ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ JACARTA MANAGEMENT SYSTEM 4LX

Руководство пользователя

Версия продукта	4LX
Версия документа	1.02
Статус	Служебный
Дата	9 февраля 2024 г.
Листов	71

2024

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

Оглавление

1. О документе

1.1 Назначение документа

Настоящий документ представляет собой руководство пользователя клиентских компонентов системы управления средствами аутентификации, защищенными носителями информации (ЗНИ) и средствами дистанционной работы (СДР) JaCarta Management System 4LX для среды функционирования Linux (далее – JMS).

1.2 На кого ориентирован данный документ

Документ предназначен для пользователей корпоративной информационной системы управления средствами аутентификации и ЗНИ.

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

ALO, СДР ALO	**Aladdin LiveOffice** – средство обеспечения безопасной дистанционной работы (СДР) компании Аладдин. В качестве электронного ключа (USB-носителя) использует устройство Aladdin LiveToken (далее для простоты – **СДР ALO**)
JMS	То же что «Программное обеспечение JaCarta Management System 4LX»
JWA **(JMS Web Agent)**	Программное обеспечение, реализующее взаимодействие web-клиента JMS с ЭК и ЗНИ из среды web-браузера
JWA Tray **(JMS Web Agent Tray)**	Программа, позволяющая выполнять базовые операции с ЭК/ЗНИ/СДР пользователя в фоновом режиме или через простое графическое меню. Запущенное приложение отображается значком в области уведомлений рабочего стола
Messaging-токен	Аутентификатор, позволяющий проводить аутентификацию посредством отправки OTP посредством службы SMS оператора мобильной связи
OTP	One-Time Password – одноразовый пароль
OTP-аутентификатор	Обобщённое название всех средств аутентификации, основанных на использовании OTP (включает в себя аппаратные и программные OTP-токены, Messaging-токены, а также Push OTP-токены)
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
Push OTP-токен	Виртуальный токен с использованием Push-технологии, обеспечивающей протокол аутентификации с персонально аутентифицированного доверенного устройства, не требующей от пользователя ввода аутентификационной информации
USB	Universal Serial Bus, универсальная последовательная шина
web-клиент JMS	Web-приложение Клиент JMS. Комплекс программ, состоящий из компонента JMS Web Agent из комплекта поставки ПО JMS и web-клиента, функционирующего в среде web-браузера
Аппаратный OTP-токен (HardwareOTP)	Аппаратная реализация средства аутентификации с поддержкой OTP. Один из видов аутентификаторов, поддерживаемых системой JMS
ЗНИ	Защищенный носитель информации – электронный ключ JaCarta SF/ГОСТ, обеспечивающий гарантированную защиту информации, хранимую во внутренних разделах электронного ключа (скрытые разделы RW и CD-ROM)
Клиентское ПО JMS	Все программное обеспечение (включая **JWA Tray** и **web-клиент JMS**), обеспечивающее работу конечного пользователя в JMS

Программный OTP-токен	Мобильное приложение, такое как Aladdin 2FA (A2FA) компании Аладдин (или аналогичные приложения других поставщиков), предназначенное для генерации одноразовых паролей для доступа пользователей к различным ресурсам. В среде JMS программные OTP-аутентификаторы классифицируются как OTP-токены
ПО	Программное обеспечение
СДР	Средство дистанционной работы пользователей с вычислительными и информационными ресурсами автоматизированной (информационной) системы
СКЗИ	Средство криптографической защиты информации
ЭК	Электронный ключ – электронное устройство, используемое как средство аутентификации, и/или защищенного хранения информации, и/или USB-носитель СДР

1.6 Авторские права, товарные знаки, ограничения

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 реэкспорт 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 УСТАНАВЛИВАТЬ 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 УСТАНАВЛИВАЯ 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 УСТАНАВЛИВАЙТЕ 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 нелицензионным 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 подразумевающихся 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, НЕСМОТРЯ 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 утерянные сбережения, вызванные использованием или связанные 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 УСТАНАВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ..

2. Введение

JMS - система, предназначенная для внедрения и учета аппаратных средств аутентификации, защищенных носителей информации (ЗНИ) и средств дистанционной работы (СДР) пользователей в масштабах предприятия.

JMS обеспечивает:

- централизованное управление средствами аутентификации, ЗНИ и СДР в течение всего их жизненного цикла (инициализация/выпуск, ввод в эксплуатацию/выдача, обслуживание, вывод из эксплуатации/блокирование);
- учет средств аутентификации, ЗНИ и СДР; 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», определен в Описании архитектуры безопасности [4].
Параметры (настройки) безопасности ПО JMS, доступные встроенной роли «Пользователь», и их безопасных 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 системы) следует обратиться к администратору данной ресурсной системы для разблокировки учётной записи пользователя.
Ввод неверного PIN-кода пользователя при попытке монтирования скрытых разделов ЗНИ	Ввести верный PIN-код пользователя. В случае исчерпания числа попыток ввода PIN-кода пользователя (устанавливается при инициализации ЗНИ) следует обратиться к администратору JMS с целью сбросить счетчик попыток ввода неверного PIN-кода пользователя ЗНИ.
Несоответствие контейнера .kko при попытке автономного монтирования скрытых разделов ЗНИ	В случае несоответствия контейнера .kko при попытке автономного монтирования скрытых разделов ЗНИ следует обратиться к администратору JMS для получения действующего контейнера .kko для данного экземпляра ЗНИ.

3. Общие приемы работы с ЭК/ЗНИ/СДР в JMS

Для поддержки пользовательских ЭК/ЗНИ/СДР (далее — электронных ключей) на компьютере может быть установлено приложении JMS Web Agent Tray (далее – JWA Tray), позволяющее выполнять базовые операции с электронными ключами в фоновом режиме или через простое графическое меню, не прибегая к запуску специализированного Web-приложения Клиент JMS.

Индикатором функционирования такого приложения на компьютере является отображение значка W в области уведомлений рабочего стола (Рис. 1).

Рис. 1 – Отображение значка «W» как признак установленного приложения JWA Tray

При нажатии правой кнопкой мыши на значке W открывается меню JWA Tray (Рис. 2).

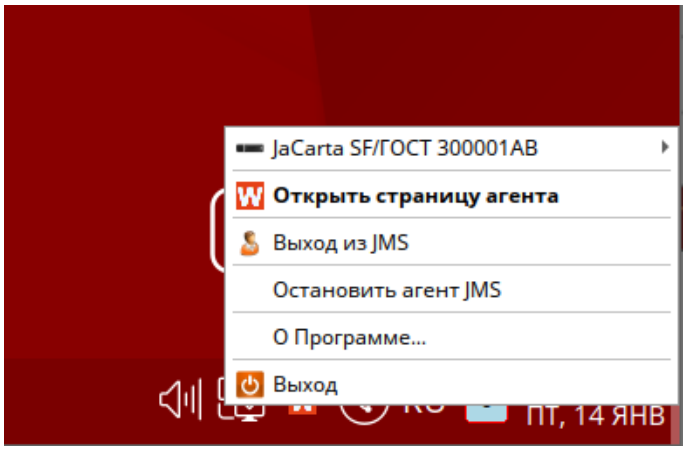


Рис. 2 – Меню JWA Tray

Описание пунктов меню представлено в Табл. 5.

Табл. 5 – Меню JWA Tray

Пункт	Описание
<Список названий и идентификаторов ЭК/ЗНИ/СДР>	В верхней части меню отображаются ЭК/ЗНИ/СДР подключенные в данный момент к компьютеру
Открыть страницу агента	Открывает страницу аутентификации web-приложения Клиент JMS в браузере, установленном в операционной системе как браузер по умолчанию (подробнее см. раздел «Порядок работы с web-приложением Клиент JMS», с. 19)
Вход в JMS / Выход из JMS	Выполняет аутентификация пользователя в JMS / Прекращает сеанс работы пользователя с JMS
Остановить агент JMS / Запустить агент JMS	Позволяет остановить / запустить *службу клиентского агента JMS* (JWA) на текущей рабочей станции
О программе	Отображает общие сведения о JMS

Пункт	Описание
Выход	Выполняет выгрузку приложения JWA Tray из оперативной памяти компьютера. Значок в области уведомлений становится недоступен

3.1 Аутентификация в приложении JWA Tray

Для обеспечения возможности поддерживать в приложении JWA Tray электронные ключи пользователя в фоновом режиме, а также выполнять онлайн-монтирование скрытых разделов ЗНИ, в этом приложении следует аутентифицироваться.

Администратор JMS имеет возможность настроить автоматическую аутентификацию пользователя. Факт такой аутентификации отображается в меню:

- нажмите на значке правой кнопкой мыши;
- если в меню присутствует пункт **Выход из JMS** (Рис. 3), то аутентификация пользователя в JMS уже выполнена.

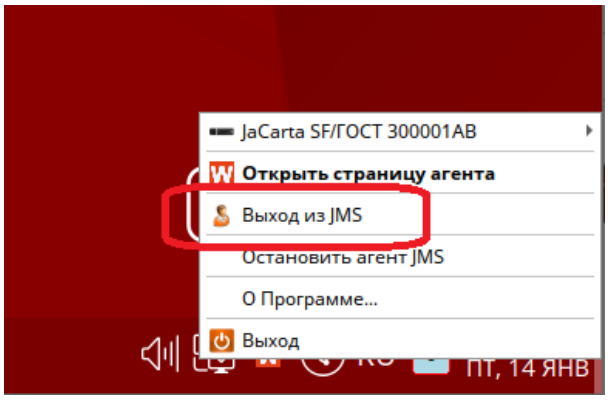


Рис. 3 – Отображение факта аутентификации пользователя в JMS

Если пользователь не аутентифицирован в JMS, выполните следующие действия.

1. Нажмите на значке правой кнопкой мыши и выберите **Вход из JMS** (Рис. 3).

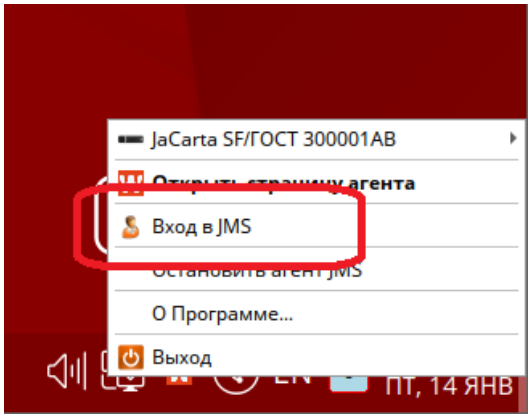


Рис. 4 – Вход в JMS

2. Отобразится окно с запросом аутентификационных данных.

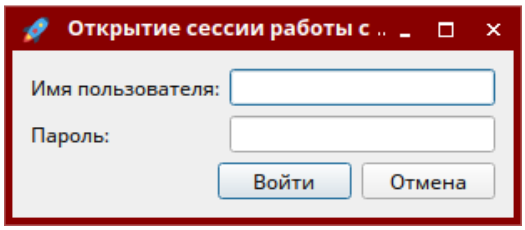


Рис. 5 – Окно ввода аутентификационных данных

3. В поле **Имя пользователя** введите логин пользователя в формате:

   <имя_ресурсной_системы>\<имя_пользователя>,

   Например:

```
DirectoryAlias\user
```

   Введите **Пароль** и нажмите **Войти**.

Примечание. Данные для аутентификации следует получить у администратора JMS.

В случае успешной аутентификации отобразится соответствующая подсказка в области уведомления, а меню JWA Tray приобретет вид с пунктом **Выход из JMS** (Рис. 3, с. 14)

3.2 Монтирование скрытых разделов SF/ГОСТ

Приложение JWA Tray позволяет монтировать скрытые диски RW и CD-ROM на электронном ключе JaCarta SF/ГОСТ (ЭН пользователя) как при открытом сеансе пользователя (после аутентификации пользователя в JMS), так и в отсутствии связи с сервером JMS (т.е. в автономном режиме).

3.2.1 Монтирование скрытых разделов дисков в режиме подключения к серверу JMS

Для монтирования скрытых разделов ЗНИ SF/ГОСТ в режиме подключения к серверу выполните следующие действия.

1. Подсоедините ЗНИ JaCarta SF/ГОСТ, на котором необходимо смонтировать скрытые разделы дисков, к компьютеру.
2. Выполните аутентификацию в приложении JWA Tray (см. «Аутентификация в приложении JWA Tray», с. 14).
3. В меню JWA Tray выберите зарегистрированный на ваше имя ЗНИ.

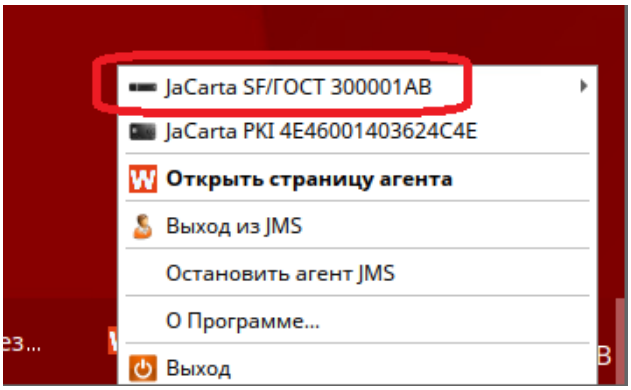


Рис. 6 – Выбор ЗНИ для монтирования скрытых разделов

Примечание. Описанное ниже монтирование скрытых разделов в режиме подключения к серверу в приложении JWA Tray возможно только для тех ЗНИ, которые были выпущены для аутентифицировавшегося пользователя. Если в режиме подключения к серверу будет выбран чужой ЗНИ, то процесс монтирования скрытых разделов потребует предъявления файла .kko, т.е. будет осуществляться по сценарию, описанному в разделе «Монтирование скрытых разделов дисков SF/ГОСТ в автономном режиме», с. 16.

4. В появившемся контекстном меню выберите **Монтировать скрытые разделы**.
5. Отобразится запрос на ввод PIN-кода пользователя данного ЗНИ.

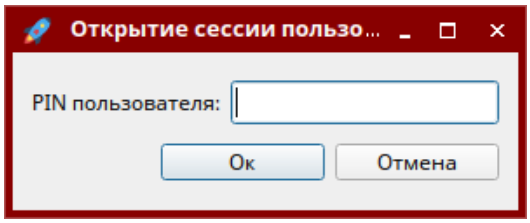


Рис. 7 – Запрос PIN-кода пользователя

6. Введите PIN-код пользователя и нажмите **Ок**.
7. По окончании монтирование отобразится сообщение следующего вида.

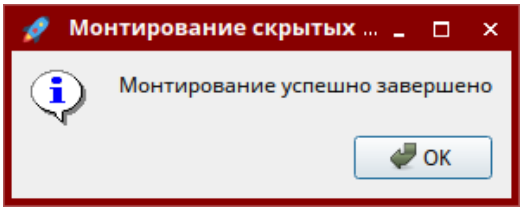


Рис. 8 – Сообщение об успешном монтировании скрытых разделов ЗНИ

8. Нажмите **OK**.

Скрытые разделы ЗНИ смонтированы на данном компьютере.

Для отключения скрытых разделов в меню JWA Tray выберите необходимый ЗНИ, как на Рис. 6 (с. 15), и нажмите **Размонтировать скрытые разделы**. В процессе размонтирования может также потребоваться ввод PIN-код пользователя.

3.2.2 Монтирование скрытых разделов дисков SF/ГОСТ в автономном режиме

Для монтирования скрытых разделов дисков ЗНИ SF/ГОСТ в автономном режиме у администратора доступа ЭН JaCarta SF/ГОСТ следует получить соответствующий файл ключевого контейнера с расширением .kko (*контейнер автономного монтирования скрытых дисков*).

Монтирование в автономном режиме осуществляется только тогда, когда аутентификация в JMS не выполнена (в меню JWA Tray отображается пункт **Вход в JMS**, как на Рис. 4, с. 14).

Чтобы смонтировать скрытые разделы в автономном режиме выполните следующие действия.

9. Подсоедините ЗНИ JaCarta SF/ГОСТ, на котором необходимо смонтировать скрытые разделы дисков, к компьютеру.

10. Не осуществляя аутентификации в JMS (т.е. не нажимая **Вход в JMS**), выберите в меню JWA Tray нужный ЗНИ.

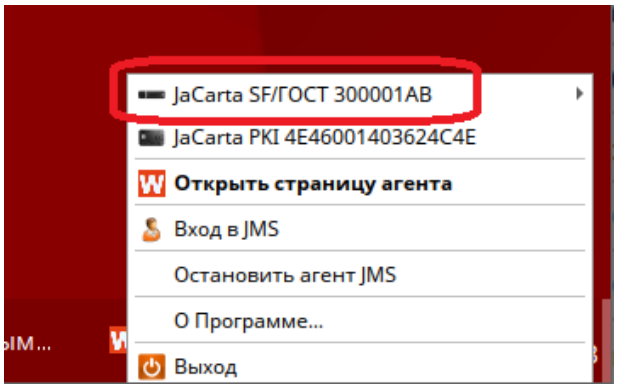


Рис. 9 – Выбор ЗНИ для монтирования скрытых разделов в автономном режиме

11. В появившемся контекстном меню выберите **Монтировать скрытые разделы**.
12. Отобразится запрос на ввод аутентификационной информации.

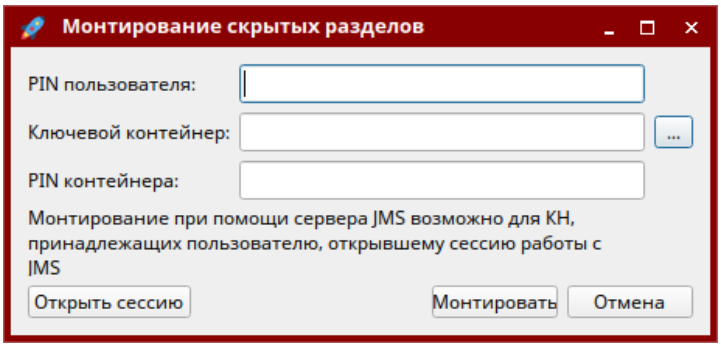


Рис. 10 – Запрос PIN-кода пользователя

Примечание. В случае если нажать кнопку **Открыть сессию**, следует выполнить аутентификацию пользователя в JMS, после чего монтирование скрытых разделов следует выполнять по сценарию, описанному в разделе «Монтирование скрытых разделов дисков в режиме подключения к серверу JMS», с. .15.

13. Введите PIN-код пользователя, нажмите кнопку ... и выберите полученный у администратора JMS файл ключевого контейнера .kko, введите его PIN-код и нажмите **Монтировать**.
14. По окончании монтирование отобразится сообщение следующего вида.

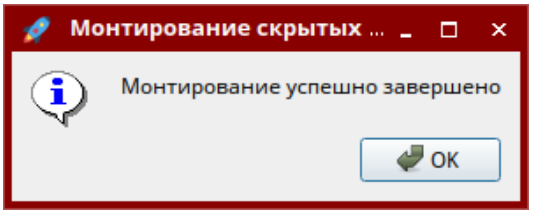


Рис. 11 – Сообщение об успешном монтировании скрытых разделов ЗНИ

15. Нажмите **OK**.

Скрытые разделы ЗНИ смонтированы на данном компьютере.

Для отключения скрытых разделов в меню JWA Tray выберите необходимый ЗНИ, как на Рис. 9 (с. 17), и нажмите **Размонтировать скрытые разделы**. В процессе размонтирования может также потребоваться ввод PIN-код пользователя

3.3 Выход из приложения JWA Tray

Для прекращения работы приложения JWA Tray на компьютере откройте его меню и нажмите **Выход**.

4. Порядок работы с web-приложением Клиент JMS

В данном разделе описаны способы работы с web-приложением Клиент JMS (далее web-клиент JMS).

Web-клиент JMS предназначен для выполнения расширенных пользовательских функций управления ЭК/ЗНИ/СДР, которые недоступны в базовом приложения JWA Tray, описанном в разделе 3, с. 12.

4.1 Запуск web-клиента JMS

4.1.1 Запуск из адресной строки

Для запуска web-клиента на компьютере выполните следующие действия.

1. Запустите веб-браузер Firefox.
2. В адресной строке введите у https://localhost:5600.
   Отобразится страница следующего вида.

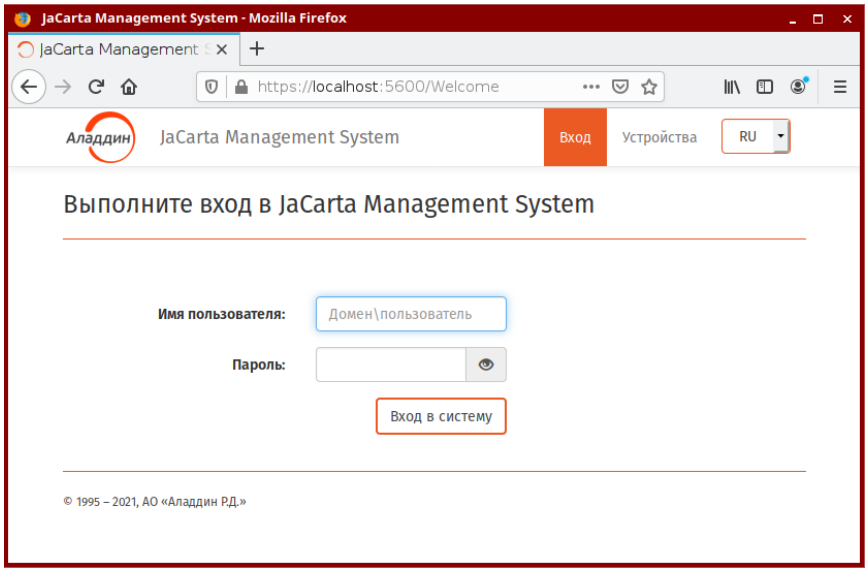


Рис. 12 – Стартовая страница Web-приложения Консоль управления JMS

4.1.2 Запуск из приложения JWA Tray

Если на компьютере установлено приложение JWA Tray, то web-клиент JMS можно запустить с помощью значка в области уведомлений (Рис. 13).

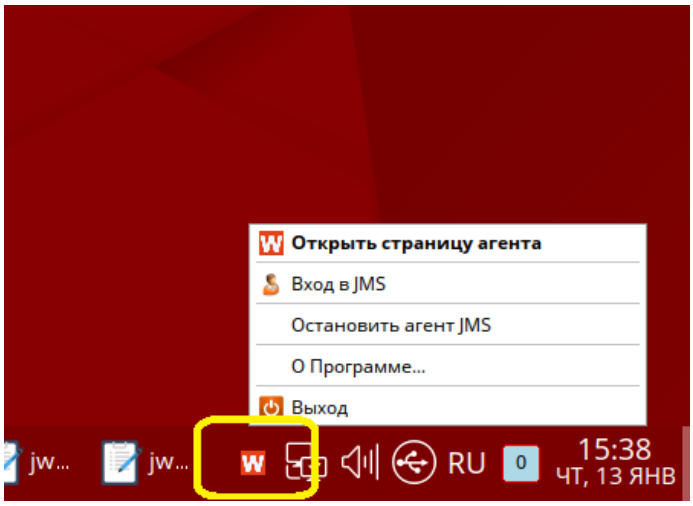


Рис. 13 – Использование меню JWA Tray для быстрого запуска web-клиента JMS

Для открытия web-клиента в браузере, установленном в ОС по умолчанию, нажмите на значке правой кнопкой мыши и выберите **Открыть страницу агента**.

(Полное описание меню приведено в Табл. 5, с. 13)

4.2 Открытие сеанса подключения к JMS

Чтобы открыть сеанс подключения к JMS, выполните следующие действия.

1. Откройте web-клиент JMS (см. раздел «Запуск web-клиента JMS», с. 19).
2. Отобразится страница аутентификации.

