в поле **Имя пользователя** допускается вводить только само имя, без указания домена. Способ ввода имени пользователя следует уточнить у администратора JMS.

3. В поле **Введите символы с картинки выше** введите содержимое поля «капча» (символы, распознаваемые человеком) и нажмите **Получить код**.

Отобразится страница следующего вида.

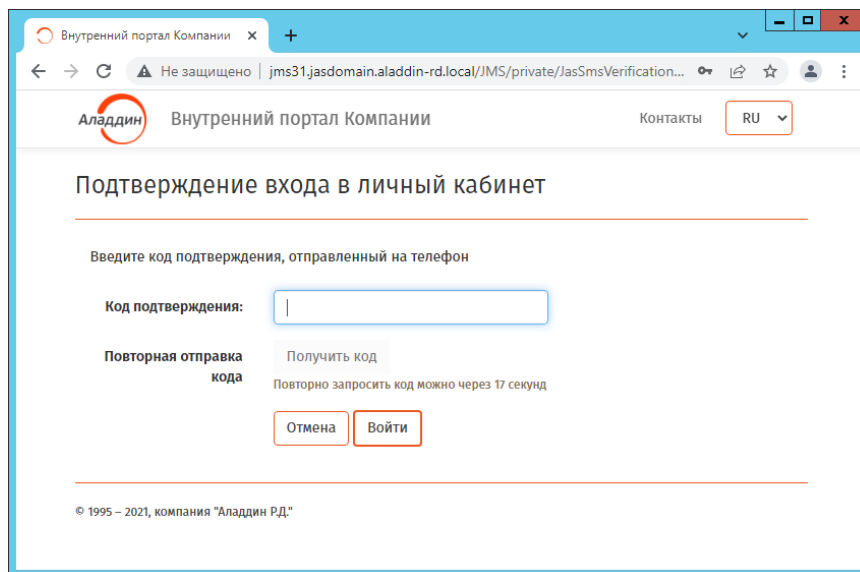


Рис. 78 – Страница ввода кода подтверждения из SMS

4. В поле **Код подтверждения** введите код, полученный в SMS на вашем мобильном телефоне.

В случае успешной аутентификации отобразится страница личного кабинета пользователя JWM.

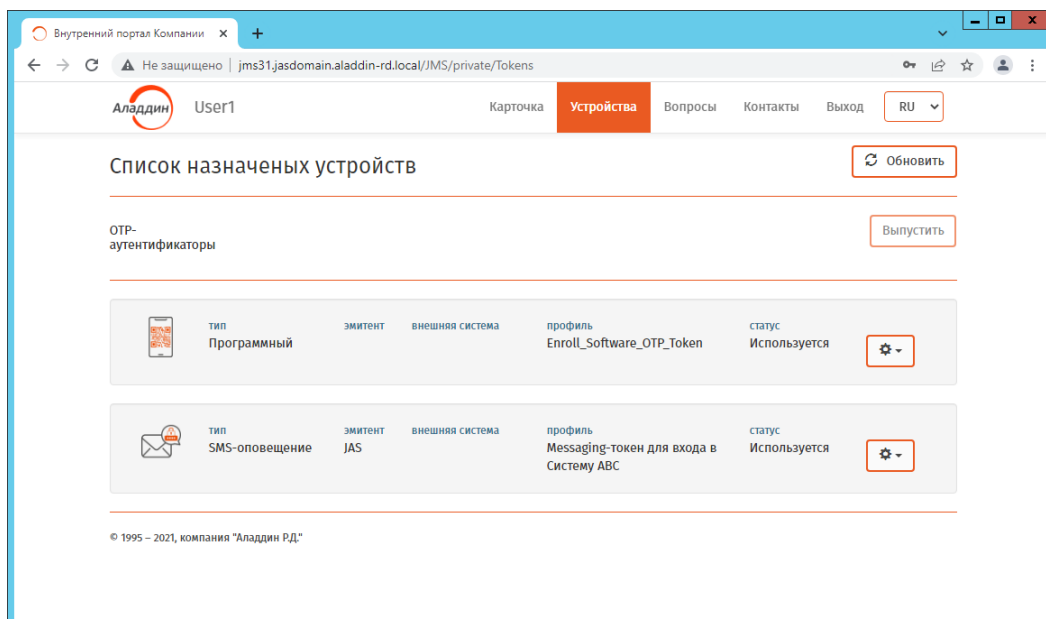


Рис. 79 – Вкладка **Устройства** личного кабинета пользователя

7.6 Функции, доступные пользователю в личном кабинете портала самообслуживания

Выполнив аутентификацию, пользователь получает доступ в свой личный кабинет на портале самообслуживания (Рис. 80).

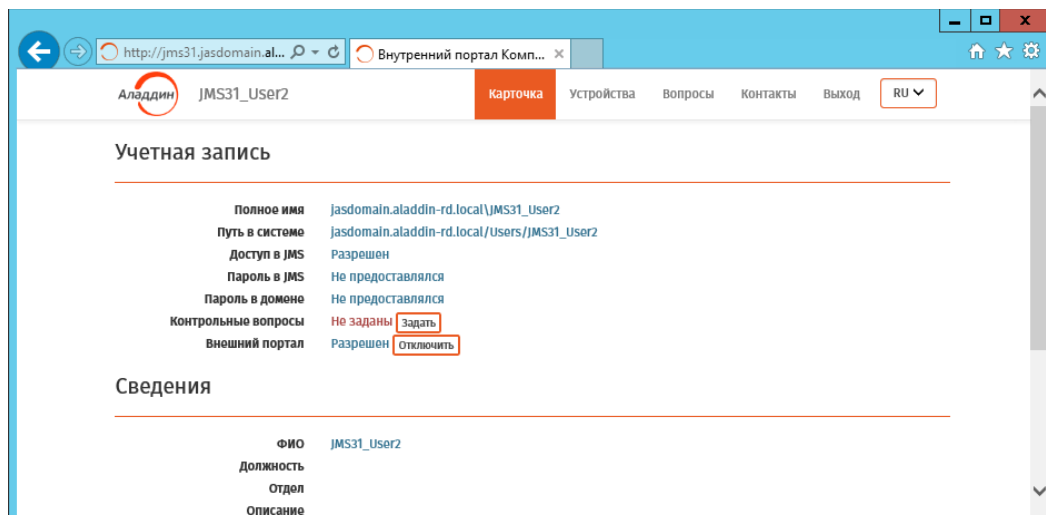




Рис. 80 – Вкладка Карточка личного кабинета пользователя на внутреннем портале самообслуживания

Пользователю доступны функции расположенные на нескольких вкладках страницы личного кабинета в соответствии с Табл. 9.

Табл. 9 – Функции, доступные пользователю в личном кабинете на внутреннем портале самообслуживания

Название вкладки	Описание
Карточка	На вкладке отображаются личные данные пользователя, его контактные данные и информация об его учетной записи в JMS.
Устройства	На вкладке отображается список электронных ключей, закрепленных за пользователем, их статус и перечень доступных операций в виде раскрывающегося списка (подробнее см. раздел «Управление электронными ключами из личного кабинета», с. 71)
Вопросы	На вкладке пользователь может определить (установить) контрольные вопросы для аутентификации (см. раздел «Управление контрольными вопросами из личного кабинета», с. 78)
Контакты	Контактная информация службы технической поддержки портала самообслуживания.  Примечание. В зависимости от настроек портала администратором вкладка Контакты в личном кабинете пользователя может отсутствовать
Выход	При нажатии на Выход происходит прекращение сеанса работы в личном кабинете пользователя

7.6.1 Выпуск OTP-аутентификатора


 Для выполнения этой процедуры вы должны иметь полномочия на самостоятельный выпуск OTP-аутентификаторов. В случае отсутствия таких полномочий для выпуска OTP-аутентификаторов обратитесь к администратору.

OTP-аутентификаторами называются средства аутентификации, доступные пользователю при использовании мобильных устройств (таких как смартфон или обычный мобильный телефон).

В личном кабинете JWM-портала пользователю доступен выпуск нескольких типов таких аутентификаторов:

- **программный OTP-токен** – для использования такого аутентификатора необходим смартфон с установленным приложением Aladdin 2FA компании Алладдин (или аналогичными приложениями других поставщиков);
- **A2FA Push-токен** – те же требования, что и для программного OTP-токена;
- **Messaging-токен** – для его использования достаточно наличие обычного мобильного телефона, поскольку для передачи одноразового пароля (OTP) используется SMS-сообщение.

Чтобы самостоятельно выпустить OTP-аутентификатор, выполните следующие действия.

 **Примечание.** В приведенном ниже примере производится выпуск программного OTP-токена.

1. Выполните аутентификацию на внутреннем портале и на странице личного кабинета откройте вкладку **Устройства** (Рис. 81).

