ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ JACARTA MANAGEMENT SYSTEM 4LX

Руководство администратора. Часть 2

Функции управления

Версия продукта	4LX
Версия документа	1.02
Статус	Публичный
Дата	15 мая 2024 г.
Листов	344

2024

Оглавление

1. О документе

1.1 Назначение документа

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

1.2 На кого ориентирован данный документ

Документ предназначен для администраторов корпоративной информационной системы управления средствами аутентификации.

1.3 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. 6	Используется для выделения перекрестных ссылок
	Важная информация
	Ссылка, примечание, заметка
	Совет
	Рекомендация

1.4 Обозначения и сокращения

Табл. 2— Обозначения и сокращения

JAS	JaCarta Authentication Server
JMS	То же, что «Программное обеспечение JaCarta Management System 4LX»
JWA **(JMS Web Agent)**	Программное обеспечение, обеспечивающее взаимодействие web-клиента JMS с ЭК/ЗНИ из среды web-браузера.
JWM	JMS Web Manager – компонент JMS, предоставляющий возможность выполнения пользовательских функций через корпоративную сеть или Интернет с помощью web-браузера по протоколам http и https
JWA Tray **(JMS Web Agent Tray)**	Программа, позволяющая выполнять базовые операции с ЭК/ЗНИ пользователя в фоновом режиме или через простое графическое меню. Запущенное приложение отображается значком в области уведомлений рабочего стола
Messaging-токен	Аутентификатор, позволяющий проводить аутентификацию путем отправки OTP посредством службы SMS оператора мобильной связи
OTP	One-Time Password – одноразовый пароль
OTP-токен	Электронный ключ – аппаратная реализация средства аутентификации с поддержкой OTP. Один из видов аутентификаторов, поддерживаемых сервером JAS
PIN-код администратора	Секретная последовательность, известная только администратору, которую необходимо предъявить для аутентификации администратора в приложении электронного ключа
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
U2F	Universal 2nd Factor – открытый стандарт протокола двухфакторной аутентификации. Разрабатывается альянсом FIDO (FIDO Alliance)
U2F-аутентификатор	Аутентификатор, представляющий собой регистрационную информацию, хранимую на сервере JAS используемую для аутентификации пользователя по протоколу U2F альянса FIDO
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

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)
КД	Ключевой документ – в терминологии JMS это ключевая информация (КИ), записанная на электронный ключ (ключевой носитель – СКЗИ) и хранящаяся на нем
КИ	Ключевая информация – в терминах JMS это сертификат открытого ключа и соответствующий данному сертификату закрытый ключ (Номер КИ – это серийный номер сертификата открытого ключа)
Клиентский агент	То же, что приложение **Клиент JMS**. Приложение с графическим пользовательским интерфейсом, предназначенное управления электронными ключами на рабочих станциях конечных пользователей.
Консольный агент	Приложение, предназначенное для конфигурирования сервера JMS. Устанавливается вместе с компонентом JMS Server
НД	Нормативный документ – в терминах JMS означает вид документов (актов), формируемых при операциях с СКЗИ в соответствии с требованиями регулятора
ПО	Программное обеспечение
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
СКЗИ	Средство криптографической защиты информации
ФКН	Функциональный ключевой носитель
ФСБ	Федеральная служба безопасности Российской Федерации
ФСТЭК	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЭК	Электронный ключ – электронное устройство, используемое как средство аутентификации и/или защищенного хранения информации

1.5 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.

1.6 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. Дополнительная документация

Рекомендуется дополнительно ознакомиться со следующими документами:

- «Руководство пользователя» [1];
- «Руководство администратора. Часть 1. Установка и настройка» [2].

3. Консоль управления JMS

Консоль управления JMS предоставляет собой web-приложение для администрирования JMS и доступна на сетевых компьютерах с web-браузером.

Примечание. Для доступа к web-консоли следует получить IP-адрес серверного приложения «Консоль управления JMS» (подробнее см. руководство по настройке и установке [2]).

Для начала сеанса управления через web-консоль выполните следующие действия.

1. В web-браузере выполните подключение к web-консоли JMS по адресу

   ```
   http://<Адрес_сервера_web-консоли>:5001
   ```

   где <Адрес_сервера_web-консоли> — FQDN-имя или IP-адрес компьютера с установленным серверным web-приложением «Консоль управления JMS».

Примечание. В случае настройки защищенного соединения по SSL/TLS в адресе укажите `https://` и порт 5000, при этом допускается указывать только FQDN-имя хоста с серверным web-приложением «Консоль управления JMS» (нельзя указывать IP-адрес)

   Отобразится страница следующего вида.

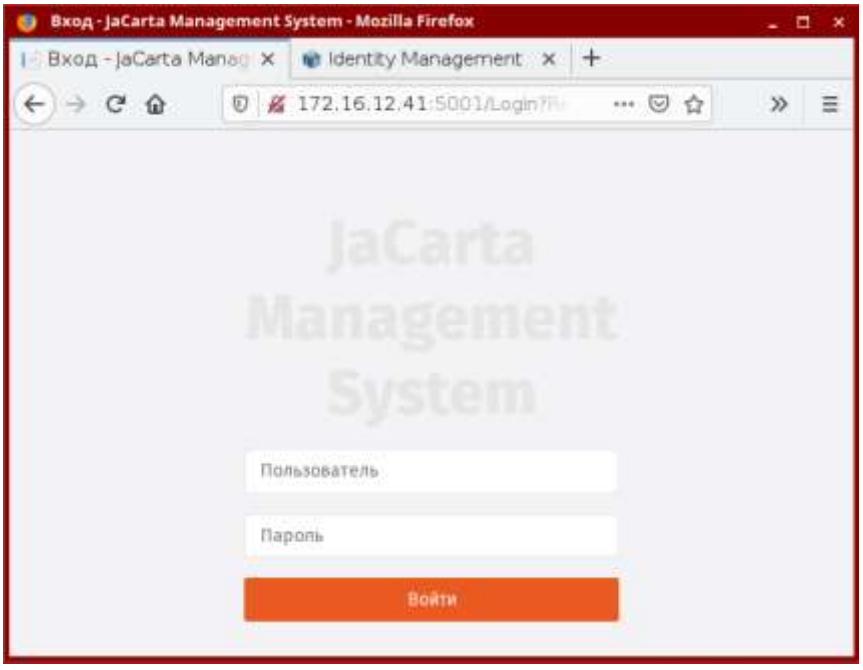


Рис. 1 – Доступ к web-консоли JMS с внешнего компьютера

2. В поле **Пользователь** введите логин пользователя в формате:
   `<тип_ресурсной_системы>\<имя_пользователя>`,

где <тип_ресурсной_системы> — значение, указанное в поле `[accountSystem] -> type` файла первоначальной конфигурации (см. [2] «Приложение 1. Параметры файла первоначальной конфигурации сервера JMS»).
Например:

```
FreeIPA\admin
```

Отобразится страница следующего вида.

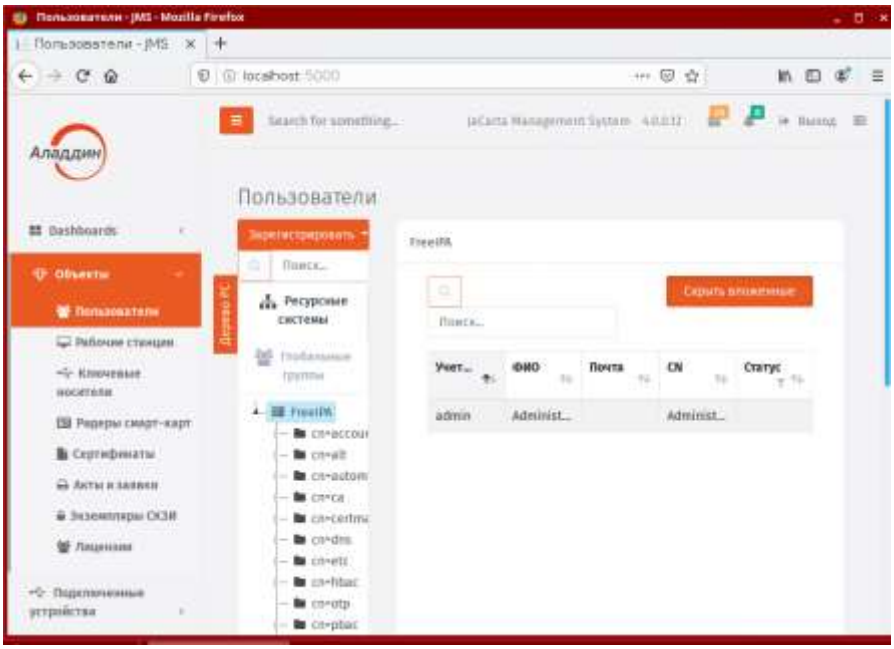


Рис. 2 – Интерфейс web-приложения «Консоли управления JMS»

3.1 Управление пользователями

3.1.1 Регистрация пользователей в JMS

Чтобы зарегистрировать новых пользователей, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Объекты -> Пользователи**.

Страница консоли будет выглядеть следующим образом.

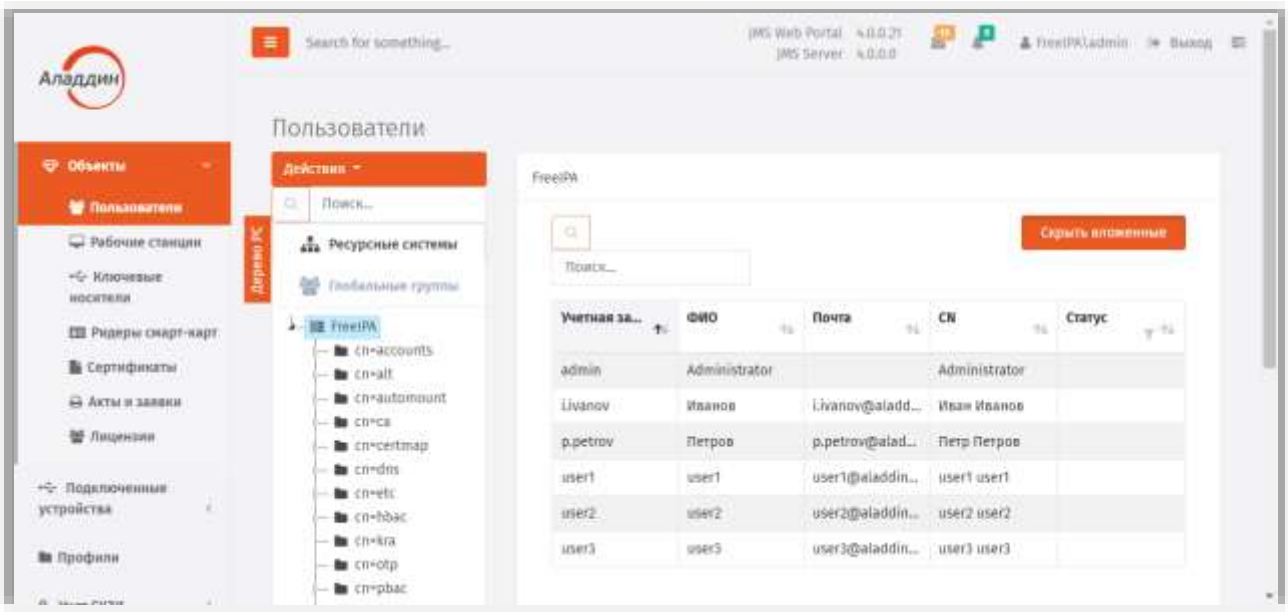


*Рис. 3 – Раздел **Пользователи** консоли управления JMS*

2. В верхней панели нажмите **Действия** и выберите **Зарегистрировать пользователей** (Рис. 4).

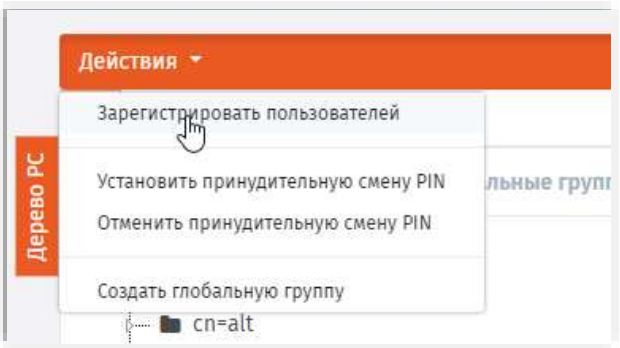


*Рис. 4 – Выбор **Регистрации пользователей***

3. Интерфейс переключится в режим регистрации пользователей (Рис. 5).

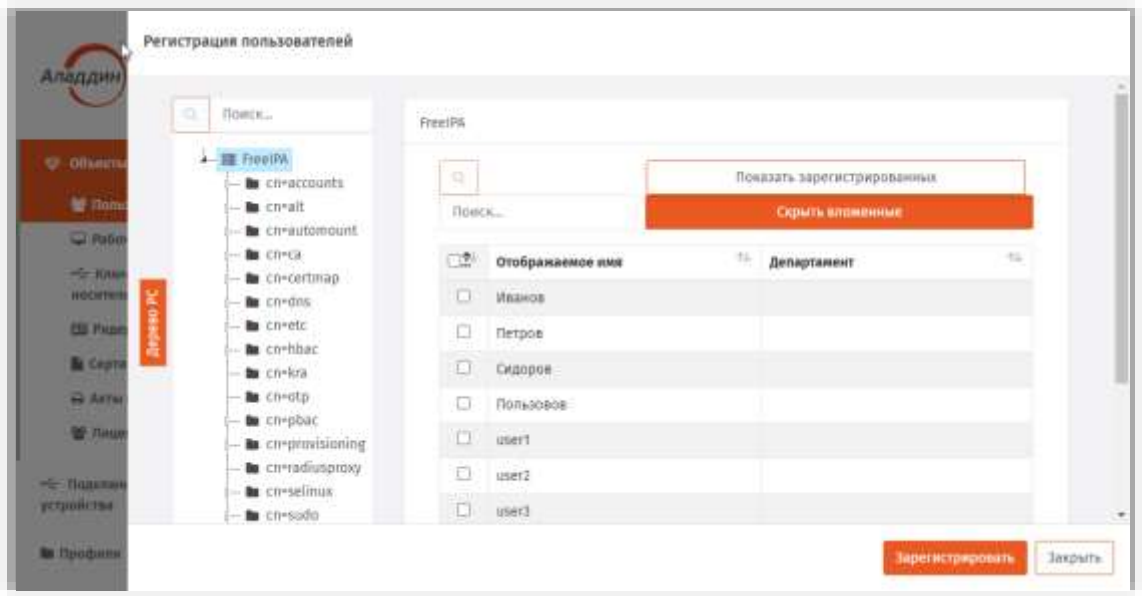


Рис. 5 – Режим регистрации пользователей

4. Выберите нужный каталог (например, **Accounts**) и выберите нужных пользователей, установив напротив соответствующих пользователей флажки, либо установите общий флажок вверху, чтобы выбрать всех пользователей из выбранного каталога и нажмите кнопку **Зарегистрировать** внизу.

Если во время регистрации пользователей из ресурсной системы, на которую наложены лицензионные ограничения (отображены в вашей лицензии JMS), будет превышен лимит пользователей, то отобразится соответствующее сообщение и регистрация будет прекращена.

5. Добавив пользователей нажмите кнопку **Закрыть**.
Зарегистрированные пользователи отобразятся в окне консоли управления JMS.

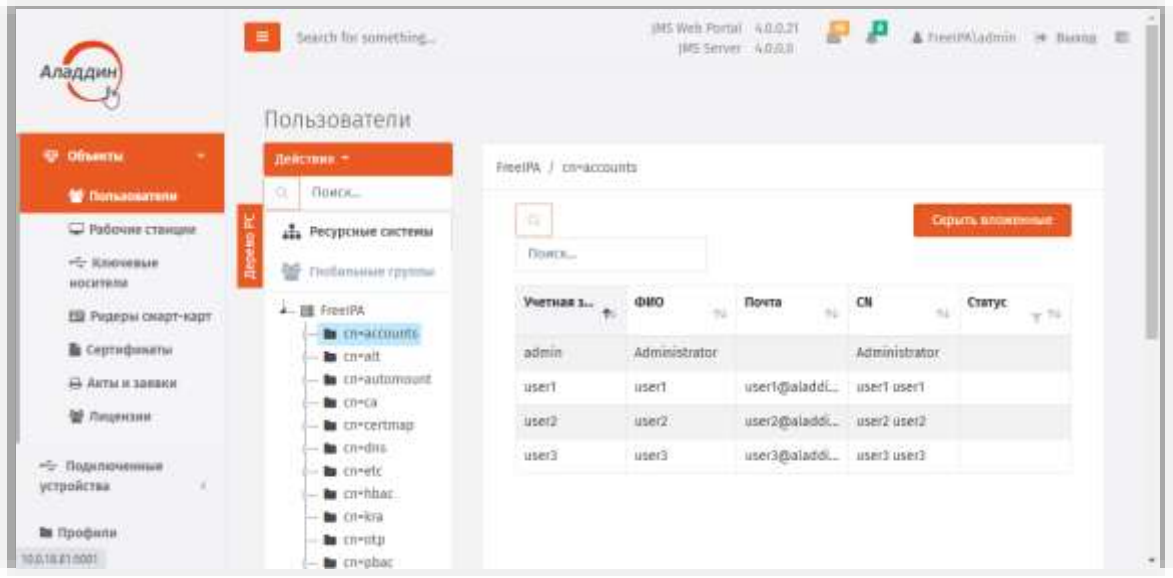


Рис. 6 – Список зарегистрированных пользователей

3.1.2 Установка и отмена назначения временного пароля для работы с JMS

JMS позволяет назначить пользователям временный пароль для работы с JMS. Это может понадобиться в тех случаях, когда пользователь временно не имеет доступа к своему электронному ключу. При установке пароля задается срок его действия, однако отменить действие времени пароля можно и раньше установленного срока действия.

3.1.2.1 Установка временного пароля

Чтобы установить временный пароль для пользователя JMS, выполните следующие действия.

1. В левой части консоли управления JMS перейдите в раздел **Объекты** -> **Пользователи** и в дереве ресурсной системы выберите контейнер, содержащий нужного пользователя.
2. В таблице справа выберите нужного пользователя, нажмите на нем правой кнопкой мыши и в контекстном меню выберите **Установить пользователю пароль для работы в JMS:**

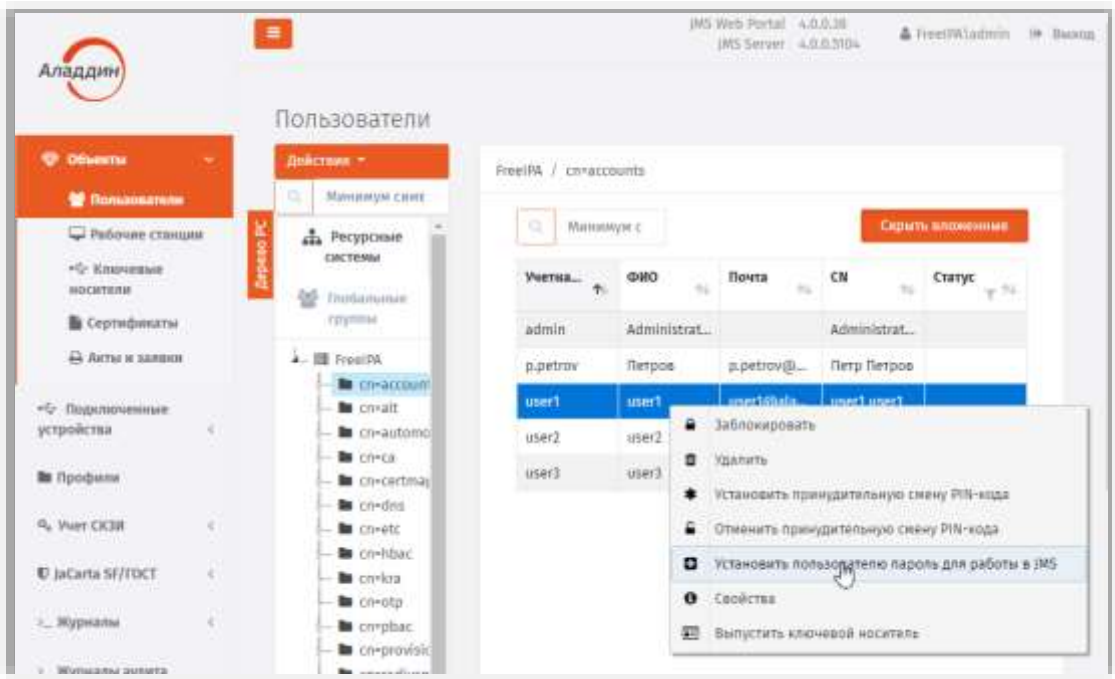


Рис. 7 – Выбор установки временного пароля JMS в контекстном меню пользователя

3. Отобразится окно установки пароля JMS.

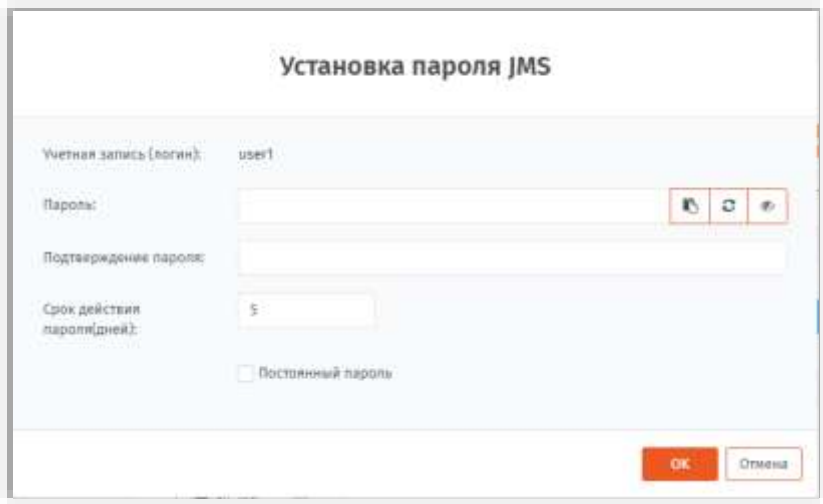


Рис. 8 – Окно установки временного пароля JMS

4. В полях **Пароль** и **Подтверждение пароля** введите временный пароль и подтверждение соответственно.

Вы также можете воспользоваться кнопкой автоматической генерации пароля ( ), чтобы сгенерировать случайное значение пароля. В этом случае поля **Пароль** и **Подтверждение пароля** будут заполнены автоматически.

5. В поле **Срок действия пароля (дней)** укажите число дней, в течение которых временный пароль будет действителен. По истечении этого срока пароль прекратит свое действие. Либо установите признак **Постоянный пароль**, в этом случае пароль станет бессрочным.
6. При необходимости воспользуйтесь дополнительными кнопками справа:
   - – отображает значение пароля;
   - – копирует в буфер значение временного пароля, чтобы его можно было передать пользователю.
7. Нажмите OK.
   Отобразится сообщение следующего вида.

Рис. 9 – Сообщение об успешной установке временного пароля

8. Нажмите **OK**, чтобы завершить процедуру.

3.1.2.2 Отмена действия временного пароля

Чтобы отменить временный пароль для пользователя JMS, выполните следующие действия.

1. В консоли управления выберите раздел **Объекты** –> **Пользователи**, в дереве ресурсной системы выберите контейнер, содержащий нужного пользователя.
2. В таблице справа выберите нужного пользователя, нажмите на нем правой кнопкой мыши и в контекстном меню выберите пункт **Отменить назначенные пользователю пароль JMS**.
3. В окне предупреждающего сообщения нажмите **ОК**, чтобы подтвердить действие.

3.1.3 Блокировка/разблокировка пользователей

JMS позволяет блокировать, а также разблокировать ранее заблокированных пользователей.

При блокировке пользователя будет приостановлена возможность использования всех электронных ключей пользователя и содержащихся в их памяти объектов.

Чтобы заблокировать пользователя, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Объекты -> Пользователи**.
2. В списке слева выберите контейнер ресурсной системы (например cn=accounts), содержащий пользователей, которых необходимо заблокировать.
3. На правой панели выберите учётные записи пользователей и нажмите на ней правой кнопкой мыши, в появившемся меню действий нажмите **Заблокировать**:

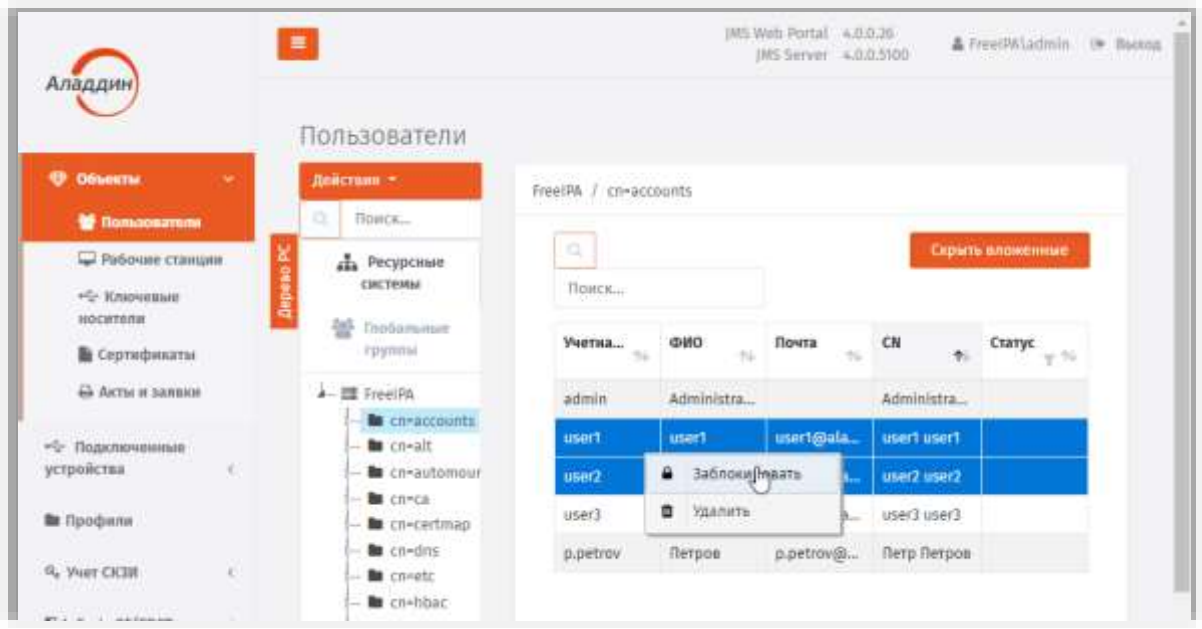


Рис. 10 – Вызов меню для блокировки пользователей

4. После блокировки пользователей в графе Статус их учётных записей отображается статус Заблокирован:.

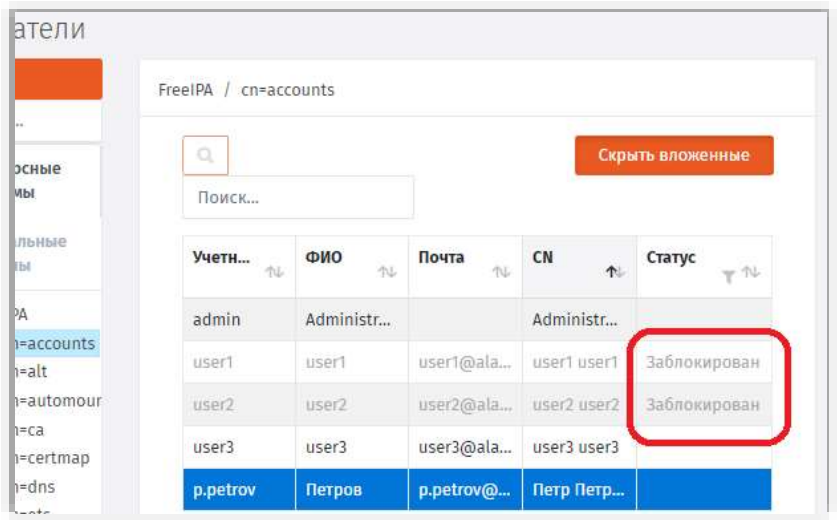


Рис. 11 – Отображение статуса заблокированных пользователей

Для разблокировки пользователя (пользователей) выберите его учётную запись и в меню действий выберите пункт **Разблокировать**.

3.1.4 Удаление пользователей из JMS

Система позволяет удалить пользователя для прекращения его учета в JMS (т.е. из базы данных JMS).

Пользователь, удаленный из JMS продолжается оставаться зарегистрированным в своей ресурсной системе (например FreeIPA или удостоверяющем центре DogTag). Поэтому удаленный из JMS пользователь может быть в последующем восстановлен путем процедуры регистрации (см. раздел «Регистрация пользователей в JMS», с. 14).

Чтобы удалить пользователя из JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Объекты -> Пользователи**.
2. В списке слева выберите контейнер ресурсной системы (например cn=accounts), содержащий пользователей, которых необходимо удалить.