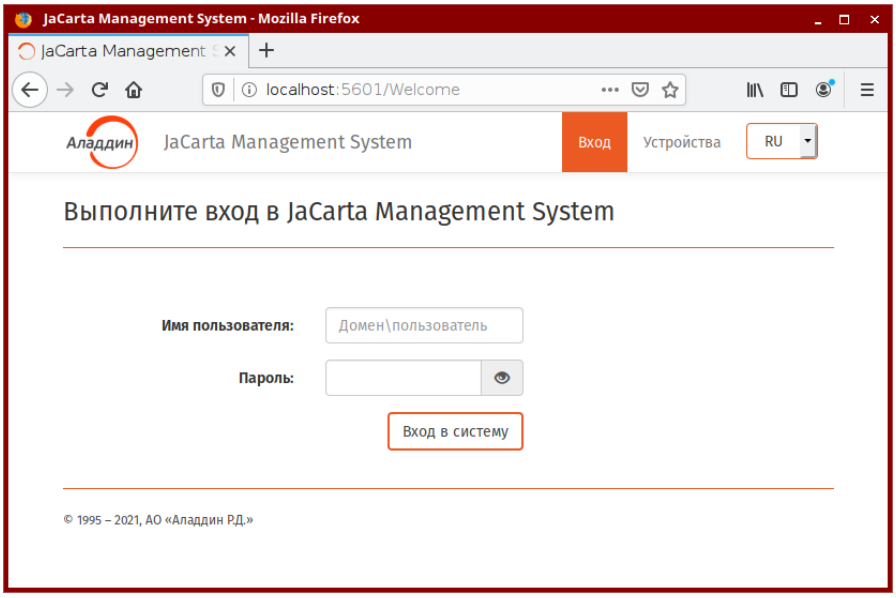


Рис. 14 – Страница аутентификации в JMS

3. В поле **Имя пользователя** введите логин пользователя в формате:
   `<имя_ресурсной_системы>\<имя_пользователя>`,

Например:

```
DirectoryAlias\user
```

Введите **Пароль** и нажмите **Войти**.

Примечание. Данные для аутентификации следует получить у администратора JMS.

4. Отобразится страница с открытой вкладкой **Устройства**.

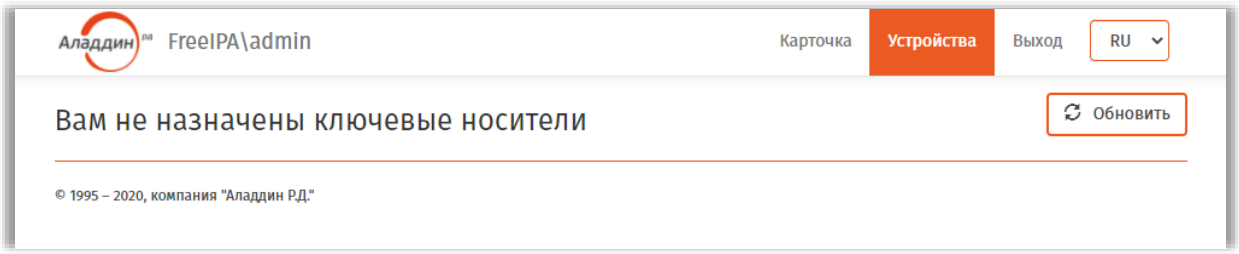


Рис. 15 – Открытый пользовательский сеанс работы с JMS

В результате выполненных действий на данной рабочей станции открыт сеанс подключения пользователя к JMS

4.3 Просмотр сведений об ЭК/ЗНИ/СДР и OTP-аутентификаторах

Чтобы просмотреть сведения о подсоединённом электронном ключе или о любом электронном ключе, который был назначен или выпущен на ваше имя, а также об используемых OTP-аутентификаторах выполните следующие действия.

1. Подсоедините электронный ключ, сведения о котором вы хотите просмотреть, к компьютеру.
2. Выполните вход в JMS из web-клиента (см. раздел «Открытие сеанса подключения к JMS», с. 20.
3. Выберите вкладку **Устройства** (устанавливается по умолчанию после аутентификации).
4. Сведения отобразятся в центральной части окна (см. рис. 16 и табл. 6 соответственно).

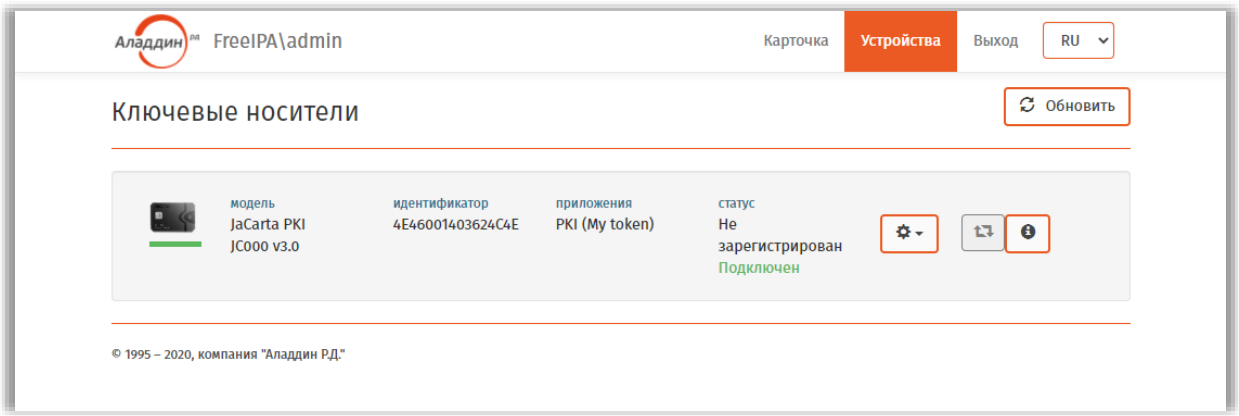


*Рис. 16 – Вкладка **Устройства***

Табл. 6 – Сведения на вкладке Устройства

Поле	Описание
Модель	Модель электронного ключа или тип OTP-аутентификатора
Идентификатор	Серийный номер электронного ключа или OTP-аутентификатора
Приложения	В случае ЭК отображается вид приложения/приложений ЭК (например, PKI) и метка ЭК (например, MyToken) В случае OTP-аутентификатора отображается имя пользователя, на которого зарегистрирован данный аутентификатор
Статус	Текущий статус электронного ключа / аутентификатора. Статус отображается двумя строками: • на первой строке отображается статус ЭК/ЗНИ/СДР/аутентификатора в JMS (например **Используется**, **Не зарегистрирован** и др.) • во второй строке отображается статус ЭК/ЗНИ/СДР по отношению к данному локальному компьютеру (например **Подключен**, **Не подключен**)
 (кнопка доступных операций)	При нажатии на кнопку открывается меню доступных действий с электронным ключом, среди которых (в зависимости от модели ЭК и его статуса) могут быть следующие: • **Выпустить** (только для ЭК)– позволяет осуществить выпуск электронного ключа (см. «Выпуск ЭК/ЗНИ» на стр. 23), ссылка отображается только в том случае, если подсоединённый электронный ключ ещё не выпущен и если самостоятельный выпуск разрешён настройками JMS; • **Сообщить об утере/поломке** – позволяет уведомить администраторов JMS об утере или поломке вашего электронного ключа, либо компрометации в случае OTP-аутентификатора (см. «Действия в случае утери или поломки ЭК/ЗНИ/СДР/OTP (отзыв электронного ключа)» на стр. 38); • **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 в JMS** – позволяет временно отключить возможность использования электронного ключа (см. «Отключение возможности использования ЭК/ЗНИ/СДР или OTP-аутентификатора» на стр. 36). • **Синхронизировать** – позволяет выполнить синхронизацию электронного ключа (см. «Синхронизация ЭК/ЗНИ» на стр. 31); • **Разблокировать <*Тип приложения*>** – позволяет разблокировать приложение указанного типа на электронном ключе. 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). • **Подключить скрытые диски с контейнером автономного монтирования** – действие предусмотрено только в отношении электронных ключей JaCarta SF/ГОСТ. Обеспечивает подключение скрытых дисков на ЭН пользователя даже в отсутствии подключения к серверу JMS (подробнее см. на стр.41).

Поле	Описание
	• **Подключить скрытые диски** – действие предусмотрено только в отношении электронных ключей JaCarta SF/ГОСТ. Обеспечивает подключение скрытых дисков на ЭН пользователя (подробнее см. на стр.40). • **Отключить скрытые диски** – действие предусмотрено только в отношении электронных ключей JaCarta SF/ГОСТ. Обеспечивает отключение скрытых дисков на ЭН пользователя (подробнее см. на стр.43). • **Изменить PIN-код** • **Изменить метку**
	Кнопка для выполнения синхронизации ЭК
	Кнопка получения расширенной информации об ЭК
	Кнопки управления монтированием скрытых разделов защищённого носителя информации (ЗНИ): Смонтировать... и Размонтировать...

4.4 Операции с ЭК/ЗНИ/СДР

Доступность тех или иных операций с ЭК/ЗНИ/СДР (далее – с электронными ключами) зависит от настроек, установленных администратором JMS. В случае возникновения вопросов относительно доступности для пользователя тех или иных действий обратитесь к администратору.

4.4.1 Выпуск ЭК/ЗНИ

Примечания:

1. Для выполнения этой процедуры вы должны иметь полномочия на самостоятельный выпуск электронных ключей. В случае отсутствия таких полномочий обратитесь к администратору.
2. Выпуск СДР ALO имеет некоторые особенности по сравнению с выпуском других электронных ключей, поэтому описание процедуры выпуска для СДР ALO вынесено в отдельный раздел «Выпуск СДР ALO», с.44.

Важно! Для выпуска ЗНИ JaCarta SF/ГОСТ данные электронные ключи должны быть подключены к компьютеру непосредственно, либо с помощью среды виртуализации, например средств виртуализации VMware. Не допускается подключение такого электронного ключа к компьютеру с клиентом JMS посредством *протокола удаленного рабочего стола* (Remote Desktop Protocol).

Чтобы самостоятельно выпустить электронный ключ, выполните следующие действия.

1. Подсоедините новый электронный ключ (т.е. ключ с заводскими настройками), который вы хотите выпустить, к компьютеру.

   Примечание. В случае ЗНИ SF/ГОСТ под новым электронным ключом подразумевается неинициализированный ЗНИ (т.е. ЗНИ с заводскими настройками).

2. Откройте сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS», с. 20)
3. Выберите вкладку **Устройства**.

4. Нажмите на кнопку настроек ( ) подсоединенного электронного ключа (Рис. 17), который вы хотите выпустить.

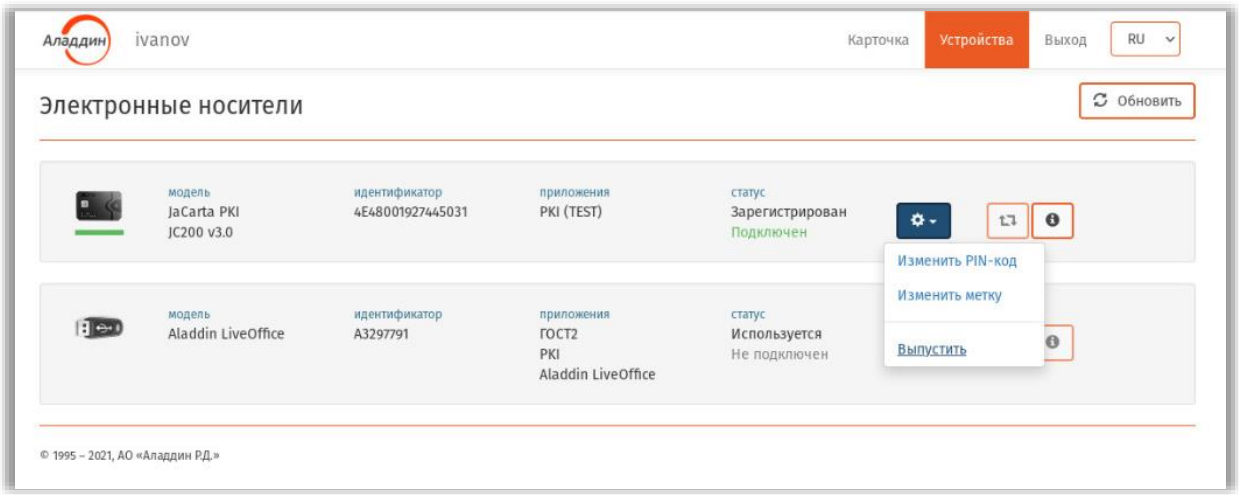


Рис. 17 – Выбор электронного ключа для выпуска

5. В появившемся меню выберите пункт **Выпустить**.
Отобразится страница следующего вида.

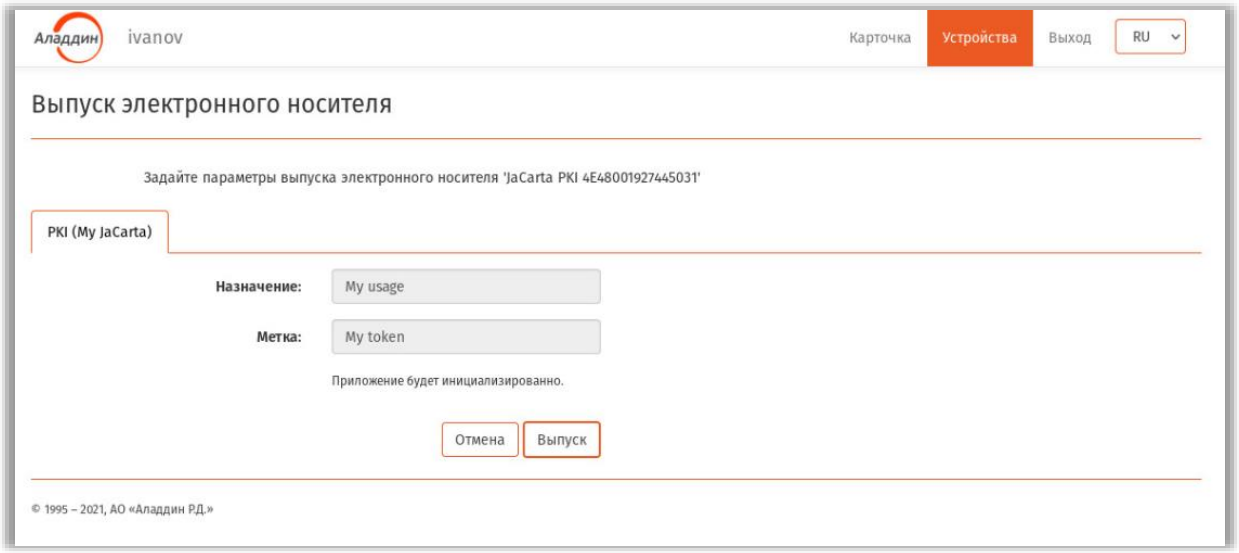


Рис. 18 – Страница задания редактируемых параметров

6. При необходимости отредактируйте значения полей **Назначение** и **Метка** (если доступно) и нажмите **Выпуск**.
7. Дождитесь окончания работы мастера (в случае запроса операционной системы действий, требующих согласия пользователя, дайте утвердительный ответ).

8. По окончании выпуска ЭК отобразится страница с отчетом о синхронизации (Рис. 19) .

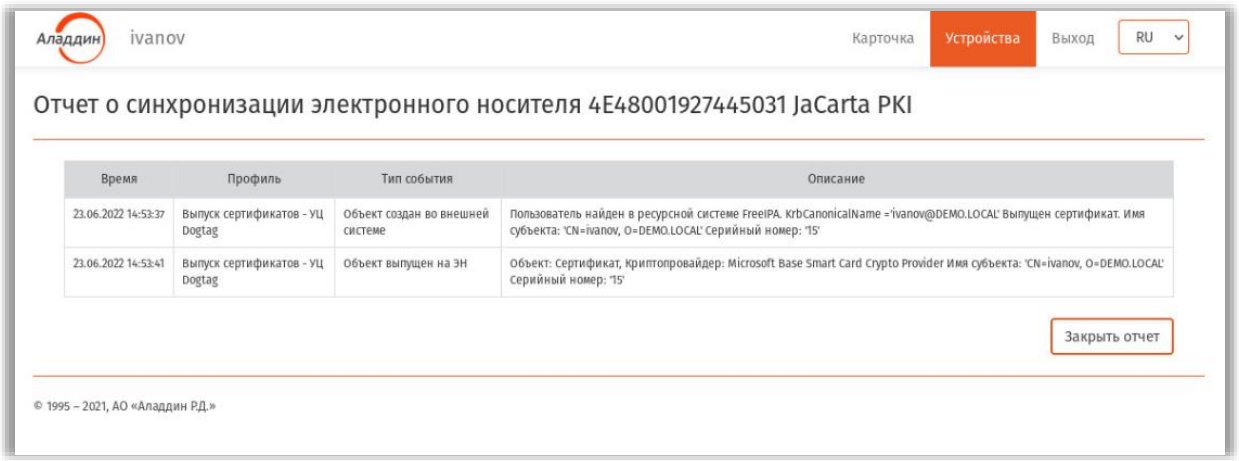


Рис. 19 – Страница с отчетом о синхронизации ЭК

9. Нажмите **Закрыть отчет**.

Выпущенный ключ будет отображаться на вкладке **Устройства** со статусом **Используется** (рис. 20).

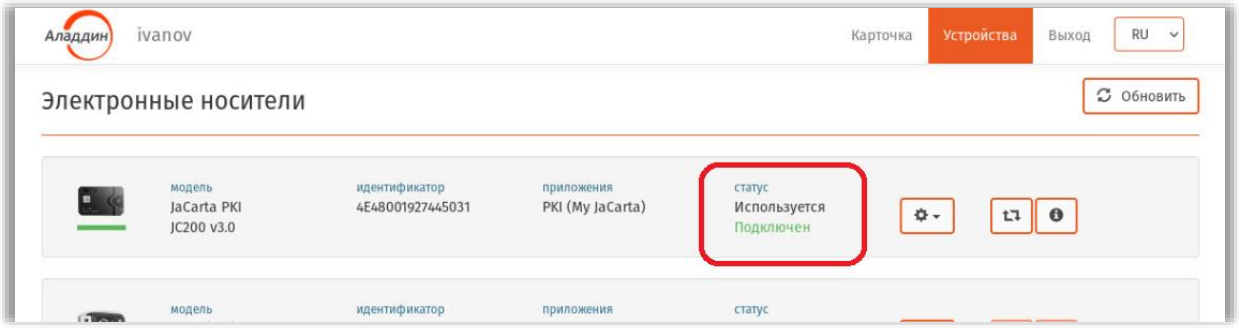


Рис. 20 – Статус выпущенного электронного ключа

4.4.2 Изменение метки в ЭК/ЗНИ

Примечание. Метка – изменяемый текстовый атрибут электронного ключа, может отображать особенности использования и принадлежности ключа, а также использоваться прикладным программным обеспечением.

Чтобы изменить метку электронного ключа, выполните следующие действия.

1. Подсоедините электронный ключ, в котором необходимо изменить метку, к компьютеру.
2. Откройте сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS», с. 20)
3. Выберите вкладку **Устройства**.
4. Нажмите на кнопку настроек ( ) подсоединенного электронного ключа (Рис. 21), с которым необходимо произвести операцию.

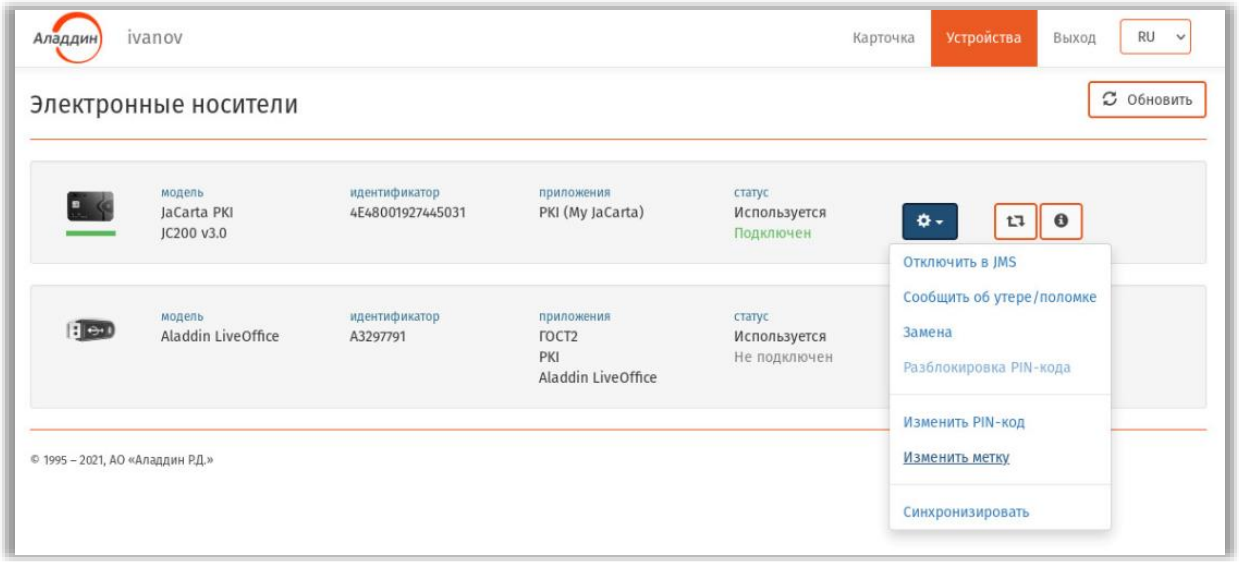


Рис. 21 – Выбор электронного ключа для смены метки

5. В появившемся меню выберите пункт **Изменить метку**.
   Отобразится страница следующего вида.

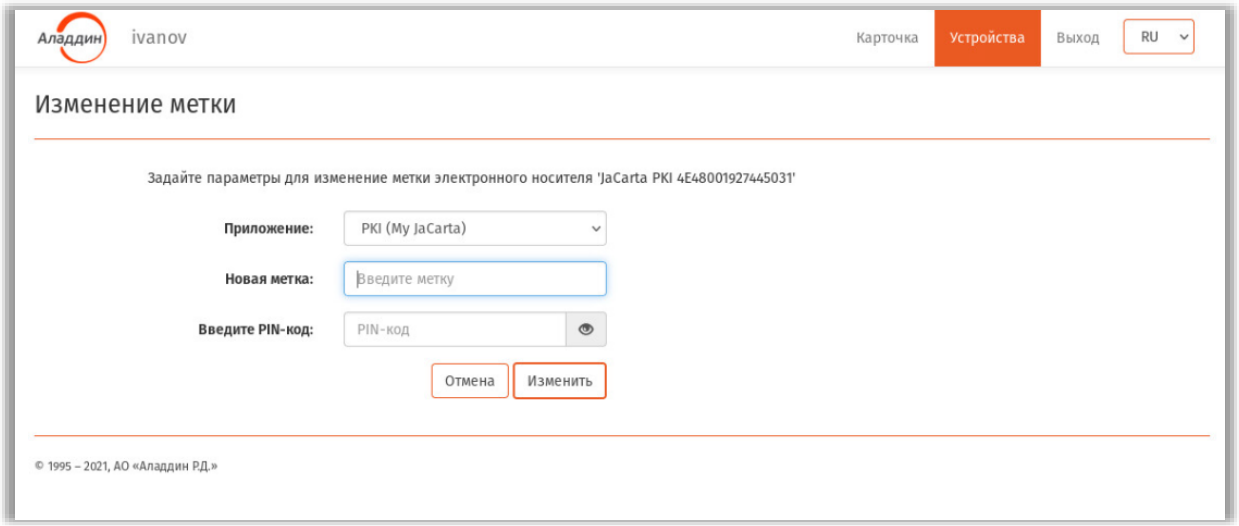


Рис. 22 – Страница ввода новой метки электронного ключа

6. Введите новое значение в поле **Новая метка**, введите **PIN-код пользователя** электронного ключа и нажмите **Синхронизация**.
7. Дождитесь окончания работы мастера.

8. По окончании операции в области уведомлений отобразится сообщение об успешной замене метки. При этом значение метки будет отображено в секции **Приложения** информации о ключе, как отображено на Рис. 23 .