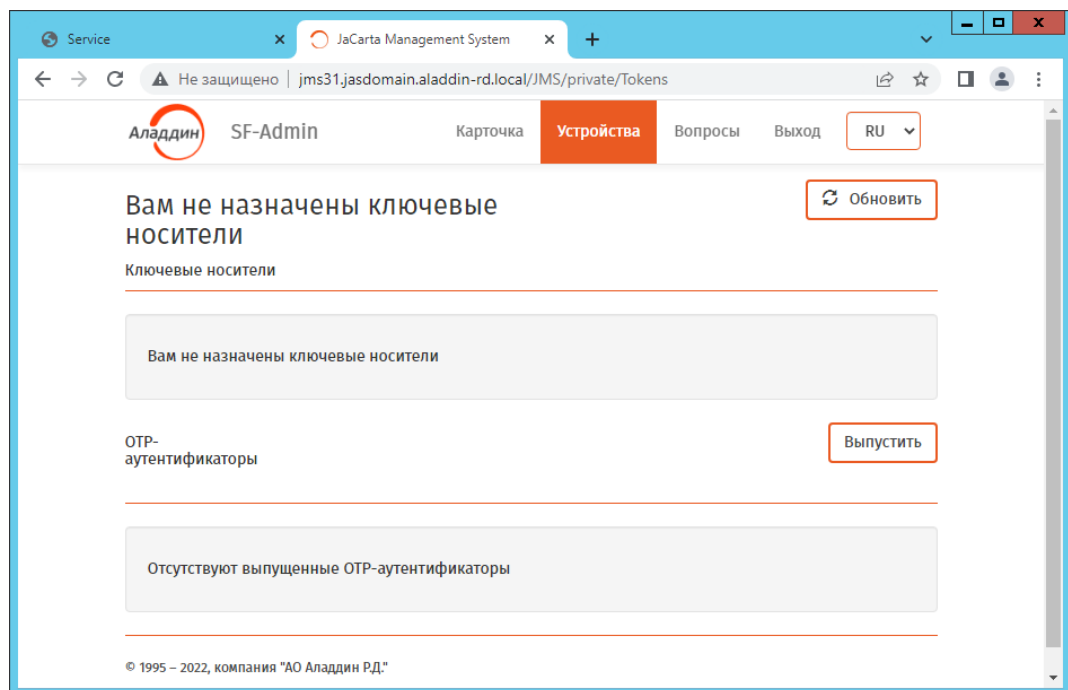


Рис. 81 – Вкладка Устройства личного кабинета пользователя на внутреннем портале самообслуживания

2. В секции OTP-аутентификаторы нажмите **Выпустить**.
Отобразится страница следующего вида.

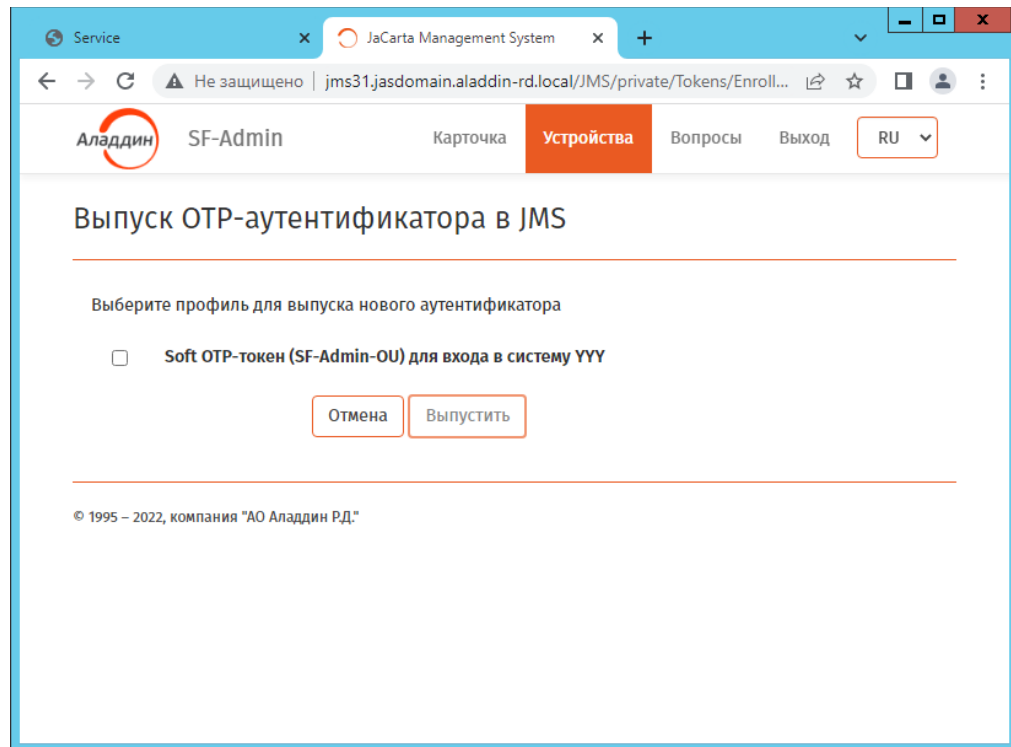


Рис. 82 – Страница выбора профиля для выпуска OTP-аутентификатора

3. В списке доступных профилей OTP-аутентификаторов для выпуска выберите один или несколько типов аутентификаторов (профилей), которые вам необходимы, отметив их галочкой слева, и нажмите **Выпустить**. По завершении процедуры выпуска отобразится страница следующего вида.

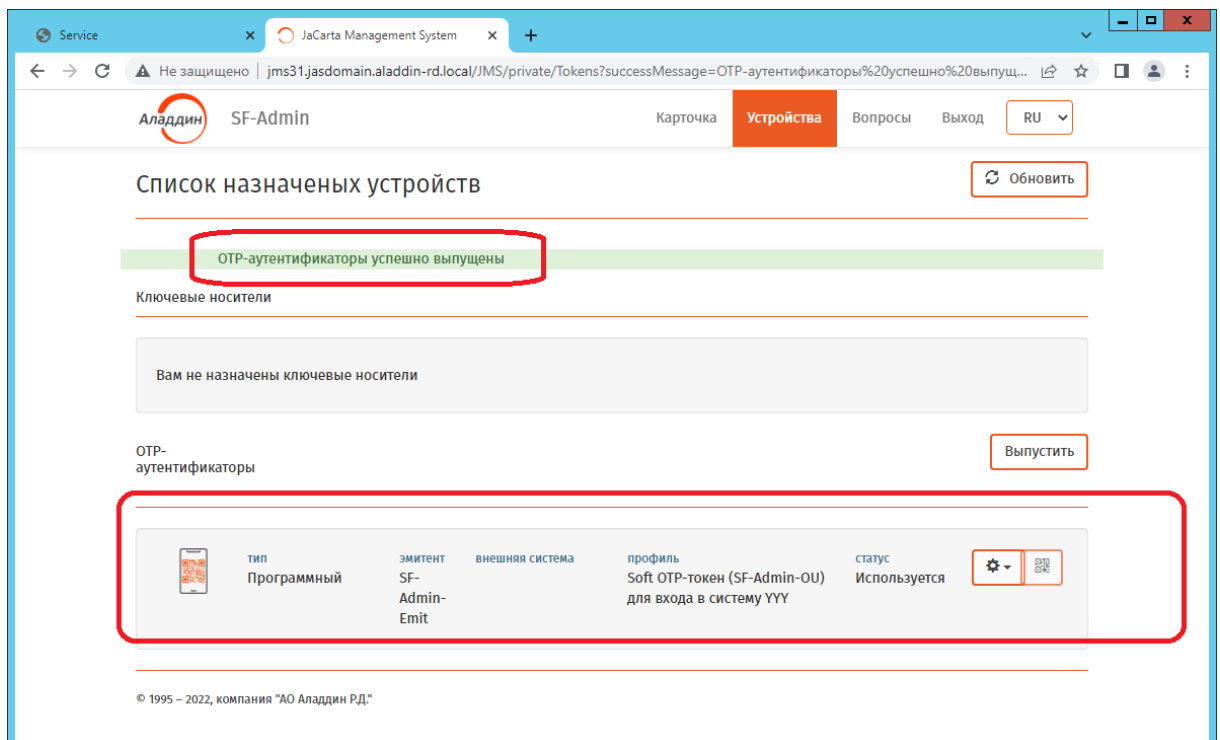


Рис. 83 – Страница с отображением выпущенного OTP-аутентификатора

В верхней части страницы отобразится уведомление об успешном выпуске OTP-аутентификаторов.

В секции **OTP-аутентификаторы** добавятся новые записи с OTP-токенами со статусом *Используется*.

Выпуск OTP-аутентификатора сопровождается передачей специальных активационных данных, которые (в зависимости от настроек администратора) направляются на адрес личной электронной почты и/или непосредственно в личный кабинет пользователя. В зависимости от того, по какому каналу были переданы активационные данные OTP-аутентификатора, пользователю следует выполнить действия, описанные в разделах:

- «Активация программного и Push OTP-токена через e-mail», с. 67 (для случая передачи активационных данных на личную электронную почту пользователя);
- «Активация программного и Push OTP-токена в личном кабинете», с. 68 (для случая передачи активационных данных непосредственно в личный кабинет пользователя).

После выпуска программного OTP-токена пользователь может открывать свой личный кабинет на JWM портале с помощью данного аутентификатора (подробнее см. раздел «Вход по OTP-паролю», с. 60).