3. На правой панели выберите учётные записи пользователя (пользователей) и нажмите на ней правой кнопкой мыши, в появившемся меню действий нажмите **Удалить**:

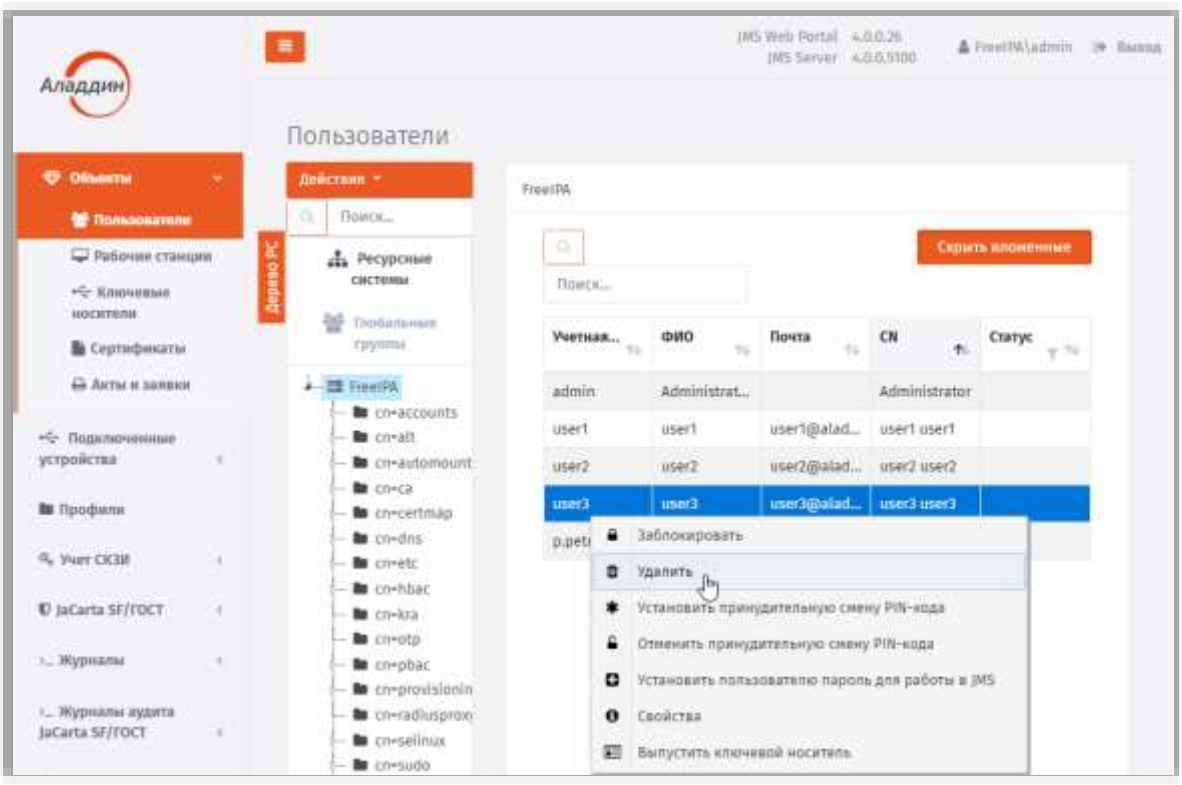


Рис. 12 – Вызов меню для удаления пользователей

4. В окне запроса на подтверждение удаления нажмите **Да**:

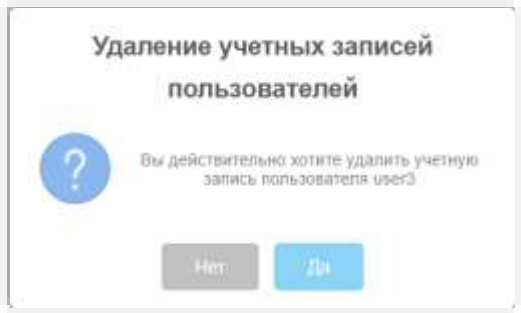


Рис. 13 – Окно запроса на удаление пользователя из JMS

3.2 Управление рабочими станциями

3.2.1 Регистрация рабочих станций в JMS

Чтобы зарегистрировать рабочие станции в JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Объекты** -> **Рабочие станции**. Страница консоли будет иметь следующий вид.

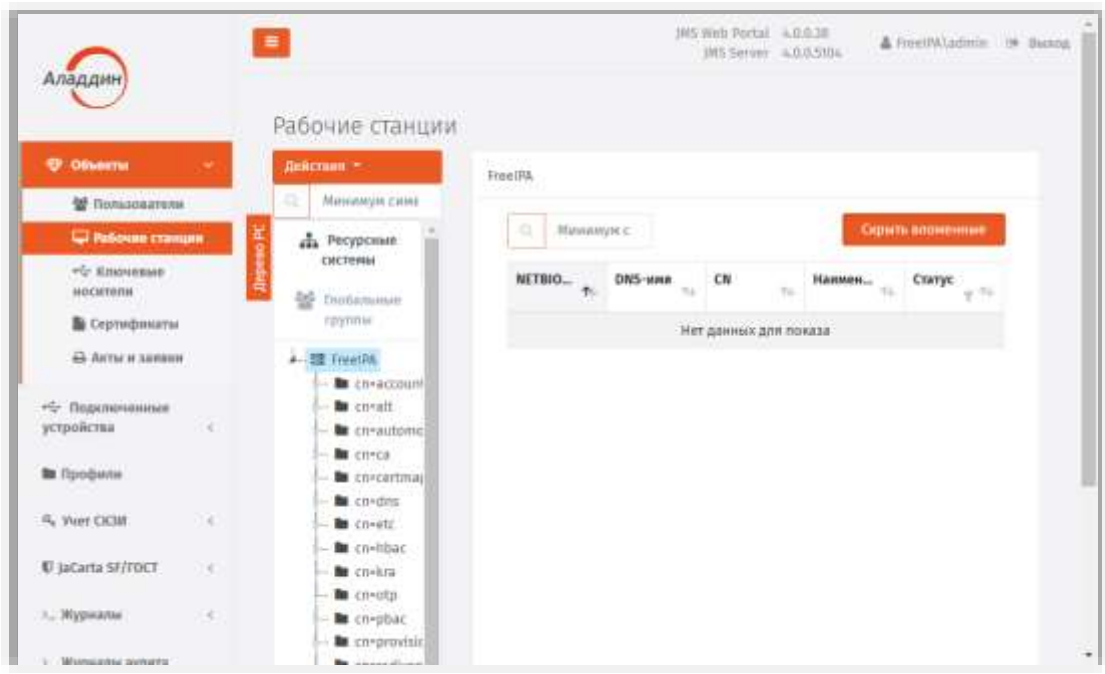


*Рис. 14 – Раздел **Рабочие станции** консоли управления JMS*

2. В меню **Действия** выберите **Зарегистрировать рабочие станции**:

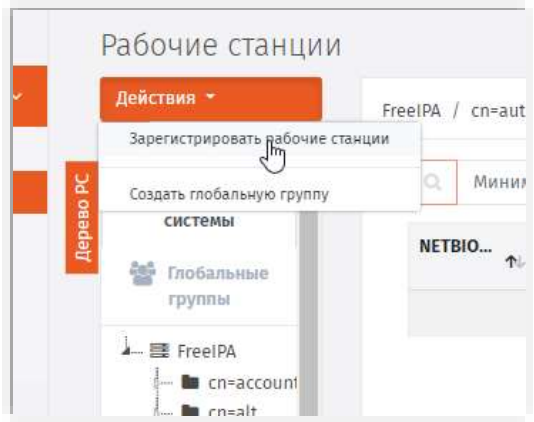


Рис. 15 – Выбор действия Зарегистрировать рабочие станции

3. Интерфейс переключится в режим регистрации рабочих станций:

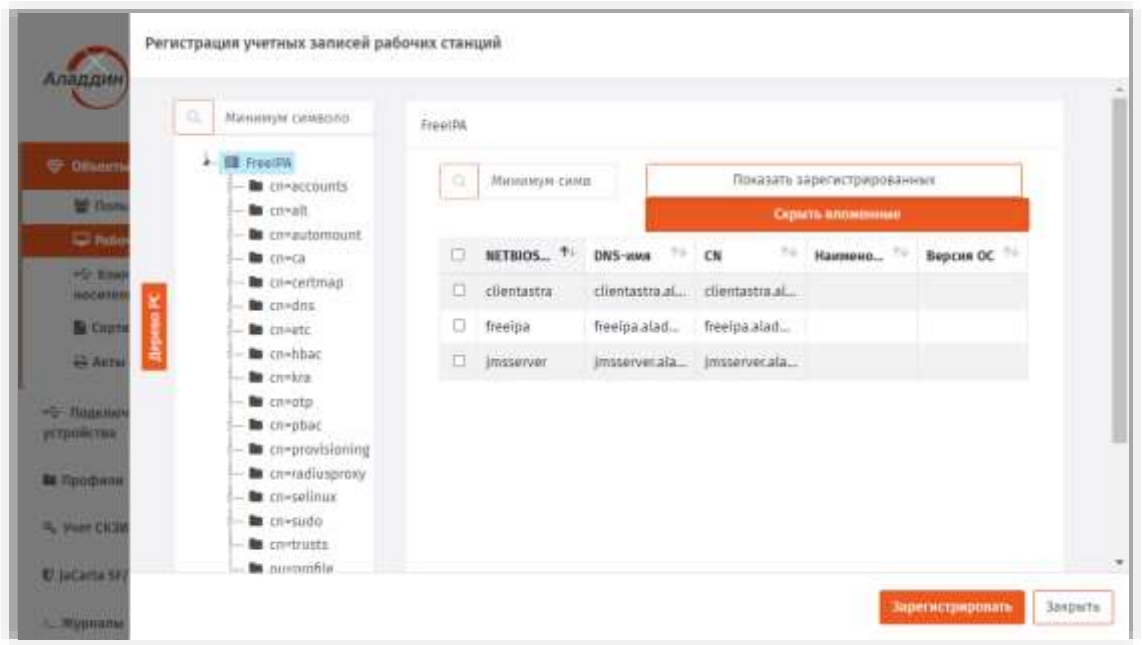


Рис. 16 – Страница регистрации рабочих станций

4. Выберите нужный контейнер (например, **cn = accounts**) и выберите нужные рабочие станции, установив напротив них флажки, либо установите общий флажок вверху, чтобы пометить все рабочие станции из выбранного контейнера и нажмите кнопку **Зарегистрировать** внизу.
5. Добавив рабочие станции нажмите кнопку **Закрыть**.
   Зарегистрированные рабочие станции отобразятся в окне консоли управления JMS:

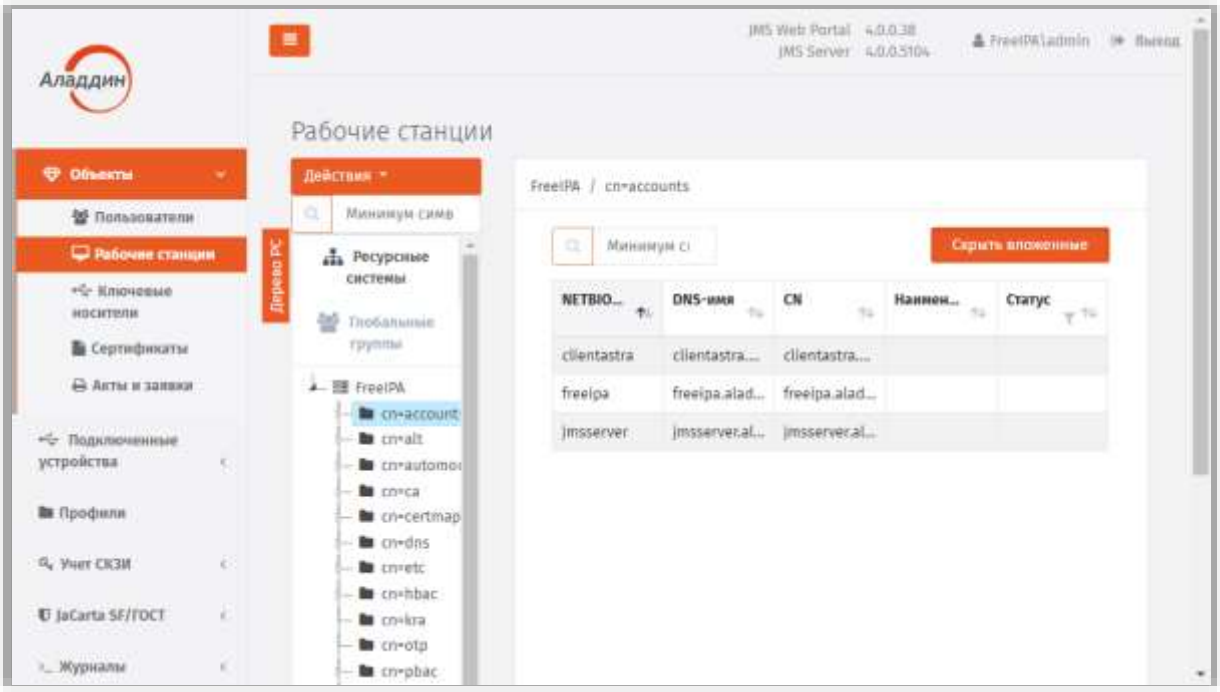


Рис. 17 – Список зарегистрированных рабочих станций

3.2.2 Блокировка/разблокировка рабочих станций

Примечание. В текущей версии продукта блокировка рабочей станции заключается в следующих ограничениях ее функционирования:

1. при синхронизации рабочей станции:
   - не выполняется учет сертификатов в хранилищах на рабочей станции;
   - на рабочей станции не выполняется поиск экземпляров СКЗИ;
2. не выполняется передача журналов аудита с клиентского приложения JMS на сервер JMS.

JMS позволяет блокировать, а также разблокировать ранее заблокированные рабочие станции. Чтобы заблокировать или разблокировать рабочую станцию, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Объекты** -> **Рабочие станции**.
2. В дереве ресурсных систем (**Дерево РС**) отметьте контейнер ресурсной системы, содержащий рабочие станции, которые нужно заблокировать или разблокировать (например **cn = accounts**).
3. В таблице справа выберите рабочую станцию, нажмите на ней правой кнопкой мыши и в контекстном меню выберите **Заблокировать**:

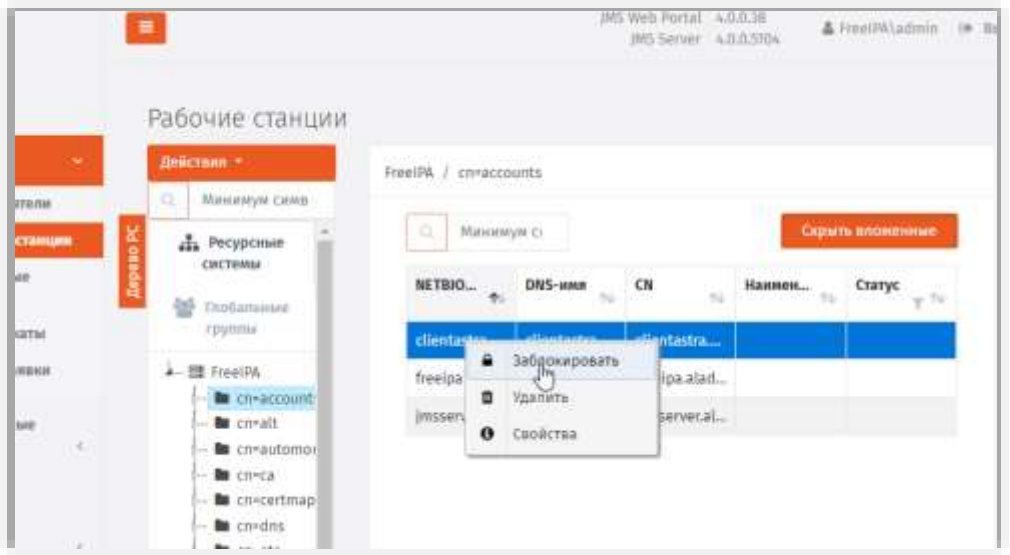


Рис. 18 – Список зарегистрированных рабочих станций

4. В окне подтверждения действия нажиме Да.

Рис. 19 – Запрос на подтверждение операции

В списке рабочих станций заблокированная станция будет отображена со статусом **Заблокирована**:

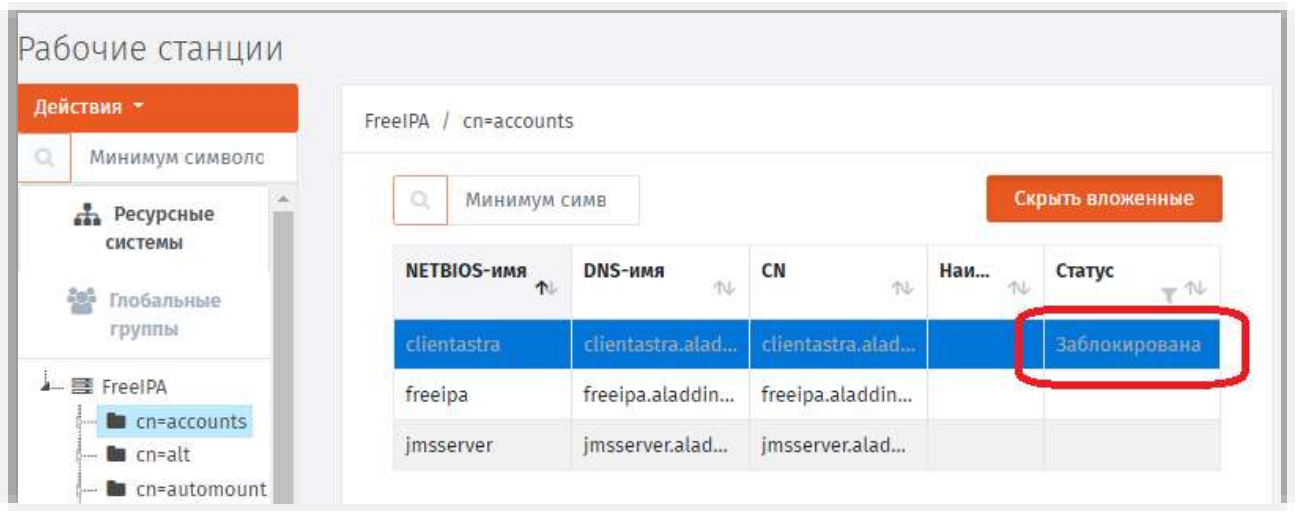


Рис. 20 – Отображение статуса заблокированной рабочей станции

Для разблокировки рабочей станции выполните те же шаги, что и для блокировки, только в контекстном меню для заблокированной рабочей станции выберите **Разблокировать**.

3.2.3 Внедоменные рабочие станции

Сервер JMS позволяет автоматически регистрировать рабочие станции, не входящие в домен Windows, в котором развернута система JMS.

Учет внедоменных рабочих станций предоставляет следующие возможности:

- работа с журналом клиентских уведомлений (журнал **Клиентские события**) от внедоменных станций;
- привязка профилей к внедоменным рабочим станциям;
- включение внедоменных рабочих станций в глобальные группы;
- использование внедоменных рабочих станций в учете СКЗИ;
- блокировка / разблокировка и удаление внедоменных рабочих станций.

Регистрация внедоменной рабочей станции выполняется только автоматически и только при аутентификации рабочей станции на сервере JMS (внедоменную рабочую станцию нельзя зарегистрировать вручную из консоли управления JMS или в результате выполнения плана обслуживания). После регистрации рабочей станции ее учетная запись появится консоли управления JMS в разделе **Объекты -> Рабочие станции** в отдельной ресурсной системе с названием **Внедоменные рабочие станции** (отображается последней в списке зарегистрированных ресурсных систем, Рис. 21).

.

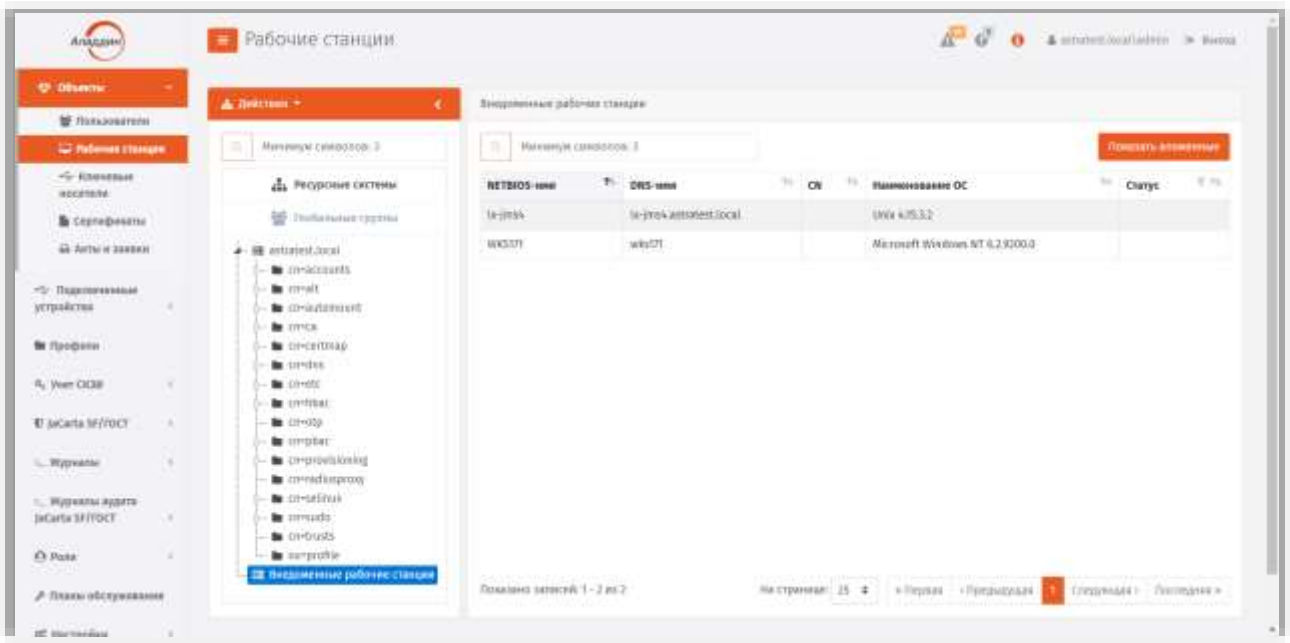


Рис. 21 – Работа с внедоменными рабочими станциями в JMS

Попытка автоматической регистрации внедоменной станции осуществляется каждый раз при ее аутентификации на сервере JMS. Если в процессе аутентификации внедоменной рабочей станции выяснится, что она еще не зарегистрирована, выполняется ее регистрация; если же станция уже зарегистрирована, то выполняется обновление ее атрибутов (таких, как NetBIOS-имя, DNS-имя и др.), если они изменились со времени ее последней аутентификации.

Операции блокировки / разблокировки и удаления с внедоменными рабочими станциями осуществляется так же, как и с обычными рабочими станциями.

3.3 Операции с сертификатами

Операции с сертификатами выполняются в разделе **Объекты -> Сертификаты** консоли управления JMS. (Рис. 22).

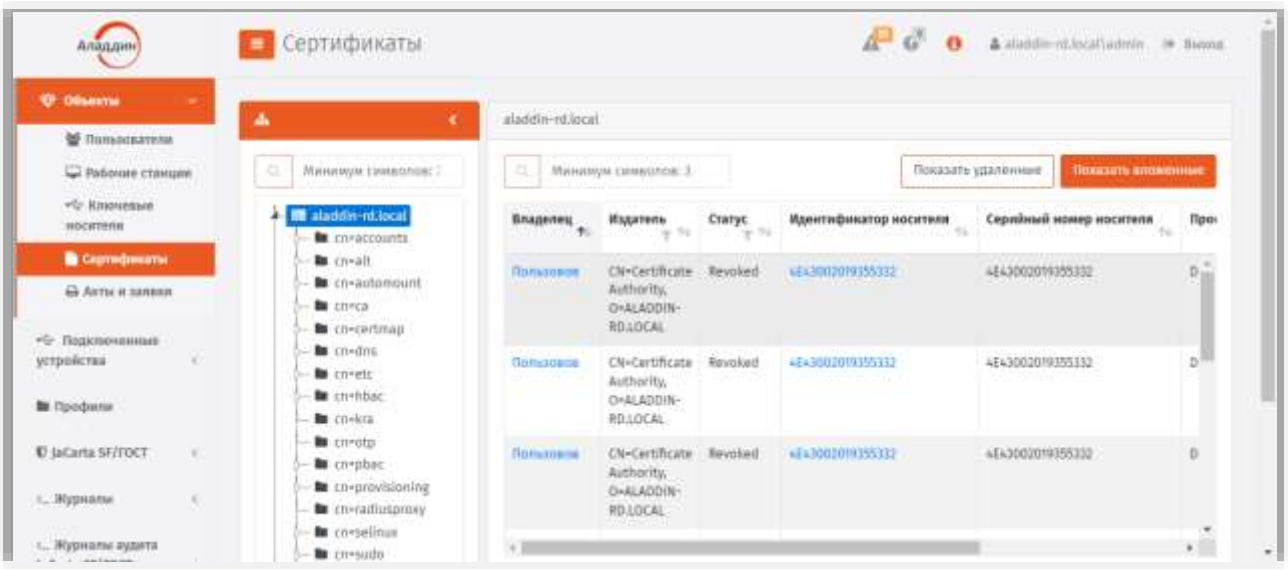


*Рис. 22 – Раздел **Объекты -> Сертификаты** консоли управления JMS*

3.3.1 Отзыв сертификата

Операция **Отозвать** инициирует отзыв сертификата в удостоверяющем центре, выпустившем данный сертификат.

Отзыв сертификата доступен только для сертификатов, находящихся в состоянии **Сохранен на КН**.

После отзыва сертификат приобретает статус **Сохранен на КН и отозван во внешней системе**.

Чтобы отозвать сертификат, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Объекты -> Сертификаты.**
2. В списке справа выберите сертификат, который необходимо отозвать.
3. Нажмите в строке выбранного сертификата правой кнопкой мыши и выберите **Отозвать**.
4. В диалоговом окне с запросом на отзыв выбранного сертификата нажмите **Да**.

3.3.2 Приостановка/восстановление действия сертификата

JMS позволяет временно приостановить, а затем возобновить действие сертификата, выпущенного по запросу из JMS. При этом в удостоверяющем центре, на котором был выпущен сертификат, производятся стандартные операции по приостановке/восстановлению действия данного сертификата.

Операции **Отключить**/**Включить** доступны только для сертификатов, находящихся в состоянии **Сохранен на КН**.

После приостановки действия сертификат приобретает статус **Сохранен на КН и заблокирован во внешней системе**. (По восстановлении его действия – снова возвращается в состояние **Сохранен на КН**).

Чтобы приостановить/возобновить действие сертификата, выполните следующее.

1. В консоли управления JMS перейдите в раздел **Объекты -> Сертификаты**.
2. В списке справа выберите сертификат, действие которого вы хотите приостановить/возобновить.
3. Нажмите в строке выбранного сертификата правой кнопкой мыши и выберите:
   - **Отключить** – чтобы приостановить действие сертификата;
   - **Включить** — чтобы возобновить действие сертификата.
4. В диалоговом окне с запросом на выполняемое действие нажмите **Да**.

3.3.3 Импорт резервной копии закрытого ключа, связанного с сертификатом

В JMS реализована возможность добавить/восстановить резервную копию закрытого ключа, связанного с сертификатом, для еще не удаленных из JMS сертификатов, которые имеют один из следующих статусов:

- **Выпущен на КН**;
- **Сохранен на КН**;
- **Заблокирован во внешней системе** (действие сертификата приостановлено в выпустившем его удостоверяющем центре);
- **Отозван во внешней системе** (сертификат отозван в выпустившем его удостоверяющем центре).

Чтобы импортировать в JMS резервную копию закрытого ключа, связанного с сертификатом, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Объекты -> Сертификаты**.
2. В правой части окна выберите сертификат, копию закрытого ключа для которого необходимо импортировать, нажмите на нём правой кнопкой мыши и выберите Импорт резервных копий

Примечание. Для выполнения операции **Импорт резервных копий** пользователь должен быть наделен ролью, в которой добавлено право на выполнение операции **Ключевые носители** -> **Импорт резервных копий сертификатов**. (Поскольку ни одна из встроенных ролей JMS не содержит такого права, соответствующую роль необходимо создать вручную. Подробнее см. «Создание, редактирование и назначение ролей JMS», с. 264)

Отобразится окно мастера импорта резервных копий сертификата.

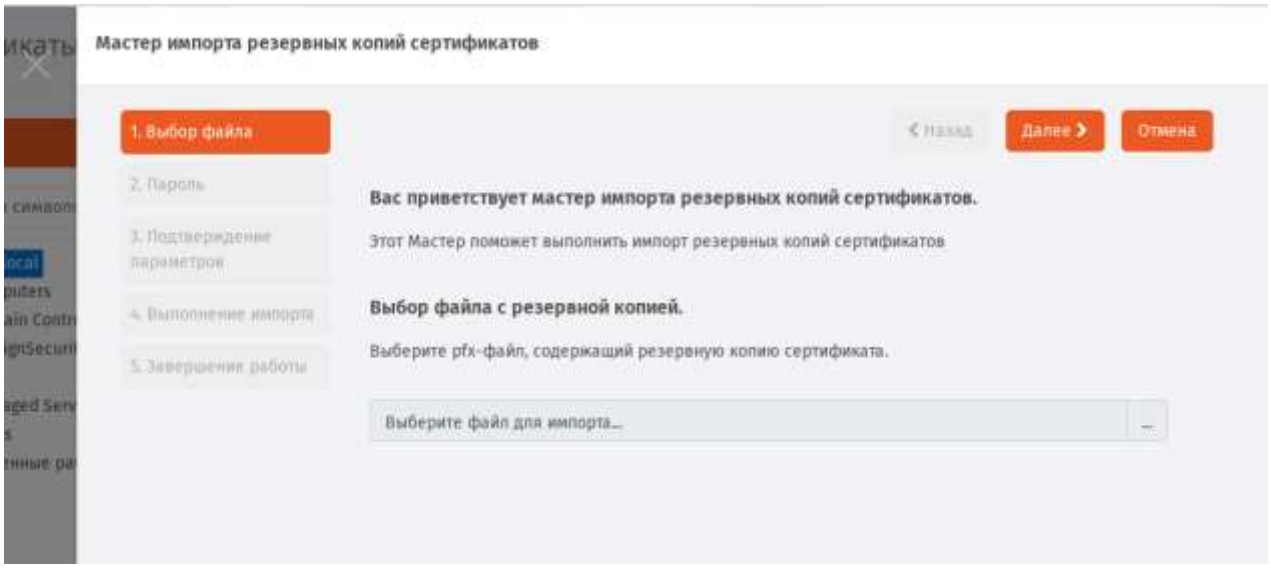


Рис. 23 – Приветственное окно мастера импорта резервных копий сертификатов

3. Следуйте указаниям мастера до завершения процедуры импорта резервной копии закрытого ключа.