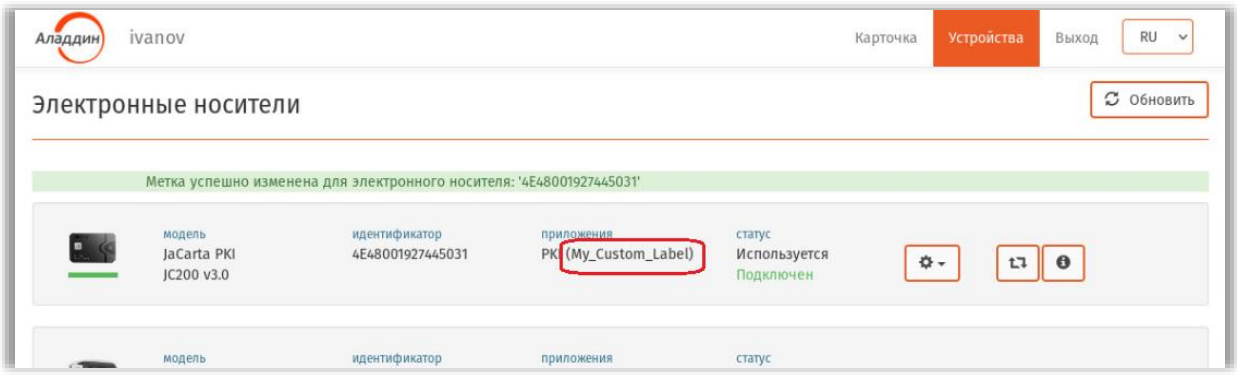


Рис. 23 – Уведомление об успешном изменении метки электронного ключа

4.4.3 Изменение PIN-кода пользователя в ЭК/ЗНИ

Чтобы изменить PIN-код пользователя в электронном ключе, выполните следующие действия.

1. Подсоедините электронный ключ, в котором необходимо изменить PIN-код пользователя, к компьютеру.
2. Откройте сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS», с. 20)
3. Выберите вкладку **Устройства**.
4. Нажмите на кнопку настроек ( ) подсоединенного электронного ключа (Рис. 24), с которым необходимо произвести операцию.

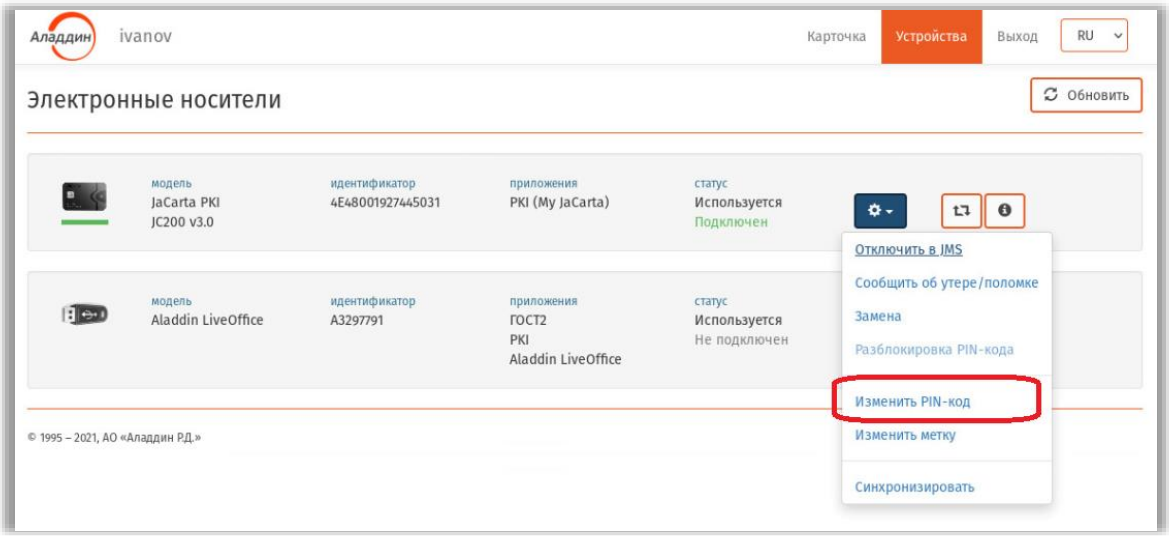


Рис. 24 – Выбор электронного ключа для изменения PIN-кода

5. В появившемся меню выберите пункт **Изменить PIN-код**.

Отобразится страница следующего вида.

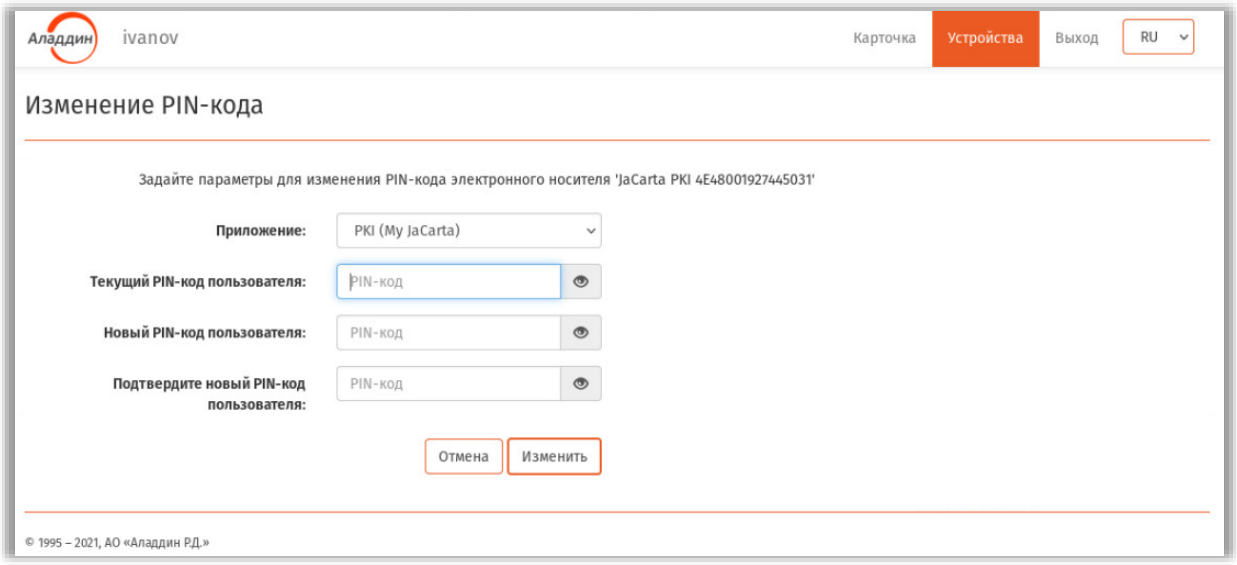


Рис. 25 – Страница смены PIN-кода пользователя в электронном ключе

6. Введите значения в полях **Текущий PIN-код пользователя**, **Новый PIN-код пользователя**, подтверждение нового PIN-кода и нажмите **Изменить**.

Примечания:

1. В случае если PIN-код пользователя изменяется впервые (текущее значение PIN-кода «по умолчанию» было установлено при выпуске электронного ключа), данное значение следует узнать у администратора JMS.
2. Требования к PIN-коду (минимальная длина, набор символов) следует узнать у системного администратора.
3. Запомните новый PIN-код или сохраните в защищённом месте. PIN-код используется для аутентификации пользователя при выполнении операций с электронным ключом или для входа во внешние информационные системы.

7. Дождитесь окончания работы мастера.
8. По окончании операции в области уведомлений отобразится сообщение об успешном изменении PIN-кода (Рис. 26).

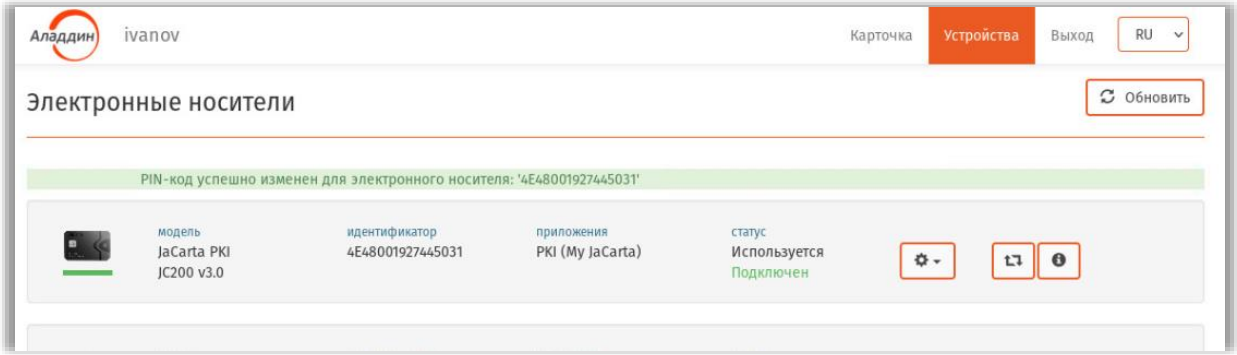


Рис. 26 – Уведомление об успешном изменении PIN-кода пользователя в электронном ключе

4.4.4 Разблокировка PIN-кода пользователя в ЭК

В случае превышения попыток ввода PIN-кода при аутентификации в электронном ключе происходит его блокировка (блокировка PIN-кода пользователя). Выполнив аутентификацию в Web-клиенте JMS, пользователь может самостоятельно разблокировать PIN-код. При определенных настройках такая разблокировка допускается только при наличии контакта (по телефонному или другому каналу связи) с администратором JMS.

Чтобы разблокировать PIN-код пользователя в электронном ключе, выполните следующие действия.

1. Подсоедините электронный ключ, в котором необходимо разблокировать PIN-код пользователя, к компьютеру.
2. Откройте сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS», с. 20)
3. Выберите вкладку **Устройства**.
4. Нажмите на кнопку настроек ( ) подсоединенного электронного ключа (Рис. 24), с которым необходимо произвести операцию. (Электронный ключ с заблокированным PIN-кодом отображается красным цветом текста в секции **Приложения**)

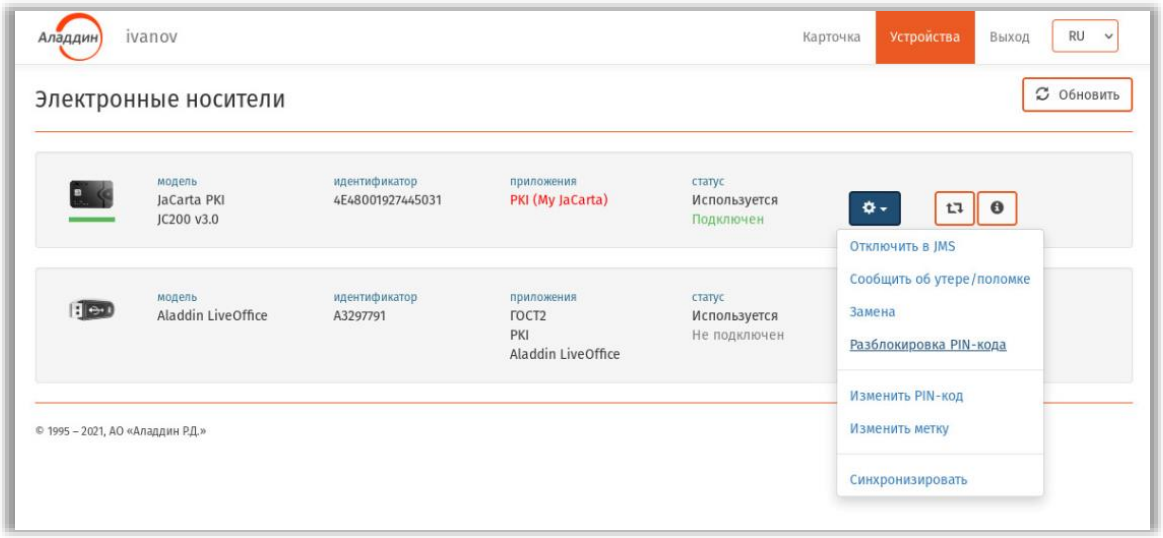


Рис. 27 – Выбор электронного ключа для разблокировки PIN-кода

5. В появившемся меню выберите пункт **Разблокировка PIN-кода**.

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

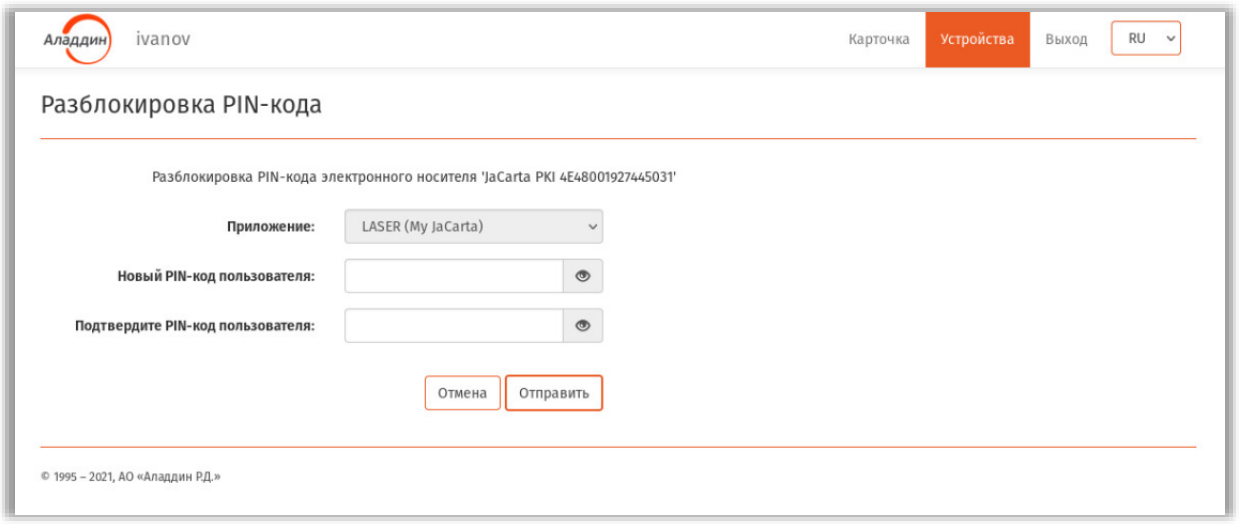


Рис. 28 – Страница для случая автоматической разблокировки PIN-кода

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

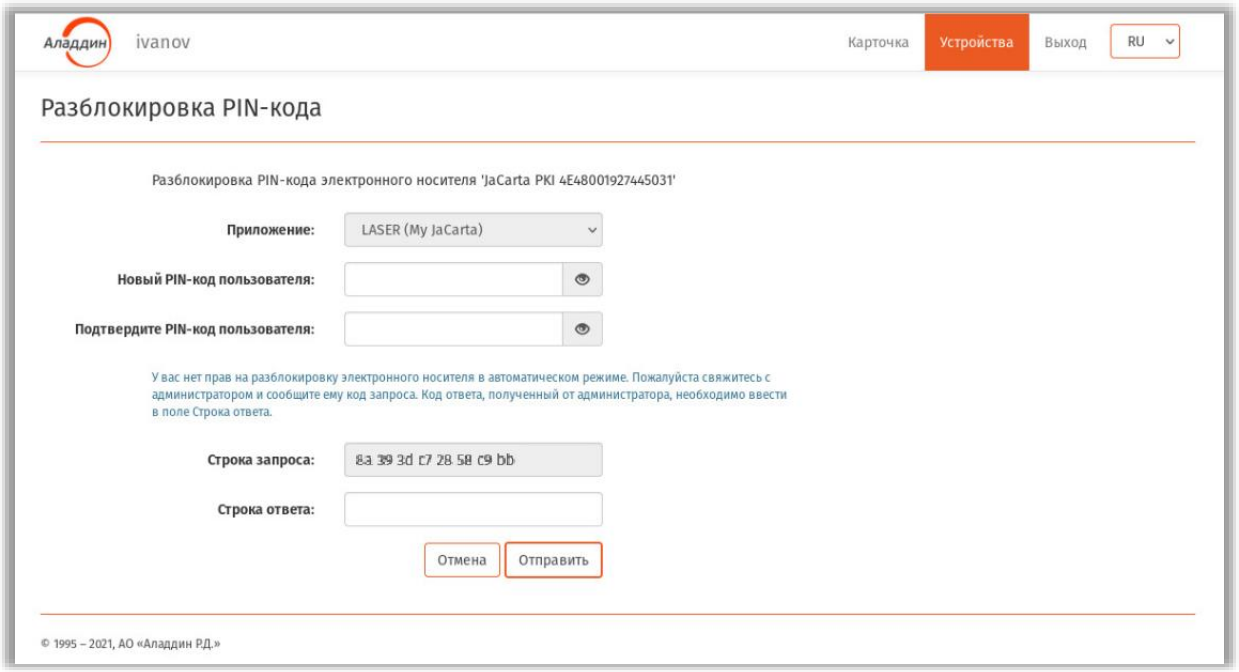


Рис. 29 – Страница ввода строки запроса для разблокировки PIN-кода

6. В полях **Новый PIN-код пользователя** и **Подтвердите PIN-код пользователя** введите значение PIN-кода пользователя.
7. В случае автоматической разблокировки (Рис. 28) переходите к шагу 11.
8. В случае разблокировки с участием администратора (Рис. 29) свяжитесь с администратором для разблокировки электронного ключа (например, по телефону) и сообщите ему код запроса, отображаемый в поле **Строка запроса**.
9. Администратор сообщит вам код ответа.

10. Введите код ответа в поле **Строка ответа**.
11. Нажмите **Отправить**.
12. Дождитесь окончания работы мастера.
13. По окончании операции в области уведомлений отобразится сообщение об успешной разблокировке электронного ключа.

Разблокированный электронный ключ готов к дальнейшей эксплуатации.

4.4.5 Уведомление о необходимости синхронизировать электронный ключ

В случае если в системе JMS были установлены новые настройки для электронного ключа после его выпуска для пользователя, в интерфейсе Клиента JMS такой электронный ключ выделяется красным индикатором и дополнительной строкой статуса *Требуется синхронизация*:

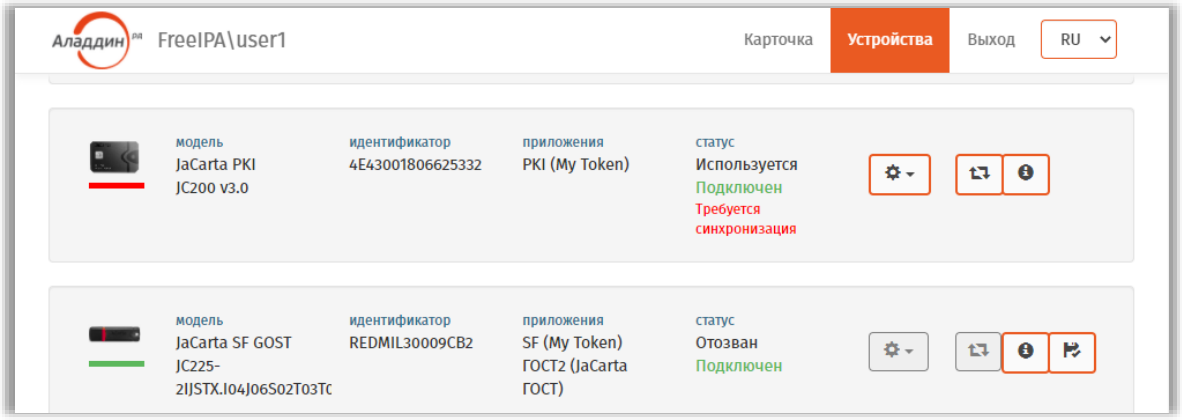


Рис. 30 – Уведомление пользователя о необходимости синхронизировать электронный ключ

Для синхронизации электронного ключа выполните действия, приведенные в разделе «Синхронизация ЭК/ЗНИ», ниже.

4.4.6 Синхронизация ЭК/ЗНИ

Примечание. Синхронизация СДР ALO имеет некоторые особенности по сравнению с синхронизацией других электронных ключей, поэтому описание процедуры синхронизации для СДР ALO вынесено в отдельный раздел «Синхронизация СДР ALO», с.49.

Чтобы синхронизировать электронный ключ, выполните следующие действия.

1. Подсоедините электронный ключ, который вы хотите синхронизировать, к компьютеру.
2. Откройте сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS», с. 20)
3. Выберите вкладку **Устройства**.
4. Нажмите на кнопку настроек ( ) подсоединенного электронного ключа (Рис. 31), который вы хотите синхронизировать.

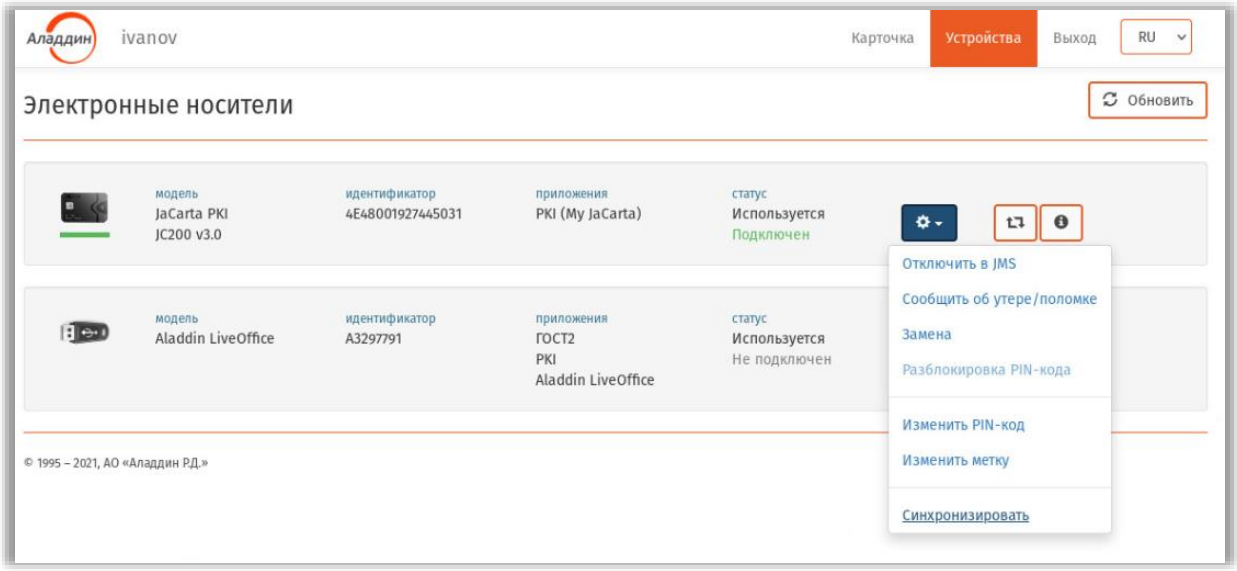


Рис. 31 – Выбор электронного ключа для синхронизации

5. В появившемся меню выберите пункт **Синхронизировать** (для синхронизации можно также воспользоваться кнопкой синхронизации). Отобразится страница следующего вида.

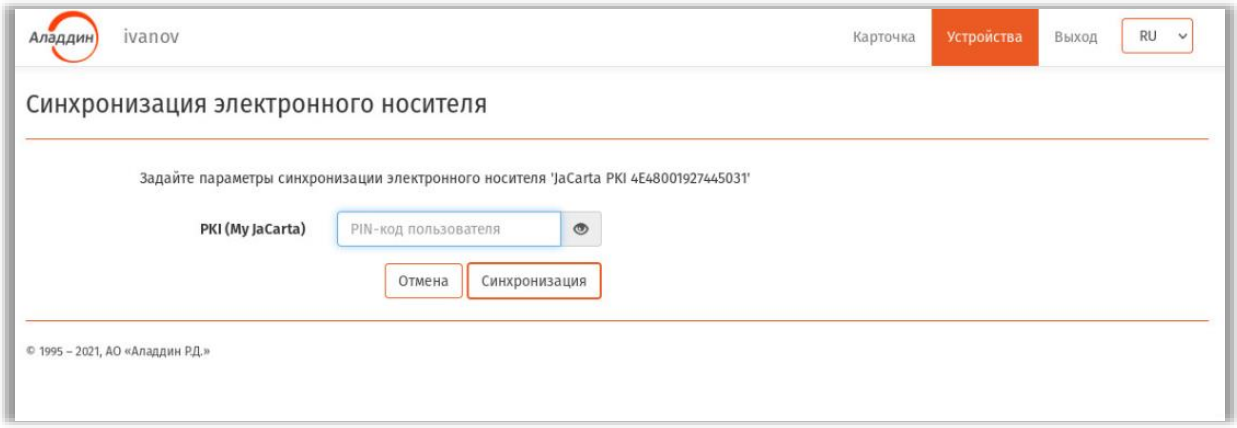


Рис. 32 – Страница синхронизации электронного ключа

6. Введите **PIN-код пользователя** электронного ключа и нажмите **Синхронизация**.
7. Дождитесь окончания работы мастера.
8. По окончании синхронизации электронного ключа отобразится страница с отчетом о синхронизации (Рис. 19, с. 25) .
9. Нажмите **Закрыть отчет**.