7.6.2 Активация программного и Push OTP-токена через e-mail

Для активации программного или Push OTP-токена в своем мобильном приложении Aladdin 2FA компании Аладдин (или в аналогичном приложении другого поставщика) с помощью уведомления в e-mail выполните следующие действия.



Примечание. Активация Push OTP-токена доступна только в мобильном приложении A2FA компании Аладдин.

1. Откройте свой почтовый аккаунт и найдите письмо, полученное в момент выпуска программного или Push OTP-токена с темой «*[JMS] Регистрация программного OTP-токена*», например:

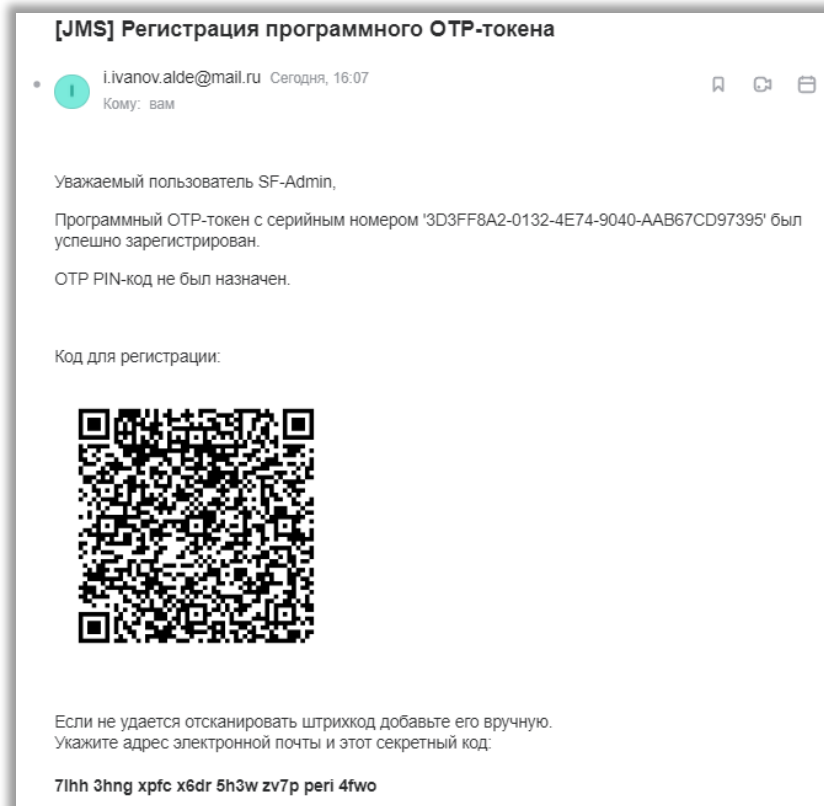


Рис. 84 - Сообщение, содержащее QR-код для активации программного OTP-токена

2. С помощью приложения Aladdin 2FA компании Аладдин, установленного на вашем мобильном устройстве, отсканируйте отобразившийся QR-код.

После этого OTP-токен в приложении станет активным (например, в случае программного OTP-токена, начнёт отображать одноразовый пароль).

7.6.3 Активация программного и Push OTP-токена в личном кабинете



Примечания:

1. О доступности активации данного типа в вашем личном кабинете (зависит от настроек системы) следует узнать у администратора JMS.
2. Активация данного типа доступна только для мобильного приложения A2FA компании Аладдин.

Для активации программного или Push OTP-токена в своем мобильном приложении A2FA компании Аладдин в личном кабинете выполните следующие действия.

1. Выполните аутентификацию на внутреннем портале и на странице личного кабинета откройте вкладку **Устройства** (Рис. 85).

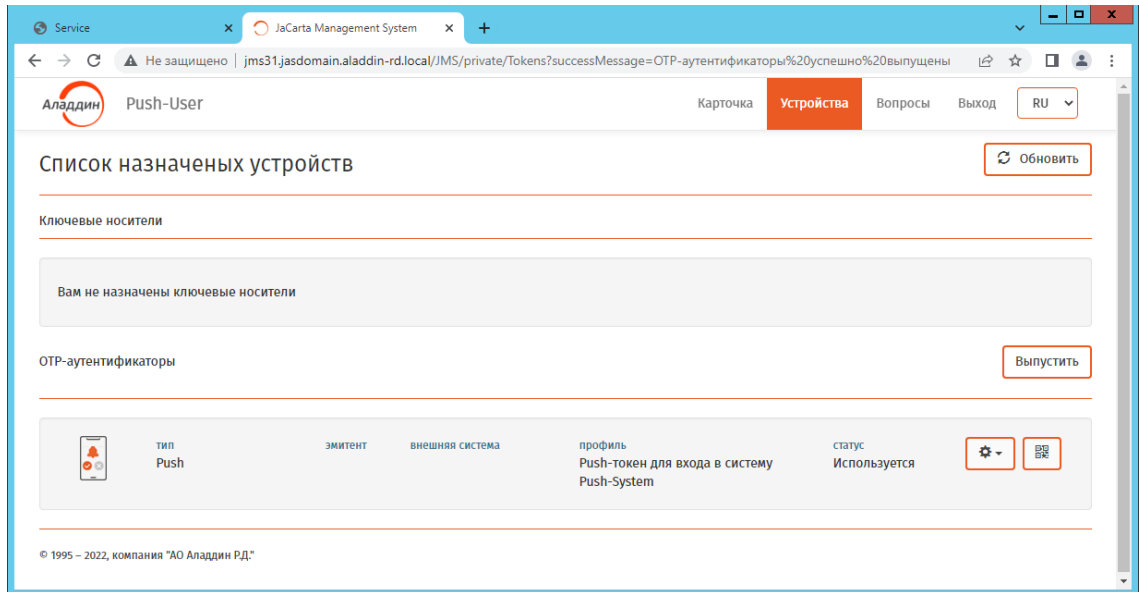


Рис. 85 – Отображение ОТР-аутентификатора на вкладке Устройства личного кабинета

2. В секции **ОТР-аутентификаторы** выберите ОТР-токен для активации (например Push ОТР-токен, как на Рис. 85).
3. В правой части строки с описанием ОТР-токена нажмите пиктограмму с QR-кодом.

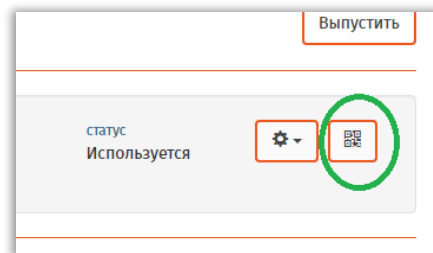


Рис. 86 – Пиктограмма QR-кода для активации токена

4. Отобразится окно следующего вида.

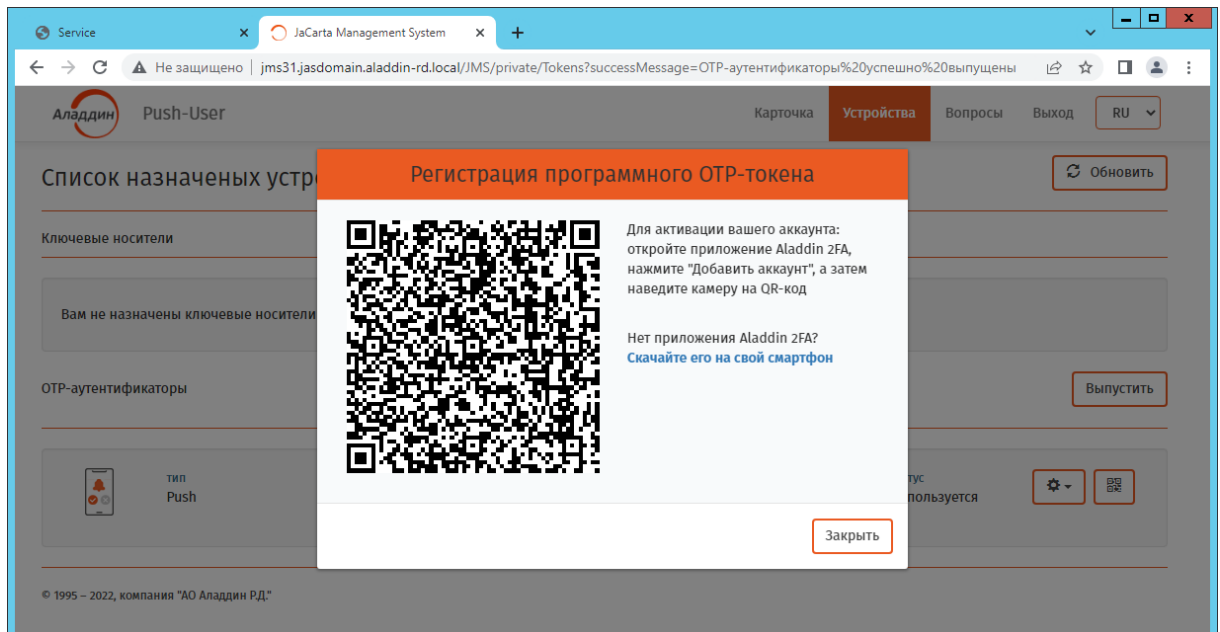



Рис. 87 – Окно с QR-кодом для активации OTP-токена

5. С помощью приложения Aladdin 2FA компании Аладдин, установленного на вашем мобильном устройстве, отсканируйте отобразившийся QR-код.
6. Нажмите **Заккрыть**.