3.4 Операции с ЭК/ЗНИ

3.4.1 Жизненный цикл ЭК/ЗНИ

Обобщенная диаграмма жизненного цикла ЭК/ЗНИ (в пользовательском интерфейсе – ключевого носителя, КН) отображена на Рис. 24. На данной диаграмме в скобках указываются приложение – *Консоль управления JMS* и/или *Клиент JMS*, – из которых доступно соответствующее действие (операция), в результате которого происходит переход от одного состояния КН к другому.

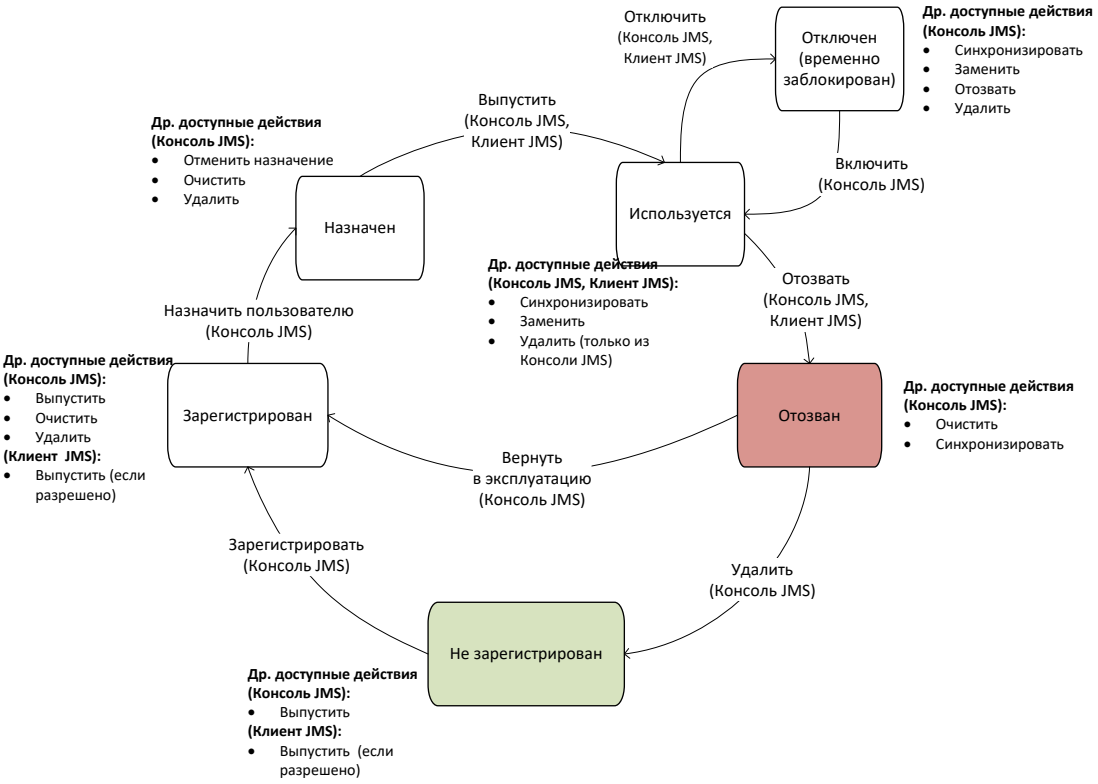


Рис. 24 – Диаграмма жизненного цикла ключевого носителя (электронного ключа/ЗНИ)

Ниже приведено краткое описание операций с КН, доступных в зависимости от его текущего состояния в соответствии с Рис. 24.

Регистрация КН (операция **Зарегистрировать**). В результате регистрации КН привязывается к объекту ресурсной системы и в JMS создается запись с его общими реквизитами. Запись о КН начинает отображаться в разделе **Ключевые носители** консоли управления JMS. Операция регистрации КН может быть использована для ограничения возможности выпуска из клиентского приложения JMS (используя профиль клиентского агента, см. «Настройка профиля клиентского агента», с. 101) тех КН, которые еще не зарегистрированы в JMS. Подробное описание операции регистрации КН см. в разделе «Регистрация подсоединенных ЭК/ЗНИ в JMS», с. 30.

Назначение КН (операция **Назначить пользователю**). В результате выполнения операции ключевому носителю назначается пользователь – владелец КН. Операция назначения КН пользователю может быть использована для ограничения возможности выпуска из клиентского приложения JMS (используя профиль клиентского агента, см. «Настройка профиля клиентского агента», с. 101) тех КН, которые еще не назначены пользователю. Подробнее об операции назначения КН см. в разделе «Назначение / отмена назначения ЭК/ЗНИ пользователю», с. 35.

Выпуск КН (операция **Зарегистрировать и выпустить**). Данная операция выполняет полную подготовку КН к его эксплуатации. В процессе выпуска, в зависимости от профилей, привязанных к пользователю – владельцу КН или к содержащему данного пользователя контейнеру (см. «Привязка профилей», с. 195), КН может быть проинициализирован, в нем может быть сгенерирована ключевая пара, а также записаны необходимые объекты JMS (в т.ч. сертификаты открытого ключа). Подробное описание операции см. в разделе «Выпуск ЭК/ЗНИ администратором», с. 39.

Отключение КН (операция **Отключить**). В результате отключения КН происходит его временная блокировка в JMS (НЕ ПУТАТЬ с физической блокировкой КН, связанной блокировкой PIN-кода. см. «Разблокировка подсоединенного электронного ключа», с. 59), после чего пользователю становятся недоступным открытие с помощью данного КН открытие пользовательского сеанса в

клиенте JMS. Подробнее см. раздел «Отключение/включение возможности использования ЭК/ЗНИ », с. 44.

Включение КН (операция **Включить**). Включение КН – процедура, обратная его временной блокировке (см. Отключение КН, выше). В результате включения КН пользователь вновь получает возможность выполнять аутентификацию с помощью данного КН в клиенте JMS и производить другие действия, доступные в состоянии КН *Используется*. Подробнее см. раздел «Отключение/включение возможности использования ЭК/ЗНИ », с. 44.

Отзыв КН (операция **Отозвать**). В результате отзыва КН переходит на завершающую стадию жизненного цикла (состояние *Отозван*). При этом в зависимости от настроек привязанного профиля выпуска сертификата из КН могут отзываться (удаляться, а также отзываться из УЦ, в случае сертификата открытого ключа) все объекты, выпущенные с помощью JMS. Операция отзыва производится автоматически при замене одного КН на другой (см. «Замена ЭК/ЗНИ», с. 52), а также вручную при прекращении эксплуатации КН, например, по причине его компрометации или в случае смены его владельца. Подробнее об операции отзыва см. в разделе «Отзыв ЭК/ЗНИ », с. 50.

Удаление КН (операция **Удалить**). При удалении КН выполняется его отзыв (см. Отзыв КН, выше); КН переходит в состояние *Не зарегистрирован*; запись о КН перестает отражаться в списке зарегистрированных КН в консоли управления JMS (раздел **Объекты** -> **Ключевые носители**). Подробнее об операции удаления КН см. в разделе «Удаление ЭК/ЗНИ », с. 62.

Описание других операций, отображенных на диаграмме жизненного цикла приведено в следующих разделах:

- «Замена ЭК/ЗНИ», с. 52;
- «Синхронизация ЭК/ЗНИ», с. 47;
- «Очистка ЭК/ЗНИ», с. 45;
- «Назначение / отмена назначения ЭК/ЗНИ пользователю», с. 35.

Помимо перечисленных операций с КН, могут быть выполнены и другие, не отраженные на диаграмме жизненного цикла, такие как смена и разблокировка PIN-кода, PIN-кода подписи и т.п. Детальный список доступных операций над КН зависит от его текущего статуса, роли пользователя, выполняющего над ним операции, привязанных к нему профилей и их настроек. Подробное описание этих условий приведено в соответствующих разделах настоящего руководства.

3.4.2 Регистрация подсоединенных ЭК/ЗНИ в JMS

Чтобы зарегистрировать подсоединенный электронный ключ в JMS, выполните следующие действия.

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

2. В консоли управления перейдите в раздел **Подключенные устройства -> Ключевые носители:**

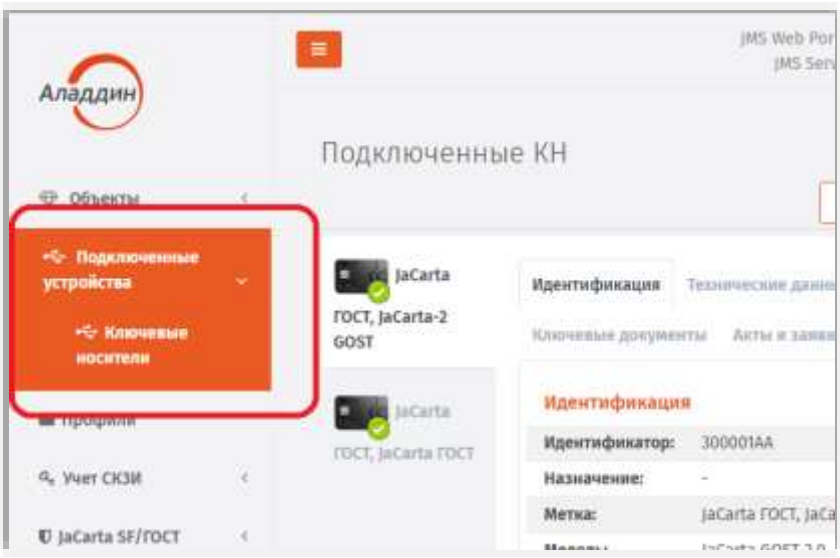


*Рис. 25 – Выбор раздела **Подключенные устройства** -> **Ключевые носители** в консоли управления JMS*

3. Выберите электронный ключ, который необходимо зарегистрировать:

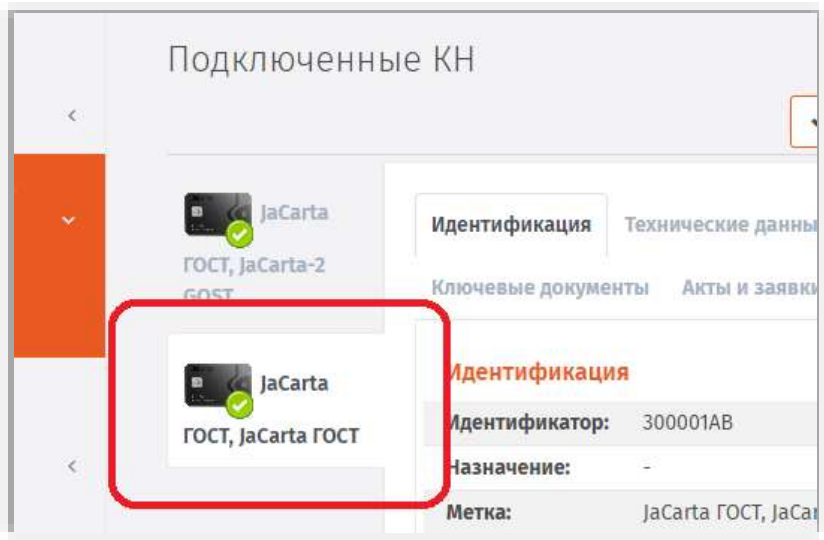


Рис. 26 – Выбор электронного ключа для регистрации

4. В меню действий выберите **Зарегистрировать**:

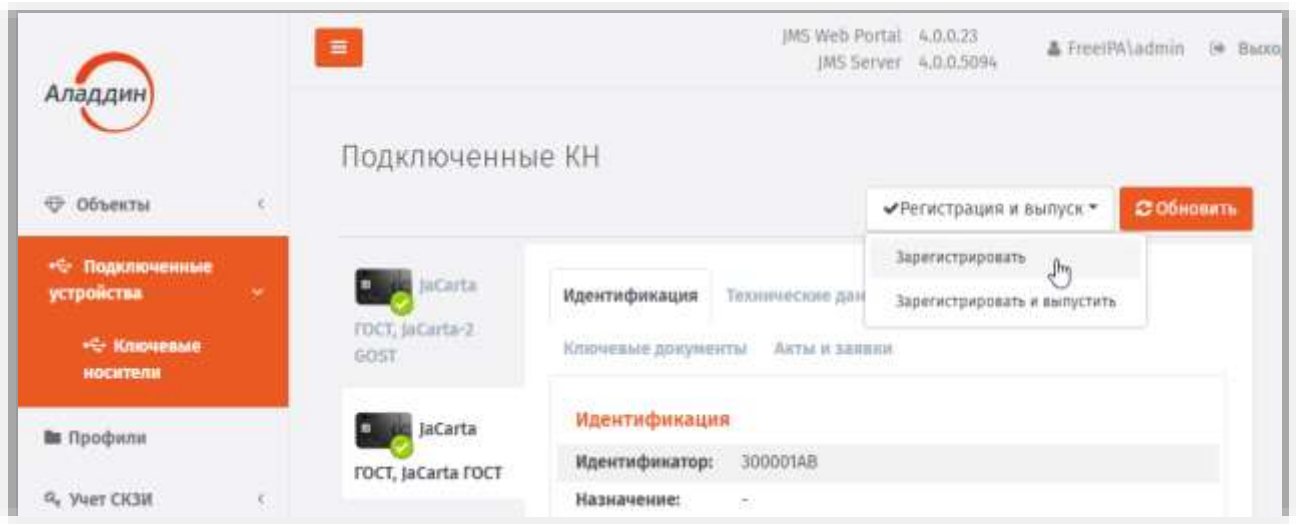


*Рис. 27 – Выбор действия **Зарегистрировать***

5. Выберите группу или организационную единицу, к которой будет привязан зарегистрированный электронный ключ, после чего нажмите **Далее**.
6. При необходимости укажите дополнительные данные (**Номер корпуса**, **Номер СКЗИ** и **Номер СЗИ**) и нажмите **Далее**.

   Примечание. При регистрации электронного ключа как СКЗИ в поле **Номер СКЗИ** следует ввести *регистрационный номер* соответствующего СКЗИ, указанный в его паспорте.
7. Дождитесь окончания работы мастера регистрации.

У зарегистрированного электронного ключа значение в поле **Статус** изменится на *Зарегистрирован:*

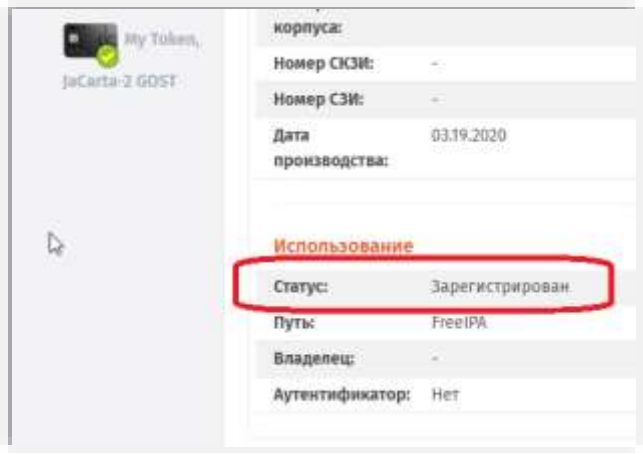


Рис. 28 – Значение статуса у зарегистрированного ЭК

3.4.3 Импорт (пакетная регистрация) ЭК/ЗНИ в JMS

Для пакетной регистрации электронных ключей в JMS следует воспользоваться файлом со списком электронных ключей компании-поставщика (предоставляется только компанией Аладдин для электронных ключей JaCarta по запросу заказчика).

Чтобы импортировать электронные ключи в JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Объекты** -> **Ключевые носители**.

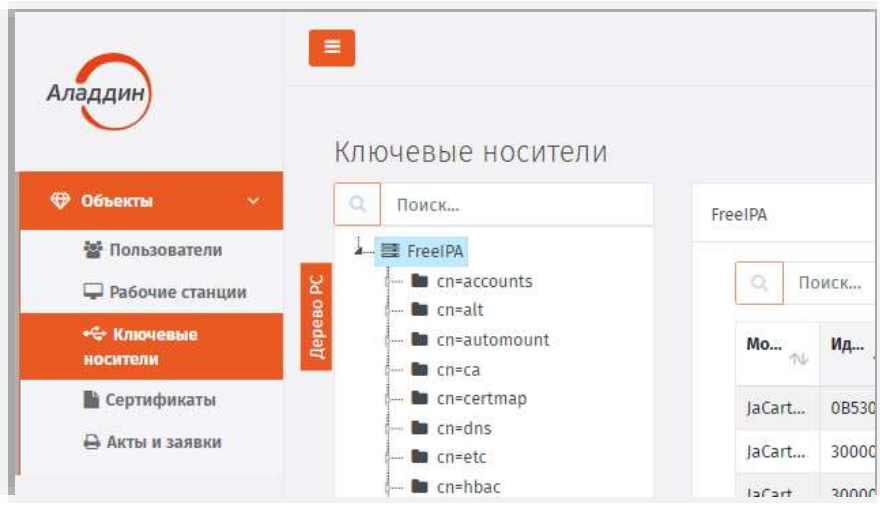


*Рис. 29 – Выбор раздела **Объекты** -> **Ключевые носители** в консоли управления JMS*

2. В дереве ресурсной системы выберите контейнер, в котором необходимо зарегистрировать электронные ключи, нажмите на нем правой кнопкой мыши и выберите **+Импорт**.

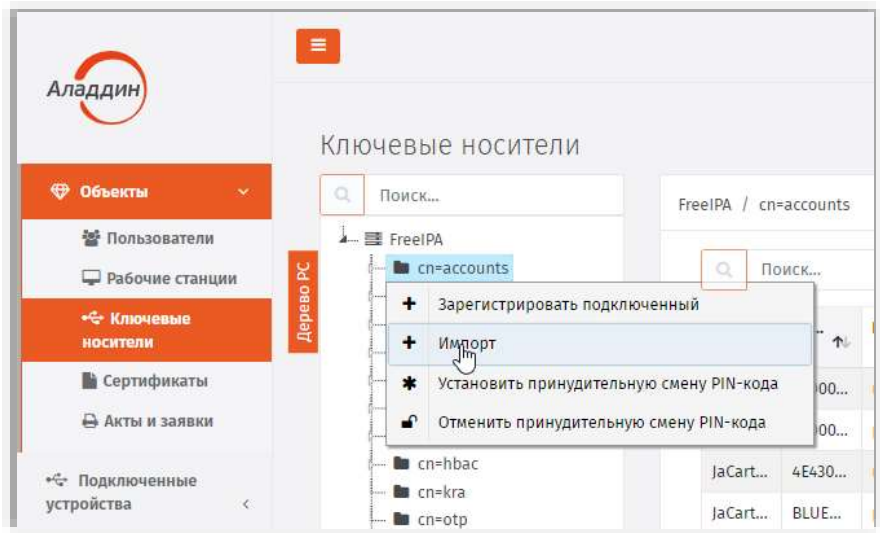


*Рис. 30 – Выбор раздела **Объекты** -> **Ключевые носители** в консоли управления JMS*

3. Откроется страница мастера импорта электронных ключей:

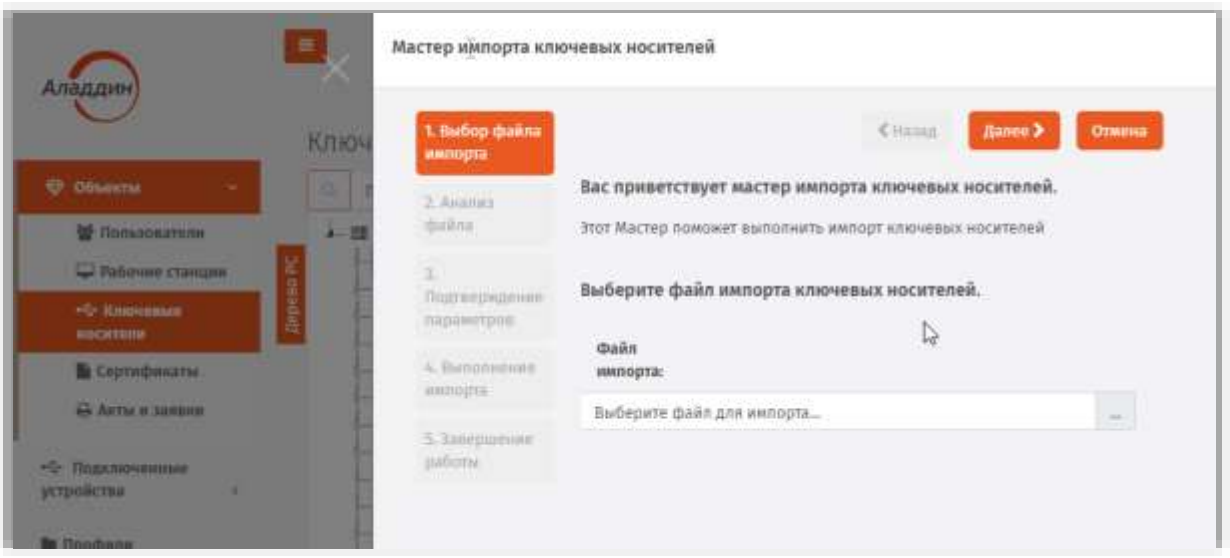


Рис. 31 – Стартовая страница мастера импорта электронных ключей

4. В поле **Файл импорта** нажмите три точки (**...**), выберите XML-файл для импорта и нажмите **Далее**.
5. Следуйте указаниям мастера до окончания процедуры импорта.
6. По окончании импорта отобразится страница завершения работы мастера:

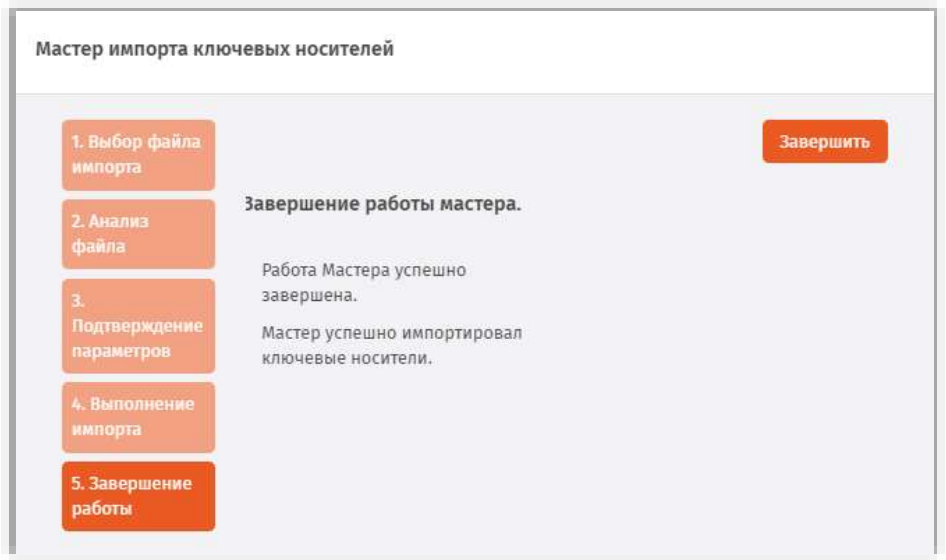


Рис. 32 – Страница завершения мастера импорта электронных ключей

Чтобы завершить работу мастера, нажмите **Завершить**.

Импортированные ключи отобразятся в разделе **Объекты** –> **Ключевые носители** со статусом *Зарегистрирован* в указанном пользователе контейнере ресурсной системы:

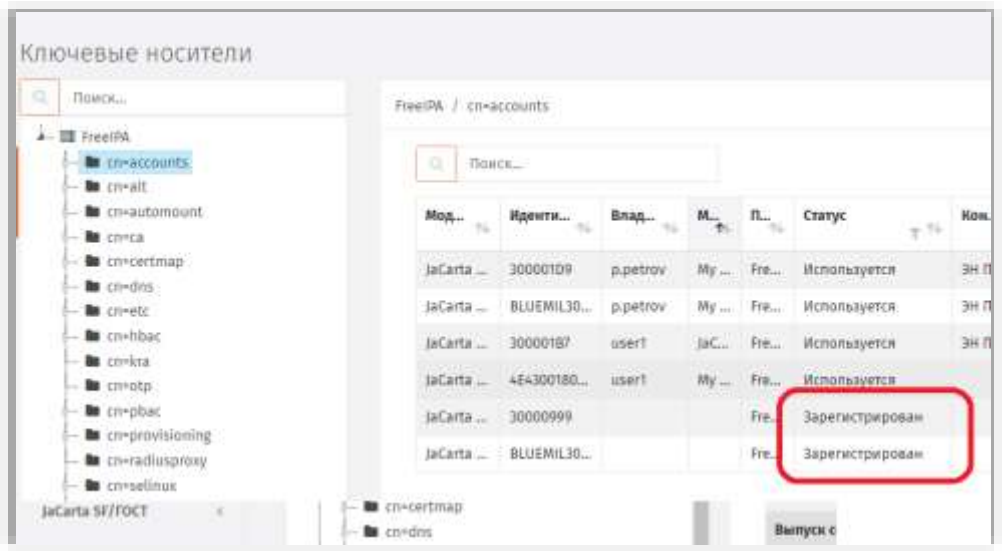


Рис. 33 – Результат пакетной регистрации электронных ключей

3.4.4 Назначение / отмена назначения ЭК/ЗНИ пользователю

3.4.4.1 Назначение пользователю

Перед назначением электронного ключа пользователю необходимо настроить профиль выпуска электронных ключей. После этого необходимо выполнить привязку настроенного профиля к пользователю либо к группе, в которую входит пользователь, которому назначается электронный ключ.

Подробнее см.:

- «Настройка профилей JMS», с. 95;
- «Настройка профиля выпуска электронных ключей», с. 97;
- «Привязка профилей», с. 195.

Назначить пользователю можно только зарегистрированный ранее электронный ключ (см. «Регистрация подсоединенных ЭК/ЗНИ в JMS», с. 30)

Чтобы назначить пользователю зарегистрированный электронный ключ в JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в один из следующих разделов:
   - **Объекты -> Ключевые носители**;
   - **Подключенные устройства** -> **Ключевые носители**.

В последнем случае электронный ключ, для которого необходимо выполнить назначение пользователю, должен быть подключен к компьютеру.