Синхронизированный электронный ключ будет отображаться на вкладке **Устройства** со статусом **Используется** (Рис. 33).

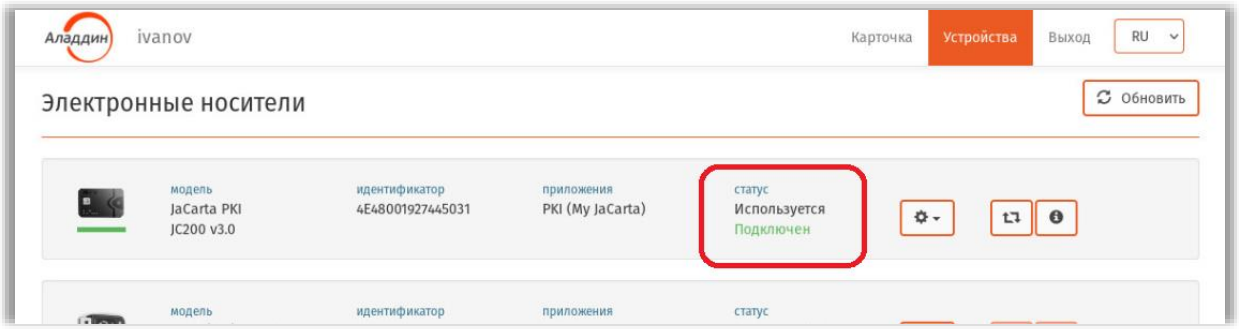


Рис. 33 – Отображение синхронизированного электронного ключа

При синхронизации ЗНИ JaCarta SF/ГОСТ в случае предопределенного настройками обновления встроенного ПО (прошивки ЗНИ) или ISO-образа необходимо подтвердить согласие на эту операцию.

Прежде чем дать согласие на обновление в ЗНИ встроенного ПО, убедитесь, что сделана копия хранящихся на ЗНИ данных для предотвращения их утраты.

Важно! По окончании синхронизации ЗНИ JaCarta SF/ГОСТ, в случае если в нем было произведено обновление встроенного ПО, следует отключить и затем заново подключить ЗНИ к компьютеру с тем, чтобы обеспечить дальнейшую корректную работу с данным ЗНИ.

4.4.7 Замена ЭК/СДР

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

Примечание. Для выполнения этой процедуры вы должны иметь полномочия на самостоятельную замену электронных ключей. В случае отсутствия таких полномочий обратитесь к администратору.

Важно! Для замены СДР ALO новый электронный ключ должен быть подключен к компьютеру непосредственно, либо с помощью среды виртуализации, например средств виртуализации VMware. Не допускается подключение такого электронного ключа к компьютеру с клиентом JMS посредством *протокола удаленного рабочего стола* (Remote Desktop Protocol).

Чтобы произвести замену электронного ключа, выполните следующие действия.

1. Подсоедините новый электронный ключ (т.е. ключ с заводскими настройками), на который вы хотите ранее выпущенный в JMS ключ, к компьютеру.
2. Откройте сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS», с. 20)
3. Выберите вкладку **Устройства**.
4. Нажмите на кнопку настроек ( ) подсоединенного электронного ключа (Рис. 34), которым вы хотите заменить ранее выпущенный.

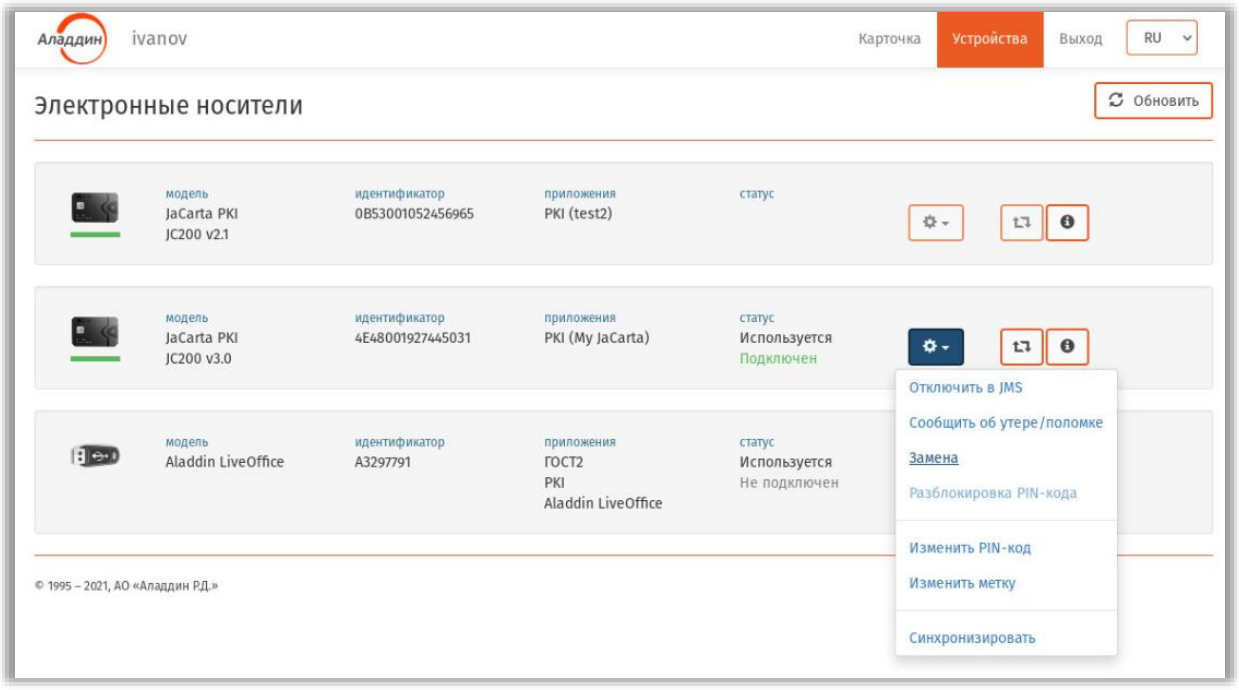


Рис. 34 – Выбор электронного ключа для замены ранее выпущенного в JMS

5. В появившемся меню выберите пункт **Замена**.
   Отобразится страница следующего вида.

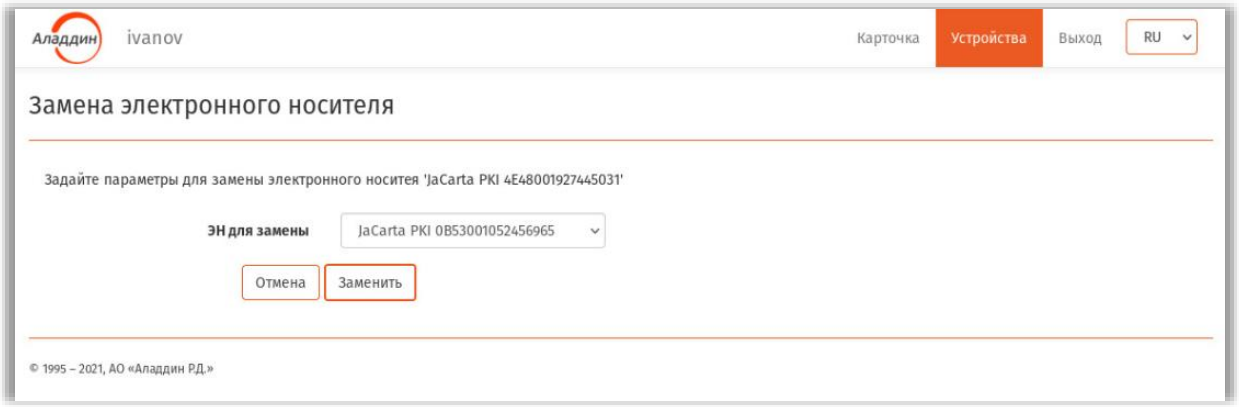


Рис. 35 – Страница выбора электронного ключа, подлежащего замене

6. В поле **ЭН для замены** выберите ранее выпущенный в JMS электронный ключ, подлежащий замене и нажмите **Заменить**.

Отобразится страница следующего вида.

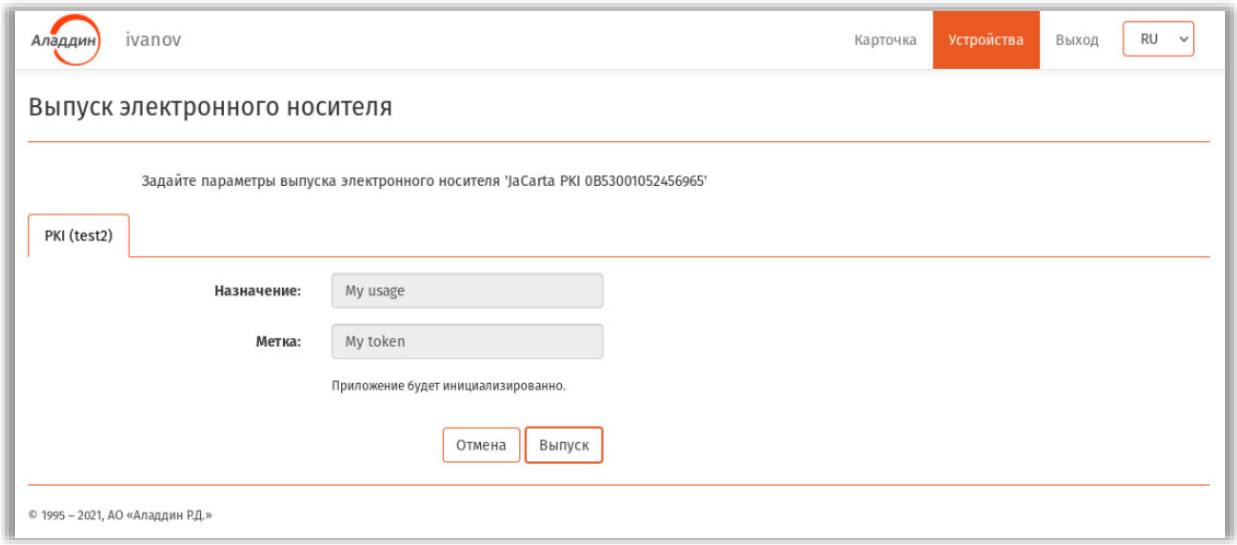


Рис. 36 – Страница задания редактируемых параметров

7. При необходимости отредактируйте значения полей **Назначение** и **Метка** (если доступно) для нового электронного ключа и нажмите **Выпуск**.
8. Дождитесь окончания работы мастера (в случае запроса операционной системы действий, требующих согласия пользователя, дайте утвердительный ответ).
9. По окончании выпуска ЭК отобразится страница с отчетом о синхронизации (Рис. 19, с. 25).
10. Нажмите **Закрыть отчет**.
    Отобразится страница следующего вида.

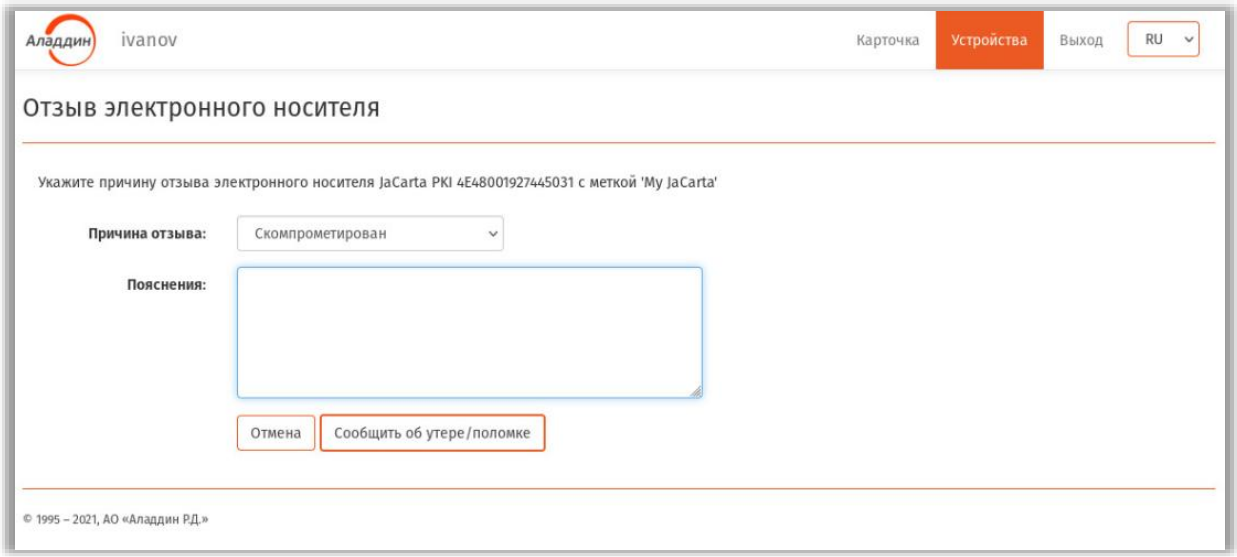


Рис. 37 – Страница отзыва электронного ключа

11. Выберите значение в поле **Причина отзыва** для заменяемого электронного ключа и введите свой комментарий о причине отзыва в поле **Пояснение**, после чего нажмите **Сообщить об утере/поломке**.

Выпущенный на замену электронный ключ будет отображаться на вкладке **Устройства** со статусом **Используется**, в то время как замененный ключ будет отображаться со статусом **Отозван** (Рис. 38).

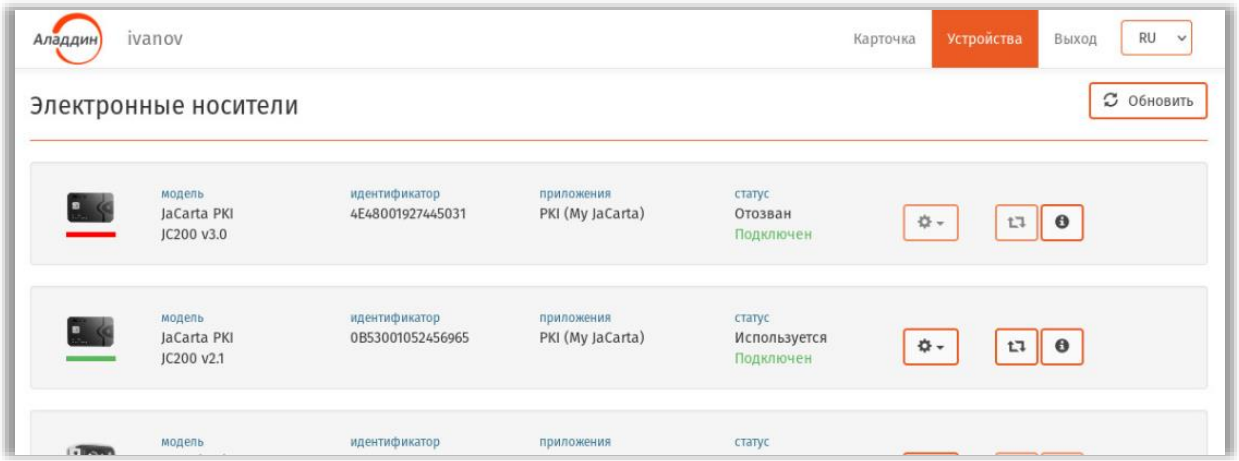


Рис. 38 – Статус электронных ключей по завершении процедуры замены

4.4.8 Отключение возможности использования ЭК/ЗНИ/СДР или OTP-аутентификатора

Чтобы на время отключить возможность использования электронного ключа или OTP-аутентификатора, выполните следующие действия.

Примечание. Для отключения возможности использования ЭК/ЗНИ/СДР, последний не обязательно подсоединять к компьютеру. Операция может быть выполнена без подсоединения ЭК/ЗНИ/СДР.

После отключения возможности использования электронного ключа или OTP-аутентификатора включить такую возможность может только администратор.

Чтобы отключить электронный ключ или OTP-аутентификатор, выполните следующие действия.

1. Откройте сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS», с. 20)
2. Выберите вкладку **Устройства**.
3. Нажмите на кнопку настроек ( ) ЭК/аутентификатора (Рис. 39), который вы хотите отключить.

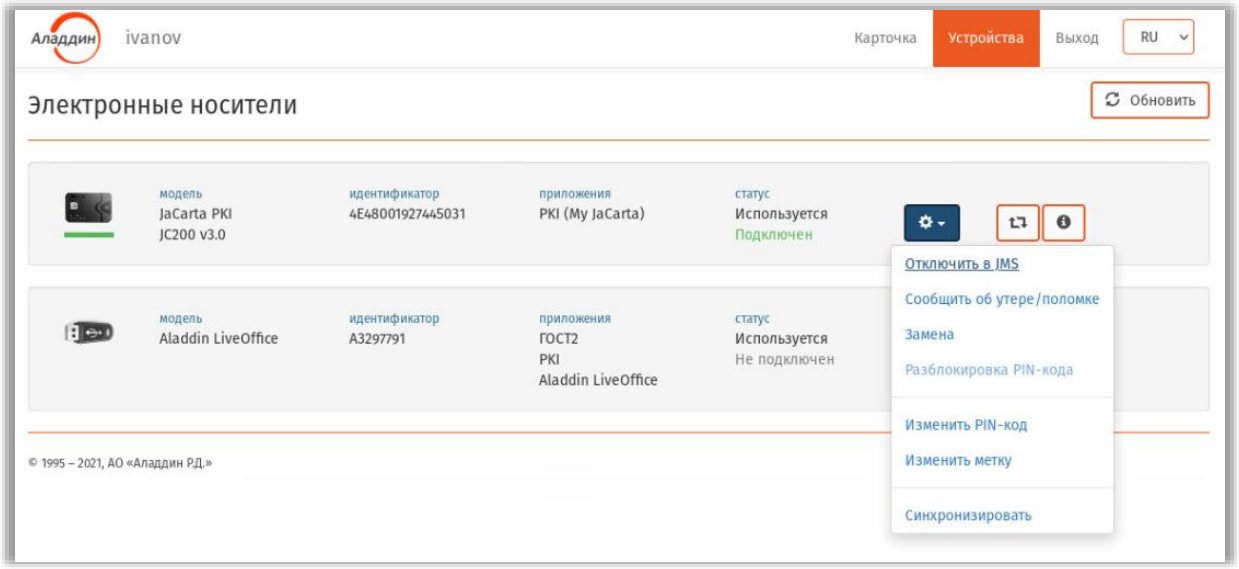


Рис. 39 – Выбор электронного ключа для отключения

4. В появившемся меню выберите пункт **Отключить в JMS**.
   Отобразится страница следующего вида.

Рис. 40 – Страница отключения электронного ключа

5. Нажмите **Отключить**.
6. Дождитесь окончания работы мастера.

Отключенный ЭК/аутентификатор будет отображаться на вкладке **Устройства** со статусом **Отключен в JMS** (Рис. 41).

Примечание. Статус **Подключен** на Рис. 41 отображает состояние ключа по отношению к локальному компьютеру.

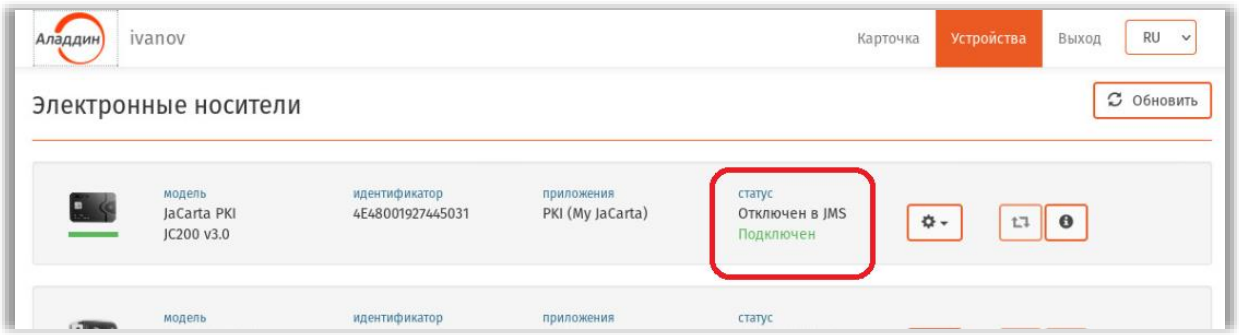


Рис. 41 – Отображение электронного ключа, отключенного в JMS

4.4.9 Действия в случае утери или поломки ЭК/ЗНИ/СДР/OTP (отзыв электронного ключа)

Чтобы сообщить об утере или поломке ЭК/ЗНИ/СДР или компрометации OTP-аутентификатора, выполните следующие действия.

Примечание. Для отзыва ЭК/ЗНИ/СДР, электронный ключ не обязательно подсоединять к компьютеру. Операция может быть выполнена без подсоединения.

1. Откройте сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS», с. 20)
2. Выберите вкладку **Устройства**.
3. Нажмите на кнопку настроек ( ) утраченного или неисправного электронного ключа или скомпрометированного OTP-аутентификатора (Рис. 42).

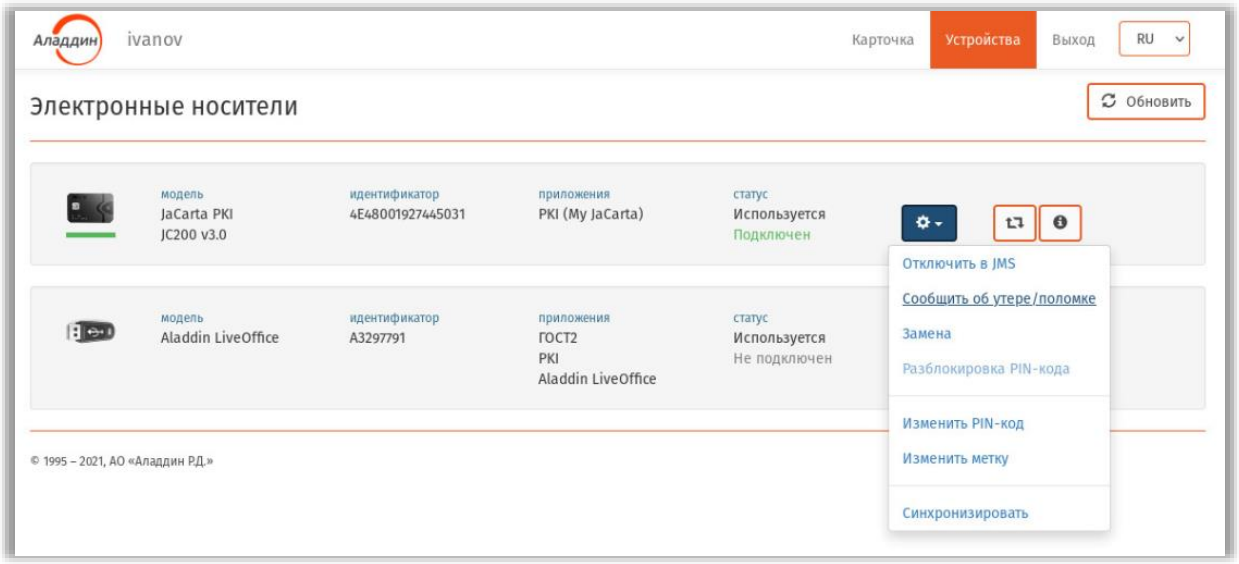


Рис. 42 – Выбор электронного ключа для монтирования скрытых разделов

4. В появившемся меню выберите пункт **Сообщить об утере/поломке**.

Отобразится страница следующего вида.