После этого OTP-токен в мобильном приложении станет активным (например в случае программного OTP-токена, начнёт отображать одноразовый пароль).

7.6.4 Управление OTP-аутентификаторами из личного кабинета

Для управления своими OTP-аутентификаторами выполните следующие действия.

1. Войдите в личный кабинет на JWM-портале откройте вкладку **Устройства** (Рис. 83, с. 66).
2. Выберите OTP-аутентификатор в секции **OTP-аутентификаторы** и нажмите значок . Отобразится контекстное меню следующего вида.

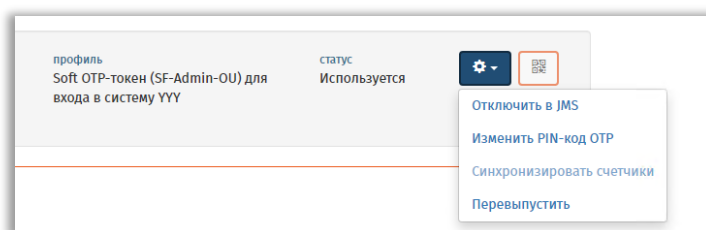




Рис. 88 – Контекстное меню операций с OTP-аутентификаторами

3. В зависимости от имеющихся у вас прав выполните доступную операцию в соответствии с Табл. 10.

Табл. 10 – Операции с OTP-аутентификаторами в личном кабинете на вкладке Устройства

Операция	Описание
Отключить в JMS	То же, что операция Отключить в клиенте JMS по отношению к электронному ключу (см. «Отключение возможности использования электронного ключа», с. 26).
Включить в JMS	Операция позволяет включить возможность использования электронного ключа после его отключения (см. операцию Отключить в JMS , выше). Аналогична операции по отношению к электронному ключу, описанной в разделе «Включение возможности использования электронного ключа», с. 75
Изменить PIN-код OTP	<p>Операция позволяет установить (если еще не установлен) или изменить PIN-код OTP (дополнительный параметр аутентификации, вводимый пользователем при входе в целевую систему).</p> <p> Примечание. При изменении <i>PIN-кода OTP</i> на адрес электронной почты пользователя приходит соответствующее уведомление со значением нового PIN-кода.</p> <p>Операция выполняется по согласованию с администратором системы.</p>
Синхронизировать счётчики	<p>Служебная операция настройки функционирования OTP-аутентификатора.</p> <p>Операция выполняется по согласованию с администратором системы.</p>
Перевыпустить	<p>Операция позволяет повторно выпустить OTP-аутентификатор в соответствии с установленным профилем. При этом на адрес электронной почты пользователя придет новый QR-код с активационной информацией для запуска нового токена в мобильном приложении (см. «Активация программного и Push OTP-токена», с. 67).</p> <p> Примечание. После активации нового программного OTP-токена в мобильном приложении, прежний OTP-токен перестает быть актуальным и его следует удалить.</p> <p>Операция выполняется по согласованию с администратором системы.</p>

7.6.5 Управление электронными ключами из личного кабинета

Для управления своими электронными ключами выполните аутентификацию на внутреннем портале и на странице личного кабинета откройте вкладку **Устройства** (Рис. 89).

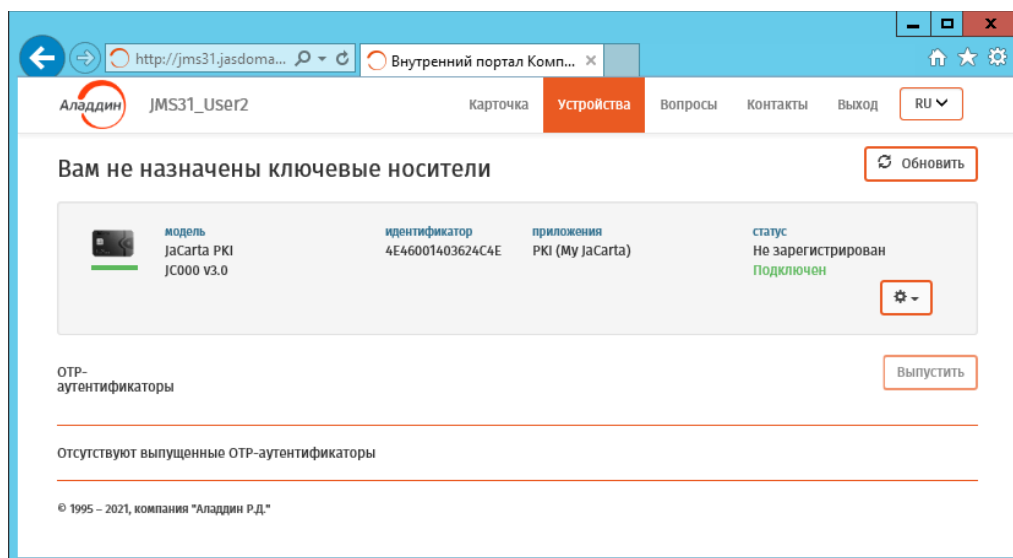



Рис. 89 – Вкладка Устройства личного кабинета пользователя на внутреннем портале самообслуживания

Выберите на странице электронный ключ и в зависимости от его статуса выполните доступную операцию в соответствии с Табл. 11.

Табл. 11 – Операции с электронными ключами в личном кабинете на вкладке Устройства


Операция	Описание
Отключить в JMS	То же, что операция Отключить в клиенте JMS (см. «Отключение возможности использования электронного ключа», с. 26).
Включить в JMS	Операция позволяет включить возможность использования электронного ключа после его отключения (см. операцию Отключить в JMS , выше). Порядок включения описан в разделе «Включение возможности использования электронного ключа», с. 75
Сообщить об утере\поломке	То же, что операция Сообщить об утере\поломке в клиенте JMS (см. «Действия в случае утери или поломки электронного ключа», с. 34)
Разблокировка PIN-кода	Позволяет разблокировать PIN-код пользователя в электронных ключах JaCarta и eToken. Подробнее см. раздел «Разблокировка PIN-кода в электронных ключах на портале самообслуживания», с. 76.

7.6.5.1 Выпуск электронного ключа

 Для выполнения этой процедуры вы должны иметь полномочия на самостоятельный выпуск электронных ключей. В случае отсутствия таковых для выпуска электронного ключа обратитесь к администратору.

Чтобы самостоятельно выпустить электронный ключ, выполните следующие действия.

1. Подсоедините электронный ключ, который вы хотите выпустить, к компьютеру.

 В JMS может быть настроен автоматический выпуск электронного ключа. Если процедура выпуска запустилась автоматически, без инициативы с вашей стороны, выполните действие (установка метки электронного ключа), представленное в шаге 4 настоящей процедуры, и дождитесь окончания автоматического выпуска электронного ключа.

2. Выполните аутентификацию на внутреннем портале и на странице личного кабинета откройте вкладку **Устройства** (Рис. 89, с. 72).

3. Выберите электронный ключ, который необходимо выпустить, и в раскрывающемся меню справа выберите опцию **Зарегистрировать и выпустить** или **Выпустить** (Рис. 90).

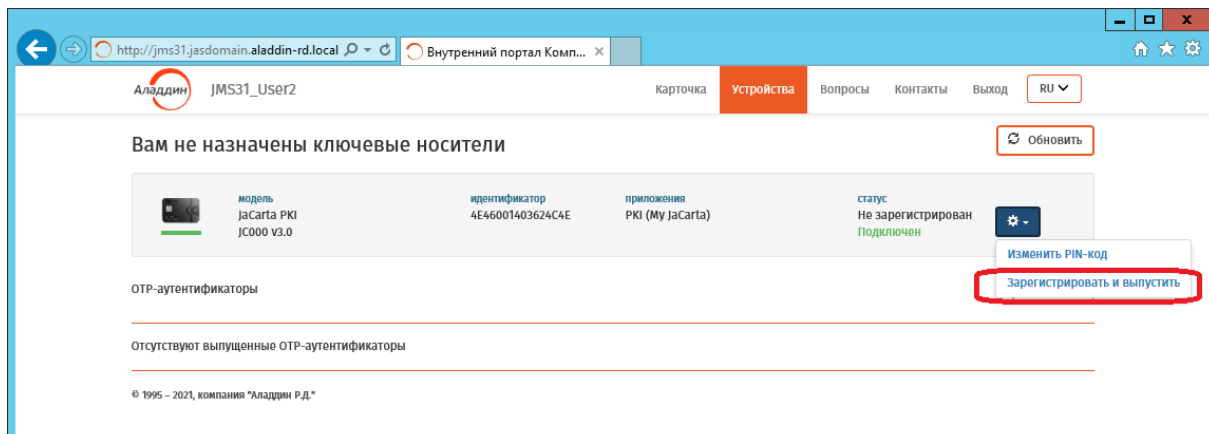


Рис. 90 – Выбор опции **Зарегистрировать и выпустить**

Примечания:

1. В случае запроса браузера на аутентификацию, выполните аутентификацию и продолжите процедуру выпуска электронного ключа
2. Электронный ключ, если он был назначен или выпущен на ваше имя, будет отображаться даже в том случае, если он не подсоединён к компьютеру (при этом действие **Выпустить** будет недоступно). Чтобы обеспечить возможность выпуска, убедитесь в соединении электронного ключа с компьютером.