1.1. При действии из раздела **Объекты -> Ключевые носители** в центральной части окна выберите ключ, нажмите на нем правой кнопкой мыши и в появившемся меню выберите **Назначить**;

1.2. На странице назначения пользователя выберите на панели слева контейнер, содержащий пользователя, в центре экрана – пользователя, которому следует назначить электронный ключ, и нажмите **Назначить (**Рис. 34**).**

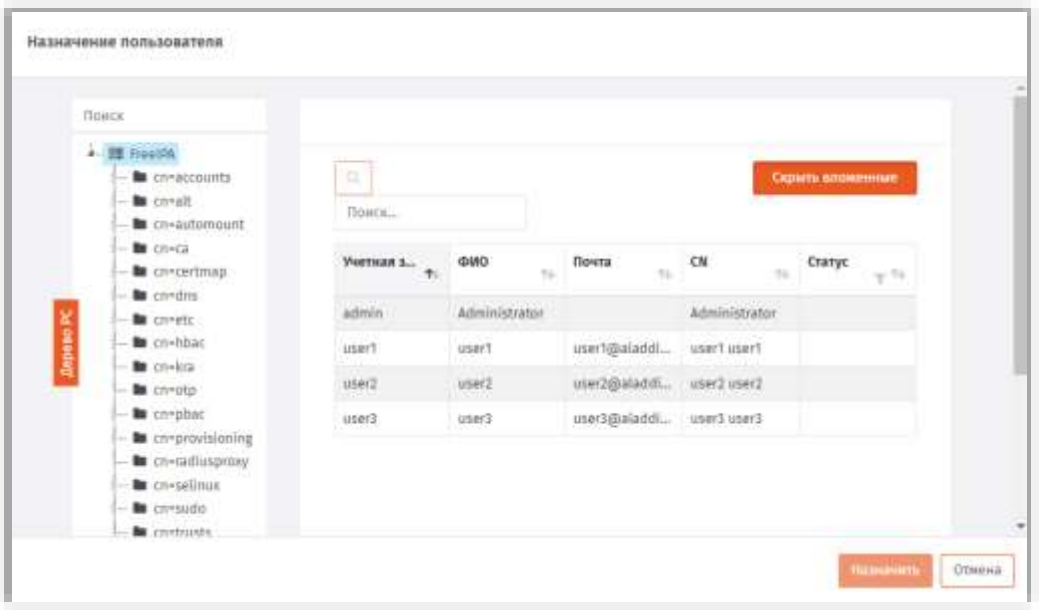


Рис. 34 – Страница назначения ЭК пользователю

2. При действии из раздела **Подключенные устройства -> Ключевые носители** в центральной части окна отметьте ключ, который вы хотите назначить пользователю:

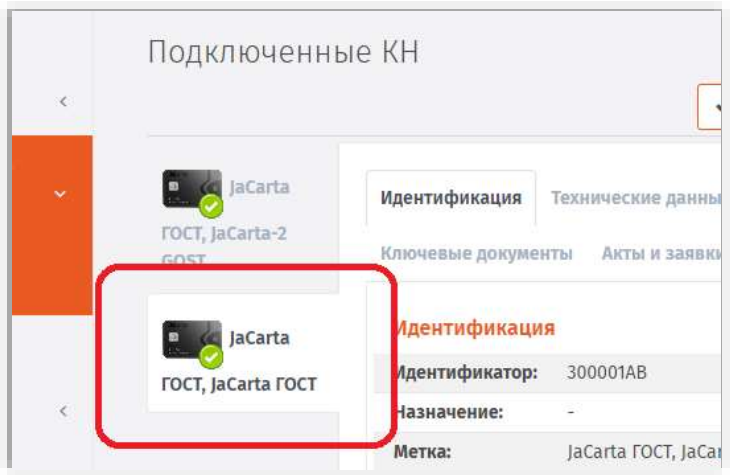


Рис. 35 – Выбор электронного ключа для назначения пользователю

2.1. вверху, в области выбора действий **Назначение**, выберите пункт **Назначить пользователю**:

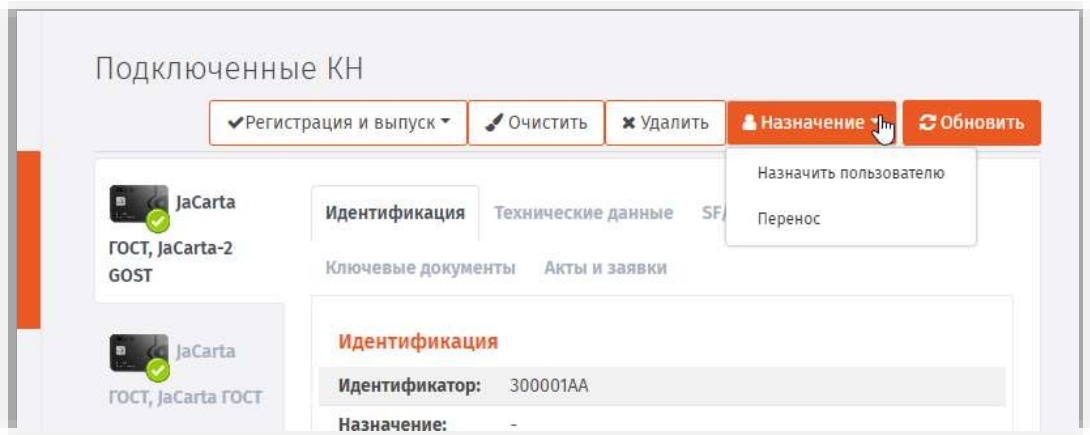


*Рис. 36 – Выбор действия **Назначить пользователю***

2.1. На странице назначения пользователя выберите на панели слева контейнер, содержащий пользователя, в центре экрана – пользователя, которому следует назначить электронный ключ, и нажмите **Назначить** (Рис. 34).

У электронного ключа, назначенного пользователю, значение в поле **Статус** изменится на *Назначен:*

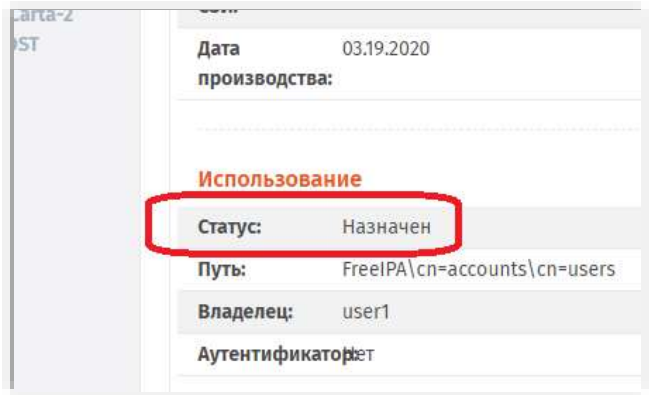


Рис. 37 – Значение статуса у ЭК, назначенного пользователю

Примечание. В случае если электронный ключ был ранее зарегистрирован как СКЗИ, при назначении его пользователю будет сформирован нормативный документ «Акт передачи СКЗИ новому ответственному пользователю».

3.4.4.2 Отмена назначения

Отмена назначения электронного ключа пользователю также как и назначение может производиться из следующих разделов консоли управления:

- **Объекты -> Ключевые носители**;
- **Подключенные устройства** -> **Ключевые носители**.

В последнем случае электронный ключ, для которого необходимо выполнить назначение пользователю, должен быть подключен к компьютеру.

Действия по отмене назначения электронного ключа пользователю производятся по аналогии с назначением (см. «Назначение пользователю», выше), при этом в меню действий следует выбирать пункт **Отменить назначение**.

При нажатии на **Отменить назначение** следует выполнить следующие действия.

1. В окне запроса на отмену назначения нажать **Да**:

Рис. 38 – Окно запроса на отмену назначения ЭК пользователю

2. На странице выбора контейнера ресурсной системы следует выбрать контейнер, которому будет назначен в JMS данный электронный ключ.

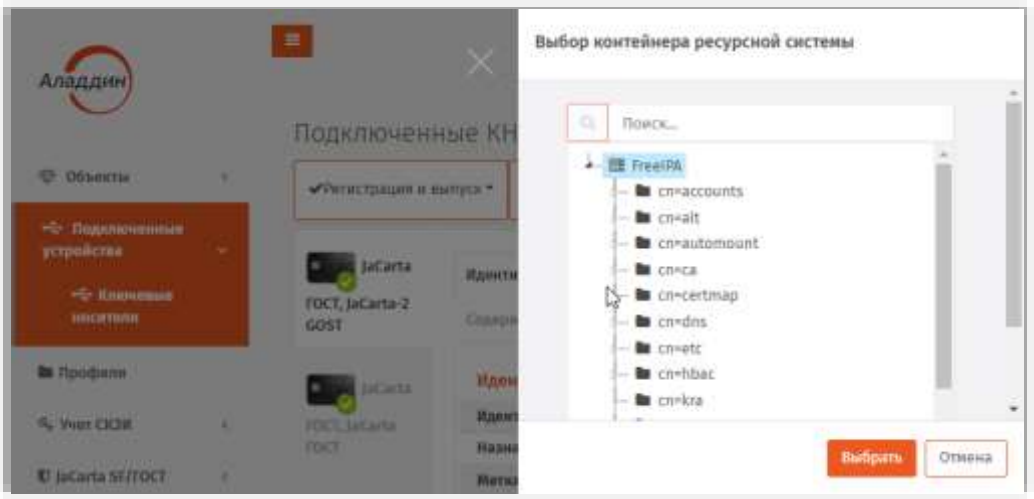


Рис. 39 – Страница выбора контейнера ресурсной системы для назначения ему ЭК

Статус электронного ключа после отмены его назначения пользователю меняется на *Зарегистрирован:*

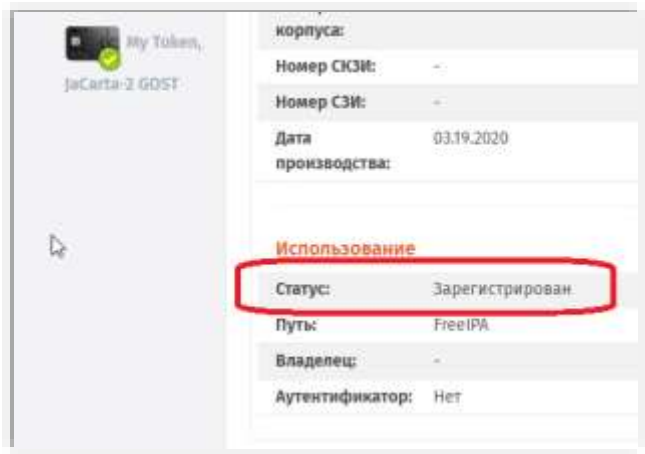


Рис. 40 – Значение статуса ЭК после отмены назначения пользователю

3.4.5 Выпуск ЭК/ЗНИ администратором

Процедура выпуска электронного ключа может отличаться в зависимости от настроек профилей (см. «Настройка профилей JMS», с. 95).

Чтобы выпустить подсоединенный электронный ключ в JMS, выполните следующие действия.

1. Подсоедините электронный ключ, который вы хотите выпустить, к компьютеру.
2. В консоли управления перейдите в раздел **Подключенные устройства -> Ключевые носители:**

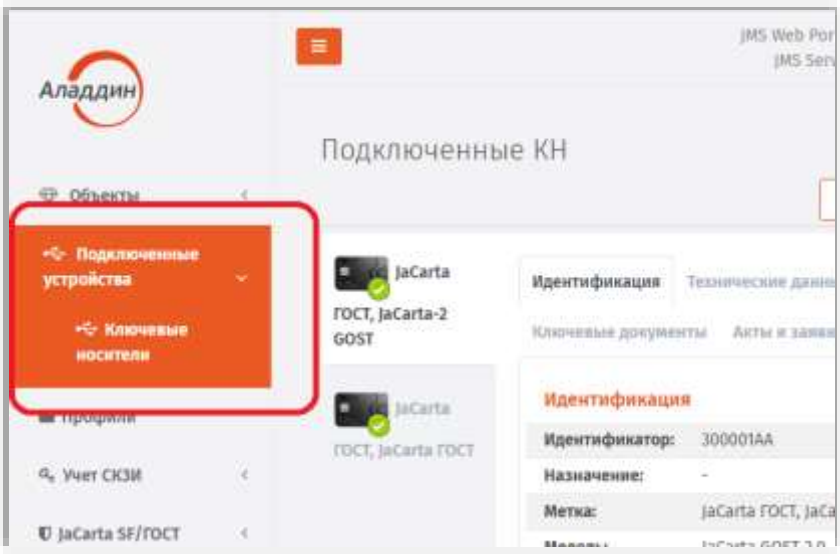


*Рис. 41 – Выбор раздела **Подключенные устройства -> Ключевые носители** в консоли управления JMS*

3. Выберите электронный ключ, который необходимо выпустить:

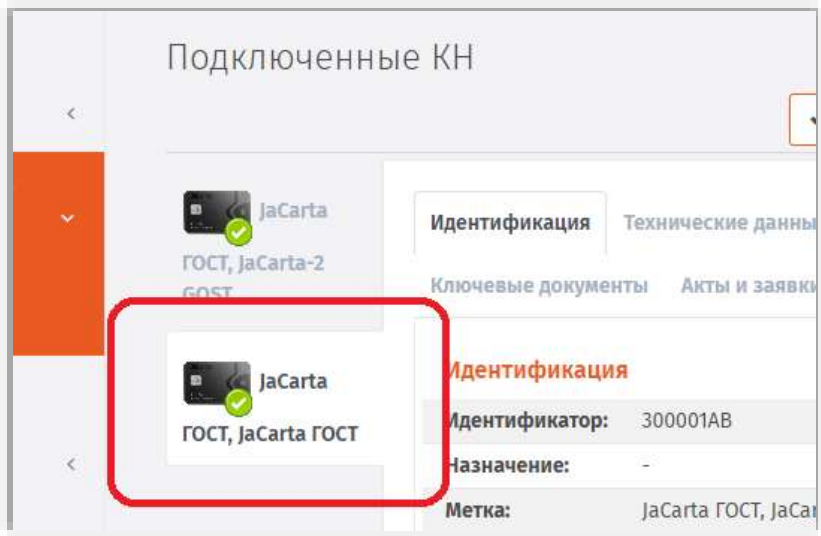


Рис. 42 – Выбор электронного ключа для регистрации

4. В меню действий выберите **Зарегистрировать и выпустить**:

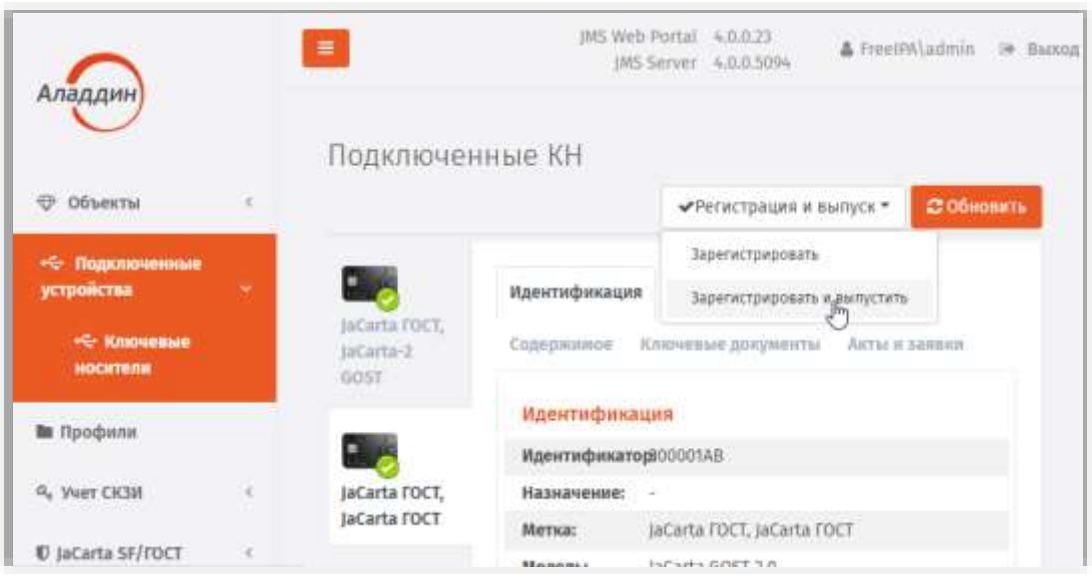


*Рис. 43 – Выбор действия **Зарегистрировать***

5. На странице **Выбор пользователя** выберите пользователя, на чье имя будет выпущен электронный ключ, после чего нажмите **Выбрать**:

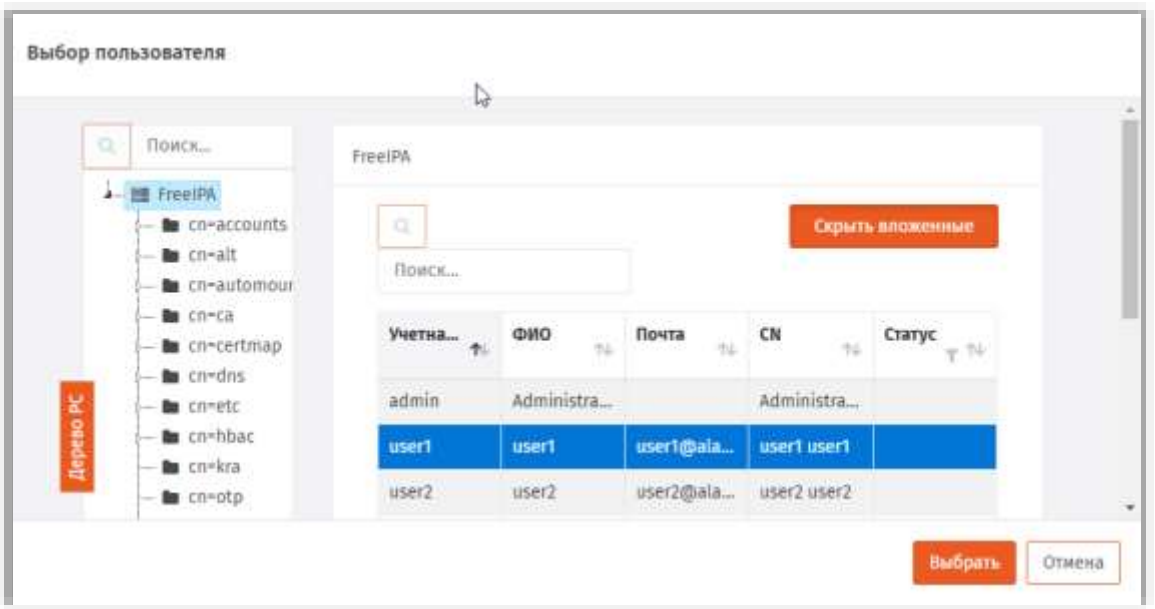


Рис. 44 – Выбор пользователя для выпуска ЭК

6. Откроется страница мастера выпуска электронных ключей, после чего нажмите **Далее:**

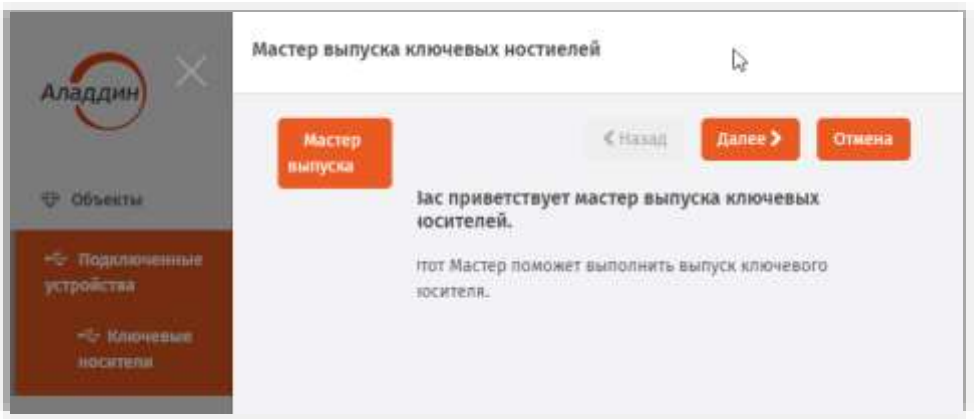


Рис. 45 – Стартовая страница мастера выпуска ЭК

7. Откроется страница ввода атрибутов ключевого носителя. При необходимости укажите дополнительные данные (**Номер корпуса**, **Номер СКЗИ** и **Номер СЗИ**) и нажмите **Далее**.

Примечание. При регистрации электронного ключа как СКЗИ в поле **Номер СКЗИ** следует ввести *регистрационный номер* соответствующего СКЗИ, указанный в его паспорте.

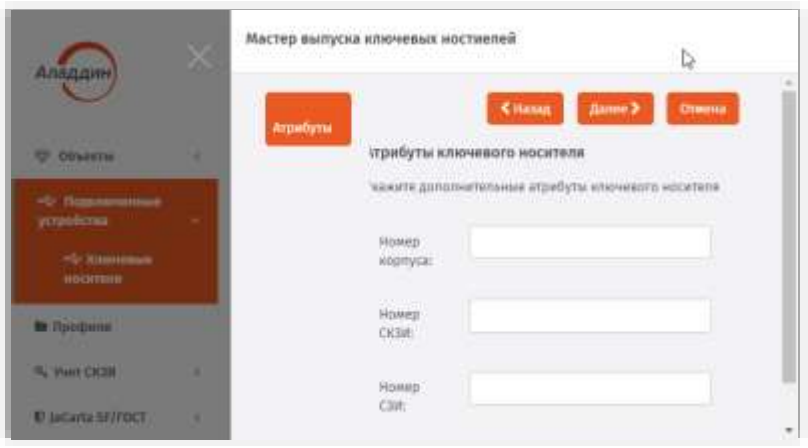


Рис. 46 – Страница ввод дополнительных параметров ЭК

8. Следуйте указаниям мастера. На странице указания информации о владельце электронного ключа (для моделей JaCarta SF/ГОСТ) при необходимости укажите информацию о владельце и нажмете **Далее**.

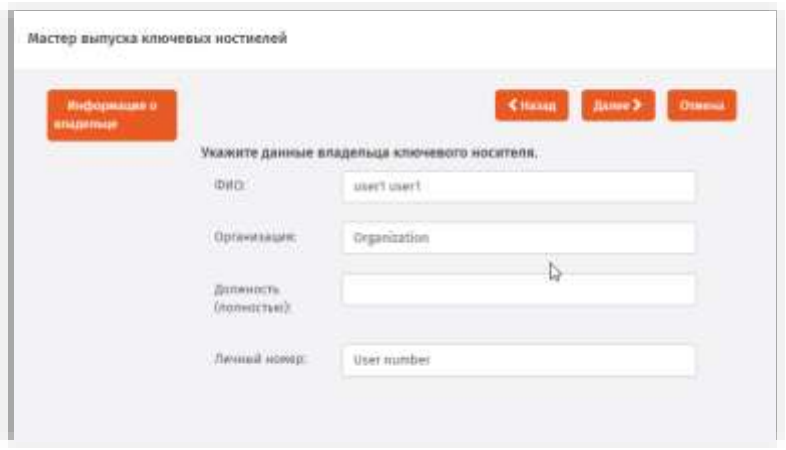


Рис. 47 – Страница для указания информации о владельце ЭК

9. На странице указания параметров приложения при необходимости укажите запрашиваемую информацию и нажмете **Далее**.

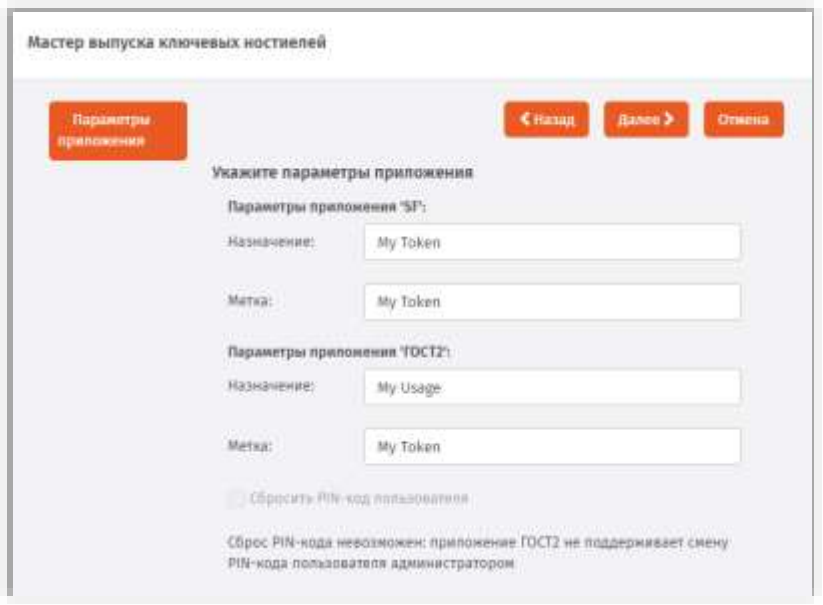
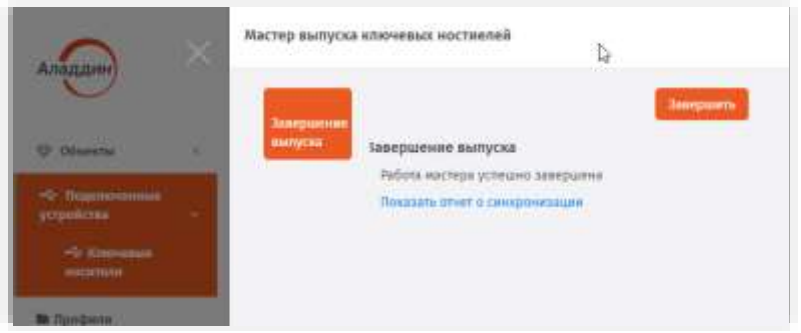


Рис. 48 – Страница для указания параметров приложения на ЭК

10. Следуйте указаниям мастера, после чего дождитесь окончания процедуры выпуска электронных ключей.

По завершении процедуры выпуска отобразится следующая страница:



:

Рис. 49 – Значение статуса у зарегистрированного ЭК

Чтобы посмотреть результаты работы мастера нажмите **Показать отчет о синхронизации**.

Чтобы завершить работу мастера, нажмите **Завершить**.

У электронного ключа, выпущенного на имя пользователя, значение в поле **Статус** изменится на *Используется:*

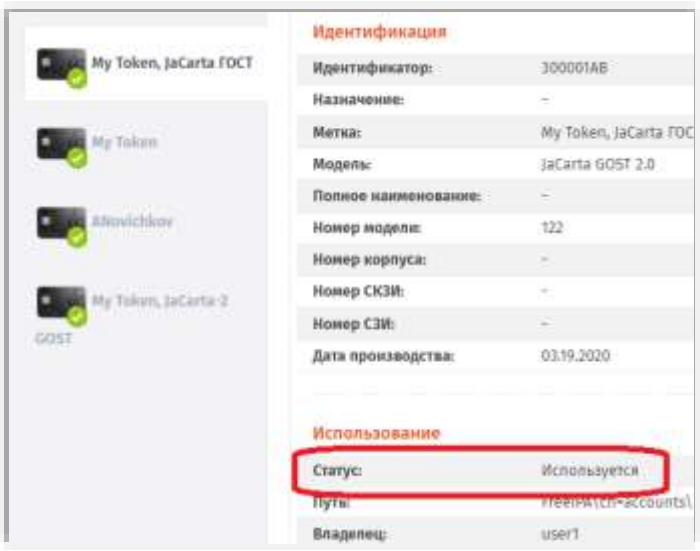


Рис. 50 – Значение статуса у ЭК, выпущенного на имя пользователя

3.4.6 Отключение/включение возможности использования ЭК/ЗНИ

JMS позволяет временно отключить, а затем включить возможность использования электронного ключа. Чтобы отключить/включить возможность использования электронного ключа, выполните следующие действия.

Отключение возможности использования электронного ключа означает, что объекты в его памяти, не будучи измененными, приостанавливают свое действие. При последующем включении возможности использования электронного ключа действие объектов в его памяти возобновляется.

1. В консоли управления JMS перейдите в один из следующих разделов:

   - **Объекты -> Ключевые носители**;
   - **Подключенные устройства** -> **Ключевые носители**.

В последнем случае электронный ключ, возможность использования которого вы хотите включить/отключить, должен быть подключен к компьютеру.

2. При действии из раздела **Объекты -> Ключевые носители** в центральной части окна выберите ключ, возможность использования которого вы хотите включить/отключить.

2.1. нажмите на нем правой кнопкой мыши и в появившемся меню выберите:

2.1.1. **Отключить** – чтобы временно отключить возможность использования электронного ключа;
2.1.2. **Включить** - чтобы возобновить возможность использования электронного ключа;

2.2. в окне запроса на отключение нажмите **Да.**

3. При действии из раздела **Подключенные устройства -> Ключевые носители** в центральной части окна отметьте ключ, возможность использования которого вы хотите включить/отключить.

3.1. вверху, в области выбора действий, выберите пункт:

3.1.1. **Отключить** – чтобы временно отключить возможность использования электронного ключа;

3.1.2. **Включить** - чтобы возобновить возможность использования электронного ключа;

3.1.3. в окне запроса на подтверждение действия нажмите **Да.**

Статус «Отключен» отображается в любом из представлений электронного ключа, например в разделе **Объекты -> Ключевые носители**:

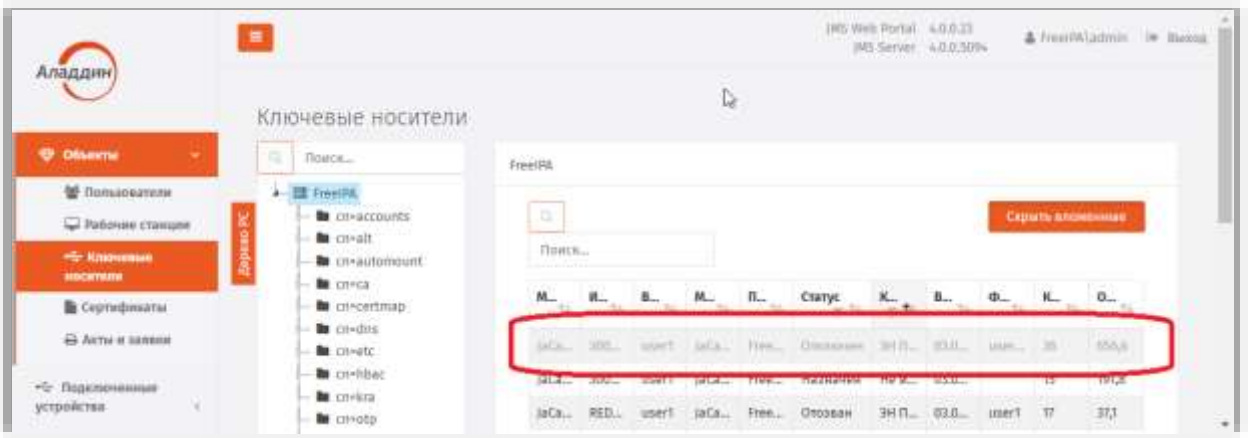


Рис. 51 – Значение статуса у ЭК, отключенного администратором

3.4.7 Очистка ЭК/ЗНИ

Функция очистки позволяет удалить из заданных приложений на электронном ключе все объекты (при этом их копии в JMS также удаляются, т.е. приобретают статус *Удаленный*), а также инициализировать данные приложениях в соответствии с выбранным профилем их инициализации.

Чтобы очистить электронный ключ, выполните следующие действия.