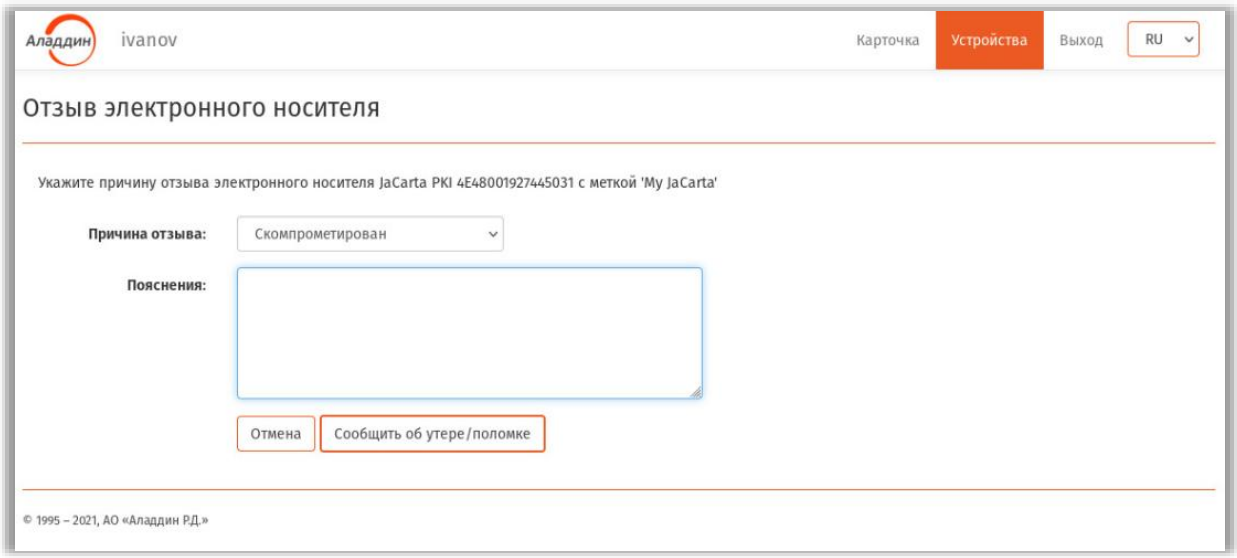


Рис. 43 – Страница отзыва электронного ключа

5. Выберите значение в поле **Причина отзыва** и введите свой комментарий о причине отзыва электронного ключа в поле **Пояснение**, после чего нажмите **Сообщить об утере/поломке**.
6. Дождитесь окончания работы мастера.

У отозванного электронного ключа изменится статус на **Отозван** (Рис. 44).

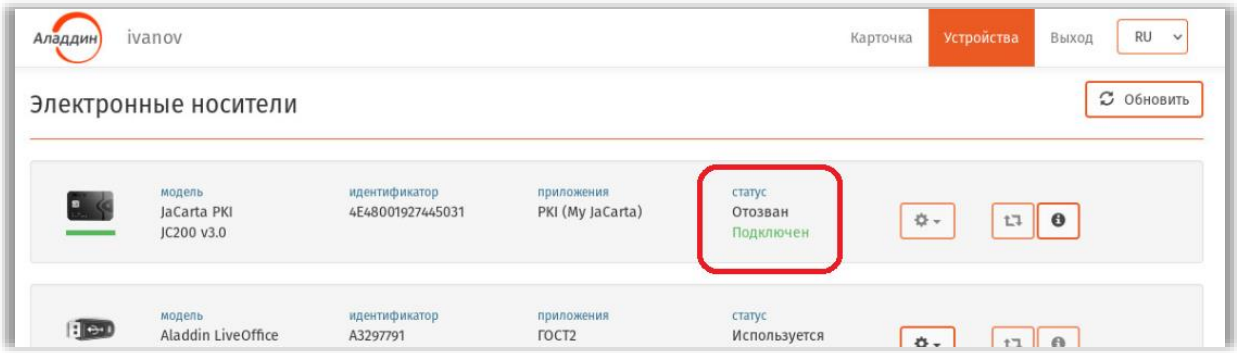


Рис. 44 – Отображение статуса отозванного электронного ключа

Отозванный ЭК/аутентификатор больше не сможет быть использован в системе JMS и связанных с ней внешних системах.

4.5 Особенности работы с ЗНИ SF/ГОСТ

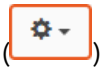
4.5.1 Монтирование скрытых разделов SF/ГОСТ

Web-клиент JMS позволяет монтировать скрытые диски RW и CD-ROM на электронном ключе JaCarta SF/ГОСТ (ЭН пользователя) как при открытом сеансе пользователя (после

аутентификации пользователя в JMS), так и в отсутствии связи с сервером JMS (т.е. в автономном режиме).

4.5.1.1 Монтирование скрытых разделов дисков в режиме подключения к серверу JMS

Для монтирования скрытых разделов ЗНИ SF/ГОСТ в режиме подключения к серверу выполните следующие действия.

1. Подсоедините электронный ключ JaCarta SF/ГОСТ, на котором необходимо смонтировать скрытые разделы дисков, к компьютеру.
2. Откройте сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS», с. 20)
3. Выберите вкладку **Устройства**.
4. Нажмите на кнопку настроек () подсоединенного электронного ключа (Рис. 45), на котором нужно смонтировать скрытые разделы.

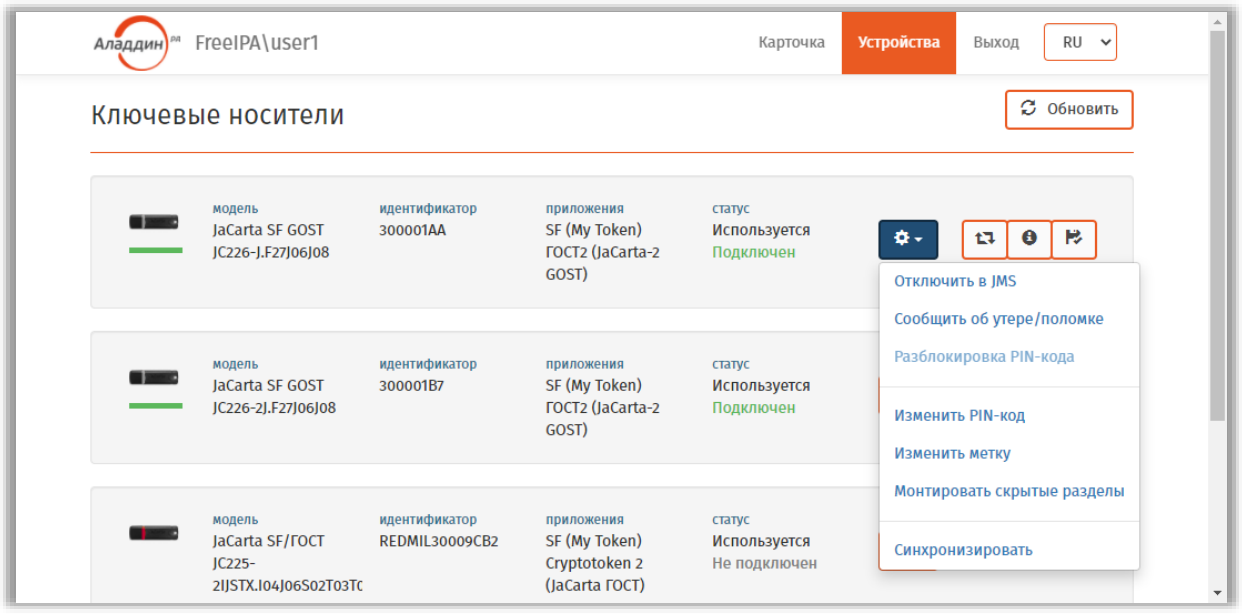


Рис. 45 – Выбор электронного ключа для монтирования скрытых разделов

5. В появившемся меню выберите пункт **Монтировать скрытые разделы** или нажмите кнопку  (**Монтировать скрытые разделы ключевого носителя)**.
6. На странице монтирования скрытых разделов (Рис. 46) введите PIN-код пользователя ЭК JaCarta SF/ГОСТ и нажмите **Монтировать**.

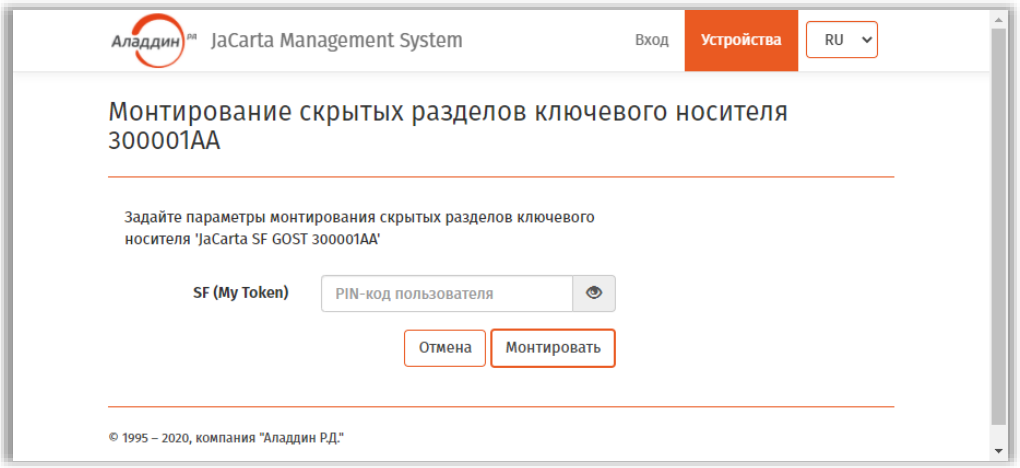


Рис. 46 – Страница монтирования скрытых разделов

7. Дождитесь окончания работы мастера.

У электронного ключа со смонтированными скрытыми разделами изменится значок состояния скрытых дисков (Рис. 47) на статус «Смонтированы» ( ).

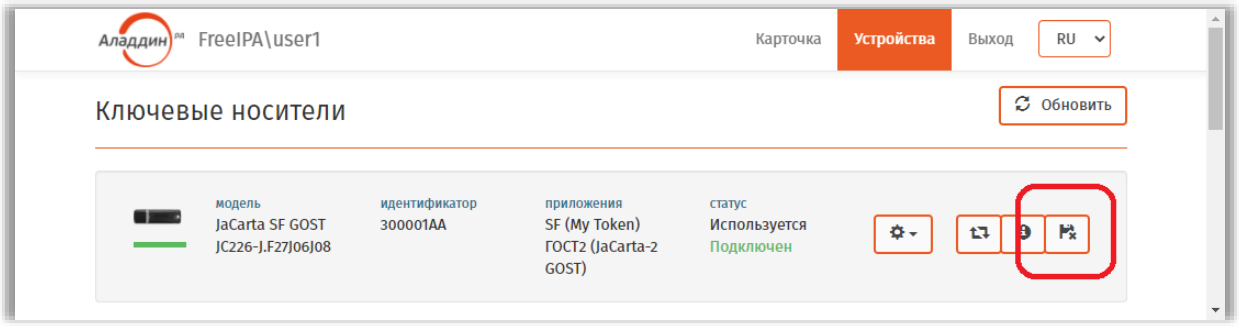


Рис. 47 – Отображение электронного ключа со смонтированными скрытыми разделами

После автоматического монтирования скрытых разделов они будут готовы к использованию.

4.5.1.2 Монтирование скрытых разделов дисков SF/ГОСТ в автономном режиме

Для монтирования скрытых разделов дисков ЗНИ SF/ГОСТ в автономном режиме у администратора доступа ЭН JaCarta SF/ГОСТ следует получить соответствующий файл ключевого контейнера с расширением .kko (*контейнер автономного монтирования скрытых дисков*).

Чтобы смонтировать скрытые разделы в автономном режиме выполните следующие действия.

1. Подсоедините электронный ключ JaCarta SF/ГОСТ, на котором необходимо смонтировать скрытые разделы дисков, к компьютеру.
2. Откройте web-клиент JMS (см. «Запуск web-клиента JMS», с. 19)
3. Не осуществляя аутентификации в JMS (т.е. не нажимая **Вход**), выберите вкладку **Устройства**.
4. Нажмите на кнопку настроек ( ) подсоединенного электронного ключа (Рис. 48), на котором нужно смонтировать скрытые разделы.

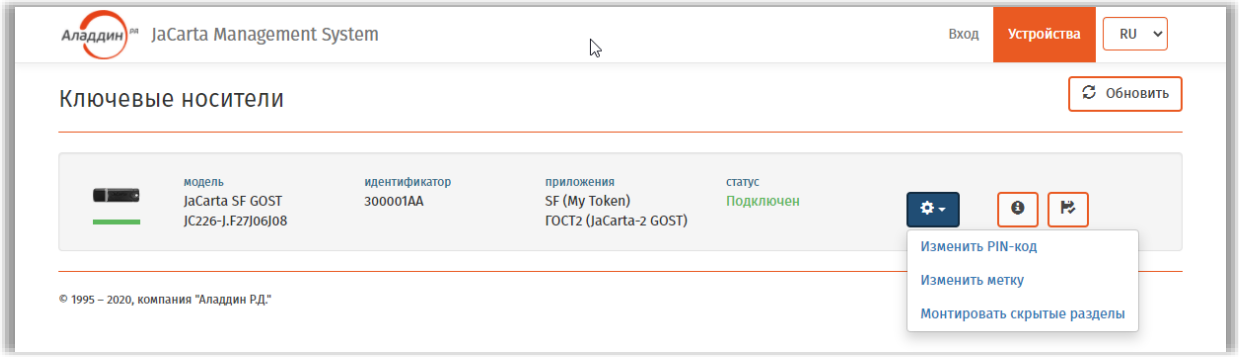


Рис. 48 – Выбор электронного ключа для монтирования скрытых разделов

5. В появившемся меню выберите пункт **Монтировать скрытые разделы** или нажмите кнопку (**Монтировать скрытые разделы ключевого носителя)**.
6. На странице монтирования скрытых разделов (Рис. 49) выполните следующие действия:

6.1. Введите PIN-код пользователя ЭК JaCarta SF/ГОСТ.
6.2. Выберите контейнер kko для монтирования скрытых дисков в автономном режиме (для вызова окна выбора нажмите значок)
6.3. Введите PIN-код контейнера для монтирования скрытых дисков в автономном режиме.
6.4. Нажмите кнопку **Монтирование**.

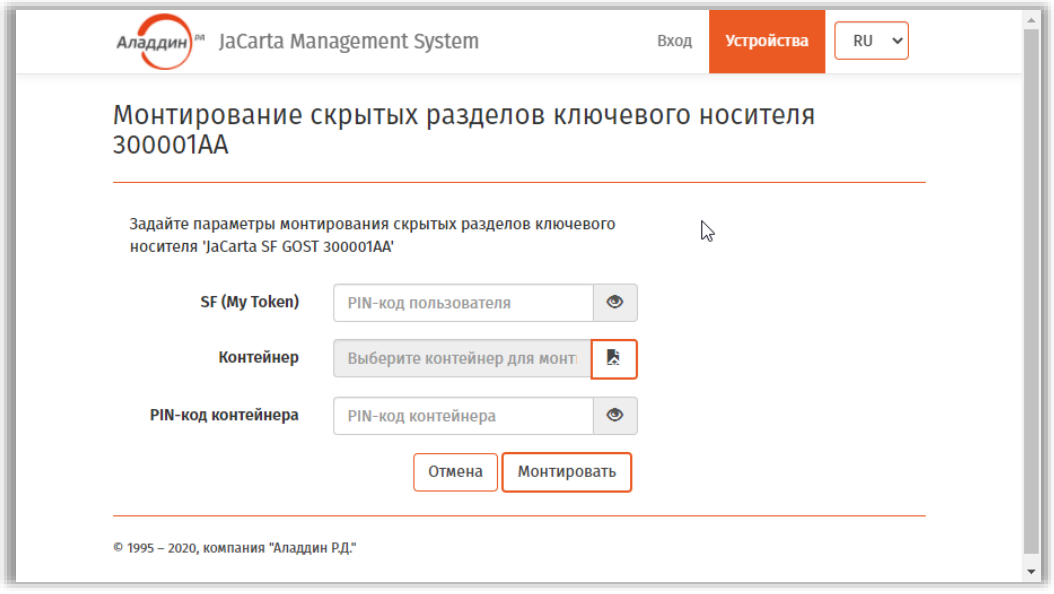


Рис. 49 – Страница монтирования скрытых разделов в автономном режиме

7. Дождитесь окончания работы мастера.

У электронного ключа со смонтированными скрытыми разделами изменится значок состояния скрытых дисков (Рис. 50) на статус «Смонтированы» ( ).

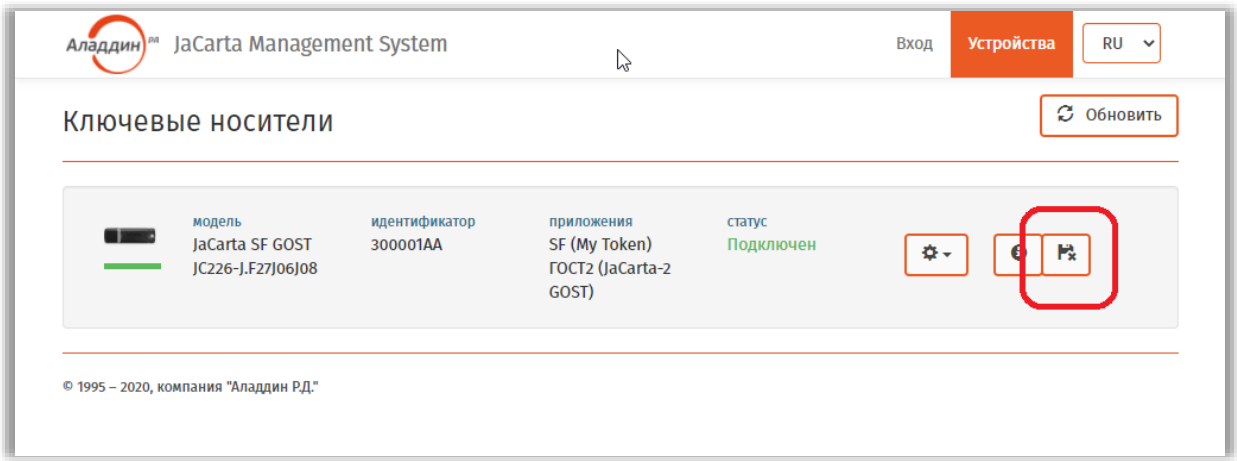


Рис. 50 – Отображение электронного ключа со смонтированными скрытыми разделами

После автоматического монтирования скрытых разделов они будут готовы к использованию.

Отключение скрытых дисков выполняется согласно разделу «Отключение скрытых разделов SF/ГОСТ», ниже.

4.5.1.3 Отключение скрытых разделов SF/ГОСТ

Для отключения скрытых разделов на электронных ключах JaCarta SF/ГОСТ выполните следующие действия.

1. В web-клиенте JMS выберите вкладку **Устройства**.
2. Нажмите на кнопку настроек ( ) подсоединенного электронного ключа (Рис. 51), на котором нужно отключить скрытые разделы.

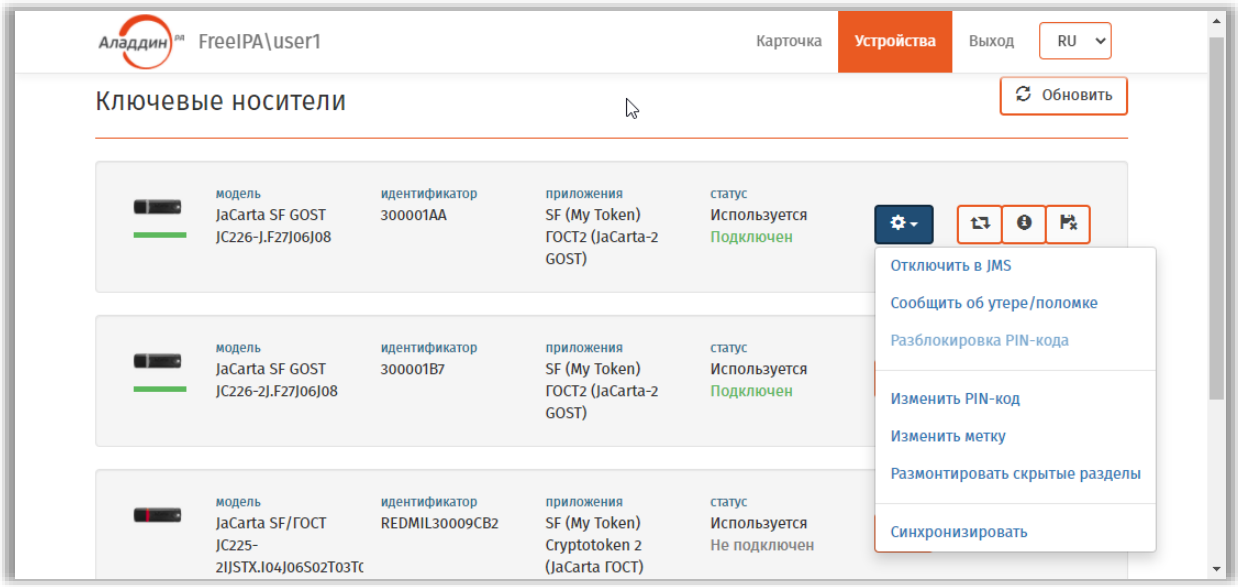


Рис. 51 – Выбор электронного ключа для отключения скрытых разделов

3. В появившемся меню выберите пункт **Размонтировать скрытые разделы** или нажмите кнопку  (**Размонтировать скрытые разделы ключевого носителя)**..
4. На странице размонтирования скрытых разделов (Рис. 52) введите **PIN-код пользователя** ЭК JaCarta SF/ГОСТ и нажмите **Размонтировать**.

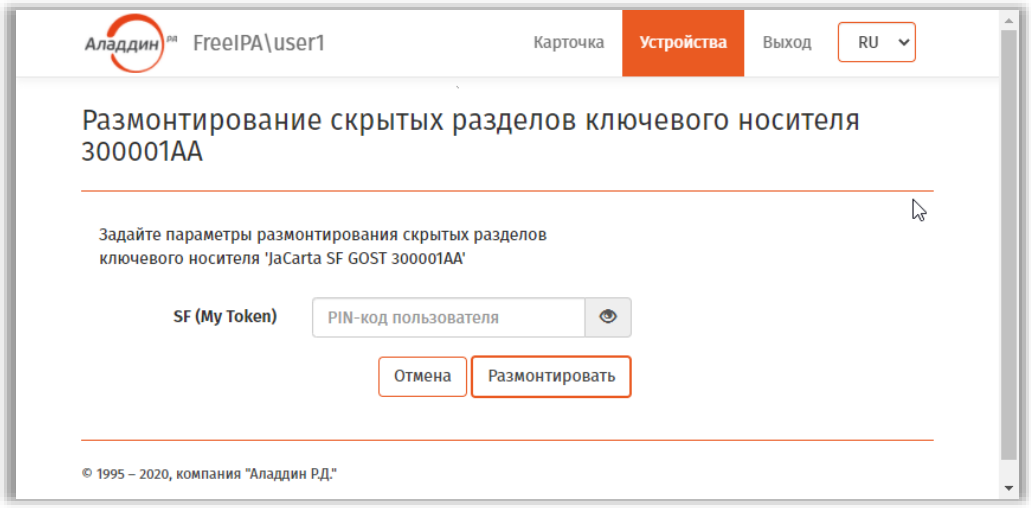
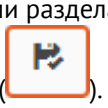


Рис. 52 – Страница размонтирования скрытых разделов

5. Дождитесь окончания работы мастера.

После произведенных действий скрытые разделы будут отключены.

У электронного ключа со отключенными скрытыми разделами изменится значок состояния скрытых дисков (Рис. 53) на статус «Отключены» ().