Отобразится страница следующего вида.

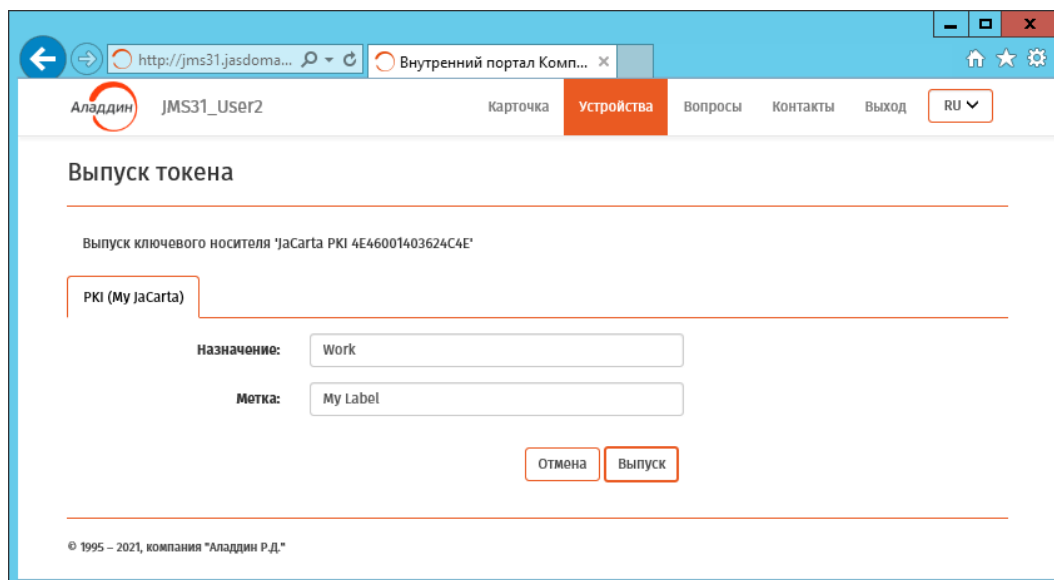



Рис. 91 – Страница задания метки и назначения электронного ключа

4. Если на странице допускается внесение изменений в полях **Назначение** или **Метка** электронного ключа, можете это выполнить при необходимости.

 **Примечание.** В случае если электронный ключ выпускается без инициализации, в интерфейсе будет также запрошен *PIN-код пользователя*. Для завершения такой операции необходимо ввести данный PIN-код.

5. Нажмите **Выпуск**.

По завершении процедуры выпуска электронный ключ будет отображаться со статусом *Используется*.

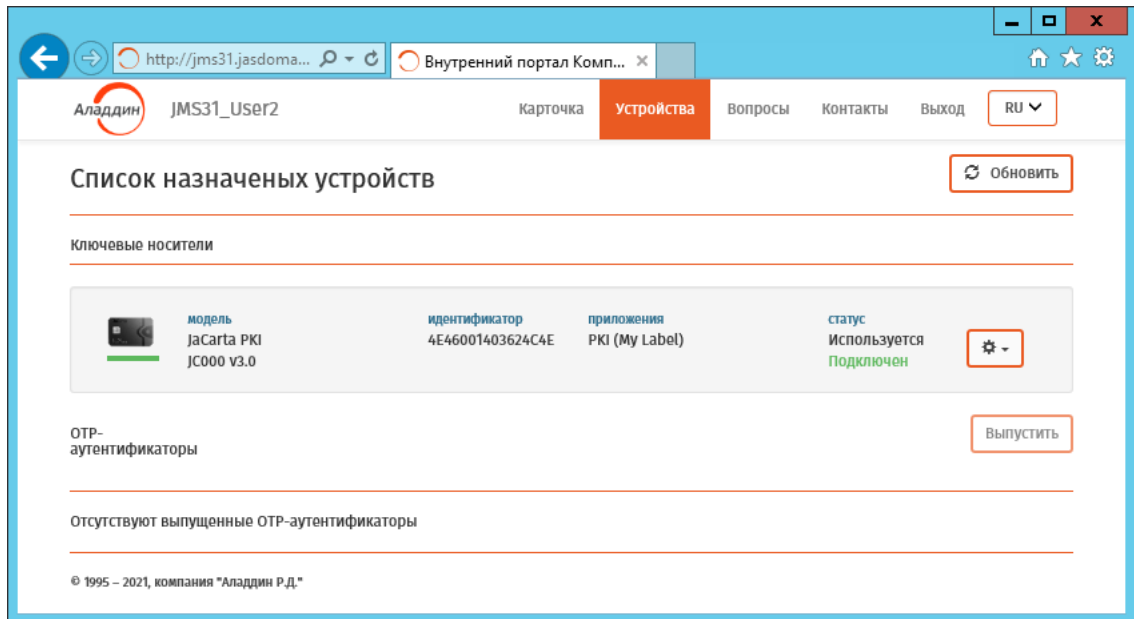


Рис. 92 – Статус выпущенного электронного ключа

7.6.5.2 Синхронизация электронного ключа

Для синхронизации электронного ключа, выполните следующие действия.

1. Подсоедините электронный ключ, который вы хотите выпустить, к компьютеру.
2. Выполните аутентификацию на внутреннем портале и на странице личного кабинета откройте вкладку **Устройства** (Рис. 89, с. 72).
3. Выберите электронный ключ, который необходимо синхронизировать, и в раскрывающемся меню справа выберите опцию **Синхронизировать**.

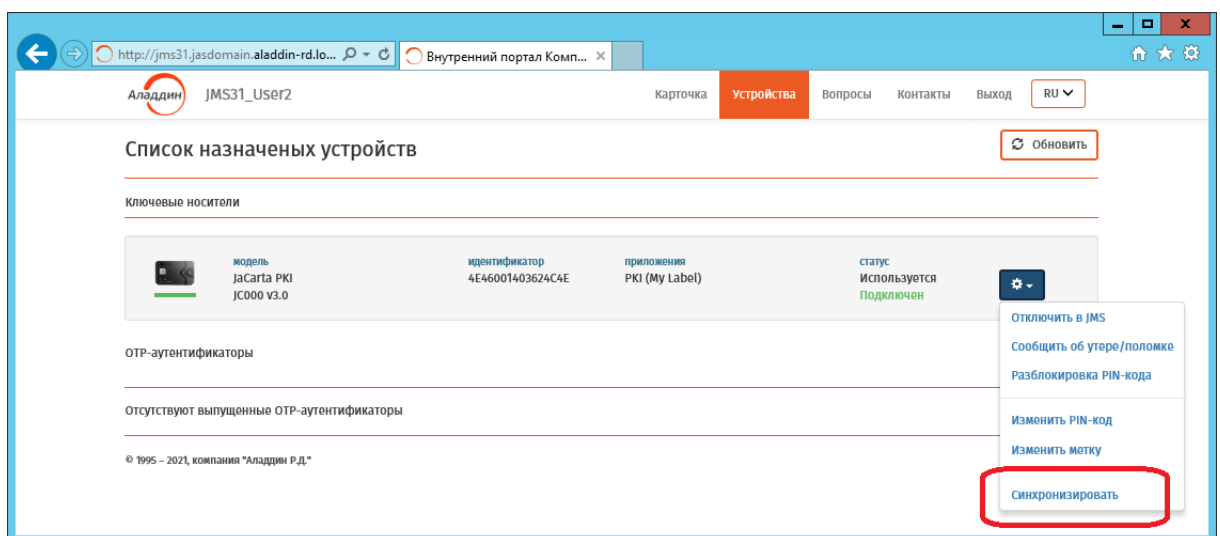


Рис. 93 – Выбор опции **Синхронизировать**

Примечание. В случае запроса браузера на аутентификацию, выполните аутентификацию и продолжите процедуру выпуска электронного ключа

4. Отобразится страница с запросом PIN-кода пользователя. Для продолжения процедуры введите PIN-код пользователя для данного электронного ключа и нажмите **Синхронизация**.

По окончании процедуры вверху окна на несколько секунд появится уведомление об успешной синхронизации электронного ключа.

7.6.5.3 Включение возможности использования электронного ключа

Операция позволяет включить возможность использования электронного ключа после его отключения (см. «Отключение возможности использования электронного ключа», с. 26).

Для включения возможности использования электронного ключа выполните следующие действия.