1. Подсоедините электронный ключ, требующий очистки, к компьютеру.
2. В консоли управления JMS перейдите в раздел **Подключенные устройства** -> **Ключевые носители**.

Примечание. Функция очистки доступна только для электронных ключей, имеющих статус в JMS **Зарегистрирован**, **Назначен** или **Отозван**.

3. Выберите электронный ключ, который необходимо очистить.

4. На панели действий нажмите **Очистить**:

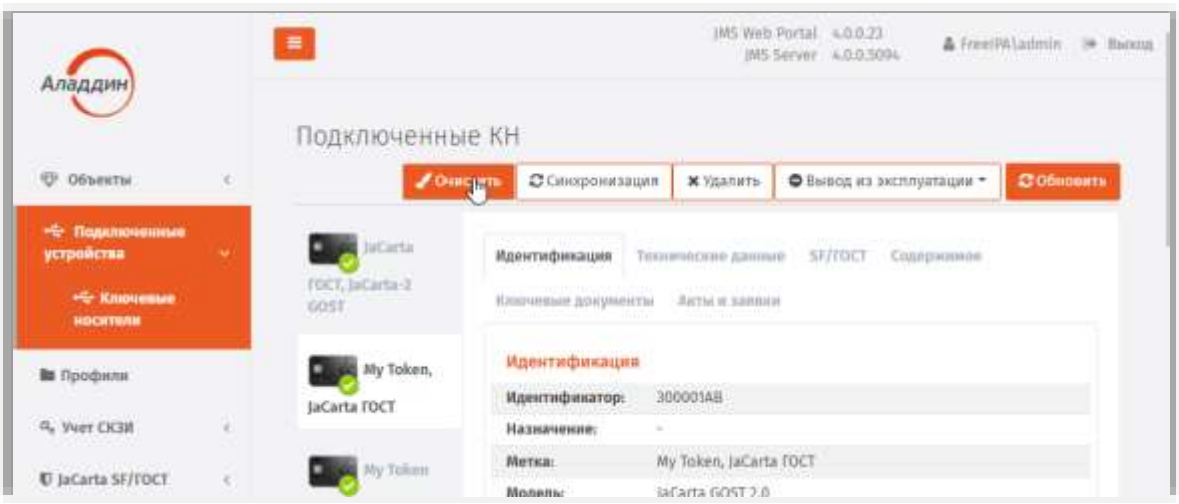


*Рис. 52 – Выбор действия **Очистить***

5. Откроется страница мастера очистки электронных ключей**:**

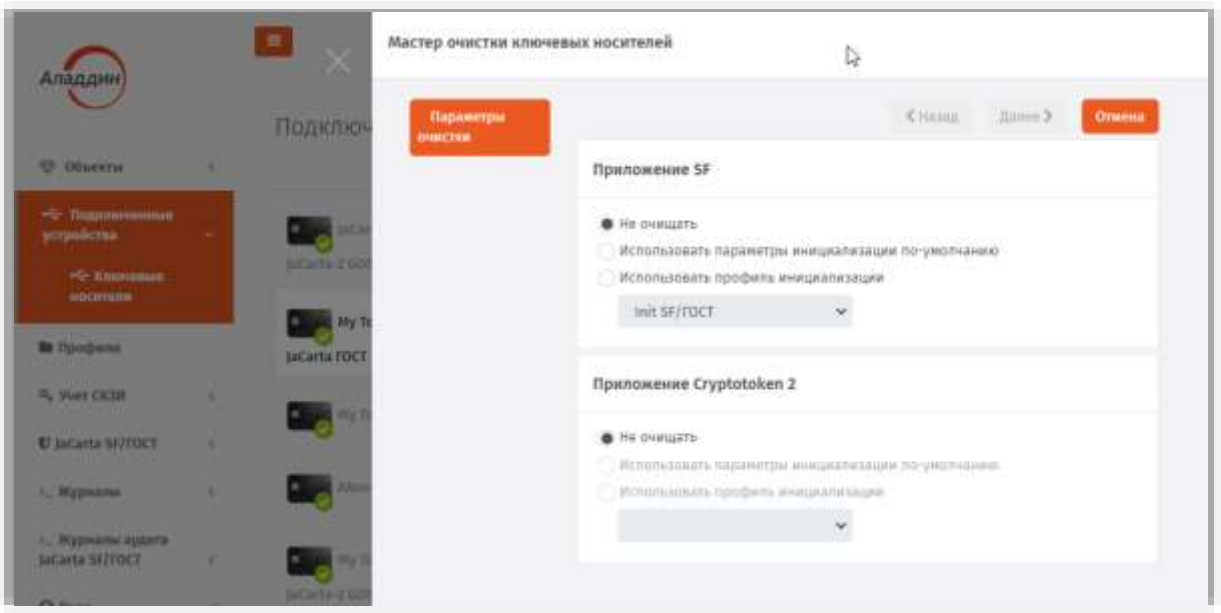


Рис. 53 – Стартовая страница мастера очистки ЭК

6. В каждом из приложений в предложенном списке в зависимости от требований к очистке данного приложения выберите один из вариантов:

   - **Не очищать** – в случае если данное приложение не требует очистки;
   - **Использовать параметры инициализации по умолчанию** – в случае если для инициализации приложения следует использовать соответствующий *профиль по умолчанию*;
   - **Использовать профиль инициализации** – в случае если необходимо выбрать созданный заранее профиль инициализации из раскрывающегося списка.

7. Нажмите **Далее** и следуйте указаниям мастера до завершения процедуры очистки.

По окончании процедуры очистки отобразится следующая страница:

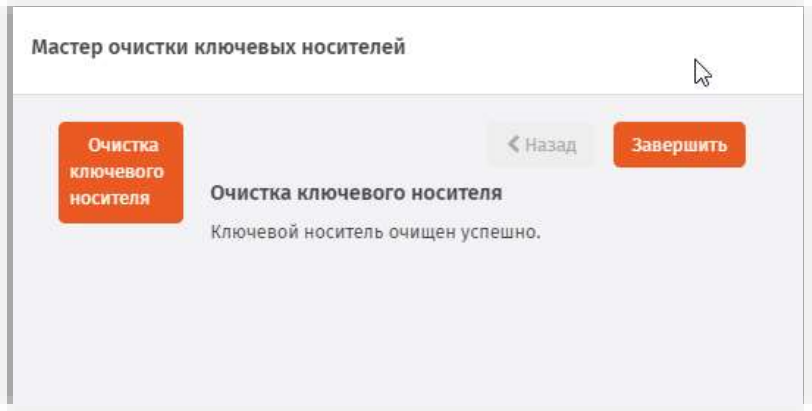


Рис. 54 – Страница завершения работы мастера очистки ЭК

Для закрытия мастера очистки нажмите **Завершить**.

По окончании процедуры очистки электронный ключ своего статуса (например, **Отозван**) не меняет.

3.4.8 Синхронизация ЭК/ЗНИ

В процессе синхронизации содержимое электронного ключа приводится в соответствие с привязанными профилями выпуска объектов JMS (например, профилями управления ISO-образами, обновления встроенного ПО и др.,).

Примечание. При синхронизации применение профилей выпуска и инициализации ЭК/ЗНИ не выполняется. Данные профили применяются к ЭК/ЗНИ только при его выпуске.

Синхронизации подлежат только электронные ключи, ранее выпущенные в JMS и имеющие статус *Используется*, *Отключен* или *Отозван*.

Примечание. При работе с ЗНИ JaCarta SF/ГОСТ в результате процедуры синхронизации происходит загрузка всех журналов регистрации событий из ЗНИ в БД на сервере JMS, после чего содержимое журналов в ЗНИ удаляется, что позволяет избежать их переполнения.

Чтобы синхронизировать электронный ключ с сервером JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Подключенные устройства** -> **Ключевые носители** (Рис. 25, с. 31).

Синхронизируемый электронный ключ должен быть при этом подсоединен к компьютеру.

2. Выберите электронный ключ, который необходимо синхронизировать (Рис. 26, с. 31)
3. На верхней панели нажмите **Синхронизация**:

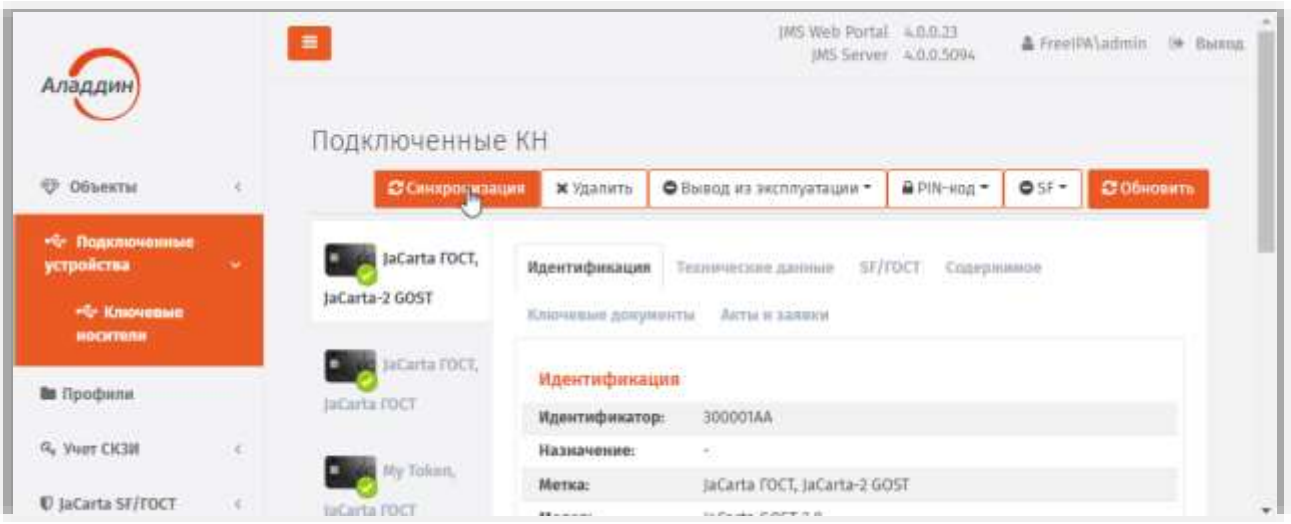


*Рис. 55 – Выбор действия **Зарегистрировать***

4. Откроется страница мастера синхронизации электронных ключей. Нажмите **Далее:**

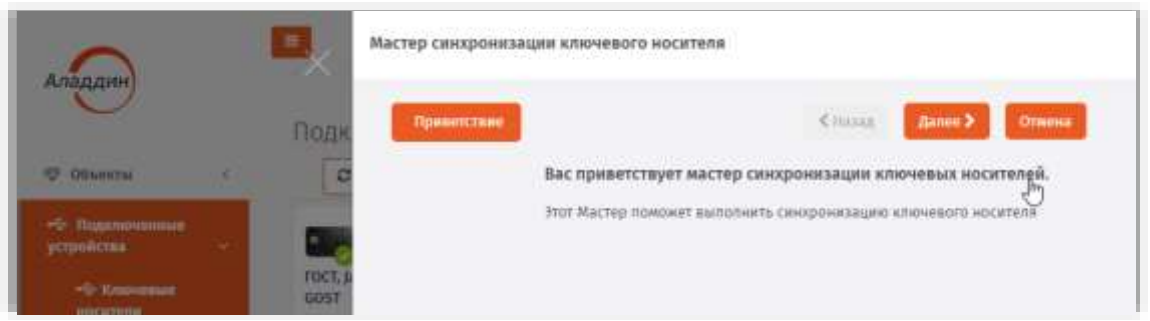


Рис. 56 – Стартовая страница мастера синхронизации ЭК

5. Следуйте указаниям мастера до завершения процедуры синхронизации ЭК.

По окончании процедуры синхронизации отобразится следующая страница:

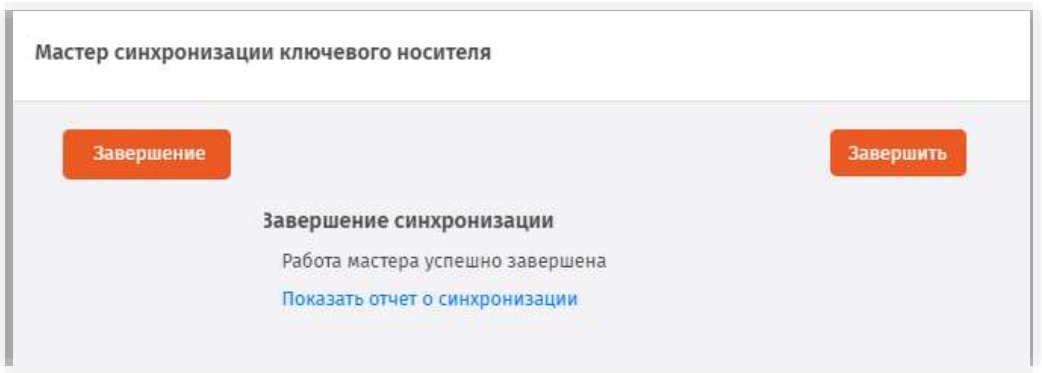


Рис. 57 – Страница завершения работы мастера очистки ЭК

Для просмотра отчета нажмите **Показать отчет о синхронизации**.

Для закрытия мастера синхронизации нажмите **Завершить**.

3.4.8.1.1 Типы синхронизации электронных ключей из приложения Клиент JMS

С целью увеличения ресурса постоянной памяти (EEPROM) электронных ключей в JMS дифференцируются два типа их синхронизации, производимой из приложения Клиент JMS:

- **обычная синхронизация** – выполняется в случае внесения в БД JMS изменений в статус объектов, хранимых на электронных ключах, посредством консоли управления JMS (например удаление/отзыв сертификата) или внесение изменений в профиль выпуска сертификатов, привязанного к данным электронным ключам (включая смену / прекращение привязки такого профиля). Данный тип синхронизации в частности выполняется при наступлении событий, перечисленных на вкладке **Синхронизация** в профиле настройки клиентского агента (см. «Настройка профиля клиентского агента», с. 101).
- **принудительная (расширенная) синхронизация**. Во время такой синхронизации помимо процедур, выполняемых в рамках обычной синхронизации, из постоянной памяти электронного ключа производится также считывание объектов с последующим анализом их состава/состояния в сравнении с эталонной информацией о данных объектах, хранимой в БД JMS.

В результате принудительной (расширенной) синхронизации могут выполняться следующие действия:

- в случае если в память электронного ключа были добавлены новые объекты (сертификаты) не средствами JMS, то данные объекты загружаются в БД JMS;
- в случае если из памяти электронного ключа были удалены объекты (не средствами JMS), ранее зарегистрированные в JMS, например сертификаты со статусами **Выпущен на КН** и **Сохранен на КН,** то такие объекты будут восстановлены в памяти электронного ключа.

Принудительная (расширенная) синхронизация для электронных ключей производится только при нажатии на кнопку (или пункт меню) **Синхронизировать** в приложении **Клиент JMS** на вкладке **Устройства** (см. документ «Руководство пользователя», [1]).

Табл. 3 – Значения параметров по умолчанию профиля настройки клиентского агента

Параметр профиля настройки клиентского агента	Значение параметра по умолчанию
Запускать проверку синхронизации при возникновении событий	
Запускать проверку необходимости синхронизации после старта агента	Да
Запускать проверку необходимости синхронизации после подключения КН	Да
Запускать проверку необходимости синхронизации по расписанию	Да
Запускать проверку необходимости синхронизации после разблокировки сессии ОС	Да
Дополнительные настройки синхронизации клиентского агента	
Разрешать синхронизацию для отключенного КН	Да
Разрешать синхронизацию для отозванного КН	Да
Настройки расписания синхронизации	
Обычная синхронизация	60 минут
Ускоренная синхронизация	5 минут
Количество повторов неудачной синхронизации	5
Настройки автоматической разблокировки	
Разрешать автоматическую разблокировку	Нет

Параметр профиля настройки клиентского агента	Значение параметра по умолчанию
Настройки самостоятельного выпуска ключевых носителей	
Самостоятельный выпуск назначенных КН	Запрещен
Самостоятельный выпуск незарегистрированных КН	Запрещен
Самостоятельный выпуск зарегистрированных КН	Запрещен
Работа с ключевыми носителями	
Разрешать замену	Нет
Разрешать отключение	Нет
Разрешать сообщение об утере/поломке	Нет
Разрешать разблокировку	Да
Настройки параметров принудительной смены PIN-кода пользователя	
Время, отводимое пользователю для смены PIN-кода с момента установки опции	24 часа
Периодичность напоминания о необходимости смены PIN-кода до истечения срока	60 минут
Периодичность напоминания о необходимости смены PIN-кода после истечения срока	30 минут

3.4.9 Отзыв ЭК/ЗНИ

Чтобы отозвать электронный ключ, выполните следующие действия.

После отзыва электронного ключа его статус в JMS будет изменен на **Отозван**, также будут отозваны все объекты в памяти электронного ключа.

1. В консоли управления JMS перейдите в один из следующих разделов:

   - **Объекты -> Ключевые носители**;
   - **Подключенные устройства** -> **Ключевые носители**.

В последнем случае электронный ключ, который вы хотите отозвать, должен быть подключен к компьютеру.

1.1. При действии из раздела **Объекты -> Ключевые носители** в центральной части окна выберите ключ, который вы хотите отозвать, нажмите на нем правой кнопкой мыши, и в появившемся меню выберите **Отозвать**;

1.2. При действии из раздела **Подключенные устройства -> Ключевые носители** в центральной части окна отметьте ключ и вверху, в области выбора действий, выберите пункт **Отозвать**.

2. Откроется страница мастера отзыва электронных ключей**:**

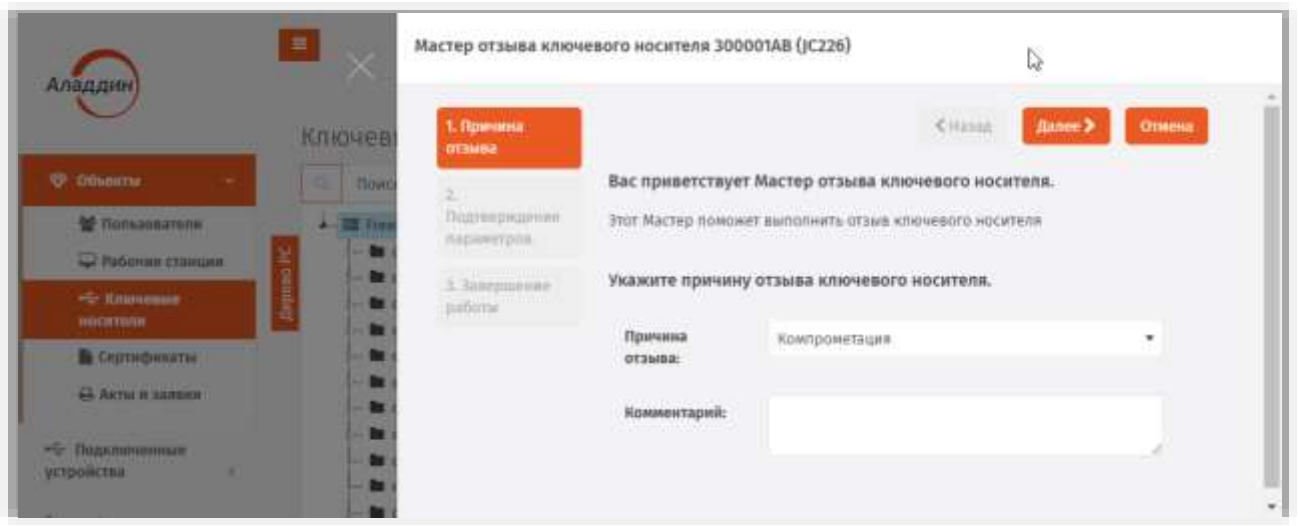


Рис. 58 – Стартовая страница мастера выпуска ЭК

3. Введите значения в поля Причина отзыва и Комментарий и нажмите **Далее**.
4. Следуйте указанием мастера до завершения процедуры отзыва.

По окончании процедуры отзыва отобразится следующая страница:

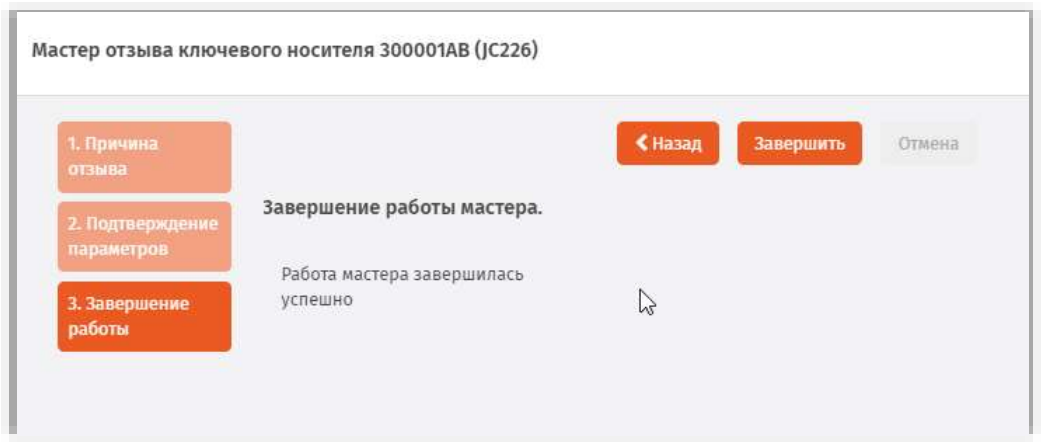


Рис. 59 – Страница завершения работы мастера отзыва ЭК

Для закрытия мастера отзыва нажмите **Завершить**.

Статус *Отозван* отображается в любом из представлений электронного ключа, например в разделе **Объекты -> Ключевые носители**:

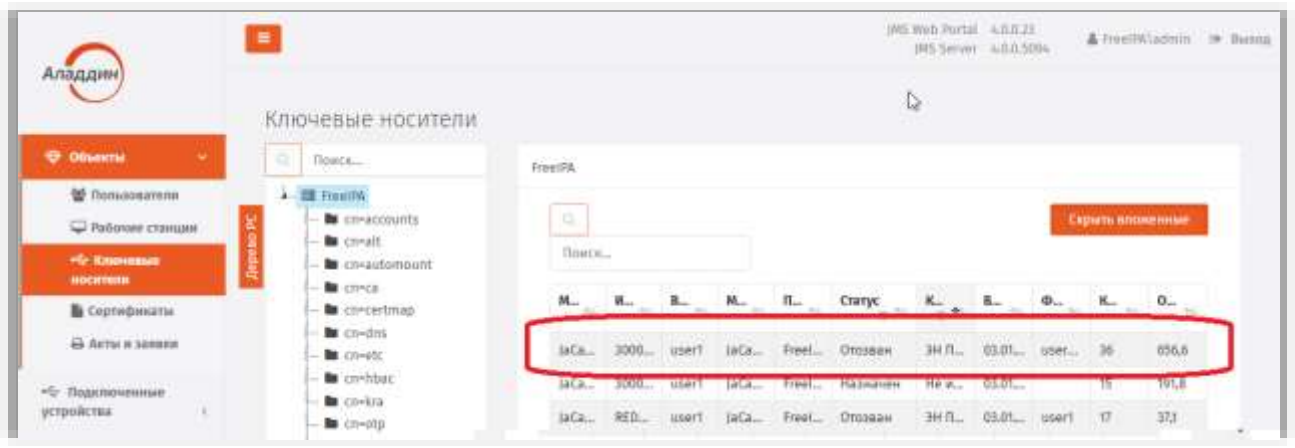


Рис. 60 – Значение статуса у ЭК, отозванного администратором

3.4.10 Замена ЭК/ЗНИ

Предусмотрено два варианта замены электронного ключа: простая замена и замена с восстановлением данных из резервной копии. В первом случае объекты в памяти нового электронного ключа создаются заново, тогда как в случае с восстановлением данных из резервной копии используются резервные копии объектов, содержащихся на старом электронном ключе.

Замена электронного ключа с восстановлением данных из резервной копии возможна только в том случае, если в профиле, который использовался при выпуске или синхронизации заменяемого электронного ключа (например, в профиле выпуска сертификатов в удостоверяющем центре DogTag) была включена настройка резервного копирования объектов.

Чтобы заменить электронный ключ, выполните следующие действия.

Электронный ключ, который выступит заменой прежнему, должен быть подсоединен к компьютеру.

1. В консоли управления JMS перейдите в один из следующих разделов:
   - **Объекты -> Ключевые носители**;
   - **Подключенные устройства** -> **Ключевые носители**.
2. При действии из раздела **Объекты -> Ключевые носители** в центральной части окна выберите ключ, который необходимо заменить на другой. Нажмите на нем правой кнопкой мыши и в появившемся меню выберите **Заменить**.

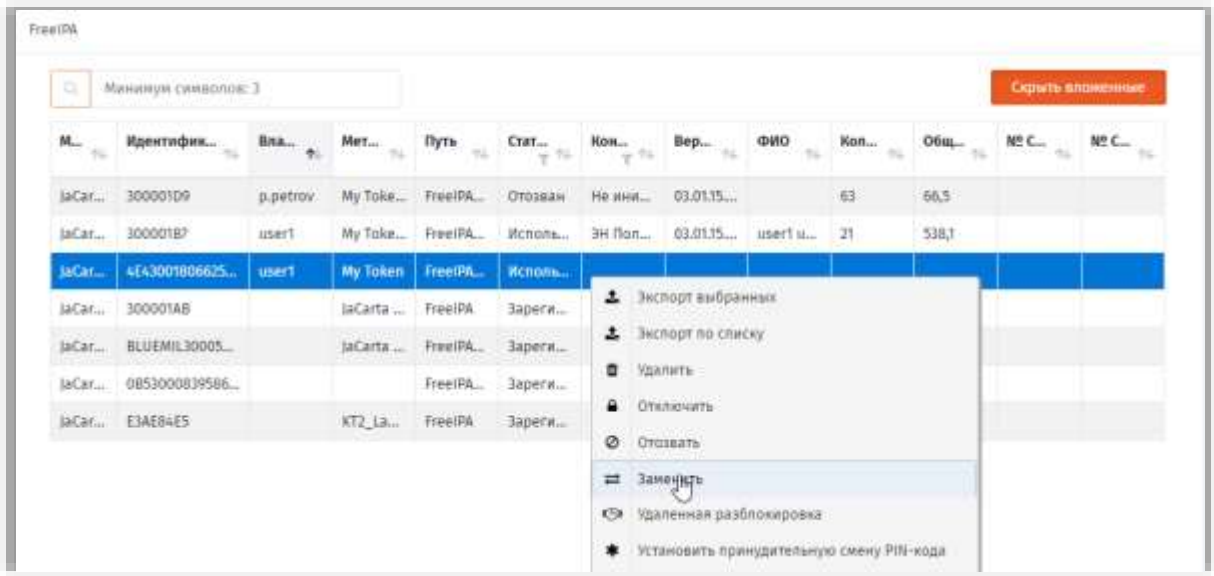


*Рис. 61 – Выбор действия **Заменить** в меню операций с выбранным ЭК*

3. Откроется страница мастера замены электронных ключей. Нажмите **Далее:**

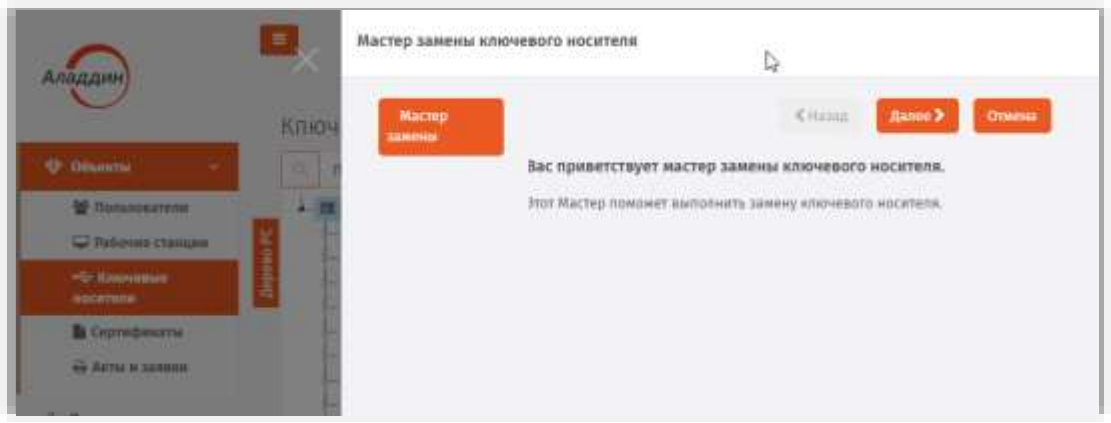


Рис. 62 – Стартовая страница мастера замены ЭК

4. На следующей странице укажите **Причину замены** и при необходимости заполните поле **Комментарий** и нажмите **Далее:**

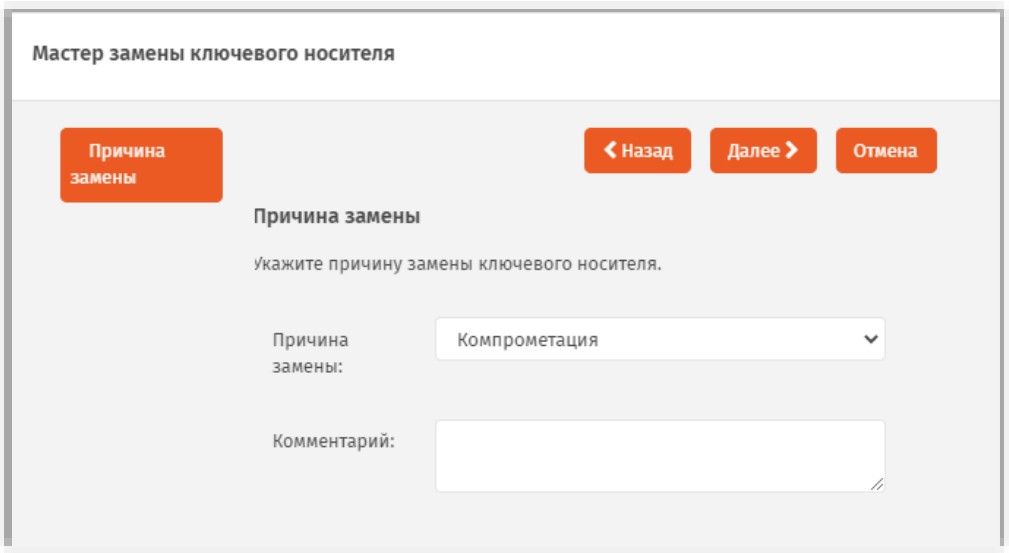


Рис. 63 – Страница выбора причины замены ЭК

5. На следующей странице выберите подсоединенный электронный ключ, которым следует заменить выбранный ранее и нажмите **Далее:**

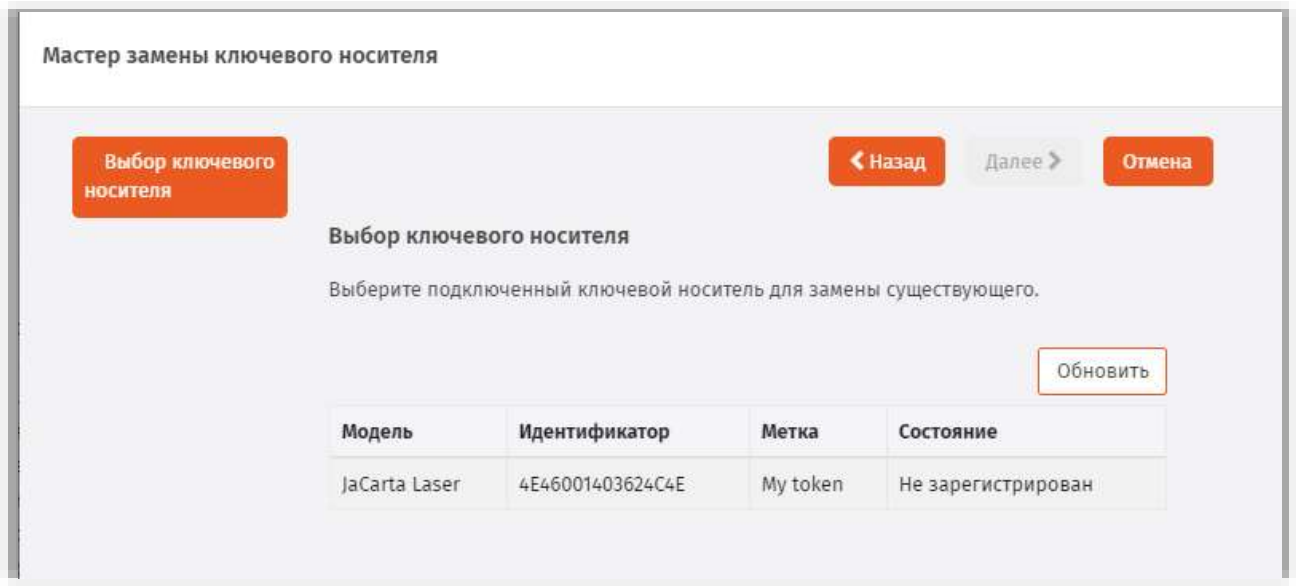


Рис. 64 – Страница выбора причины замены ЭК

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

Отобразится страница следующего вида.