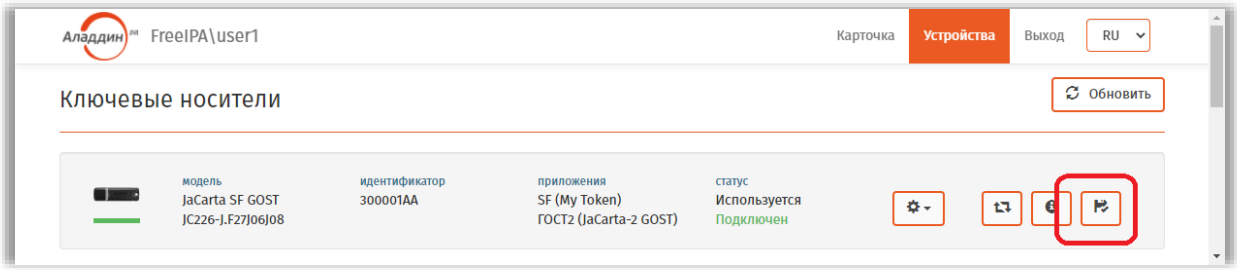


Рис. 53 – Отображение электронного ключа с отключенными скрытыми разделами

4.6 Особенности работы с СДР ALO

4.6.1 Выпуск СДР ALO

Для выполнения этой процедуры вы должны иметь полномочия на самостоятельный выпуск электронных ключей. В случае отсутствия таких полномочий обратитесь к администратору.

Важно! Для выпуска электронный ключ СДР ALO должен быть подключен к компьютеру непосредственно, либо с помощью среды виртуализации, например средств виртуализации VMware. Не допускается подключение такого электронного ключа к

компьютеру с клиентом JMS посредством *протокола удаленного рабочего стола* (Remote Desktop Protocol).

Чтобы самостоятельно выпустить СДР ALO, выполните следующие действия.

1. Подсоедините неинициализированный электронный ключ (ключ с заводскими настройками), который вы хотите выпустить, к компьютеру.
2. Откройте сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS», с. 20).
3. Выберите вкладку **Устройства**.
4. Нажмите на кнопку настроек ( ) подсоединенного электронного ключа (Рис. 54), который вы хотите выпустить.

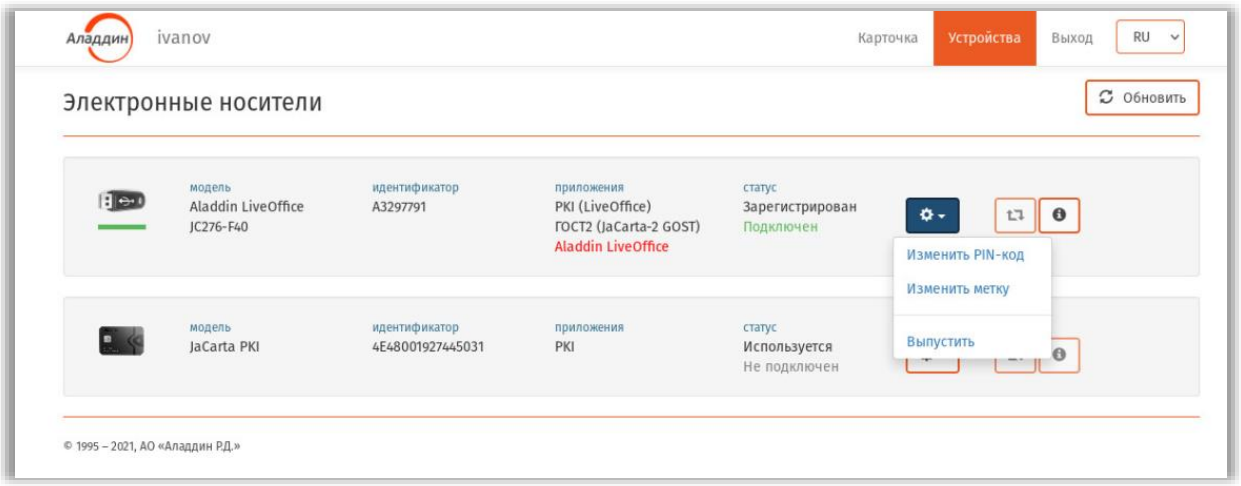


Рис. 54 – Выбор электронного ключа СДР ALO для выпуска

5. В появившемся меню выберите пункт **Выпустить**.
Отобразится вкладка приложения **PKI** следующего вида.

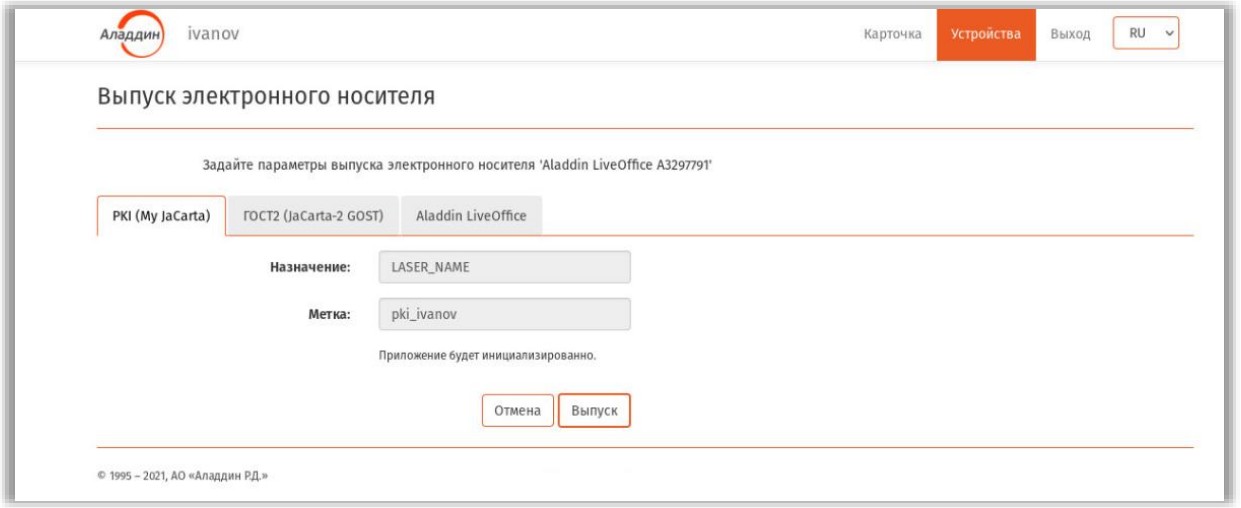


*Рис. 55 – Вид страницы выпуска электронного ключа на вкладке **PKI***

6. При необходимости отредактируйте значения полей **Назначение** и **Метка** (если доступно) и выберите вкладку приложения **ГОСТ2**.

Страница примет следующий вид.

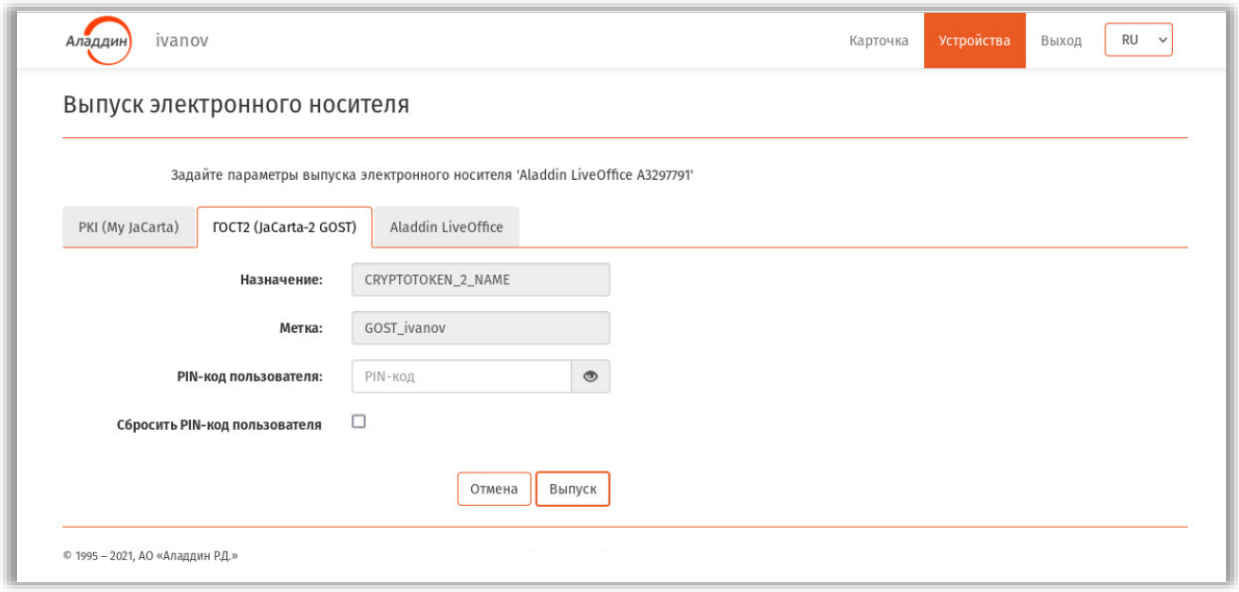


*Рис. 56 – Вид страницы выпуска электронного ключа на вкладке **ГОСТ2***

7. При необходимости отредактируйте значения полей **Назначение** и **Метка** (если доступно).
8. Введите предустановленный PIN-код пользователя для приложения ГОСТ2 (следует получить у администратора JMS, выдавшего вам электронный ключ).
9. Выберите вкладку приложения **Aladdin LiveOffice**.
   Страница примет следующий вид

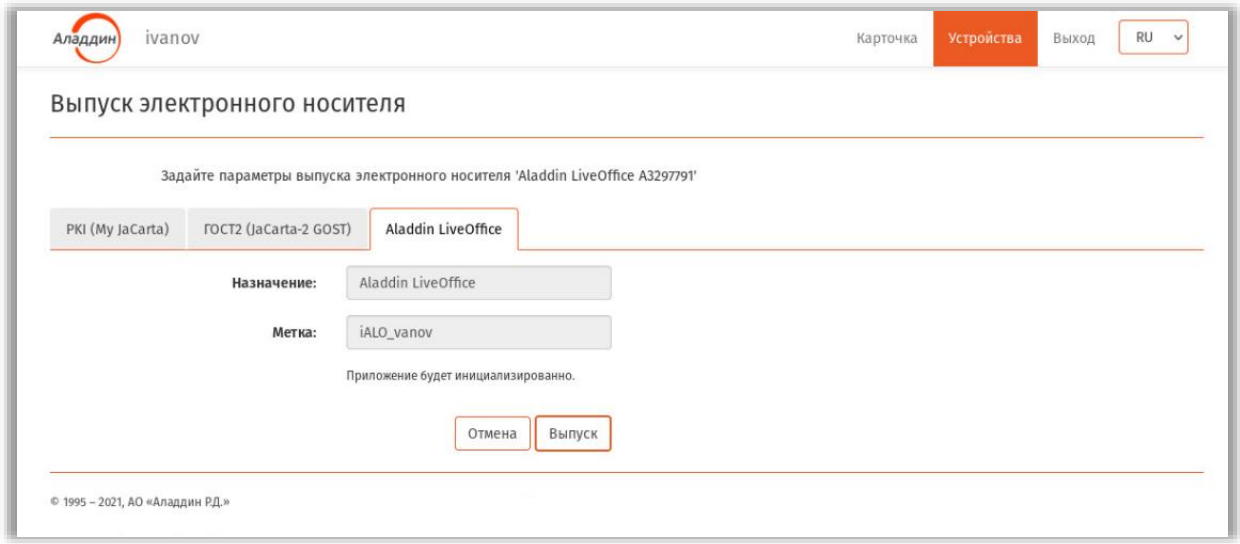


*Рис. 57 – Вид страницы выпуска электронного ключа на вкладке **Aladdin LiveOffice***

10. При необходимости отредактируйте значения полей **Назначение** и **Метка** (если доступно) и нажмите **Выпуск**.
11. Дождитесь окончания работы мастера (в случае запроса операционной системы действий, требующих согласия пользователя, дайте утвердительный ответ).

12. По окончании выпуска электронного ключа отобразится страница с отчетом о синхронизации. Убедитесь, что в отчете отсутствуют ошибки, в противном случае обратитесь к администратору.
13. На странице отчета нажмите **Закрыть отчет**.

Выпущенный ключ будет отображаться на вкладке **Устройства** со статусом **Используется** (Рис. 58).

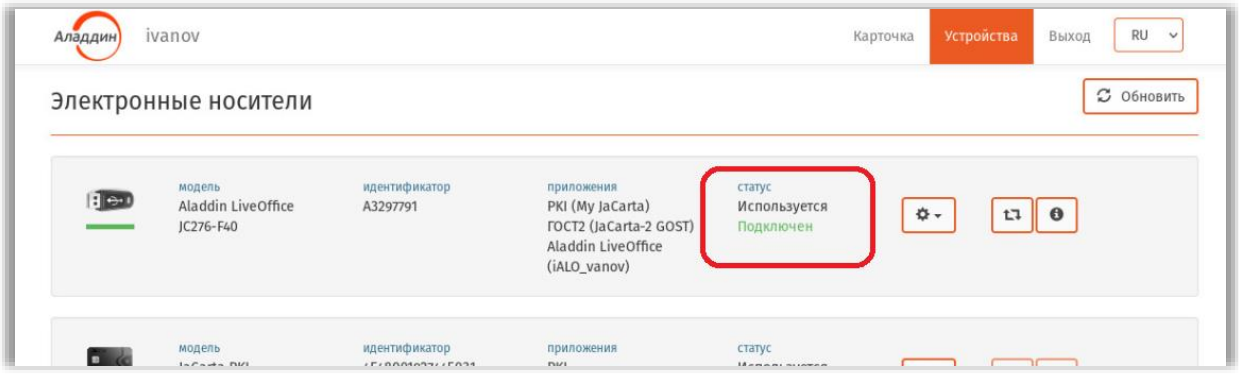


Рис. 58 – Статус выпущенного электронного ключа

4.6.2 Изменение PIN-кода пользователя в СДР ALO

Чтобы изменить PIN-код пользователя в приложении Aladdin LiveOffice на электронном ключе СДР ALO, выполните следующие действия.

1. Подсоедините электронный ключ, на котором надо выполнить смену PIN-кода, к компьютеру.
2. Откройте сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS», с. 20)
3. Выберите вкладку **Устройства**.
4. Нажмите на кнопку настроек ( ) подсоединенного электронного ключа (Рис. 59), на котором необходимо сменить PIN-код.

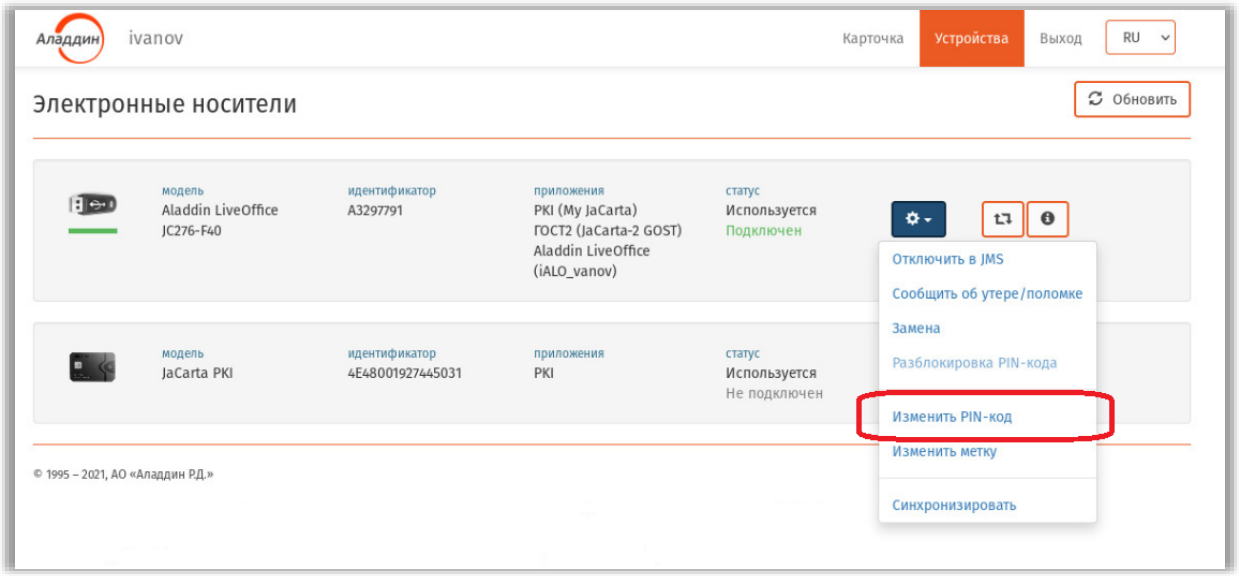


Рис. 59 – Запуск операции смены PIN-кода

5. В появившемся меню выберите пункт **Изменить PIN-код**.
Отобразится страница следующего вида.

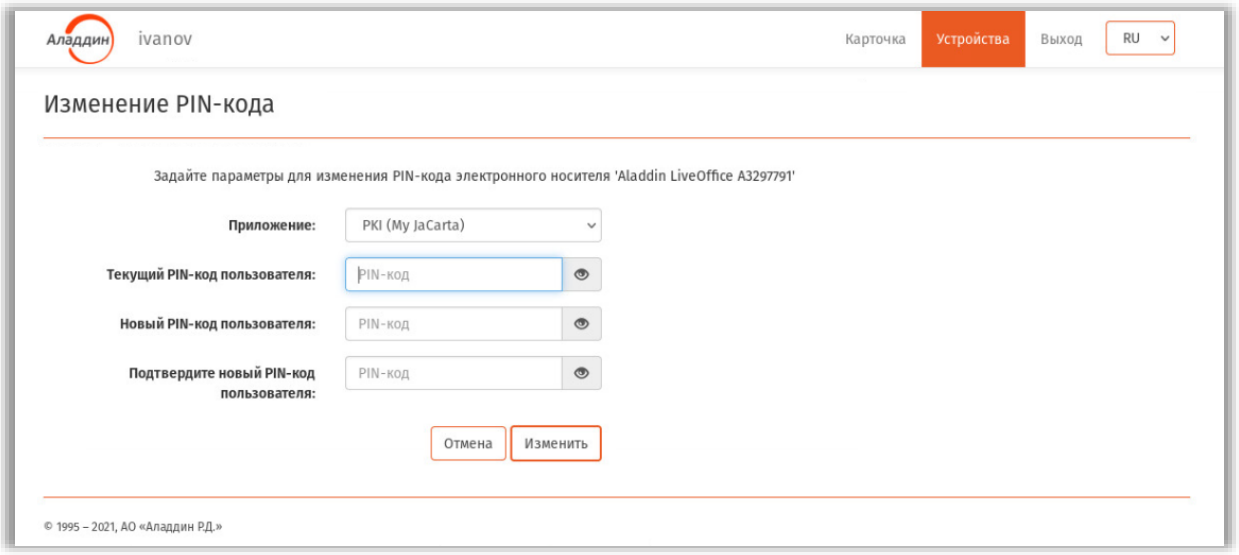


Рис. 60 – Страница смены PIN-кода

6. В поле **Приложение** выберите приложение *Aladdin LiveOffice*, как показано на Рис. 61.

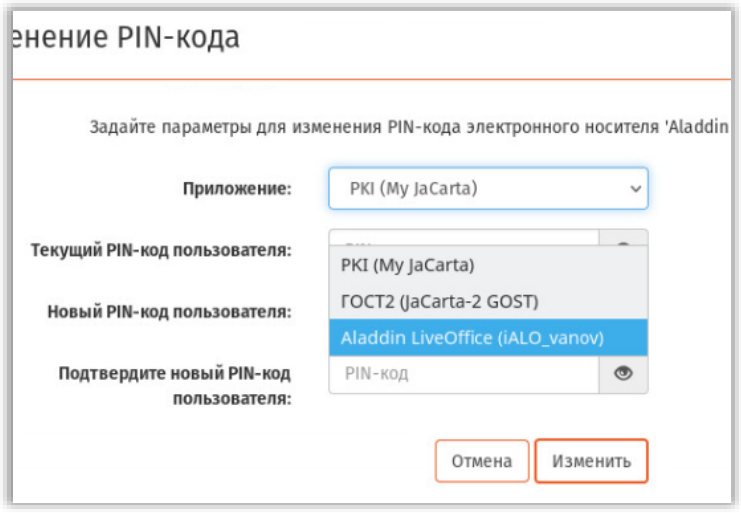


Рис. 61 – Выбор приложения Aladdin LiveOffice в электронном ключе СДР ALO

7. В соответствующих полях введите **Текущий PIN-код пользователя**, **Новый PIN-код пользователя** и его подтверждение.

Примечание. Если смена PIN-кода в приложении Aladdin LiveOffice осуществляется впервые (т.е. на новом электронном ключе), то установленное по умолчанию значение PIN-кода в этом приложении следует узнать у администратора JMS, выдавшего данный электронный ключ.

8. Нажмите **Изменить**.

При успешном завершении процедуры изменения PIN-кода на странице **Устройства** отобразится соответствующее уведомление (Рис. 62).

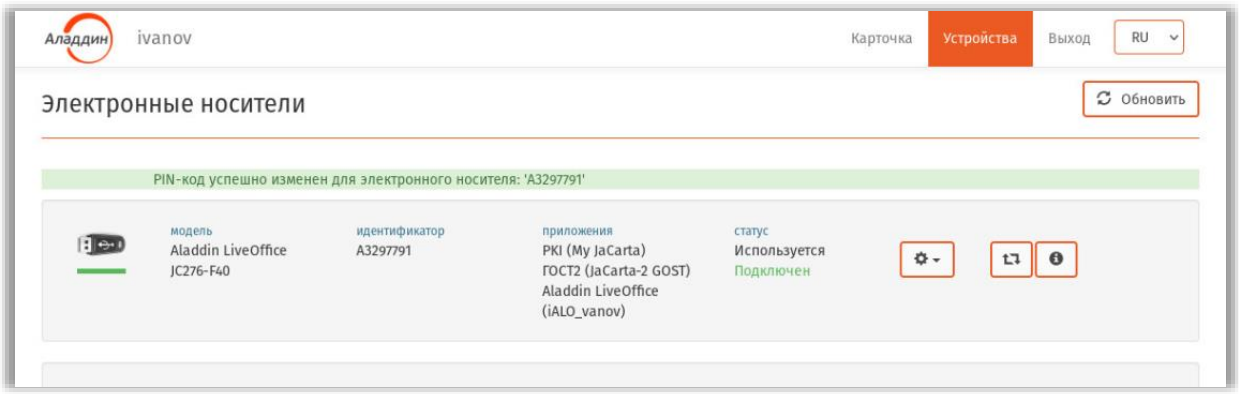


Рис. 62 – Уведомление об успешной смене PIN-кода в приложении Aladdin LiveOffice

При необходимости смены PIN-кода пользователя в приложениях *PKI* и *ГОСТ2* (Рис. 61) выполните шаги 4—8 для данных приложений.

4.6.3 Синхронизация СДР ALO

Чтобы синхронизировать СДР ALO, выполните следующие действия.

1. Подсоедините электронный ключ, который вы хотите синхронизировать, к компьютеру.
2. Откройте сеанс подключения к JMS (см. «Открытие сеанса подключения к JMS», с. 20)

3. Выберите вкладку **Устройства**.
4. Нажмите на кнопку настроек ( ) подсоединенного электронного ключа (Рис. 63), который вы хотите синхронизировать.