1. Выполните аутентификацию на внутреннем портале и на странице личного кабинета откройте вкладку **Устройства** (Рис. 89, с. 72).
2. Выберите электронный ключ, в котором нужно выполнить операцию включения (у отключенного ключа в личном кабинете отображается статус **Отключен в JMS**), и в раскрывающемся меню справа выберите опцию **Включить в JMS** (Рис. 96).

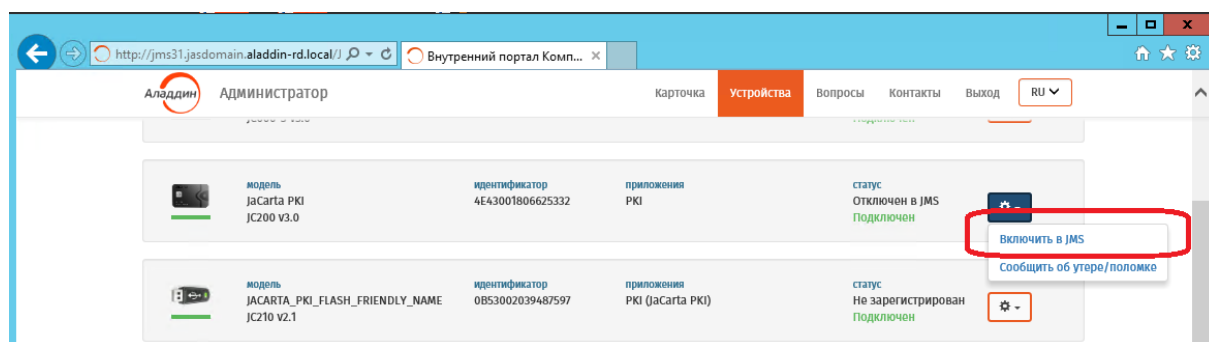


Рис. 94 – Выбор опции **Включить в JMS**

Отобразится страница следующего вида.

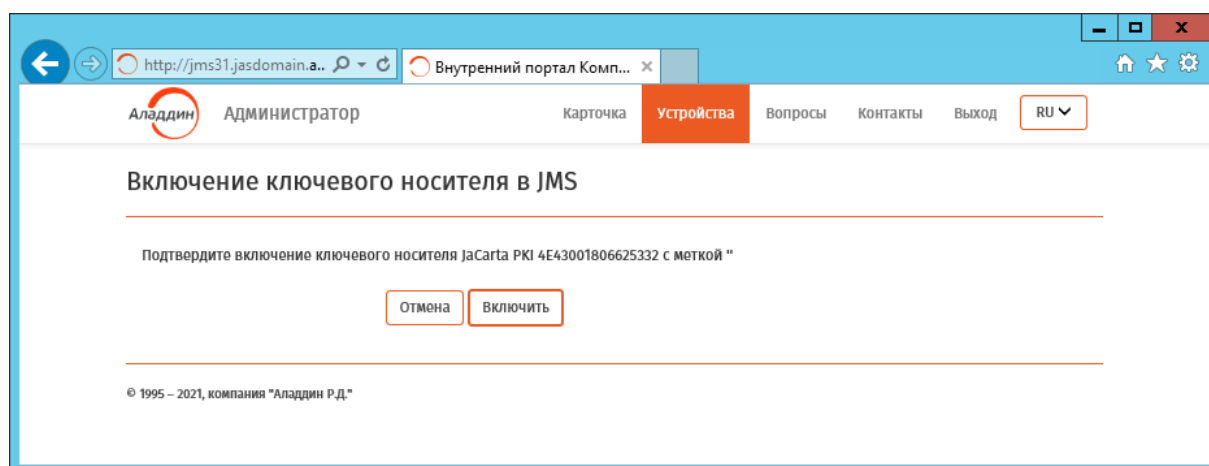


Рис. 95 – Страница запроса на включение электронного ключа

3. Нажмите **Включить**.

После включения возможности использования электронного ключа он приобретет статус **Используется**.

7.6.5.4 Разблокировка PIN-кода в электронных ключах на портале самообслуживания

Для разблокировки PIN-кода приложения в электронных ключах JaCarta (кроме JaCarta ГОСТ и JaCarta-2 ГОСТ) и eToken выполните следующие действия.

1. Выполните аутентификацию на внутреннем портале и на странице личного кабинета откройте вкладку **Устройства** (Рис. 89, с. 72).
2. Выберите электронный ключ, в котором нужно выполнить разблокировку (имя приложения заблокированного электронного ключа отображается красным цветом), и в раскрывающемся меню справа выберите операцию **Разблокировать PIN-код** (Рис. 96).

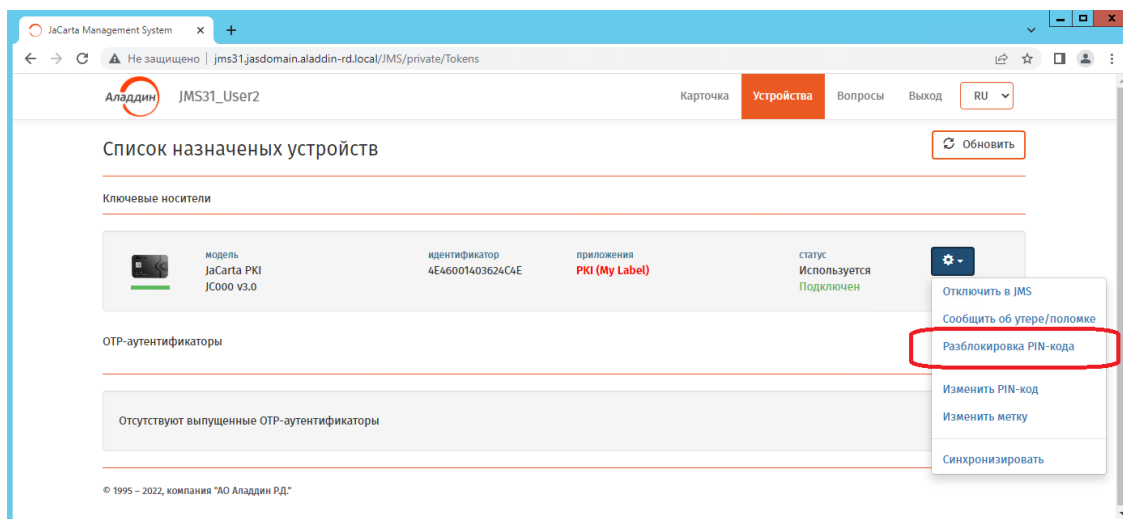


Рис. 96 – Выбор опции Разблокировать PIN-код

В случае если пользователю разрешена автоматическая разблокировка (устанавливается администратором JMS) отобразится страница следующего вида.

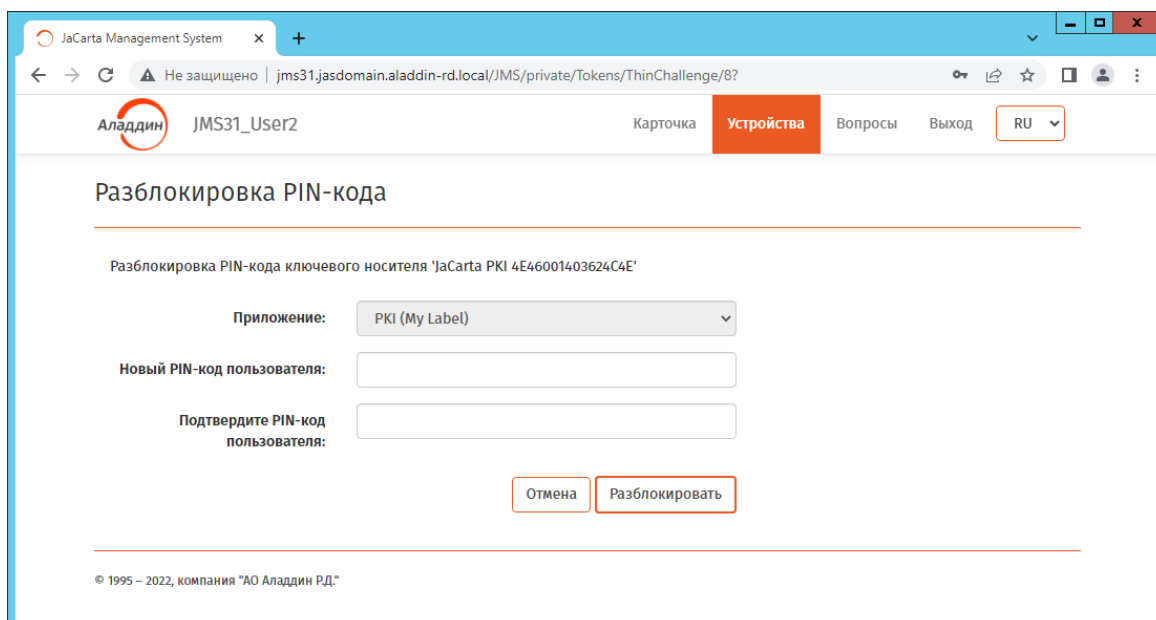
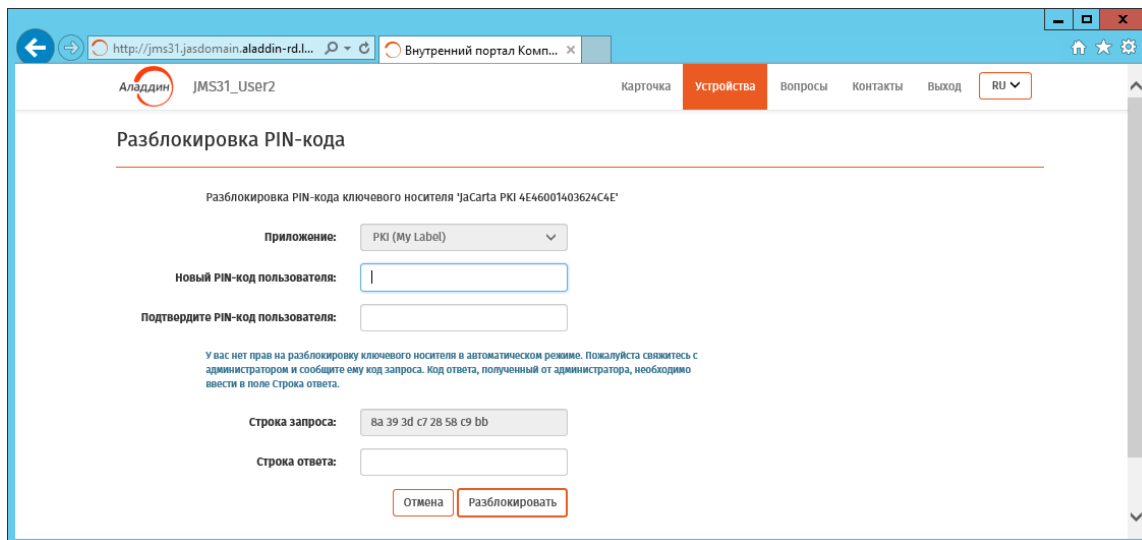