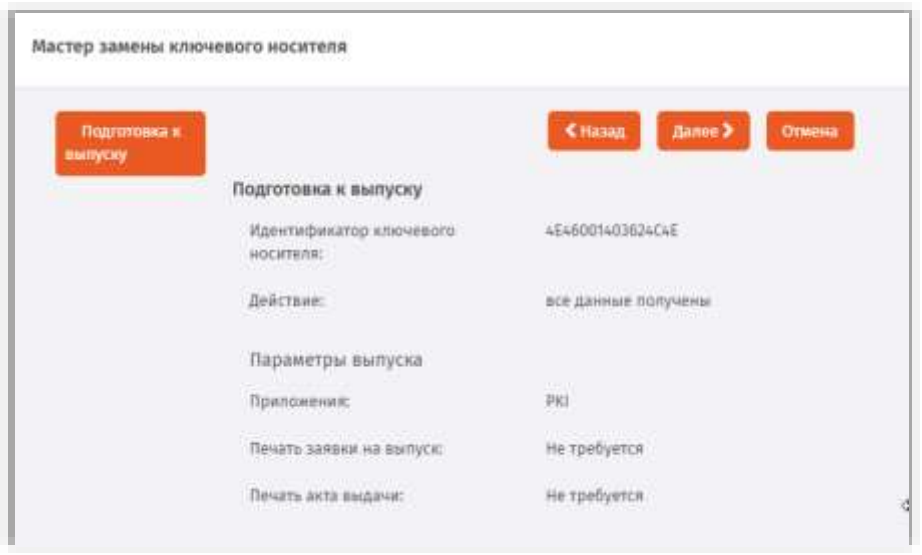


Рис. 65 – Страница подготовки к выпуску ключевого носителя

7. Нажмите **Далее**.
Отобразится следующая страница.

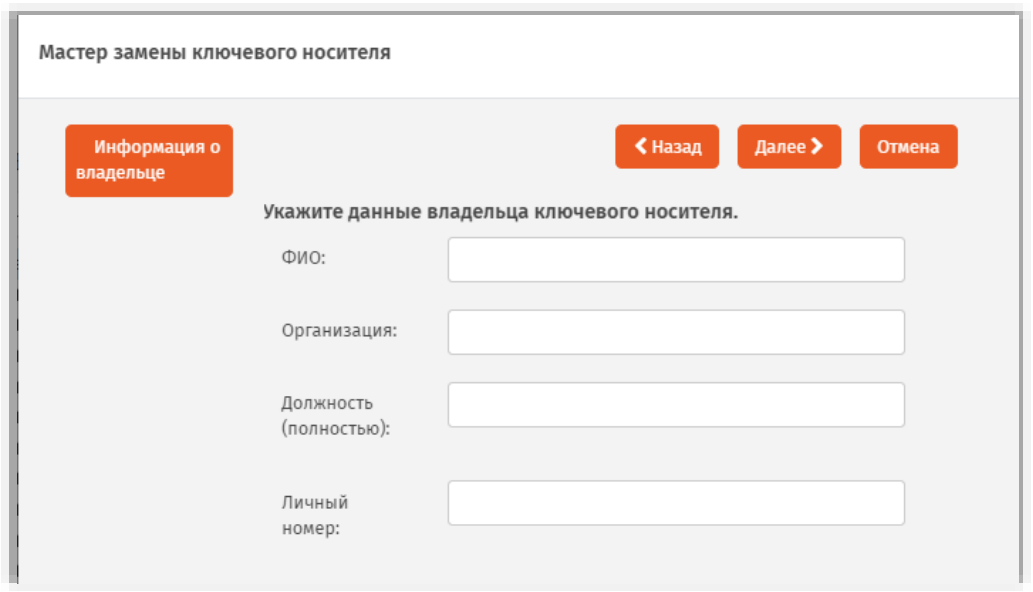


Рис. 66 – Страница ввода данных владельца электронного ключа

8. Введите необходимые данные и нажмите **Далее**.

Отобразится следующая страница.

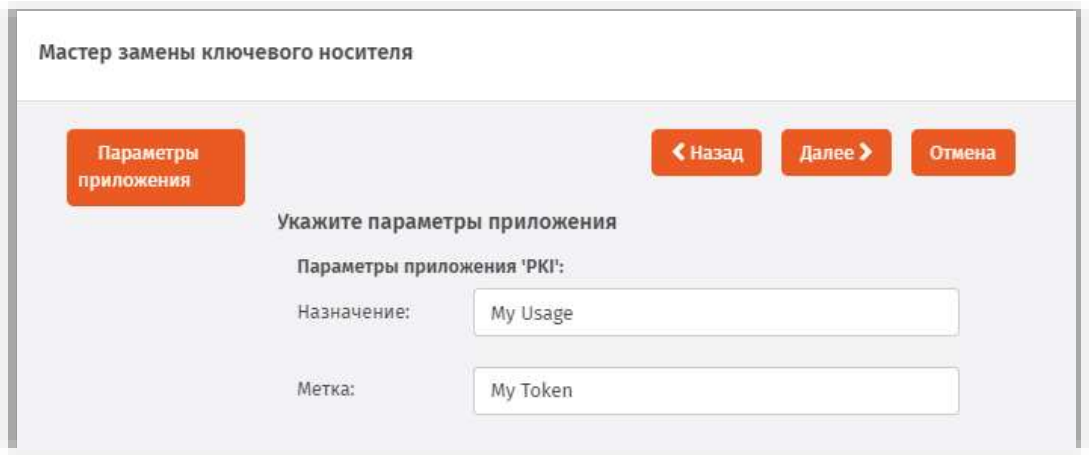


Рис. 67 – Страница настройки параметров инициализации

9. Укажите или отредактируйте назначение и метку ключевого носителя, после чего нажмите **Далее**.
   Отобразится следующая страница.

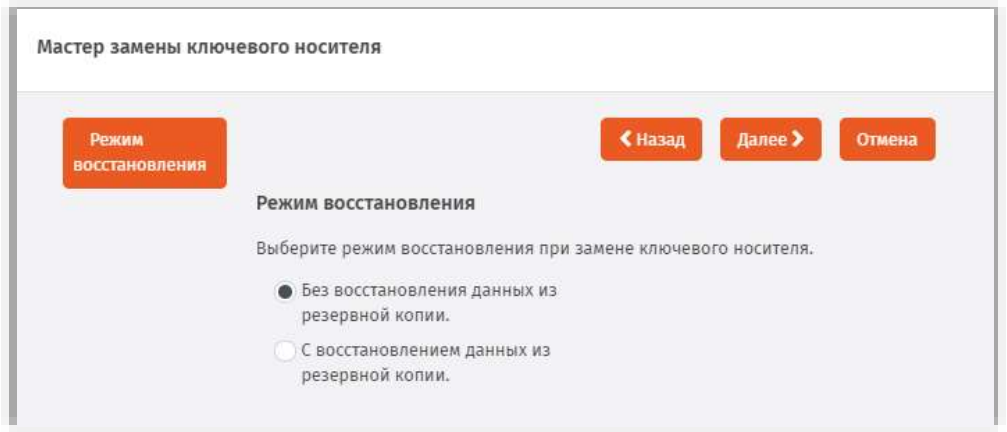


Рис. 68 – Выбор режима замени электронного ключа

10. Выберите режим замены электронного ключа, после чего нажмите **Далее**:

- **Без восстановления данных из резервной копии** – данные для выпуска нового электронного ключа будут сформированы непосредственно перед выпуском.
- **С восстановлением данных из резервной копии** – для выпуска нового электронного ключа будут использованы сохраненные данные предыдущего электронного ключа;

Отобразится страница следующего вида.

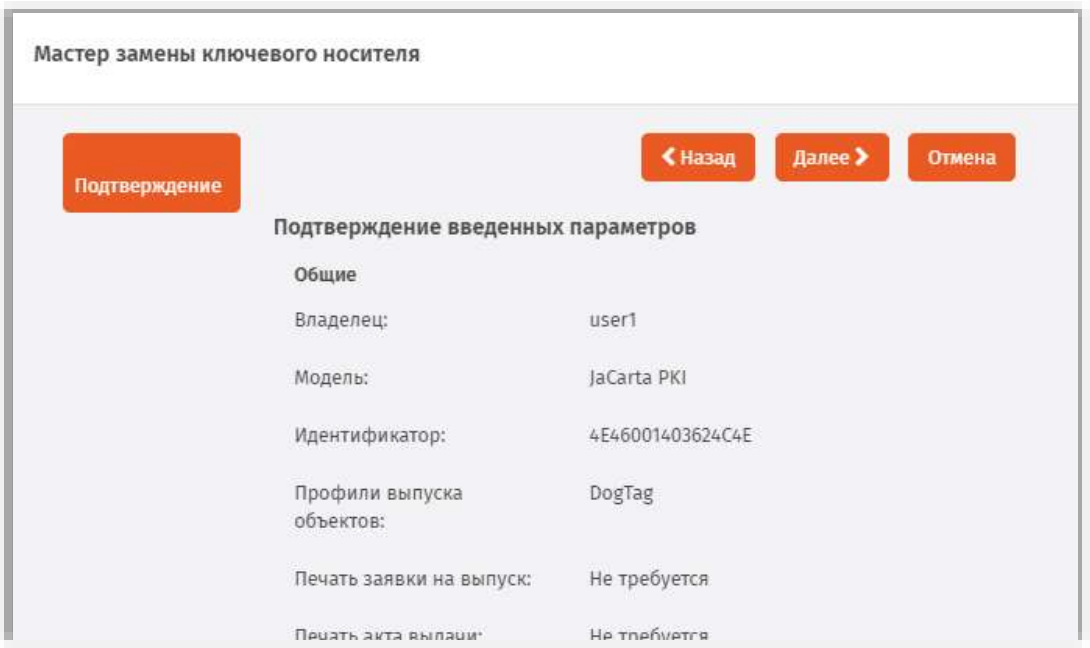


Рис. 69 – Страница подтверждения параметров заменяемого ключевого носителя

11. Нажмите **Далее**.
    По окончании процедуры записи данных на ЭК отобразится следующая страница.

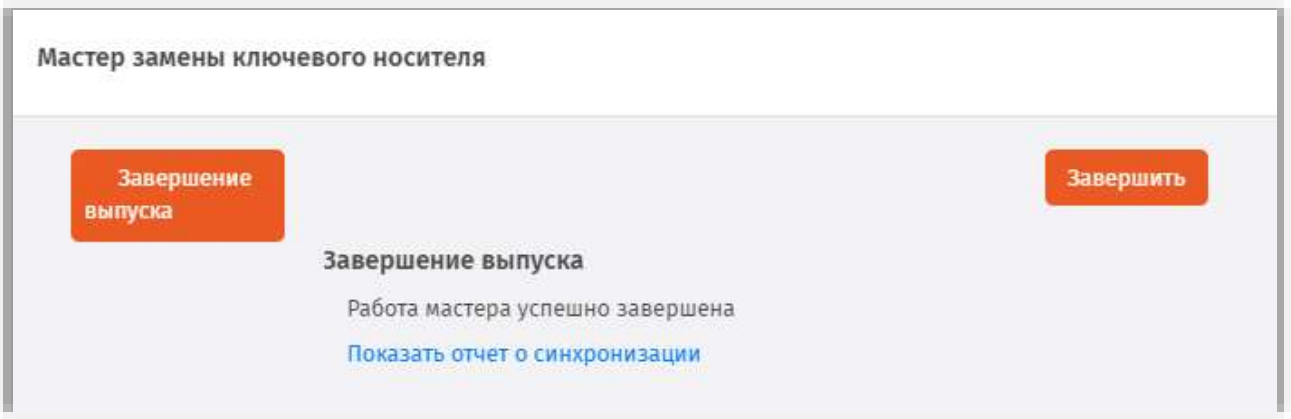


Рис. 70 – Страница завершения работы мастера замены ключевого носителя

12. Нажмите **Завершить**.

По окончании процедуры замены старый электронный ключ приобретет статус *Отозван*, новый электронный ключ приобретет статус *Используется*.

3.4.11 Возврат в эксплуатацию ЭК/ЗНИ

JMS позволяет вернуть отозванный электронный ключ (статус **Отозван**) в эксплуатацию. Для этого выполните следующие действия.

После возврата в эксплуатацию электронного ключа его статус в базе данных JMS принимает значение **Зарегистрирован**. При этом удаляется привязка электронного ключа к предыдущему владельцу.

1. В консоли управления JMS перейдите в один из следующих разделов:

   – **Объекты -> Ключевые носители**;
   – **Подключенные устройства** -> **Ключевые носители**.

В последнем случае электронный ключ, который необходимо вернуть в эксплуатацию, должен быть подключен к компьютеру.

2. При действии из раздела **Объекты -> Ключевые носители** в центральной части окна выберите ключ, который необходимо вернуть в эксплуатацию. Нажмите на нем правой кнопкой мыши и в появившемся меню выберите **Вернуть в эксплуатацию**.

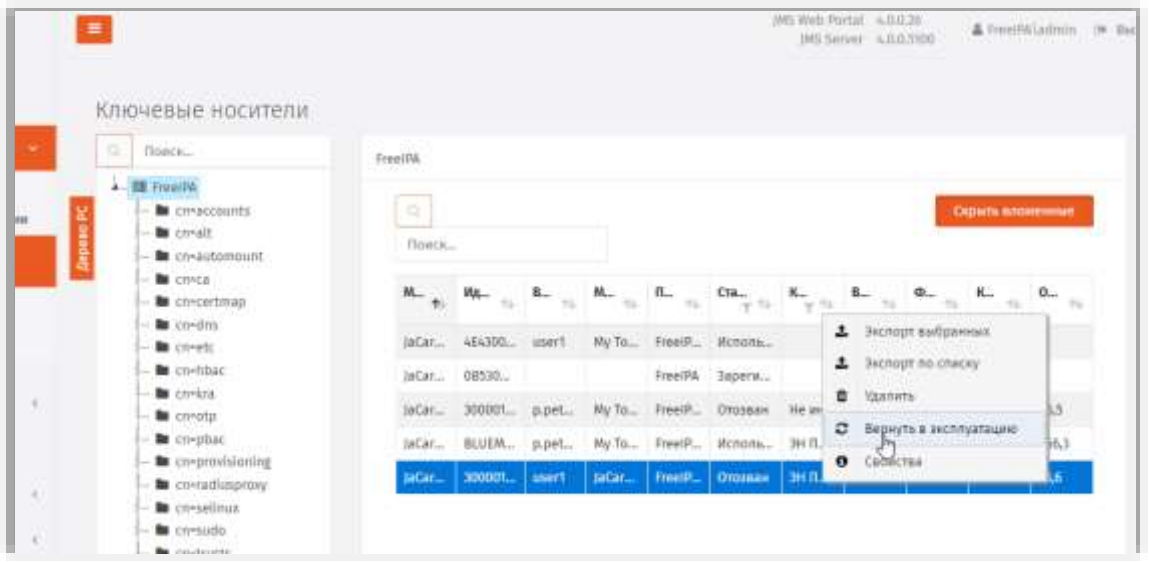


*Рис. 71 – Выбор действия **Вернуть в эксплуатацию** в меню операций с выбранным ЭК*

2.1. В окне запроса на подтверждение возврата в эксплуатацию нажмите **Да:**

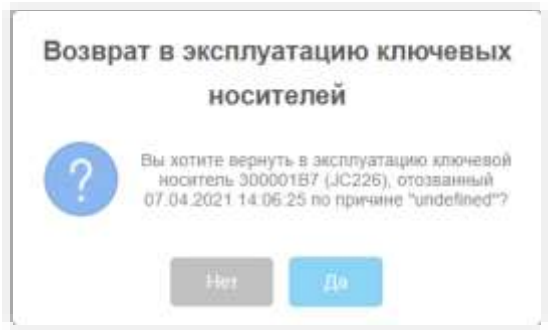


Рис. 72 – Окно подтверждения возврата ЭК в эксплуатацию

3. При действии из раздела **Подключенные устройства -> Ключевые носители** в центральной части страницы выберите ключ, который необходимо вернуть в эксплуатацию. Вверху нажмите Вывод из эксплуатации и выберите Нажмите на нем правой кнопкой мыши и в появившемся меню выберите **Вернуть в эксплуатацию**.

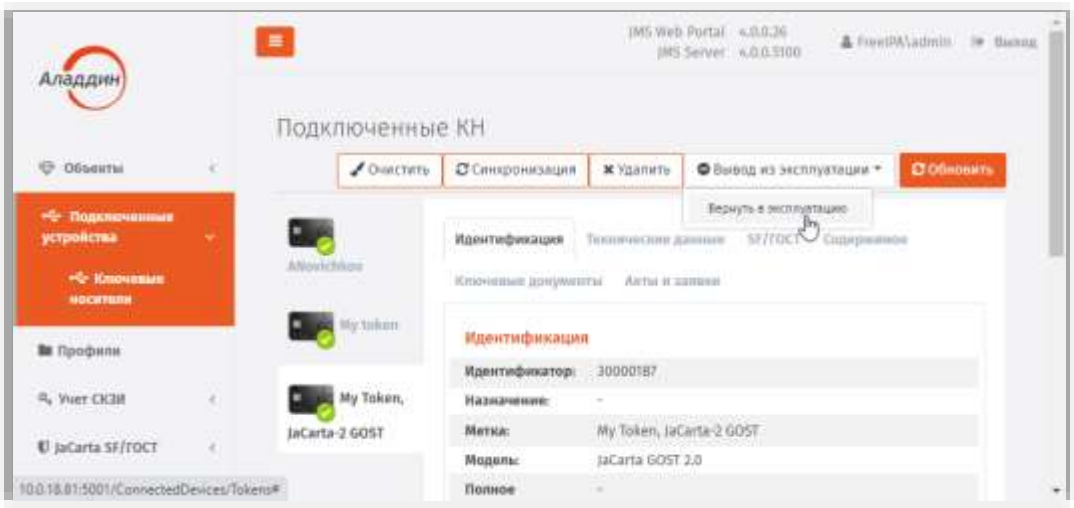


*Рис. 73 – Выбор действия **Вернуть в эксплуатацию** из раздела Подключенные устройства*

3.1. В окне запроса на подтверждение возврата в эксплуатацию нажмите **Да:**

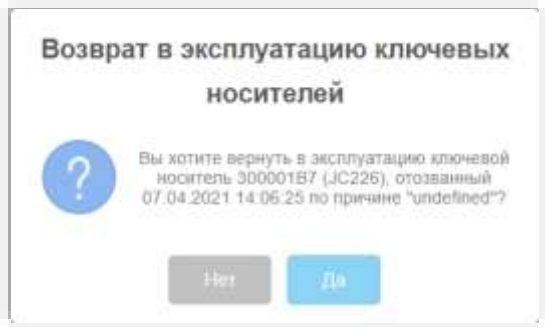


Рис. 74 – Окно подтверждения возврата ЭК в эксплуатацию

По окончании процедуры возврата в эксплуатацию электронный ключ приобретет статус *Зарегистрирован*.

Примечание. В случае если электронный ключ был ранее зарегистрирован как СКЗИ, при его возврате в эксплуатацию будет сформирован нормативный документ «Акт получения СКЗИ администратором».

3.4.12 Разблокировка подсоединенного электронного ключа

3.4.12.1 Предоставление права на разблокировку

По умолчанию встроенная роль **Администратор ИБ** в JMS не наделена правом разблокировки PIN-кода пользователя в электронных ключах через консоль управления JMS. Для предоставления такого права необходимо выполнить следующие действия:

- создать дополнительную служебную роль (см. «Создание новой роли JMS», с. 265)
- добавить созданной роли право выполнения операции **Разблокировка по PIN-коду администратора** (см. «Приложение 1. Права на выполнение операций», с. 336);
- назначить (добавить) созданную роль пользователю, которому должно быть предоставлено право разблокировки электронных ключей (например, администратору, см. «Назначение / отмена назначения ролей пользователям JMS», с. 267).

3.4.12.2 Порядок разблокировки

Чтобы разблокировать подсоединенный электронный ключ, выполните следующие действия.

1. Подсоедините электронный ключ, который необходимо разблокировать, к компьютеру.
2. В консоли управления JMS перейдите в раздел **Подключенные устройства** -> **Ключевые носители**.
3. В центральной части экрана выберите электронный ключ, который нужно разблокировать.
4. В верхней выберите **PIN-код** -> **Разблокировать**..

Если на электронном ключе содержится несколько приложений, выберите нужное в раскрывающемся списке, после чего продолжите процедуру.

5. В окне предупреждающего сообщения нажмите **Да**.
6. Отобразится страница смены PIN-кода пользователя.

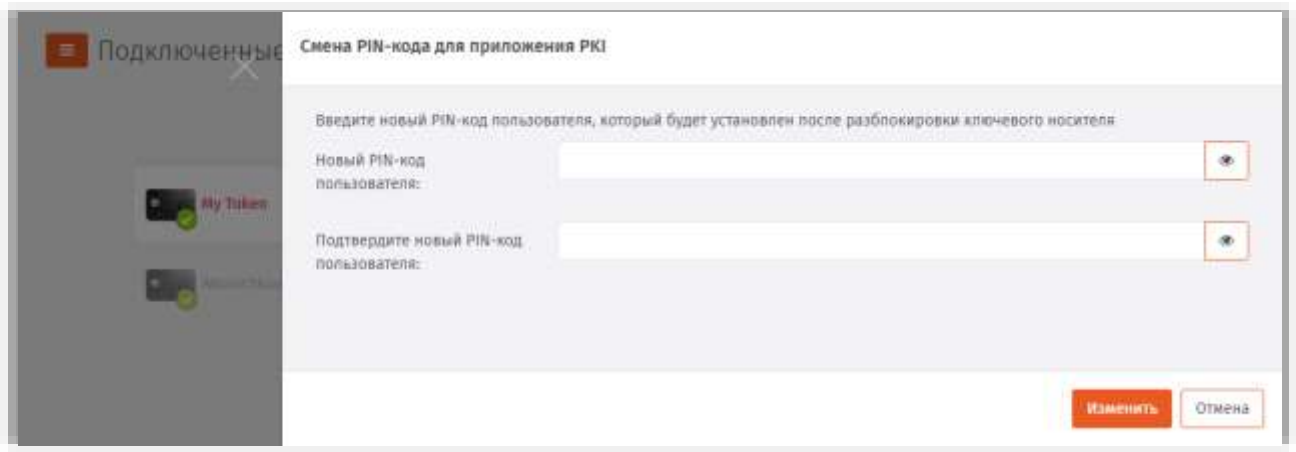


Рис. 75 – Окно подтверждения возврата ЭК в эксплуатацию

7. В полях **Новый PIN-код пользователя** и **Подтвердите новый PIN-код пользователя** задайте новый PIN-код пользователя и введите подтверждение соответственно, после чего нажмите **OK**.
8. В окне сообщения об успешной разблокировке нажмите **OK**.

3.4.13 Разблокировка электронного ключа в удаленном режиме

Процедура разблокировки в удаленном режиме неприменима к электронным ключам моделей JaCarta SF/ГОСТ, ГОСТ и ГОСТ-2.

Чтобы разблокировать электронный ключ в удаленном режиме, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Объекты** -> **Ключевые носители**.
2. Выберите электронный ключ, который нужно разблокировать.
3. Нажмите на нем правой кнопкой мыши и выберите **Разблокировать**.

Отобразится страница следующего вида.