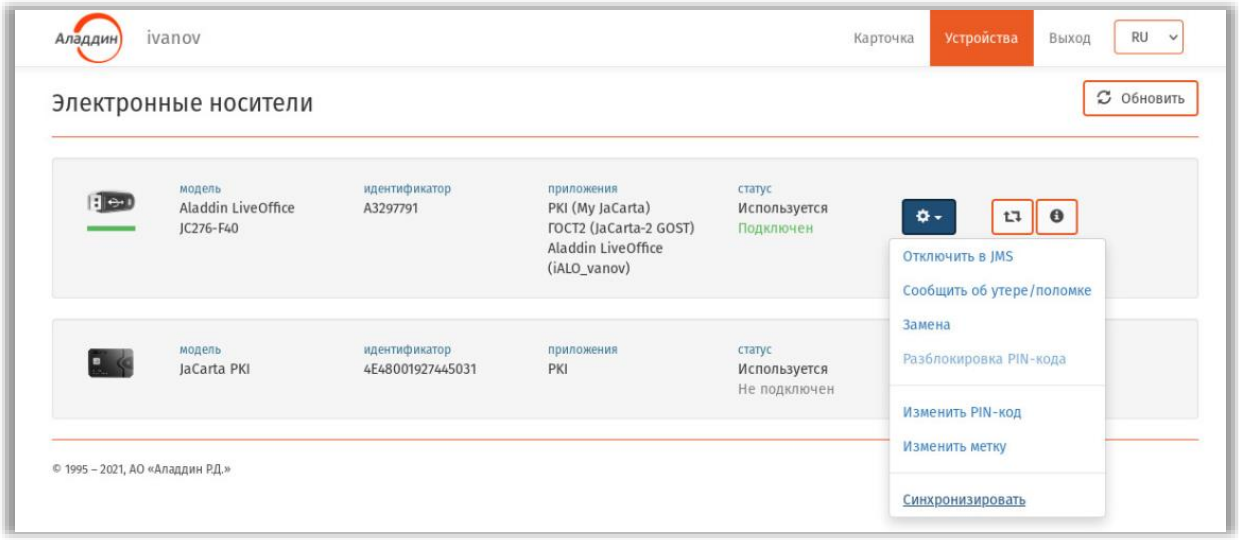


Рис. 63 – Запуск синхронизации на электронном ключе СДР ALO

5. В появившемся меню выберите пункт **Синхронизировать** (для синхронизации можно также воспользоваться кнопкой синхронизации).
Отобразится страница следующего вида.

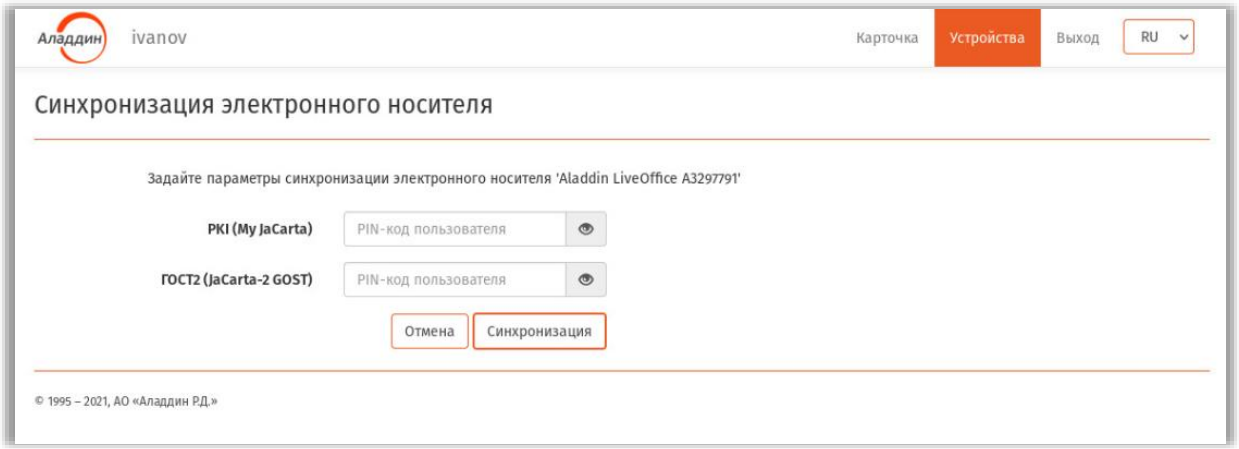


Рис. 64 – Страница синхронизации электронного ключа

6. Введите значение PIN-кода пользователя в полях приложений PKI и ГОСТ2.

Примечание. Если синхронизация электронного ключа осуществляется впервые (или если PIN-код пользователя в приложении **PKI** ни разу не менялся), то установленное по умолчанию значение PIN-кода в приложении **PKI** следует узнать у администратора JMS, выдавшего данный электронный ключ.

7. Нажмите **Синхронизация**.
8. Дождитесь окончания работы мастера.
9. По окончании синхронизации электронного ключа отобразится страница с отчетом о синхронизации.
10. Нажмите **Закрыть отчет**.

Синхронизированный электронный ключ будет отображаться на вкладке **Устройства** со статусом **Используется** (Рис. 65).

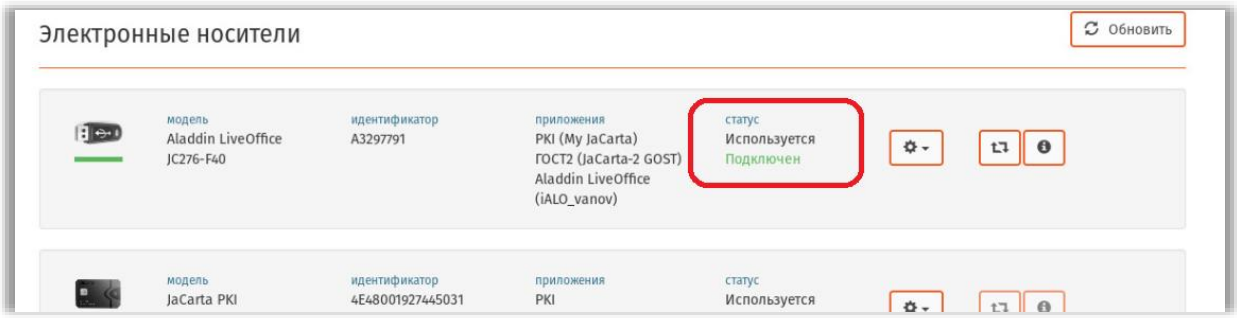


Рис. 65 – Отображение синхронизированного электронного ключа

4.6.4 Изменение метки СДР ALO

На электронном ключе СДР ALO в приложении *Aladdin LiveOffice* замена метки не предусмотрена.

Пункт меню **Изменить метку** в данном электронном ключе предназначен для замены метки в двух других сопутствующих приложениях – *PKI* и *ГОСТ2*. Замена метки в двух последних выполняется стандартным способом, т.е. как обычных электронных ключах *PKI* и *ГОСТ2* (см. раздел «Изменение метки в ЭК/ЗНИ», с. 25).

5. Web-портал самообслуживания пользователей (личный кабинет)

Личный кабинет (ЛК) позволяет пользователям управлять своими электронными ключами и OTP-аутентификаторами как внутри корпоративной сети, так и из-за её пределов через публичную сеть Интернет.

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 и OTP-аутентификаторами 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 порталу определяется правами доступа, предоставленными пользователю администратором.

5.1 Аутентификация в ЛК на внутреннем портале самообслуживания

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

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

где <JWM_FQDN> — полное доменное имя внутреннего портала JWM, например

```
jwmprivate.jms4.local
```

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

SB 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. 52;
- в два шага (двухфакторная аутентификация).

5.1.1 Обычная (одношаговая) аутентификация

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

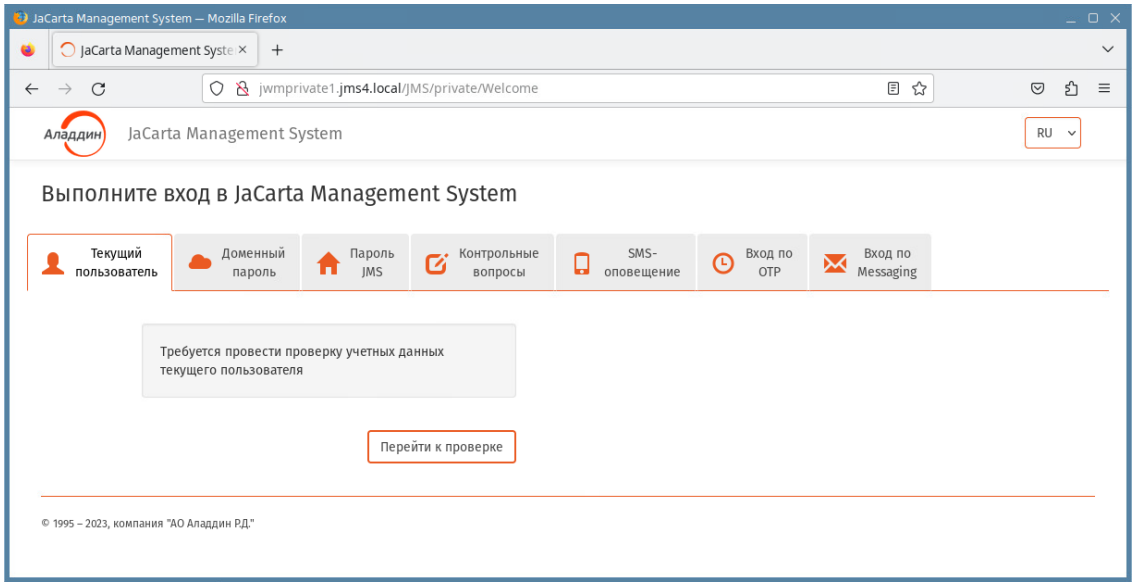


Рис. 66 – Страница аутентификации пользователя на внутреннем портале самообслуживания

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

На странице необходимо выполнить аутентификацию одним из следующих способов:

- аутентификация с использованием встроенной системы аутентификации операционной среды (прозрачная аутентификация пользователя с использование аутентификационных данных текущего сеанса работы с операционной системой, не требует ввода пароля);
- аутентификация по паролю ресурсной системы (например службы Active Directory или FreeIPA);
- аутентификация по паролю JMS;
- аутентификация посредством секретных вопросов;
- аутентификация посредством пароля, передаваемого по SMS;
- аутентификация посредством OPT-токена JMS;
- аутентификация посредством Messaging-токена JMS.

Чтобы выполнить аутентификацию выберите необходимую вкладку и выполните действия, руководствуясь Табл. 7.

Табл. 7 – Аутентификация пользователя на внутреннем портале самообслуживания

Название вкладки	Условия аутентификации	Действия по аутентификации
Текущий пользователь	Аутентификация с использованием средств аутентификации операционной среды. Пользователь, от имени которого открыт сеанс в операционной системе или запущен web-браузер, должен быть зарегистрирован в JMS, при этом его доступ в JMS не должен быть заблокирован.	Для аутентификации нажмите **Перейти к проверке** **Важно!** Данный способ аутентификации недоступен при использовании web-браузера Opera.
Доменный пароль	Аутентификация по паролю ресурсной системы (такой как Active Directory или FreeIPA). Администратор должен предоставить пользователю пароль для аутентификации в ресурсной системе	Для аутентификации следует ввести **Имя пользователя** (в формате <Имя_домена>\<Имя_пользователя>, например jms4\i_ivanov)и **Пароль** в ресурсной системе, 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 ЛК, что требует предварительной аутентификации в ЛК любым другим способом	Для аутентификации выполните следующие действия. 1. Введите **Имя пользователя** (в формате <Имя_домена>\<Имя_пользователя>), например: `jms4\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. 54
Вход по OTP	Аутентификация с помощью так называемого OTP-токена – мобильного приложения или аппаратного устройства (последнее выдается пользователю)	см. раздел «Вход по OTP-паролю», с. 55

Название вкладки	Условия аутентификации	Действия по аутентификации
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. 57

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).

5.2 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 в ЛК (Рис. 66, с. 52) выберите вкладку **SMS-оповещение**. Отобразится страница следующего вида

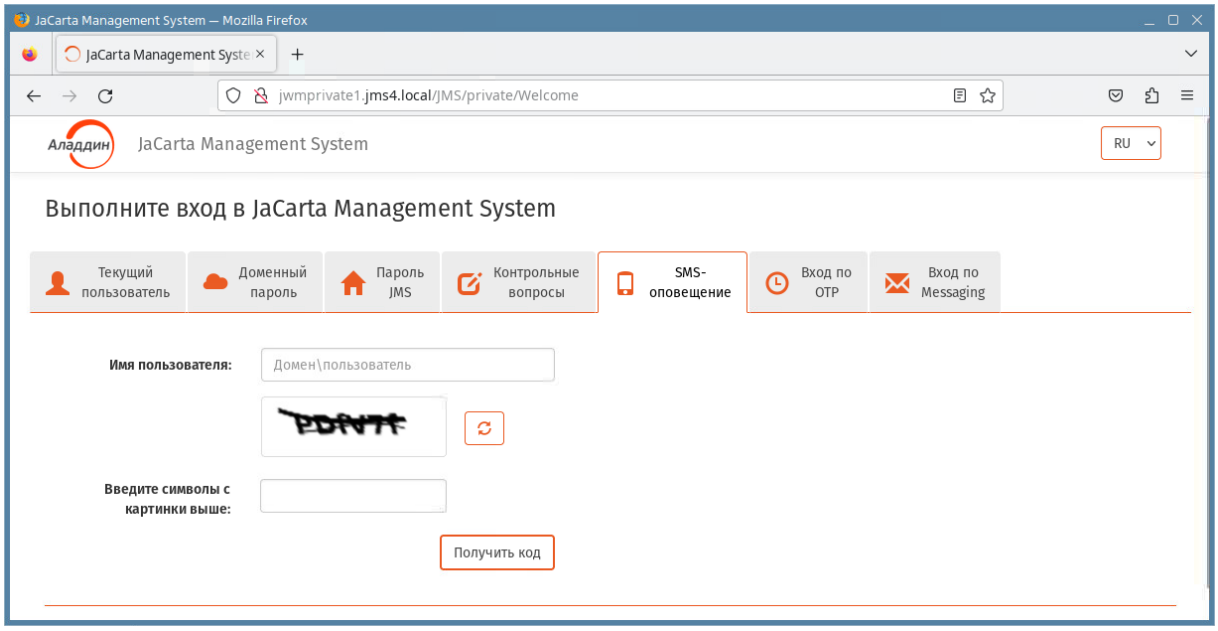


Рис. 67 – Начальная страница входа по SMS-оповещению

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

Отобразится страница следующего вида.

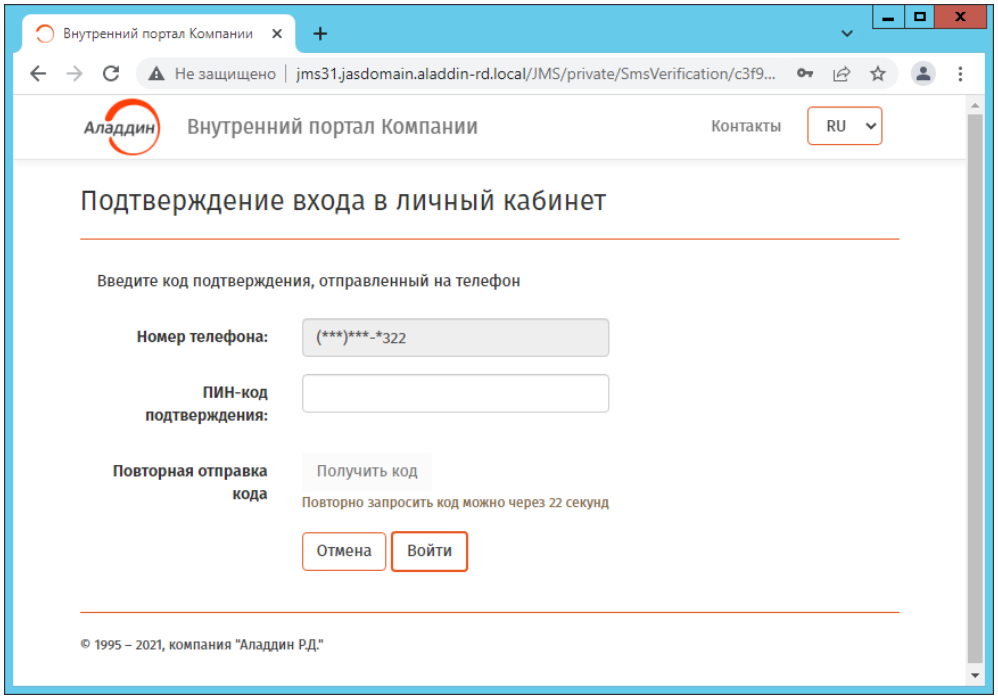


Рис. 68 –Страница ввода кода подтверждения из SMS

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**.

5.3 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. 66, с. 52) выберите вкладку **Вход по OTP**.

Отобразится страница следующего вида.

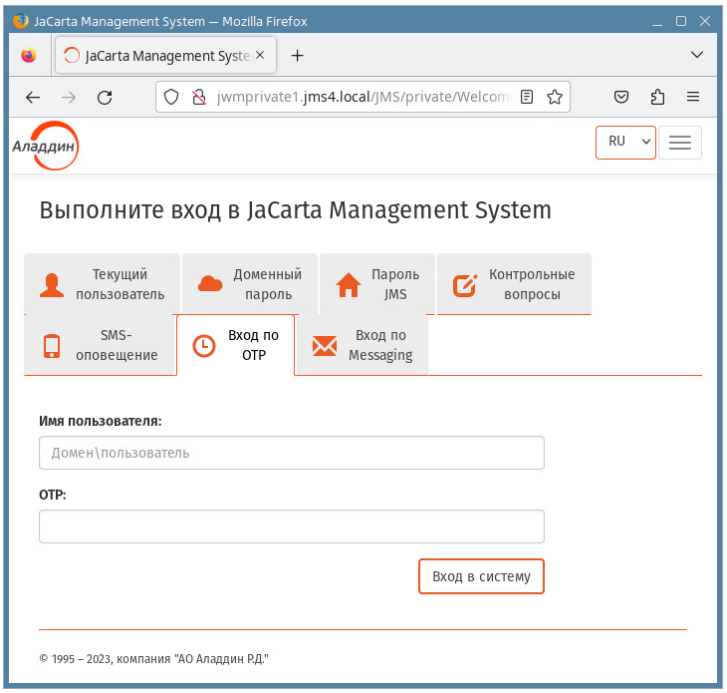


Рис. 69 – Начальная страница входа по OTP-паролю

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 и активированного в системе JMS OTP-токена (например, устройства JC-WebPass, производства компании Аладдин) или мобильного приложения Aladdin 2FA (или аналогичных приложений других поставщиков).
4. Введите полученный одноразовый пароль в поле **OTP** и нажмите **Вход в систему**.

В случае успешной аутентификации отобразится страница личного кабинета пользователя JWM.

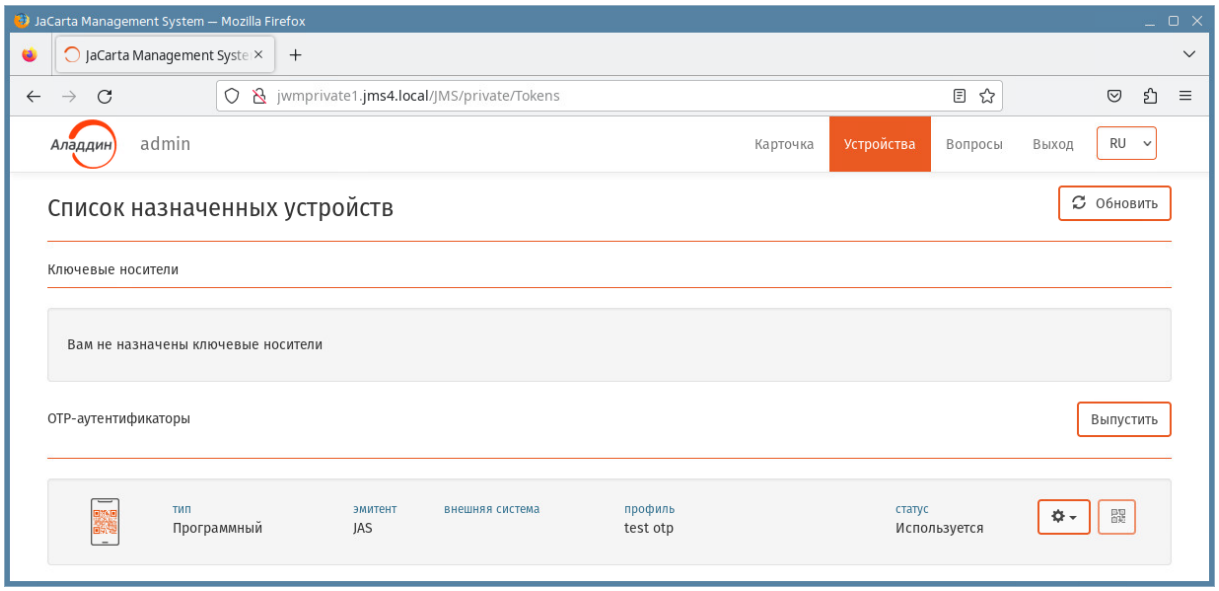


*Рис. 70 – Вкладка **Устройства** личного кабинета пользователя*

5.4 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. 66, с. 52) выберите вкладку **Вход по Messaging**.

Отобразится страница следующего вида

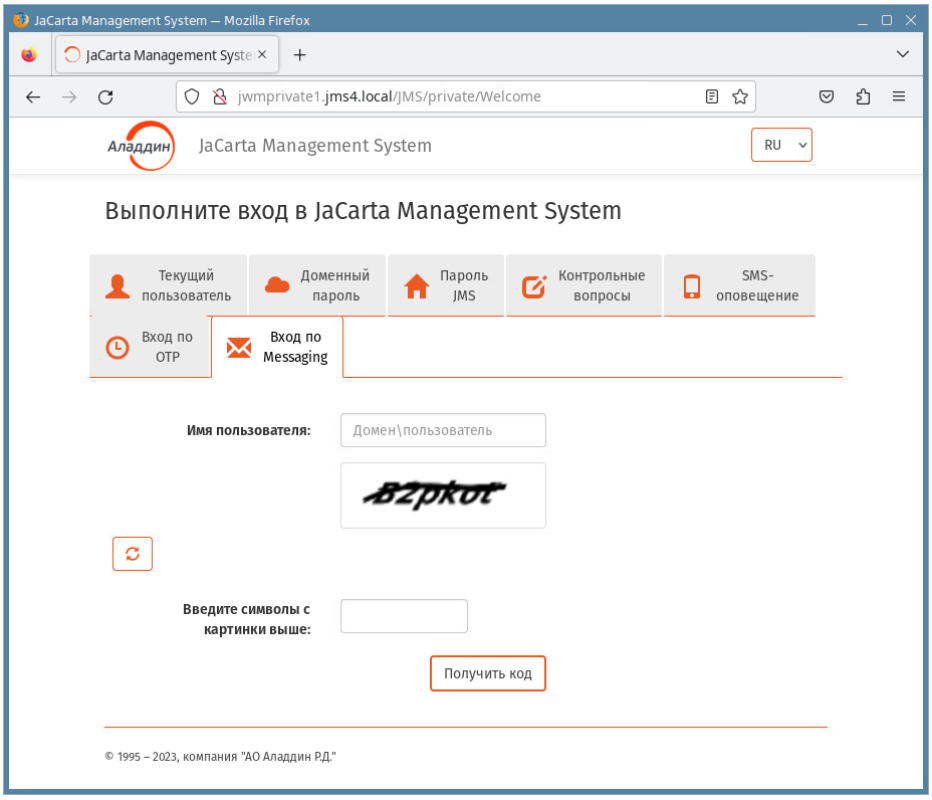


Рис. 71 – Начальная страница входа по Messaging-паролю

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.

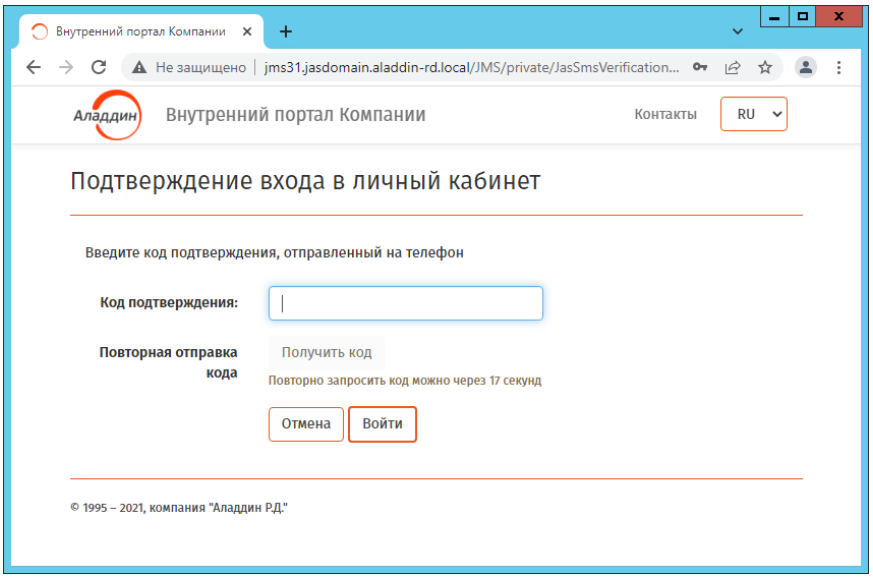


Рис. 72 –Страница ввода кода подтверждения из SMS

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

В случае успешной аутентификации отобразится страница личного кабинета пользователя JWM.