Рис. 97 – Страница для случая автоматической разблокировки PIN-кода

В случае если пользователю разрешена разблокировка только с участием администратора, отобразится страница следующего вида.



Аладдин JMS31_User2 Карточка Устройства Вопросы Контакты Выход RU

Разблокировка PIN-кода

Разблокировка PIN-кода ключевого носителя 'JaCarta PKI 4E46001403624C4E'

Приложение: PKI (My Label) ▾

Новый PIN-код пользователя:

Подтвердите PIN-код пользователя:

У вас нет прав на разблокировку ключевого носителя в автоматическом режиме. Пожалуйста свяжитесь с администратором и сообщите ему код запроса. Код ответа, полученный от администратора, необходимо ввести в поле Строка ответа.

Строка запроса: 8a 39 3d c7 28 58 c9 bb

Строка ответа:

Рис. 98 – Страница ввода строки запроса для разблокировки PIN-кода

3. В полях **Новый PIN-код пользователя** и **Подтвердите PIN-код пользователя** введите значение PIN-кода пользователя.
4. В случае автоматической разблокировки (см. окно на Рис. 97) переходите к шагу 7.
5. В случае разблокировки с участием администратора (см. окно на Рис. 98) свяжитесь с администратором для разблокировки электронного ключа (например, по телефону) и сообщите ему код запроса, отображаемый в поле **Строка запроса**.
Администратор сообщит вам код ответа.
6. Введите код ответа в поле **Строка ответа**.
7. Нажмите **Разблокировать**.

В случае успешной разблокировки отобразится страница следующего вида

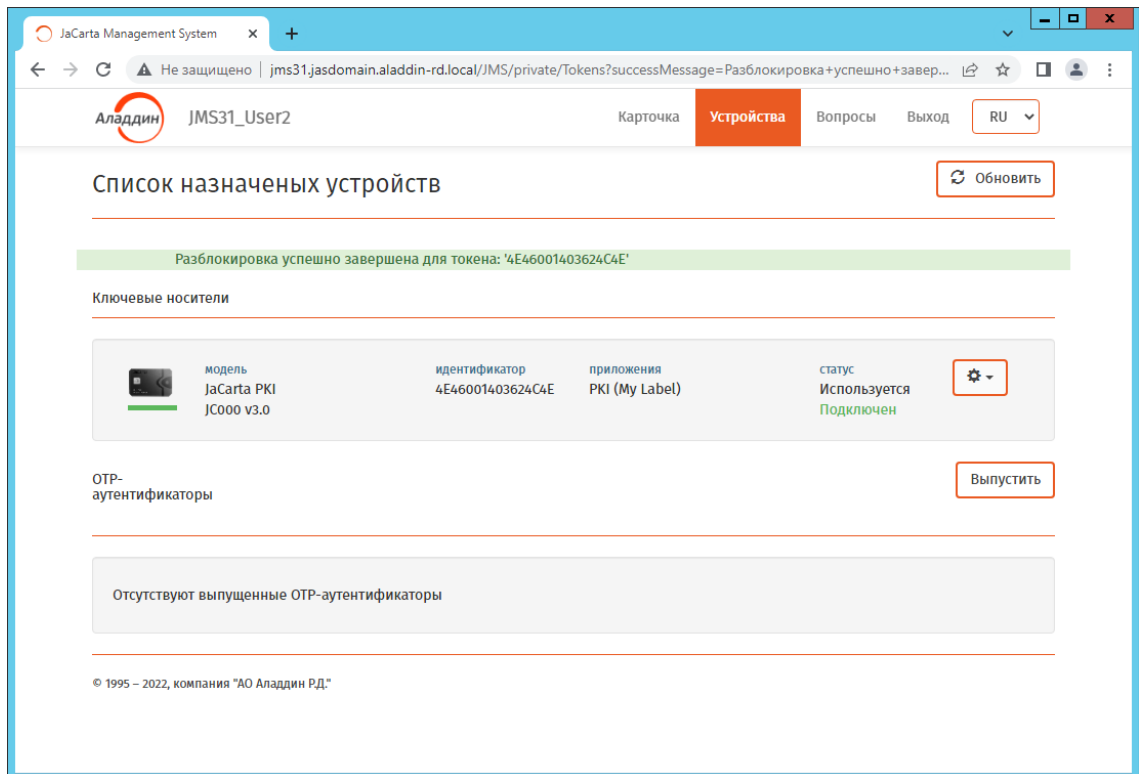


Рис. 99 – Страница с уведомлением об успешной разблокировке PIN-кода

Разблокированный электронный ключ готов к дальнейшей эксплуатации.

7.6.6 Управление контрольными вопросами из личного кабинета

Контрольные вопросы представляют собой один из механизмов аутентификации пользователя на внутреннем или внешнем web-портале самообслуживания: пользователь должен заблаговременно сформировать пары «секретный вопрос – ответ» (далее – контрольные вопросы), для того чтобы система могла аутентифицировать пользователя по ответам, известным только ему.

Для того чтобы определить (установить) контрольные вопросы выполните следующие действия.

1. Выполните аутентификацию на внутреннем портале любым методом, кроме метода Контрольные вопросы (см. «Аутентификация на внутреннем портале самообслуживания», с. 49) и на странице личного кабинета откройте вкладку **Вопросы**.

Отобразится страница следующего вида.

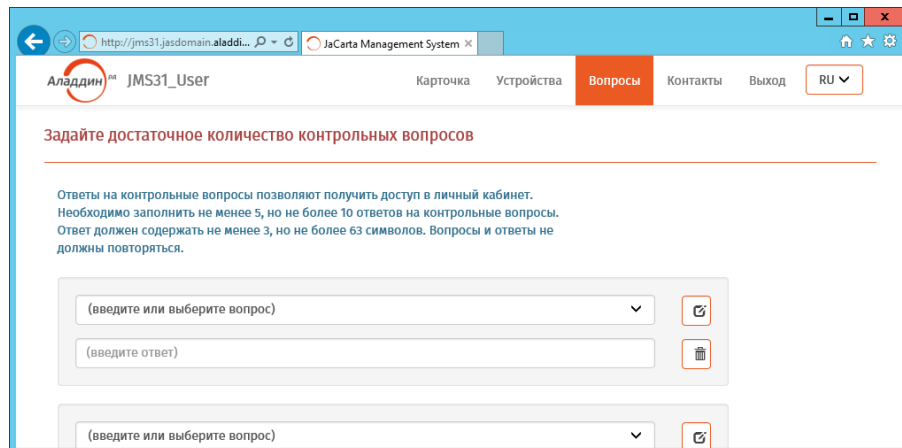



Рис. 100 – Страница настройки контрольных вопросов для аутентификации

2. Выберите один из вопросов по умолчанию, раскрыв список в поле вопроса (Рис. 101), либо введите собственный вопрос, нажав на значок редактирования поля .