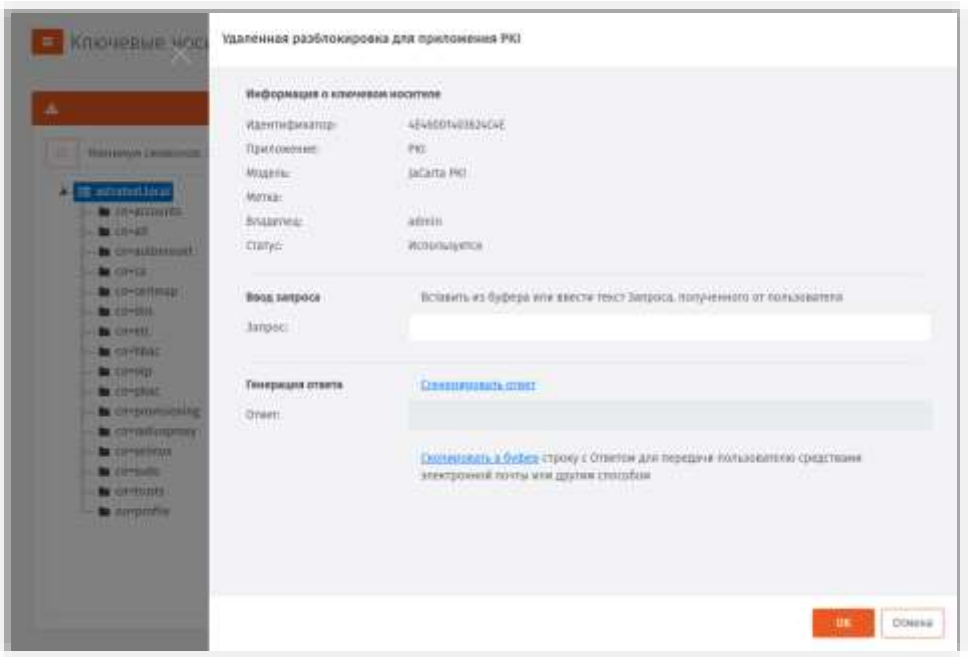


Рис. 76 – Окно удаленной разблокировки

4. Проинструктируйте пользователя (например, по телефону), как сгенерировать код запроса с помощью Клиента JMS:

4.1. пользователь должен подсоединить электронный ключ с заблокированным PIN-кодом к компьютеру.
4.2. пользователь должен открыть в браузере web-приложение клиента JMS (например, нажав правой кнопкой в области уведомлений на значке выбрать **Открыть страницу агента**);
4.3. после аутентификации в web-приложении клиента пользователь должен выбрать вкладку **Устройства**, выбрать электронный ключ с заблокированным PIN-кодом пользователя, нажать на значок управления и выбрать **Разблокировка PIN-кода**;
4.4. на экране пользователя отобразится страница разблокировки следующего вида;

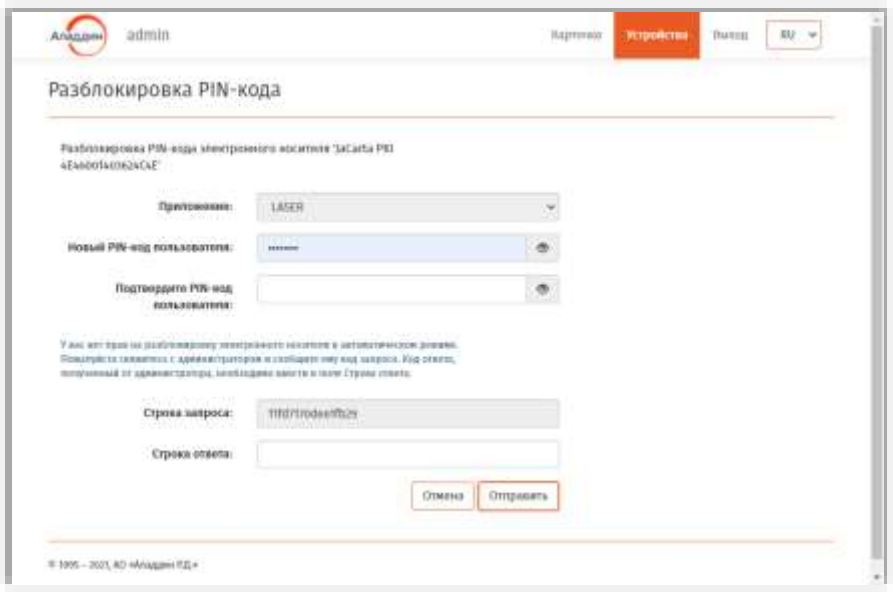


Рис. 77 – Окно разблокировки PIN-кода в web-клиенте JMS

4.5. На данной странице пользователь должен заполнить поля **Новый PIN-код пользователя** и **Подтвердите PIN-код пользователя**, и продиктовать вам значение, отображающееся в поле **Строка запроса**.

Введите продиктованное пользователем значение запроса в поле **Запрос** окна удаленной разблокировки, после чего нажмите **Сгенерировать ответ**. Сгенерированное значение отобразится в поле **Ответ** окна удаленной разблокировки (см. рис. 78).

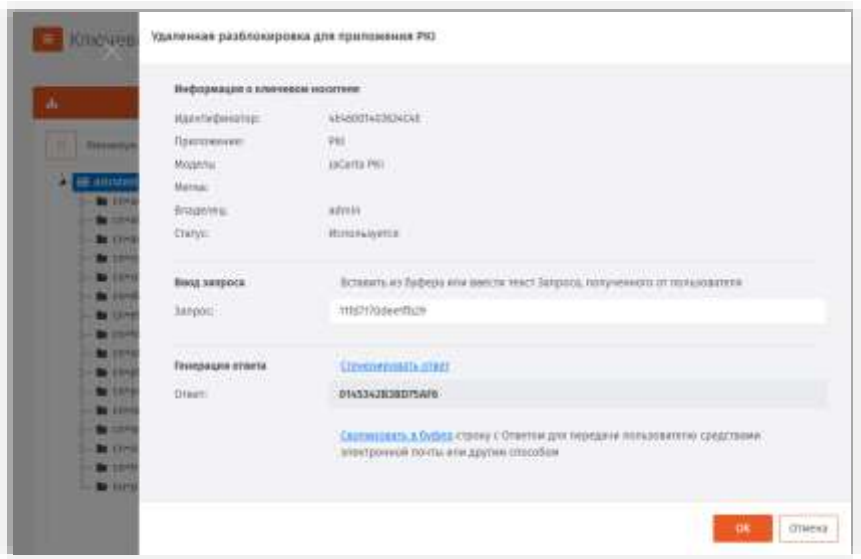


Рис. 78 – Сгенерированный код ответа

5. Продиктуйте пользователю значение ответа - пользователь должен ввести его в поле **Строка ответа (**Рис. 77**)**, после чего нажать **Отправить**.

Если значение введено верно, на странице отобразится сообщение об успешной разблокировке электронного ключа.

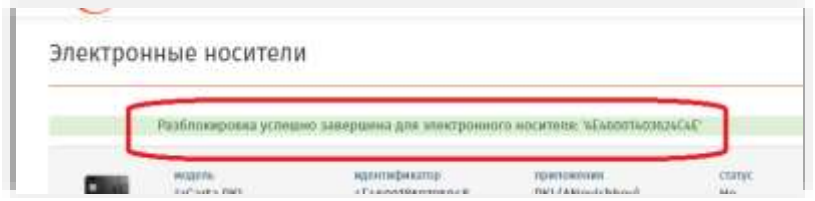


Рис. 79 – Сообщение об успешной проверке значения ответа

PIN-код пользователя разблокирован.

Примечание. Удаленная разблокировка PIN-кодов в приложениях ГОСТ и ГОСТ-2 (например, в электронных ключах JaCarta ГОСТ или JaCarta-2 ГОСТ) в JMS недоступна.

3.4.14 Удаление ЭК/ЗНИ

При удалении электронного ключа в JMS выполняются те же действия, что и при его отзыве (см. «Отзыв ЭК/ЗНИ », с. 50). При этом электронный ключ приобретает в JMS статус **Не**

зарегистрирован, а в базе данных JMS помечается как удаленный (и больше не отражается в разделе **Ключевые носители**).

Чтобы удалить электронный ключ, выполните следующие действия.

Примечание. В случае если на электронном ключе присутствуют объекты (сертификаты и др.) рекомендуется предварительно выполнить отзыв и очистку ключа (см. соответственно «Отзыв ЭК/ЗНИ », с. 50 и «Очистка ЭК/ЗНИ », с. 45).

6. В консоли управления JMS перейдите в один из следующих разделов:

   – **Объекты** ->**Ключевые носители**;
   – **Подключенные устройства** -> **Ключевые носители**.

В последнем случае электронный ключ, который необходимо удалить, должен быть подсоединен к компьютеру.

7. При действии из раздела **Объекты -> Ключевые носители** в центральной части окна выберите ключ, который необходимо удалить;

7.1. нажмите на нём правой кнопкой мыши и в появившемся меню нажмите Удалить;
7.2. в окне запроса на удаление нажмите **Да.**

8. При действии из раздела **Подключенные устройства -> Ключевые носители** в центральной части окна выберите ключ, который необходимо удалить;

8.1. вверху, в области выбора действий, нажмите кнопку **Удалить**;
8.2. в окне запроса на удаление нажмите **Да.**

После удаления электронный ключ, отображаемый в разделе **Подключенные устройства** -> **Ключевые носители** приобретает статус *Не зарегистрирован*:

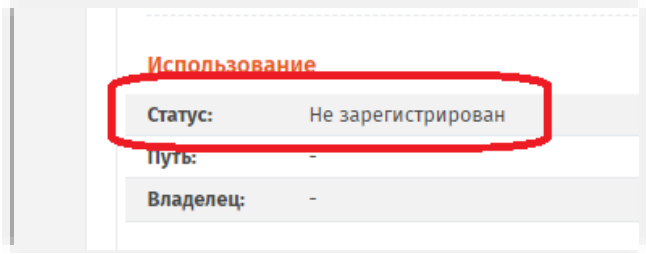


Рис. 80 – Значение статуса у ЭК, удаленного из JMS

3.4.15 Особенности работы с ЗНИ (ЭН) JaCarta SF/ГОСТ

Согласно документации из комплекта поставки ЗНИ JaCarta SF/ГОСТ (в заводской документации – ЭН, электронные носители) данные ЗНИ в зависимости от способа их инициализации бывают двух видов:

- «ЭН пользователя», т.е. электронный ключ, используемый конечным пользователем. Далее по тексту – *ЭН пользователя*;
- «ЭН администратора доступа», т.е. электронный ключ, используемый администратором безопасности для конфигурирования «ЭН пользователей» (электронных ключей) и управления правами доступа к данным электронным ключам; далее по тексту – *ЭН администратора доступа*.

Один *ЭН администратора доступа* (условно «родительский» электронный ключ) может использоваться для управления доступом к нескольким связанным с ним *ЭН пользователя*. (Подробное описание функционирования электронных ключей JaCarta SF/ГОСТ и правил их использования приводится документации из комплекта их поставки).

JMS позволяет выпускать и администрировать оба вида данных электронных ключей.

Важно! Для выпуска электронного ключа JaCarta SF/ГОСТ и проведения с ним любых других операций последний должен быть подключён к компьютеру с Консолью управления JMS (или Клиентом JMS) непосредственно, либо с помощью среды виртуализации, например средств виртуализации VMware. Не допускается подключение электронного ключа к компьютеру посредством *протокола удаленного рабочего стола* (Remote Desktop Protocol).

3.4.15.1 Запись ISO-образов

ISO-образы могут быть записаны в разделы CD-ROM (скрытые и закрытые) электронных ключей JaCarta SF/ГОСТ автоматически при синхронизации данных ключей, в частности при их выпуске.

При необходимости записи ISO-образов в разделы CD-ROM электронных ключей JaCarta SF/ГОСТ при их синхронизации следует:

1. выполнить необходимую настройку размеров CD-ROM-разделов на вкладке **Параметры** профиля **Инициализация JaCarta/SF ГОСТ** (см. раздел «Вкладка Параметры», с. 120);
2. создать профиль типа **Управление ISO-образами** (см. раздел «Профиль управления ISO-образами JaCarta SF/ГОСТ», с. 182);
3. привязать профиль управления ISO-образами к пользователю (контейнеру пользователя в ресурсной системе), см. раздел «Привязка профилей», с. 195.

3.4.15.2 Обновление встроенного ПО в ЗНИ JaCarta SF/ГОСТ

Электронные ключи (ЗНИ) JaCarta SF/ГОСТ позволяют обновлять встроенное в них микропрограммное обеспечение (далее – встроенное ПО), в частности, посредством системы JMS как в консоли администрирования JMS, так и в клиенте JMS.

При необходимости обновить встроенное ПО в ЗНИ JaCarta SF/ГОСТ следует создать соответствующий профиль (см. «Профиль обновления встроенного ПО JaCarta SF/ГОСТ», с. 185) и выполнить его привязку (см. «Привязка профилей», с. 195). Обновление встроенного ПО выполняется в момент выпуска/синхронизации ЗНИ.

Примечание. Для обновления встроенного ПО в приложении Клиент JMS требуется соответствующее разрешение в настройках профиля обновления встроенного ПО.

К ЗНИ JaCarta SF/ГОСТ может быть привязан только один профиль обновления встроенного ПО, в противном случае обновление встроенного ПО в данном ЗНИ будет невозможно выполнить (см. раздел «Проверка статуса обновления встроенного ПО», с. 64).

В процессе выпуска/синхронизации ЗНИ JaCarta SF/ГОСТ можно отказаться от обновления встроенного ПО, но при определенных настройках профиля обновления (например, при истечении срока обновления ПО) ЗНИ может быть заблокирован, о чем выдается соответствующее предупреждение. Если же JMS позволяет отказаться от обновления ПО без блокировки ЭН, то при очередной синхронизации данного ЗНИ пользователю/администратору снова будет предложено обновить встроенное ПО.

Проверка статуса обновления встроенного ПО

Чтобы выяснить, требуется ли обновление встроенного ПО на зарегистрированном в JMS электронном ключе JaCarta SF/ГОСТ, а также убедиться в корректности привязки профиля обновления встроенного ПО, следует проверить значение атрибута **Статус обновления встроенного ПО** (Рис. 81)в свойствах электронного ключа в разделе **Ключевые носители** (или **Подключенные ключевые носители**) консоли управления JMS.

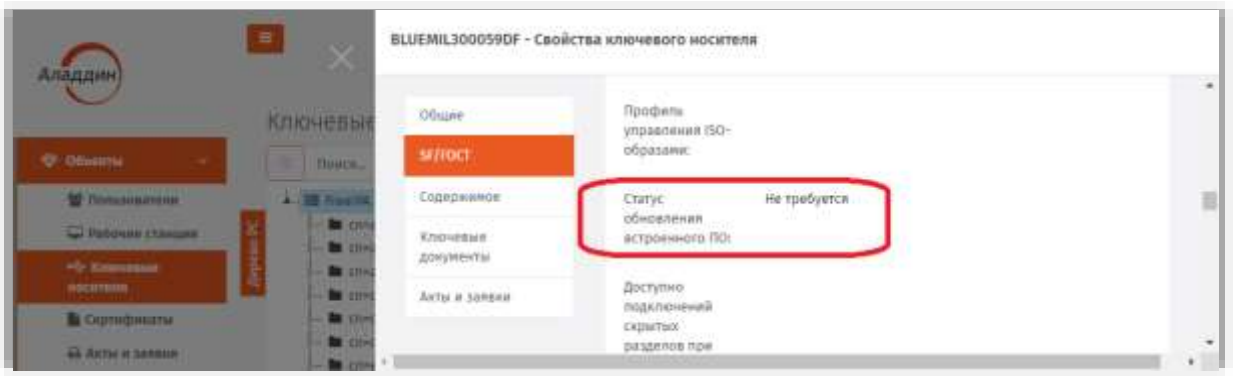


Рис. 81 – Проверка статуса обновления встроенного ПО в электронном ключе JaCarta SF/ГОСТ

Атрибут **Статус обновления встроенного ПО** может принимать следующие значения:

- **Не требуется** – у электронного ключа нет привязанного профиля обновления встроенного ПО (т.е. обновление встроенного ПО не требуется);
- **Действует более одного профиля** – к электронному ключу привязано более одного профиля обновления встроенного ПО, что является некорректной настройкой (т.е. обновление встроенного ПО выполнить невозможно);
- **Требуется** – к электронному ключу привязан профиль обновления встроенного ПО, и в соответствии с настройками данного профиля обновление требуется (версия текущего ПО в электронном ключе устарела);
- **Версия актуальна** – в электронном ключе установлена актуальная версия встроенного ПО (т.е. совпадает по номеру с версией, установленной в привязанном профиле обновления).

3.4.15.3 Создание контейнера автономного монтирования скрытых дисков (.kko)

Контейнер автономного монтирования скрытых дисков (файл с расширением kko) позволяет в клиенте JMS монтировать скрытые диски RW и CD-ROM на ЗНИ JaCarta SF/ГОСТ (ЭН пользователя) без установки соединения с сервером JMS.

Для экспорта контейнера автономного монтирования скрытых дисков в консоли управления JMS выполните следующие действия.

1. В консоли управления JMS перейдите в один из следующих разделов:

   – **Объекты** -> **Ключевые носители**;
   – **Подключенные устройства** -> **Ключевые носители**.

В последнем случае ЭН пользователя должен быть подсоединен к компьютеру.

2. Выберите ЗНИ JaCarta SF/ГОСТ со статусом *Используется*, для которого необходимо создать контейнер .kko . Нажмите на нем правой кнопкой мыши и в появившемся меню выберите **Создать контейнер автономного монтирования (.kko):**

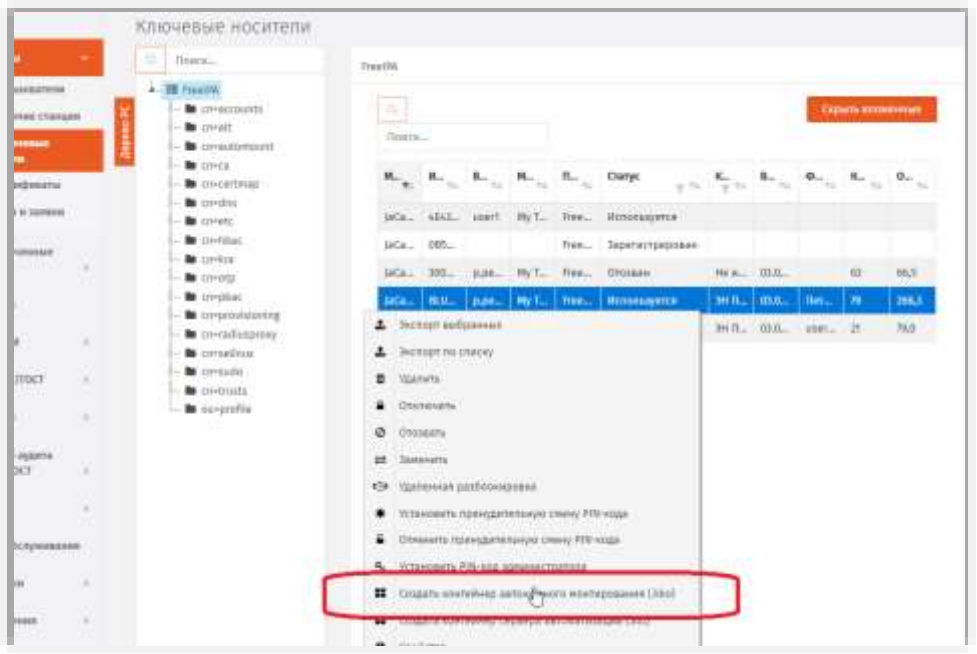


Рис. 82 – Создание контейнера .kko из консоли управления JMS

3. Отобразится страница следующего вида.

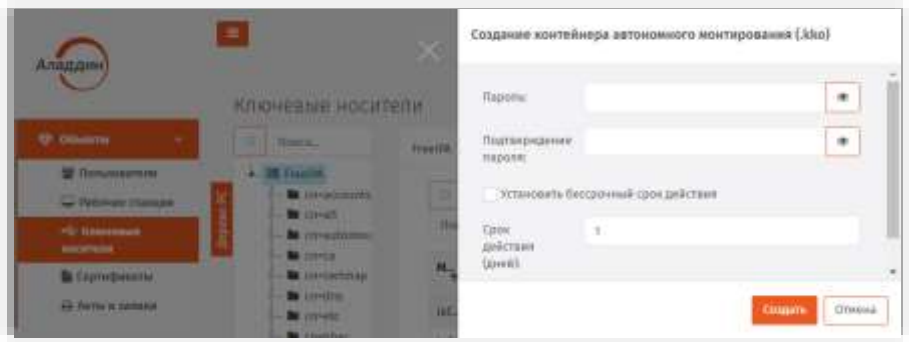


Рис. 83 – Страница установки параметров контейнера .kko

4. Выполните следующие действия.

4.1. Введите пароль и его подтверждение для создаваемого контейнера .kko.
4.2. Установите срок действия контейнера в днях или установите флаг **Установить бессрочный срок действия** для его бессрочного использования.

Важно! Для того чтобы возможность монтирования скрытых разделов с использованием контейнера .kko была отключена, по истечении указанного срока действия контейнера (или после отзыва контейнера вручную администратором безопасности, см. «Отзыв контейнера автономного монтирования скрытых дисков (.kko)», ниже) электронный ключ (ЗНИ) JaCarta SF/ГОСТ должен быть синхронизирован из консоли управления JMS (см. раздел «Синхронизация ЭК/ЗНИ », с. 47) либо с помощью приложения Клиент JMS (см. Руководство пользователя [1]).

5. Нажмите **Создать** для создания контейнера.

Файл контейнера .kko будет записан в папку, назначенную по умолчанию для загрузок (для скачанных файлов) используемого web-браузера.

Сохраненный контейнер следует передать пользователю ЗНИ для его использования на удаленном рабочем месте. Для монтирования скрытых дисков ЗНИ JaCarta SF/ГОСТ в автономном режиме пользователь может использовать как клиент JMS, так и ПО из комплекта поставки ЗНИ JaCarta SF/ГОСТ.

3.4.15.4 Отзыв контейнера автономного монтирования скрытых дисков (.kko)

Отзыв контейнера .kko возможен только у контейнеров с бессрочным использованием, или срок которых с момента выпуска еще не истек.

Важно! Для того чтобы отключить возможность монтирования скрытых разделов с использованием отозванного контейнера .kko, после его отзыва электронный ключ (ЗНИ) JaCarta SF/ГОСТ должен быть синхронизирован из консоли управления JMS (см. раздел «Синхронизация ЭК/ЗНИ », с. 47) либо с помощью приложения Клиент JMS (см. Руководство пользователя [1]).

Для отзыва контейнера автономного монтирования скрытых дисков в консоли управления JMS выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Объекты** -> **Ключевые носители**;
2. Выберите ЗНИ JaCarta SF/ГОСТ, для которого ранее был выпущен контейнер .kko . Нажмите на нем правой кнопкой мыши и в появившемся меню выберите **Отозвать контейнер автономного монтирования:**

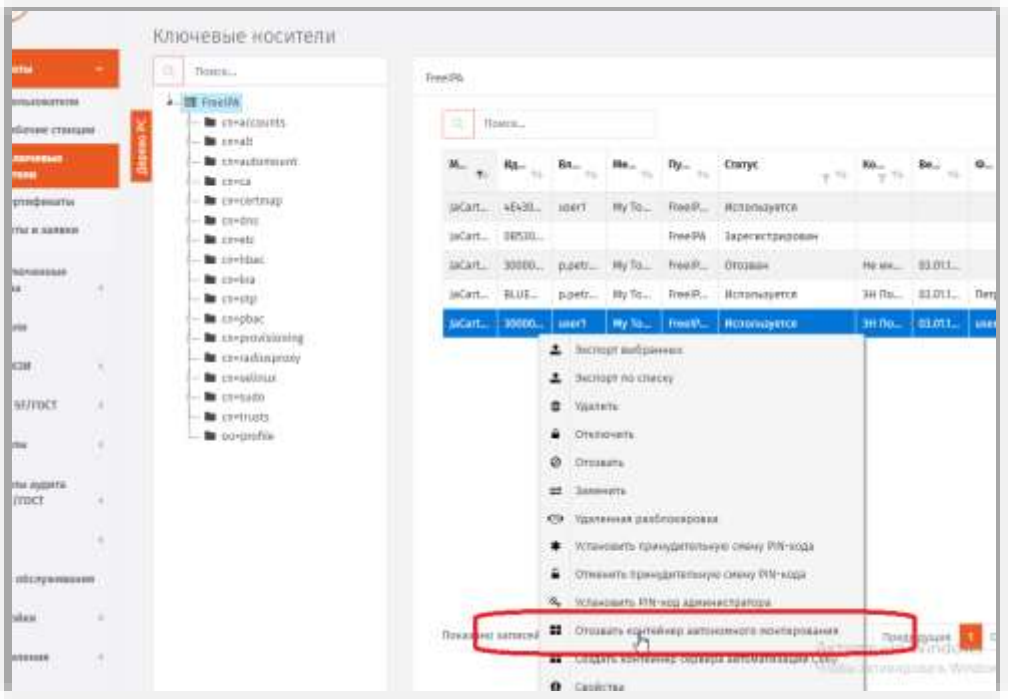


Рис. 84 – Отзыв контейнера .kko

3. В окне запроса на подтверждение отзыва контейнера .kko нажмите **Да**.

Рис. 85 – Запрос на подтверждение отзыва контейнера .kko

После отзыва контейнера .kko может быть сгенерирован новый контейнер.

3.4.15.5 Создание контейнера для локального сервера авторизации (.kkl)

Ключевой контейнер для локального сервера авторизации (файл с расширением kkl) предназначен для использования с комплектом программных средств для USB-носителя «JACARTA SF/ГОСТ», подробнее см. документацию из комплекта поставки USB-носителя [5].

Для экспорта ключевого контейнера для локального сервера авторизации выполните следующие действия.

1. В консоли управления JMS перейдите в один из следующих разделов:
   - **Объекты** -> **Ключевые носители**;
   - **Подключенные устройства** -> **Ключевые носители**.

В последнем случае ЭН пользователя должен быть подсоединен к компьютеру.

2. Выберите ЗНИ JaCarta SF/ГОСТ со статусом *Используется*, для которого необходимо создать контейнер .kkl . Нажмите на нем правой кнопкой мыши и в появившемся меню выберите **Создать контейнер сервера автоматизации (.kkl).**
3. Отобразится страница следующего вида.

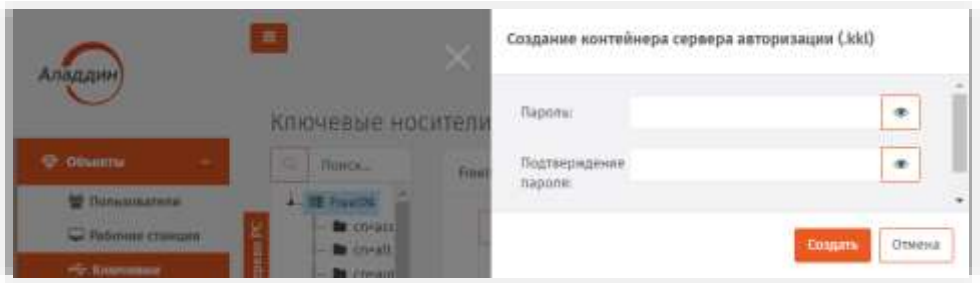


Рис. 86 – Страница установки параметров контейнера .kkl

4. Введите пароль и его подтверждение для создаваемого контейнера .kkl.
5. Нажмите **Создать** для создания контейнера.

Файл контейнера .kko будет записан в папку, назначенную по умолчанию для загрузок (для скачанных файлов) используемого web-браузера.

Сохраненный контейнер следует передать администратору доступа электронных носителей JaCarta SF/ГОСТ согласно документации из комплекта поставки USB-носителя [5].

3.4.15.6 Обезличивание ЗНИ JaCarta SF/ГОСТ

Согласно заводской документации ЗНИ (ЭН) JaCarta SF/ГОСТ операция удаления всей информации с данных носителей называется «обезличиванием». Фактически операция обезличивания означает восстановление заводских настроек ЗНИ.

Важно! Не выполнив обезличивание использовавшихся ЗНИ JaCarta SF/ГОСТ с помощью JMS (или ПО из комплекта заводской поставки данных ЗНИ), ими невозможно будет воспользоваться после передачи в другую организацию (имеющую собственную инфраструктуру для работы с ЗНИ данного типа) с целью их инициализации/выпуска и дальнейшей эксплуатации.

Чтобы обезличить ЗНИ JaCarta SF/ГОСТ, ранее выпущенный с помощью JMS, выполните следующие действия.

1. Подсоедините подлежащий обезличиванию ЗНИ JaCarta SF/ГОСТ к компьютеру с консолью управления JMS.
2. В консоли управления JMS перейдите в раздел **Подключенные устройства** -> **Ключевые носители**.
3. Выполните операцию **Отозвать** в соответствии с разделом «Отзыв ЭК/ЗНИ », с. 50.
4. Выполните операцию **Очистить** в соответствии с разделом «Очистка ЭК/ЗНИ », с. 45.

По окончании выполненных процедур (обезличивания) ЗНИ JaCarta SF/ГОСТ приобретет статус *Не инициализирован*.

3.4.16 Привязка ЭК/ЗНИ к контейнерам ресурсной системы

JMS позволяет привязать электронные ключи к определенному контейнеру ресурсной системы. Первоначальна привязка к контейнеру происходит во время регистрации электронного ключа. Также, после назначения и/или выпуска электронного ключа для какой-либо учетной записи, эти электронные ключи привязываются к контейнеру, в котором находится такая учетная запись. Консоль управления JMS предоставляет возможность изменить привязку электронных ключей, которые зарегистрированы (статус *Зарегистрирован*), но еще не назначены и/или не выпущены на имя какого-либо пользователя.

Чтобы изменить привязку электронного ключа, выполните следующие действия.

1. В консоли управления JMS перейдите в один из двух разделов:

   – **Объекты** -> **Ключевые носители**, после чего панели с деревом ресурсной системы выберите контейнер, содержащий электронные ключи, привязку которых нужно изменить;
   – **Подключенные устройства -> Ключевые носители** – в этом случае электронный ключ, привязку которого нужно изменить, должен быть подсоединен к компьютеру.

2. В центральной части интерфейса отметьте электронный ключ или ключи, привязку которых нужно изменить и нажмите правой кнопкой мыши. В появившемся меню нажмите **Перенос**.