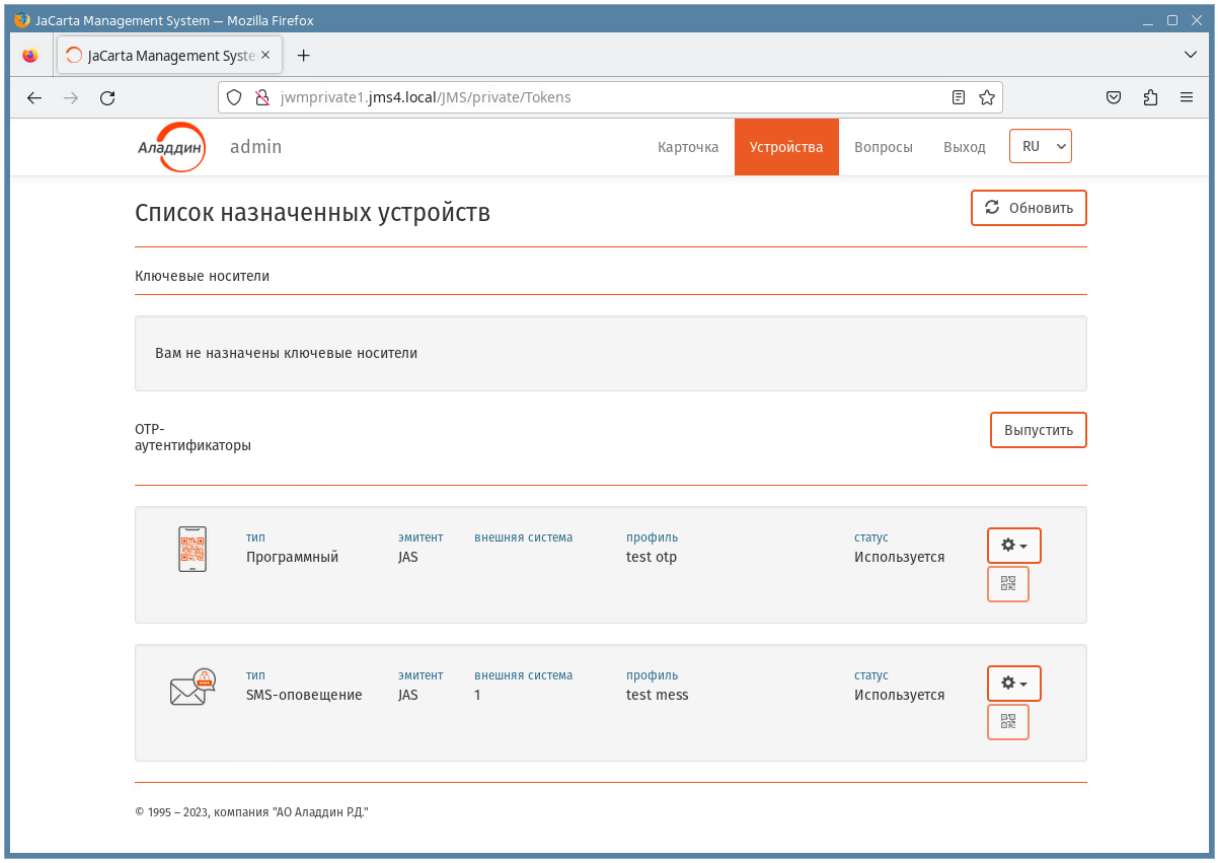


*Рис. 73 – Вкладка **Устройства** личного кабинета пользователя*

5.5 Функции, доступные пользователю в личном кабинете портала самообслуживания

Выполнив аутентификацию, пользователь получает доступ в свой личный кабинет на портале самообслуживания (Рис. 74).

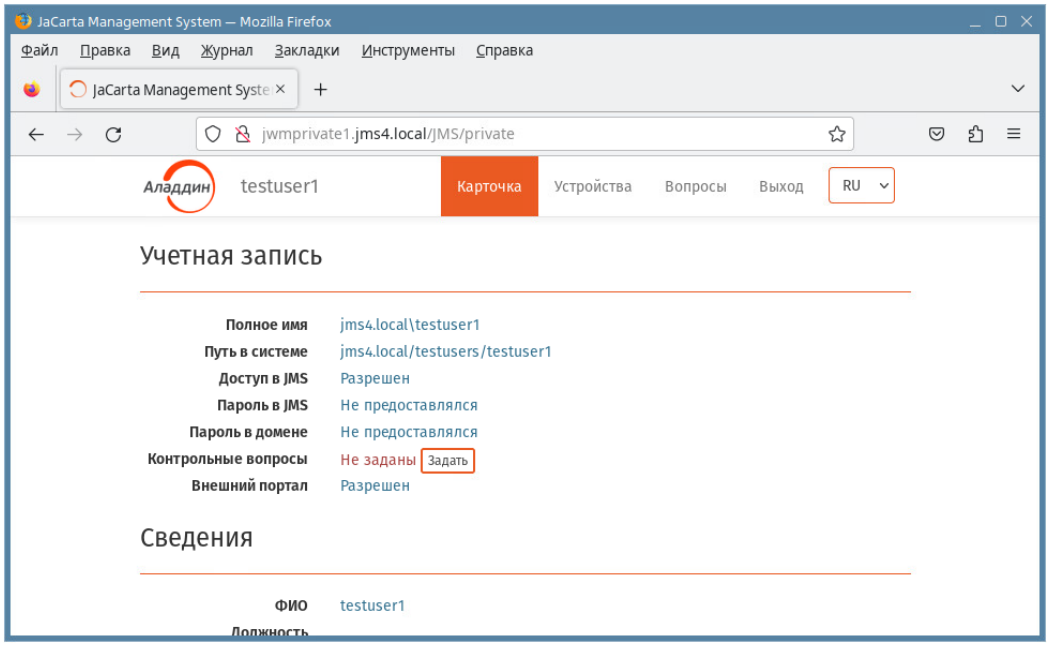


Рис. 74 – Вкладка Карточка личного кабинета пользователя на внутреннем портале самообслуживания

Пользователю доступны функции расположенные на нескольких вкладках страницы личного кабинета в соответствии с Табл. 8.

Табл. 8 – 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
Вопросы	На вкладке пользователь может определить (установить) контрольные вопросы для аутентификации
Выход	При нажатии на **Выход** происходит прекращение сеанса работы в личном кабинете пользователя

5.5.1 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 Аладдин (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. 75).

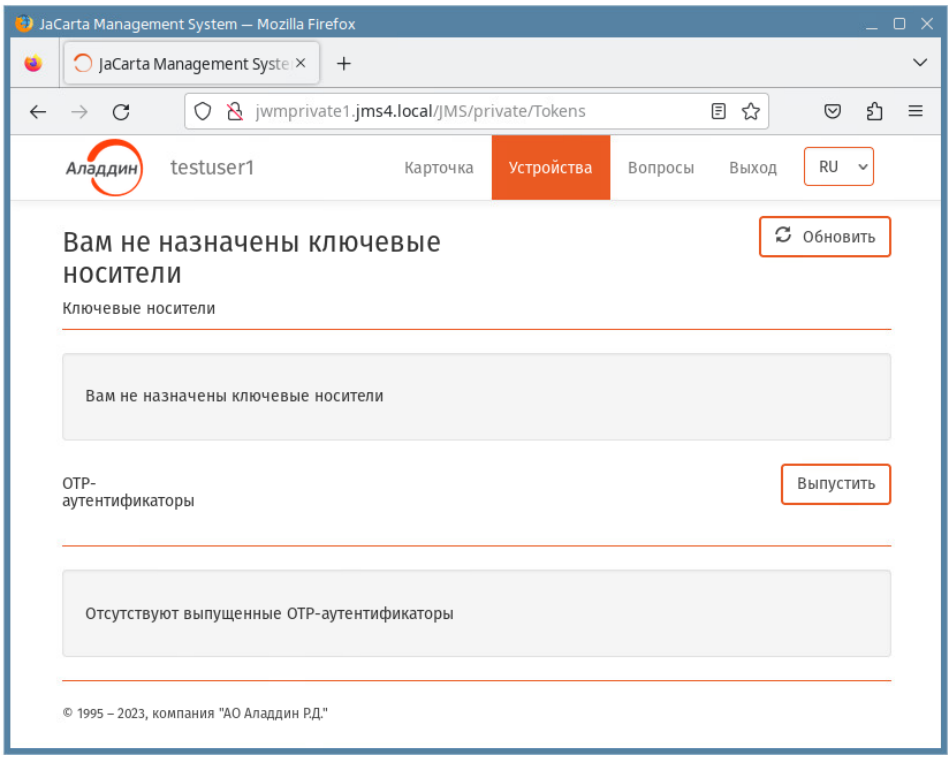


Рис. 75 – Вкладка Устройства личного кабинета пользователя на внутреннем портале самообслуживания

2. В секции OTP-аутентификаторы нажмите **Выпустить**.

Отобразится страница следующего вида.

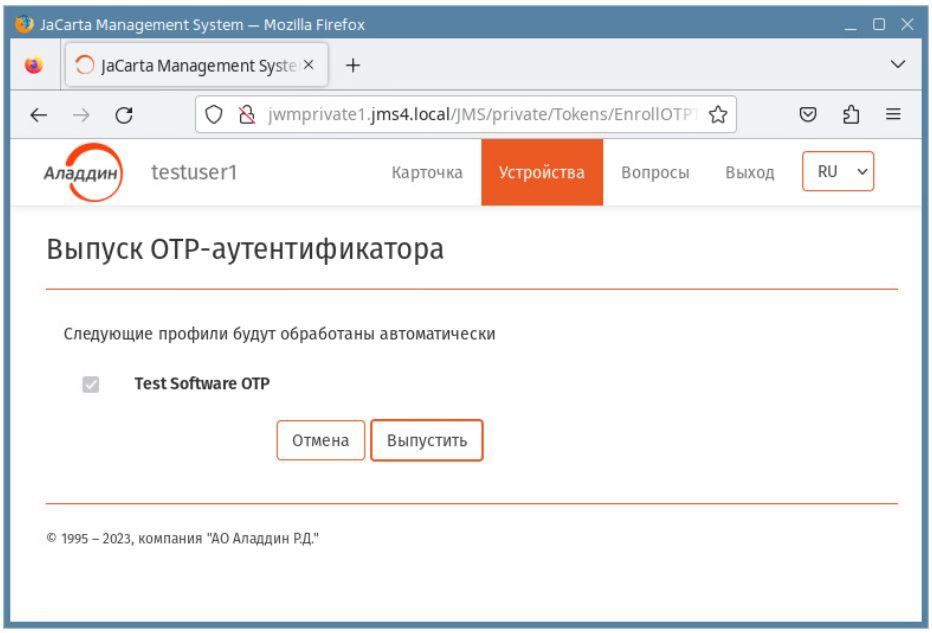


Рис. 76 – Страница выбора профиля для выпуска OTP-аутентификатора

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.

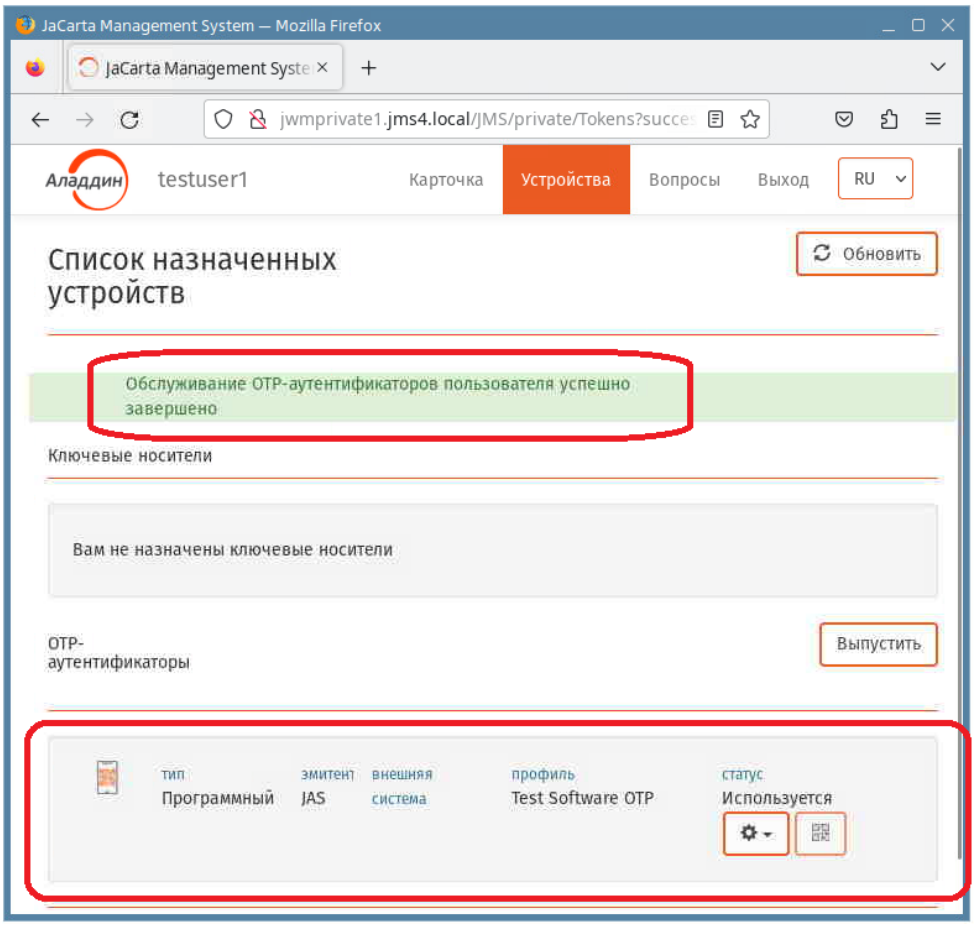


Рис. 77 – Страница с отображением выпущенного OTP-аутентификатора

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. 63 (для случая передачи активационных данных на личную электронную почту пользователя);
- «Активация программного и Push OTP-токена в личном кабинете», с. 64 (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. 55).

5.5.2 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 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. 78 - Сообщение, содержащее QR-код для активации программного OTP-токена

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

Примечание. В случае если в мобильном приложении Aladdin 2FA не удается отсканировать QR-код, можно воспользоваться двумя другими опциями активации OTP-аутентификатора:

- использовать гиперссылку в письме (если письмо открыто в мобильном устройстве);
- скопировать текстовую строку-команду *jasticket://* в конце письма и воспользоваться в мобильном приложении режимом **Добавить вручную**.

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

5.5.3 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. 79).

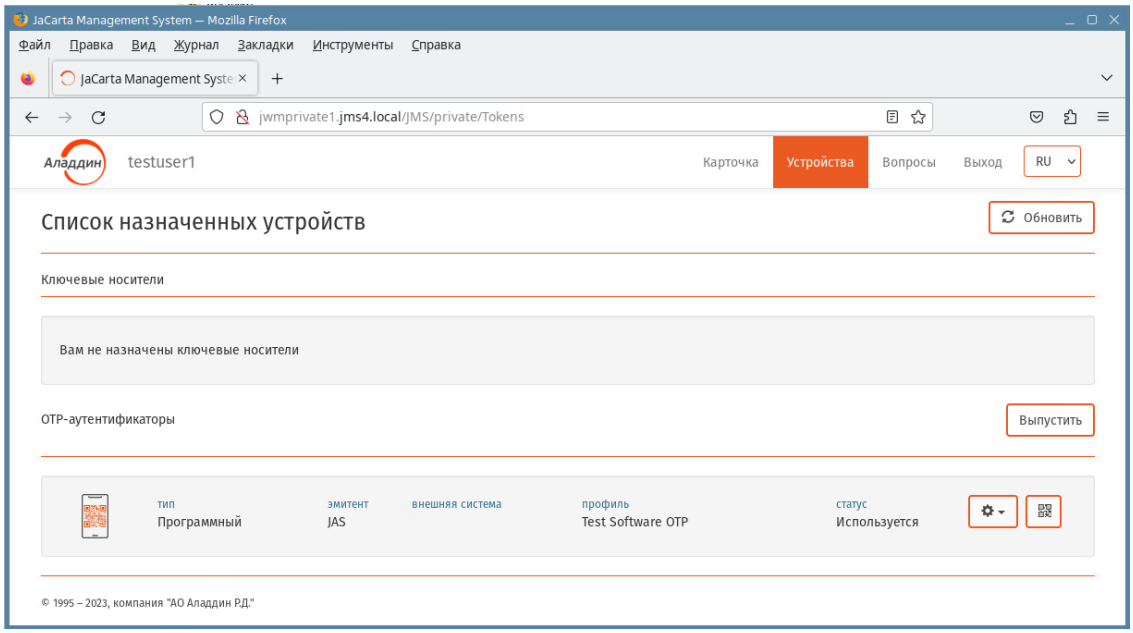


Рис. 79 – Отображение OTP-аутентификатора на кладке Устройства личного кабинета

2. В секции **OTP-аутентификаторы** выберите OTP-токен для активации (например *Программный* OTP-токен, как на Рис. 79).
3. В правой части строки с описанием OTP-токена нажмите пиктограмму с QR-кодом.

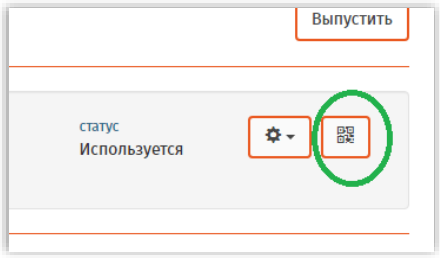


Рис. 80 – Пиктограмма QR-кода для активации токена

4. Отобразится окно следующего вида.

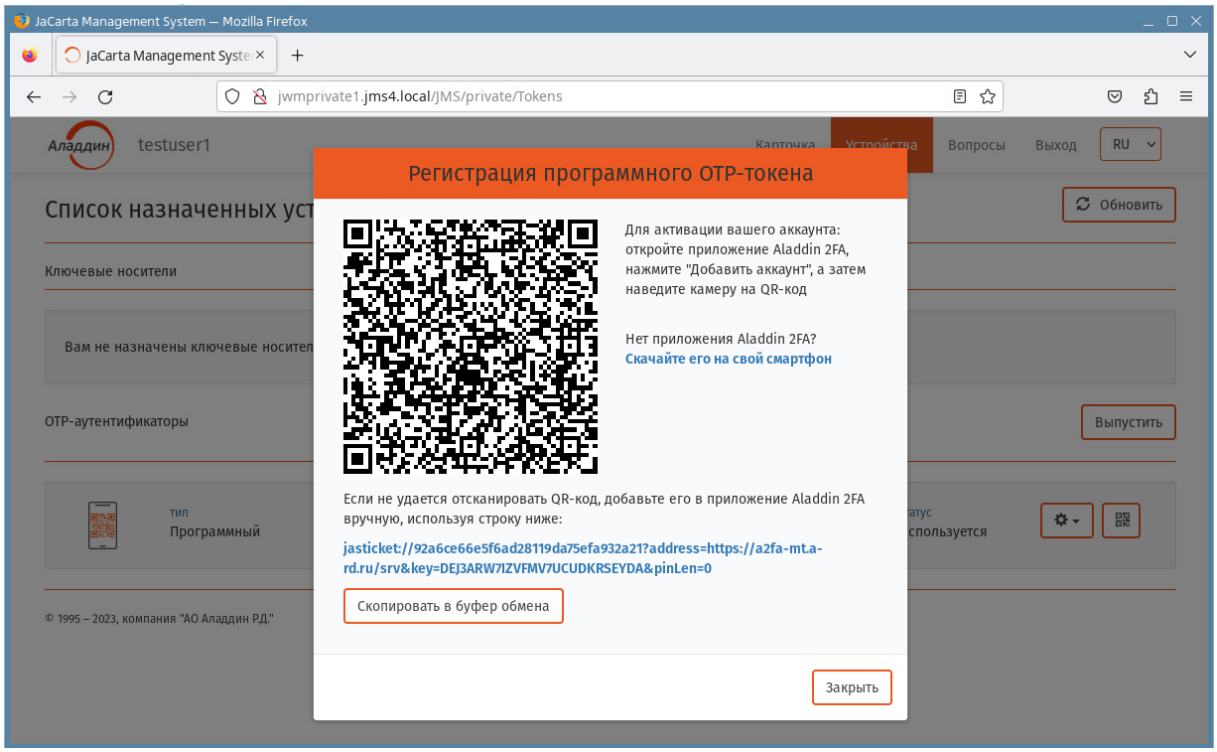


Рис. 81 – Окно с QR-кодом для активации ОТР-токена

5. С помощью приложения Aladdin 2FA компании Аладдин, установленного на вашем мобильном устройстве, отсканируйте отобразившийся QR-код. Если сканирование не удалось, можно использовать текстовую строку-команду *jasticket://* и добавить ОТР-токен в мобильное приложение, используя в нём режим **Добавить вручную**.
6. Нажмите **Закрыть**.

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

5.5.4 Управление ОТР-аутентификаторами из личного кабинета

Для управления своими ОТР-аутентификаторами выполните следующие действия.

1. Войдите в личный кабинет на JWM-портале откройте вкладку **Устройства** (Рис. 77, с. 63).
2. Выберите ОТР-аутентификатор в секции **ОТР-аутентификаторы** и нажмите значок . Отобразится контекстное меню следующего вида.

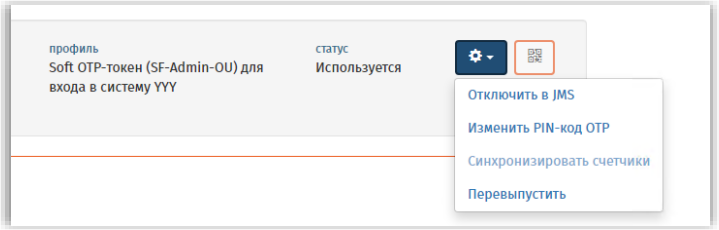


Рис. 82 – Контекстное меню операций с ОТР-аутентификаторами

3. В зависимости от имеющихся у вас прав выполните доступную операцию в соответствии с Табл. 9.

Табл. 9 – 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 ЭК/ЗНИ/СДР или OTP-аутентификатора», с. 36).
Включить в JMS	Операция позволяет включить возможность использования электронного ключа после его отключения (см. операцию **Отключить в JMS**, выше).
Изменить PIN-код OTP	Операция позволяет установить (если еще не установлен) или изменить PIN-код OTP (дополнительный параметр аутентификации, вводимый пользователем при входе в целевую систему). **Примечание.** При изменении *PIN-кода OTP* на адрес электронной почты пользователя приходит соответствующее уведомление со значением нового PIN-кода. Операция выполняется по согласованию с администратором системы.
Синхронизировать счётчики	Служебная операция настройки функционирования OTP-аутентификатора. Операция выполняется по согласованию с администратором системы.
Перевыпустить	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. 63). **Примечание.** После активации нового программного OTP-токена в мобильном приложении, прежний OTP-токен перестает быть актуальным и его следует удалить. Операция выполняется по согласованию с администратором системы.

5.5.5 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. 59) с тем отличием, что на внешнем портале в личном кабинете пользователя отсутствует вкладка **Текущий пользователь**.

Примечание. Способы аутентификации (число вкладок) на стартовой странице аутентификации в ЛК на внешнем портале, а также порядок аутентификации и некоторые параметры работы, могут отличаться от аналогичных параметров для внутреннего портала. Данная разница определяется администратором системы JMS.

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.03.16.001-05 30 01-1. Формуляр [Текст]. — «Аладдин Р.Д.»
4	RU.АЛДЕ.03.16.001-05 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
1.01	Добавлено описание поддержки СДР Aladdin LiveOffice.
1.00	Исходная версия документа

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.

Аладдин

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

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