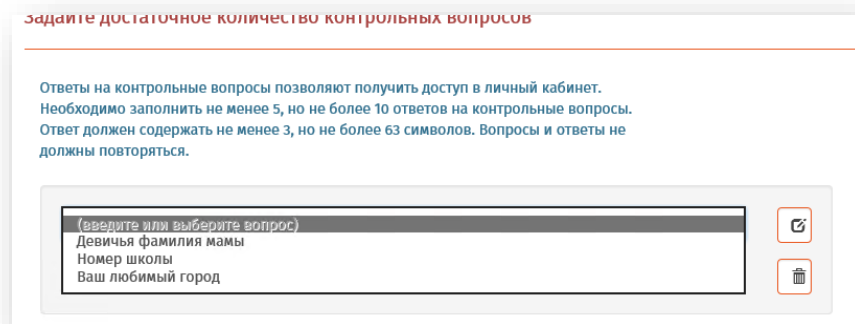


Рис. 101 – Выбор секретного вопроса среди вопросов по умолчанию

3. В поле ответа введите текст секретного ответа.
4. Повторите шаги 2–3 для оставшихся контрольных вопросов, отображенных на странице.
5. При необходимости добавьте контрольные вопросы, нажав **Добавить** внизу страницы.
6. Нажмите **Сохранить** внизу страницы и дождитесь сообщения об успешном сохранении введенных данных. (Рис. 102).

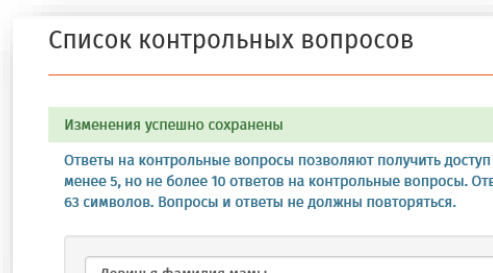


Рис. 102 – Подтверждение успешного сохранения списка контрольных вопросов

 **Примечания:**

1. Общее число контрольных вопросов не может превысить значения, оговоренного в информации, которая отображается вверху страницы (определяется администратором).
2. Ни секретные вопросы, ни ответы на них не должны повторяться.

При необходимости отредактировать ранее созданные секретные вопросы или ответы на них повторите шаги 2–3 для выбранных вопросов и нажмите **Сохранить**.

При необходимости добавьте новые контрольные вопросы, нажав **Добавить** внизу страницы, отредактируйте их и сохраните.

7.7 Аутентификация и работа на внешнем портале самообслуживания

Для аутентификации на внешнем портале самообслуживания в web-браузере откройте страницу по адресу следующего вида:

`http://<JMS_FQDN>/JMS/public`

где <JMS_FQDN> – полное доменное имя сервера JMS, например:

`jms31.jasdomain.aladdin-rd.local`



Примечание. Адрес внешнего web-портала самообслуживания следует получить у администратора JMS.

Откроется страница следующего вида:

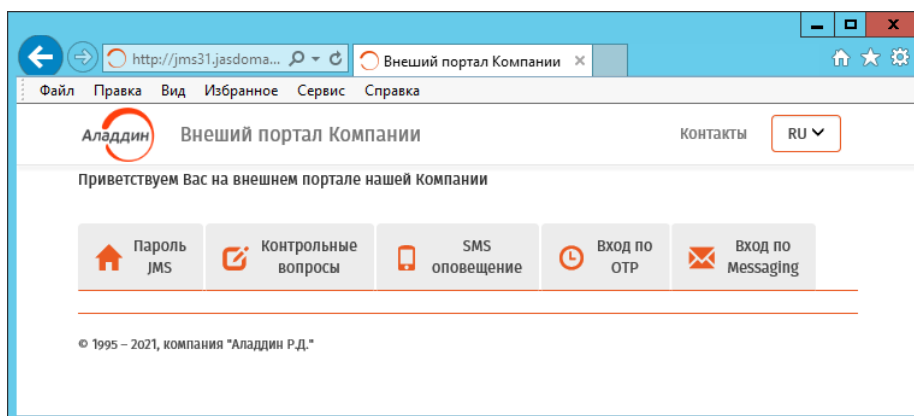


Рис. 103 – Страница аутентификации пользователя на внешнем портале самообслуживания

В зависимости от настроек портала некоторые вкладки со способами входа могут не отображаться.

Чтобы продолжить, выберите нужную вкладку, например **Пароль JMS**.

Отобразится окно следующего вида.

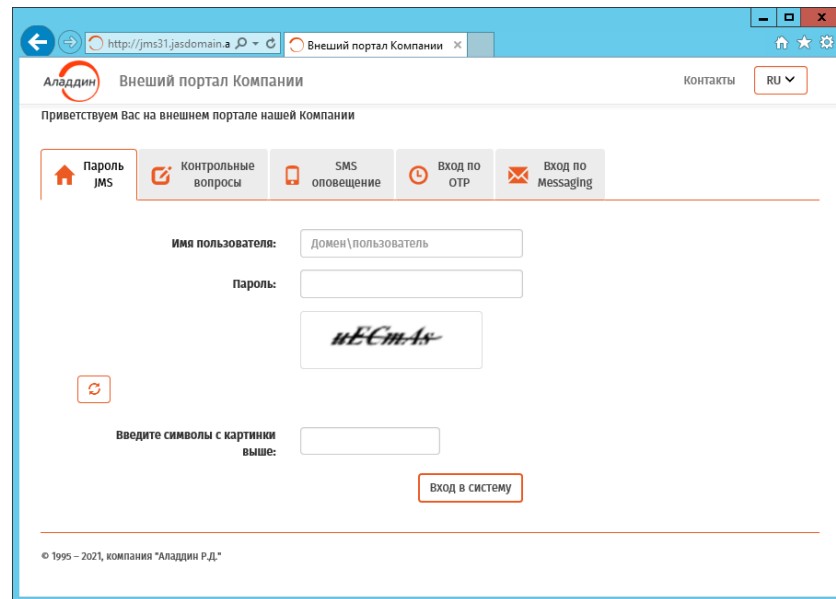


Рис. 104 – Страница с одним из способов аутентификации на внешнем портале самообслуживания

В зависимости от выбранной вкладки необходимо выполнить следующие действия:

1. Заполнить поле защиты типа «капча» (поле **Введите символы с картинки выше**).
2. Выполнить аутентификацию доступным способом, руководствуясь Табл. 8, с. 50.

7.7.1 Работа на внешнем web-портале самообслуживания

Работа на внешнем портале самообслуживания аналогична работе на внутреннем портале (см. раздел «Функции, доступные пользователю в личном кабинете портала самообслуживания», с. 63) с тем отличием, что на внешнем портале в личном кабинете пользователя отсутствует вкладка **Вопросы**, а также отсутствует возможность управлять доступом пользователя к внешнему portalу.

8. Список литературы

- 1 eToken PKI Client 5.1 SP1. Руководство пользователя [Текст]. – перевод «Аладдин Р.Д.».

- 2 Единый Клиент JaCarta. Руководство пользователя [Текст]. – «Аладдин Р.Д.»

- 3 RU.АЛДЕ.03.16.001-04 30 01-1. Формуляр [Текст]. – «Аладдин Р.Д.»

- 4 RU.АЛДЕ.03.16.001-04 90 01. Описание архитектуры безопасности [Текст]. – «Аладдин Р.Д.»

Контакты, техническая поддержка

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания «Аладдин Р. Д.».

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40.

Факс: +7 (495) 646-08-82.

E-mail: aladdin@aladdin.ru (общий).

Web: www.aladdin.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт:

www.aladdin.ru/support/index.php

Регистрация изменений

Версия	Изменения
1.00	Исходная версия документа для JMS версии 3.7.1.

Коротко о компании

Компания «Аладдин Р. Д.» основана в апреле 1995 года и является российским разработчиком (вендором) средств защиты информации.

Компания является признанным экспертом и лидером российского рынка средств двухфакторной аутентификации пользователей, электронной подписи и защиты данных.

Основные направления

- Обеспечение безопасного доступа к информационным ресурсам предприятия, веб-порталам и облачным сервисам (строгая двух- и трёхфакторная аутентификация).
- Электронная подпись (ЭП с неизвлекаемым закрытым ключом, формируемая в защищённом чипе), PKI.
- Защита персональных данных, данных на дисках компьютеров, серверов, баз данных.
- Все основные продукты имеют необходимые сертификаты ФСТЭК, ФСБ и Министерства обороны (включая работу с гостайной до уровня секретности СС).

Лицензии

- компания имеет все необходимые лицензии ФСТЭК России, ФСБ России и Министерства обороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной и производство продукции в рамках гособоронзаказа.
- Система менеджмента качества продукции в компании с 2012 г. соответствует стандарту ГОСТ ISO 9001-2011 и имеет соответствующие сертификаты.
- Система проектирования, разработки, производства и поддержки продукции соответствует требованиям российского военного стандарта ГОСТ РВ 15.002-2012, необходимого для участия в реализации гособоронзаказа.



Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.2017

Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17

Лицензия Министерства обороны РФ № 1384 от 22.08.16

Система менеджмента качества компании соответствует требованиям

ГОСТ Р ИСО 9001-2015 (ISO 9001:2015). Сертификат СМК № РОСС RU.ФК14.К00011 от 20.07.18

© АО «Аладдин Р. Д.», 1995–2024. Все права защищены

Тел. +7 (495) 223-00-01 Email: aladdin@aladdin.ru Web: www.aladdin.ru