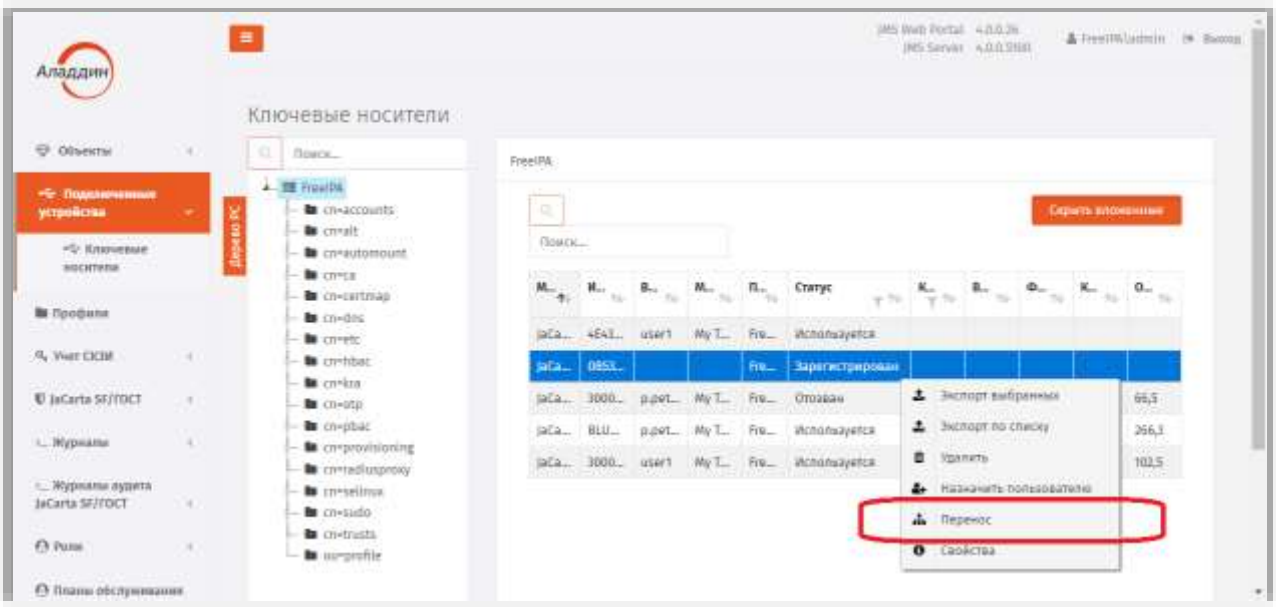


Рис. 87 – Перенос привязки электронного ключа

3. Отобразится окно запроса на подтверждение переноса электронного ключа нажмите.

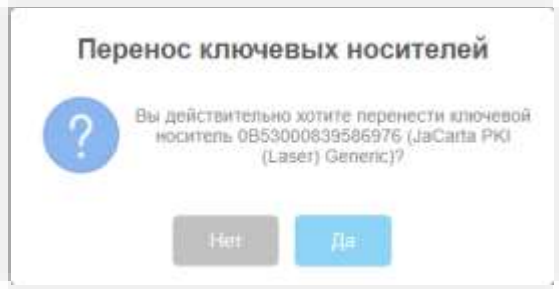


Рис. 88 – Окно подтверждения изменении привязки электронного ключа

4. Нажмите **Да**.
5. Отобразится страница выбора контейнера ресурсной системы.

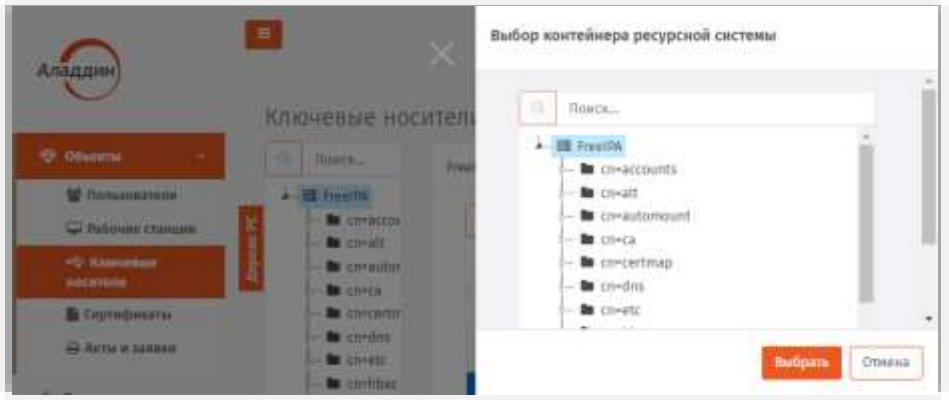


Рис. 89 – Страница выбора контейнера ресурсной системы

б. Выберите контейнер, к которому вы хотите привязать электронный ключ или ключи, и нажмите **Выбрать**.

Электронный ключ будет привязан к выбранному контейнеру.

3.5 Операции с OTP- и U2F-аутентификаторами

Операции, связанные с управлением жизненным циклом OTP- и U2F-аутентификаторов осуществляются в разделе **OTP- и U2F-аутентификаторы** (Рис. 90) консоли управления JMS.

Примечание. Операции с OTP- и U2F-аутентификаторами доступны при выполнении следующих условий:

1. В установленной в JMS лицензии указана опция на поддержку сервера JAS.
2. Сервер JAS установлен и настроен в системе JMS (см. руководство по установке и настройке JAS [3]).

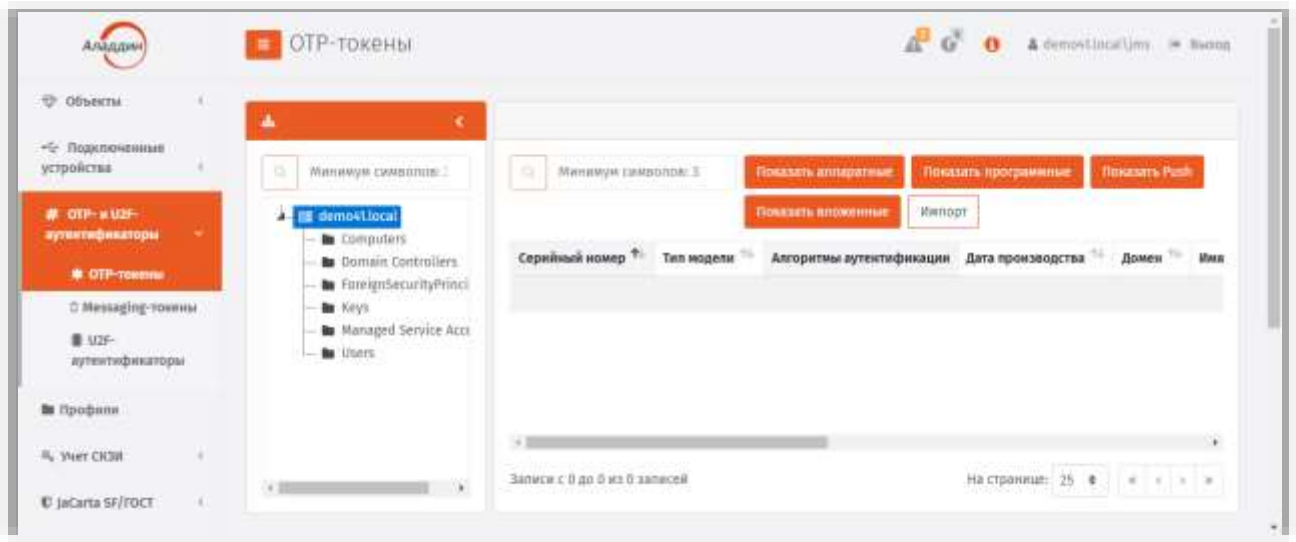


*Рис. 90 – Общий вид раздела **OTP- и U2F-аутентификаторы** консоли управления JMS*

В табл. 4 (ниже) представлен краткий перечень доступных операций (со ссылками на соответствующие подразделы настоящего руководства), а также указаны типы и модели аутентификаторов, к которым применима та или иная операция.

Также, в таблице указано, после каких операций на электронный адрес пользователя, к которому эта операция относилась, отправляется электронное письмо.

*Табл. 4 – Краткий перечень операций, доступных в разделе **OTP- и U2F-аутентификаторы***

Раздел -> Подраздел консоли управления	Операция	По завершении операции на адрес пользователя отправляется электронное письмо / SMS-сообщение	Типы аутентификаторов
OTP- и U2F-аутентификаторы -> OTP-токены	«Импорт инвентарного файла», с. 73	Нет	• eToken PASS; • eToken NG OTP; • eToken NG OTP (Java); • JC-WebPass; • Другие OTP-токены, реализующие спецификации RFC 4226 и 6238
OTP- и U2F-аутентификаторы -> OTP-токены	«Выпуск программных OTP-токенов (мобильное приложение Aladdin 2FA)», с. 80	Да (Email)	мобильное приложение Aladdin 2FA компании Аладдин
OTP- и U2F-аутентификаторы -> OTP-токены	«Установка и изменение PIN-кода для OTP», с. 82	Да (Email)	• мобильное приложение Aladdin 2FA компании Аладдин eToken PASS; • Другие OTP-токены, реализующие спецификации RFC 4226 и 6238 • eToken NG OTP; • eToken NG OTP (Java); • JC-WebPass;
OTP- и U2F-аутентификаторы -> OTP-токены	«Включение и отключение OTP-токена», с. 83	Нет	
OTP- и U2F-аутентификаторы -> OTP-токены	«Синхронизация значений OTP», с. 83		
OTP- и U2F-аутентификаторы -> OTP-токены	«Просмотр и редактирование свойств OTP-токена», с. 84		
OTP- и U2F-аутентификаторы -> OTP-токены	«Удаление сведений об OTP-токене», с. 88		
OTP- и U2F-аутентификаторы -> Messaging-токены	«Управление PIN-кодом для Messaging-токена», с. 89	Да (SMS)	Messaging-токен
OTP- и U2F-аутентификаторы -> Messaging-токены	«Включение и отключение Messaging-токена», с. 89	Нет	
OTP- и U2F-аутентификаторы -> Messaging-токены	«Просмотр свойств Messaging-токена», с. 89	Нет	
OTP- и U2F-аутентификаторы -> Messaging-токены	«Удаление сведений о Messaging-токене», с. 92	Нет	
OTP- и U2F-аутентификаторы -> U2F-аутентификаторы	«Включение и отключение U2F-аутентификатора», с. 92	Нет	U2F-аутентификатор
OTP- и U2F-аутентификаторы -> U2F-аутентификаторы	«Просмотр и редактирование свойств U2F-аутентификатора», с. 93		
OTP- и U2F-аутентификаторы -> U2F-аутентификаторы	«Удаление сведений о U2F-аутентификаторе», с. 94		

3.5.1 Операции с OTP-токенами

В настоящем разделе описаны операции, производимыми с OTP-токенами (включая их выпуск) из консоли управления JMS (т.е. администратором JMS).

Порядок настройки самостоятельного выпуска для себя OTP-аутентификаторов (включающих в себя программные OTP-, Push OTP- и Messaging-токены) пользователями из личного кабинета на портале JWM описан в разделе «Порядок настройки самостоятельного выпуска пользователями OTP-аутентификатора», с. 205.

3.5.1.1 Импорт инвентарного файла

Импорт инвентарных файлов осуществляется только для аппаратных OTP-токенов. (Регистрация программных OTP-токенов происходит автоматически и не требует инвентарных файлов).

Чтобы импортировать инвентарный файл со списком аппаратных OTP-токенов, выполните следующие действия.

Примечание. Аппаратные OTP-токены поставляются с производства вместе с инвентарными файлами. В случае если такие файлы утеряны или отсутствуют, для их получения следует обратиться в службу технической поддержки компании Аладдин (см. раздел «Контакты, техническая поддержка», с. 341).

1. В консоли управления JMS выберите раздел **OTP- и U2F-аутентификаторы -> OTP-токены.**
2. В средней части окна выберите контейнер ресурсной системы, к которому следует привязать импортируемые токены (Рис. 91).

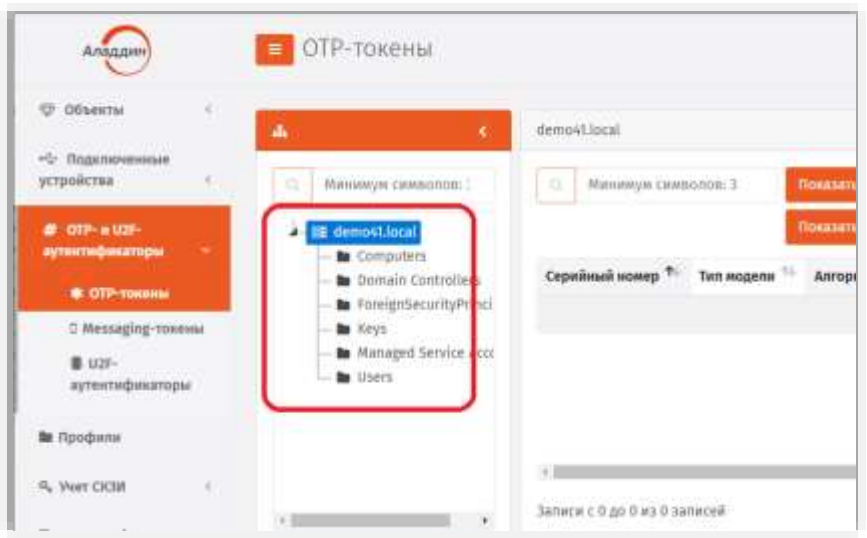


Рис. 91 – Выбор контейнера для привязки импортируемых OTP-токенов

3. В верхней панели нажмите **Импорт**.

Отобразится следующее окно.

Рис. 92 – Окно приветствия мастера импорта ключевых носителей

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

Рис. 93 – Указание пути к инвентарному файлу

5. Выберите тип инвентарного файла (.dat или .xml) и воспользуйтесь кнопкой «**...**» (три точки), чтобы указать путь к данному файлу, после чего нажмите **Далее**.

Отобразится следующее окно.

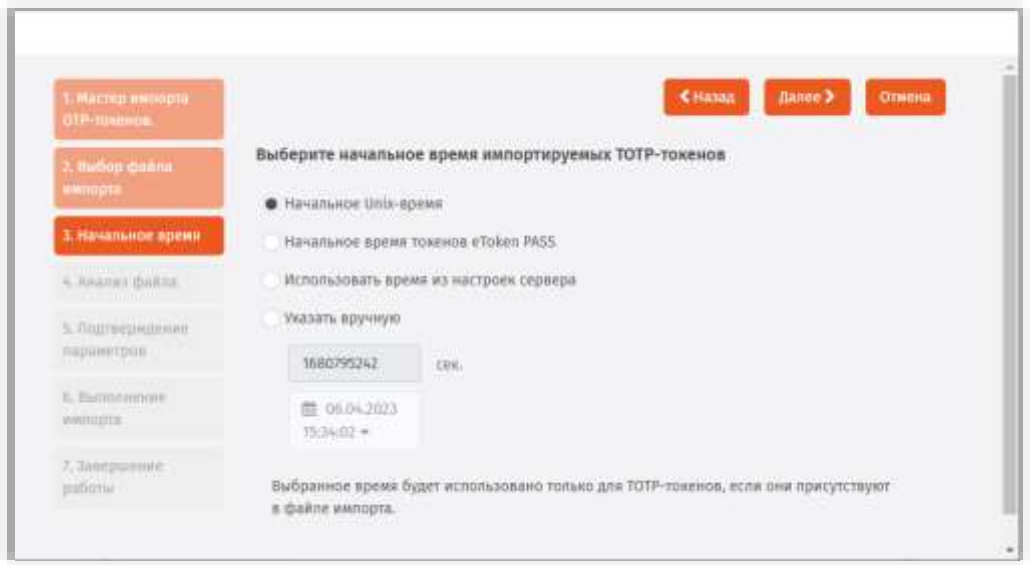


Рис. 94 – Установка начального времени для TOTP-токенов

6. Выполните необходимые настройки, руководствуясь Табл. 5, и нажмите **Далее**.

Табл. 5 – Установка начального времени для TOTP-токенов

Настройка	Описание
Начальное Unix-время	Будет выбрано начальное время, стандартное для ОС Unix (01.01.1970 0:00:00)
Начальное время токенов eToken PASS	Будет выбрано начальное время, устанавливаемое по умолчанию в токенах eToken PASS (01.01.2000 0:00:00)
Использовать время из настроек сервера	Будет выбрано начальное время, равное текущему времени, установленному на сервере JMS
Указать вручную	Установка начального времени вручную (отображается в Unix- и обычном формате)

Отобразится следующее окно.

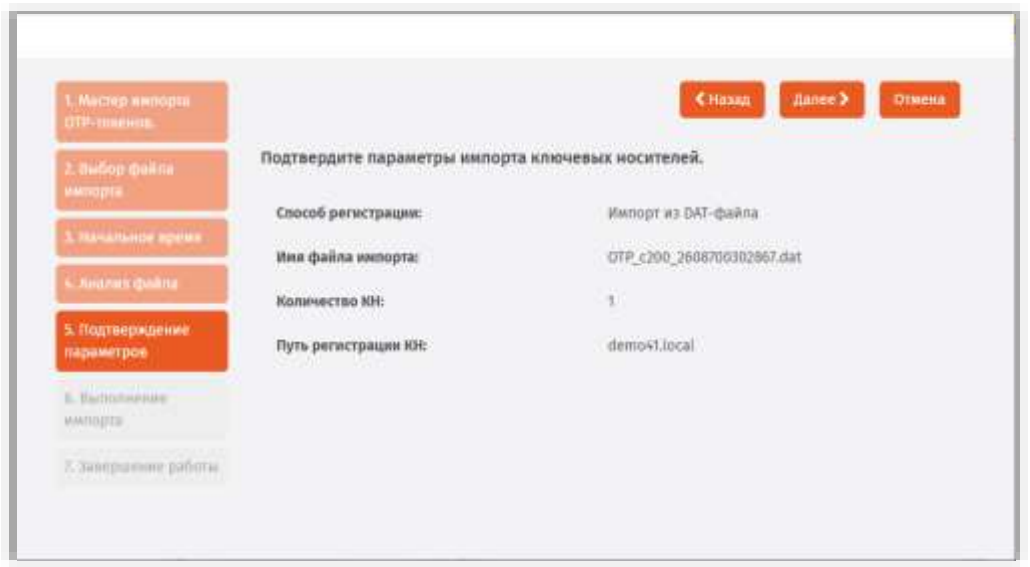


Рис. 95 – Страница подтверждения параметров импорта инвентарного файла

7. Нажмите **Далее**.
Отобразится окно следующего вида.

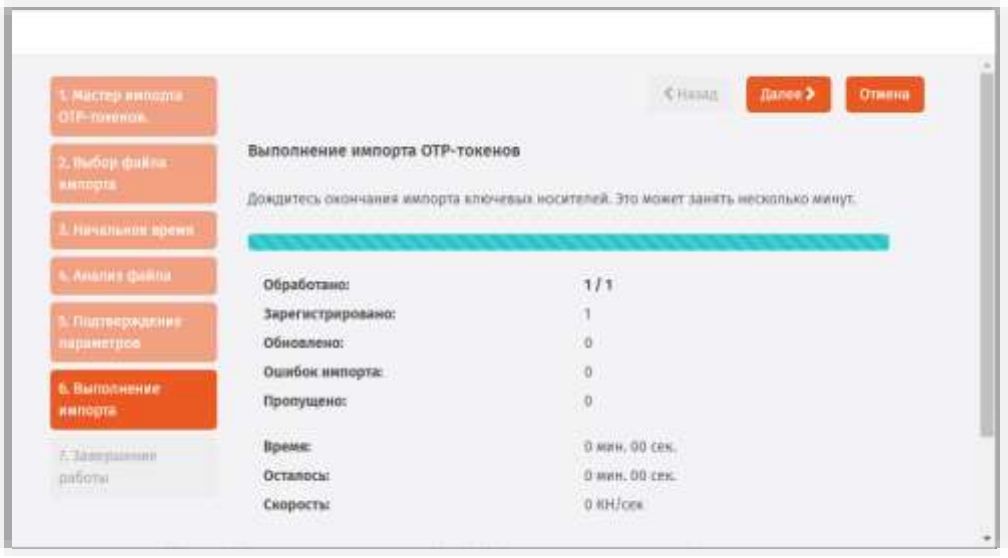


Рис. 96 – Страница отображения импорта инвентарного файла

8. Если вы хотите сохранить данные об импорте в файл журнала, выполните следующие действия (в противном случае переходите к следующему шагу процедуры):

8.1. нажмите **Сохранить лог** и укажите путь сохранения этого файла;
8.2. в окне сообщения об успешном сохранении файла журнала нажмите **ОК**.

9. В окне мастера импорта нажмите **Далее**.
Отобразится следующее окно.

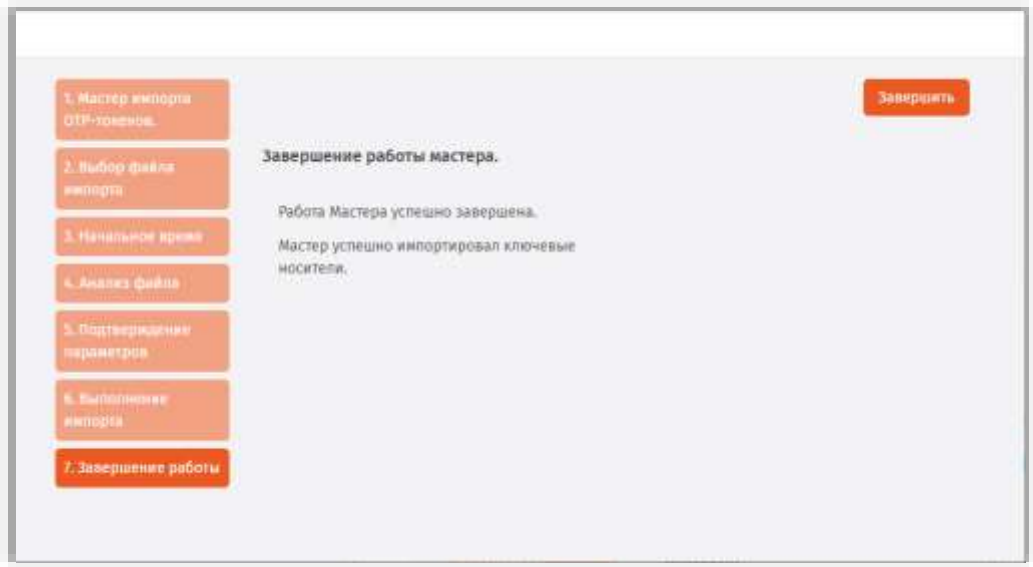


Рис. 97 – Окно завершения процедуры импорта

10. Нажмите **Завершить**.

Сведения об импортированных OTP-токенах отобразятся в правой части страницы консоли управления JMS (рис. 98). После регистрации токены имеют статус *Зарегистрирован*.

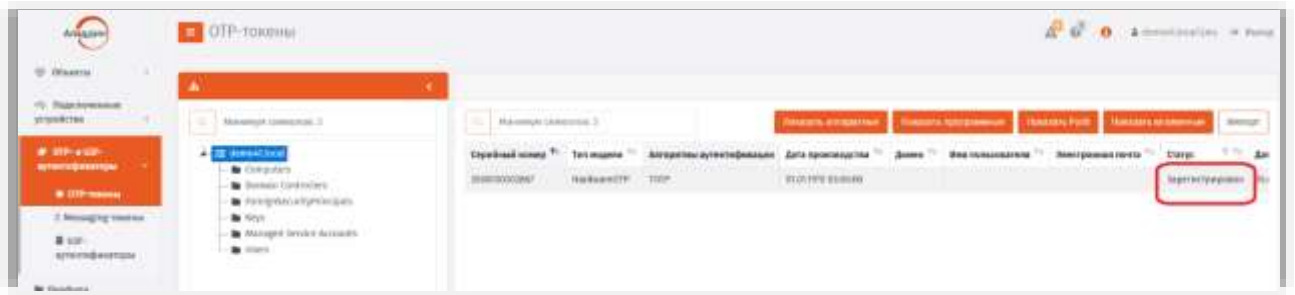


Рис. 98 – Сведения об импортированных OTP-токенах в консоли управления JMS

3.5.1.2 Назначение / отмена назначения аппаратного OTP-токена

Примечание. Назначение аппаратного OTP-токена пользователю можно выполнить только с теми токенами, которые имеют статус *Зарегистрирован* (присваивается токену после его импорта, см. раздел «Импорт инвентарного файла», с. 73).

Чтобы назначить аппаратный OTP-токен пользователю, выполните следующие действия.

1. В консоли управления JMS выберите OTP-токен, для которого вы хотите выполнить назначение и нажмите на нём правой кнопкой мыши. В контекстном меню выберите команду **Назначить пользователю** (Рис. 99).

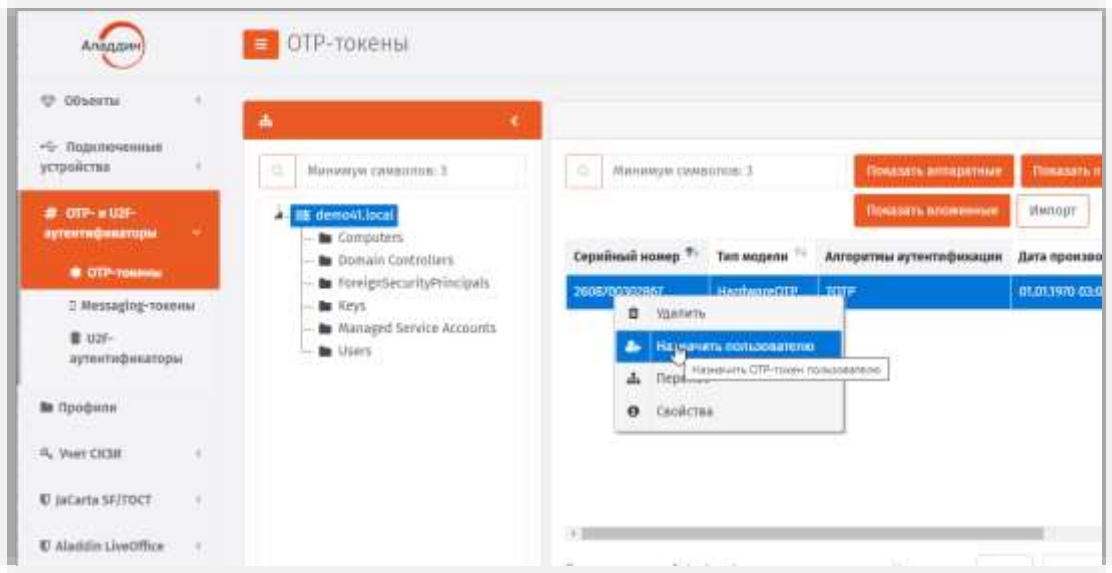


Рис. 99 –Команда назначения пользователя аппаратному OTP-токену

2. Откроется окно следующего вида.

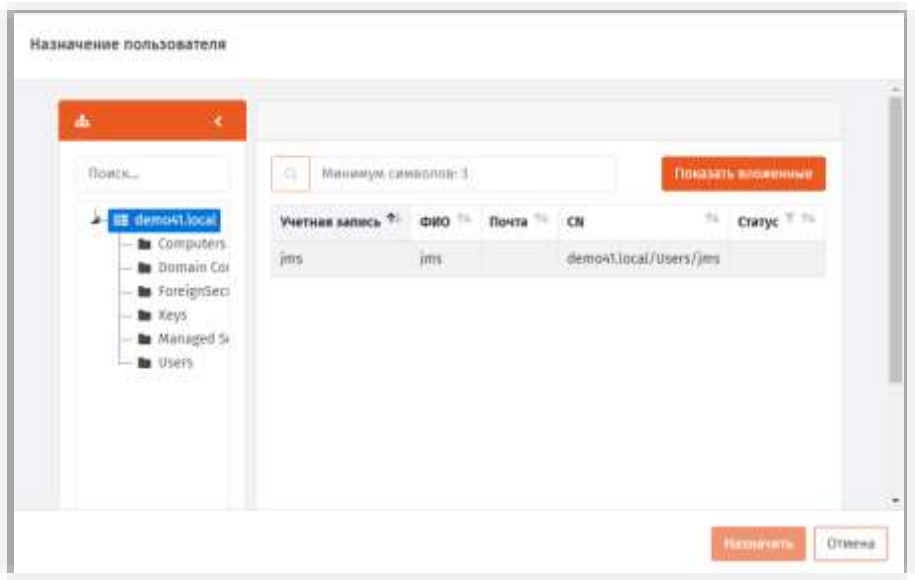


Рис. 100 –Выбора пользователя для назначения

3. Выберите пользователя в списке и нажмите **Назначить**.

В результате OTP-токен меняет статус с *Зарегистрирован* на *Назначен* (Рис. 101).

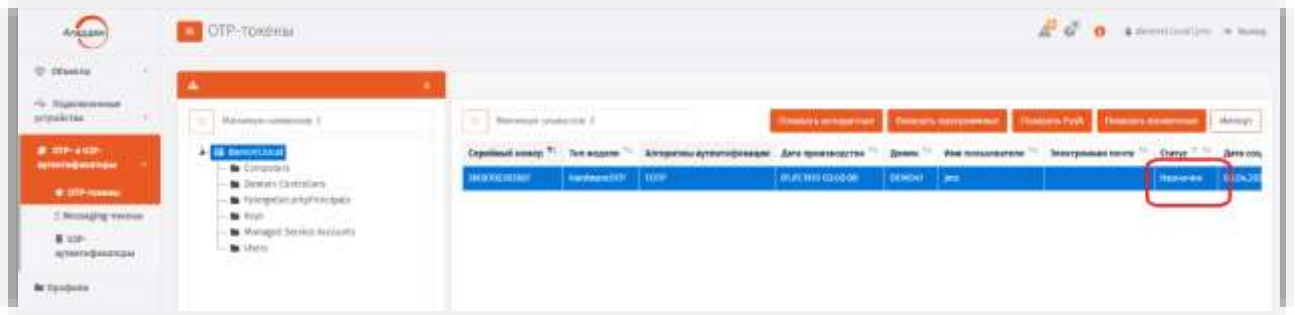


Рис. 101 –Смена статуса токена на Назначен

Для отмены назначения токена пользователю выполните следующие действия.

1. В консоли управления JMS выберите OTP-токен, для которого вы хотите отменить назначение и нажмите на нём правой кнопкой мыши. В контекстном меню выберите команду **Отменить назначение** (Рис. 99).

Отобразится диалоговое окно подтверждения.

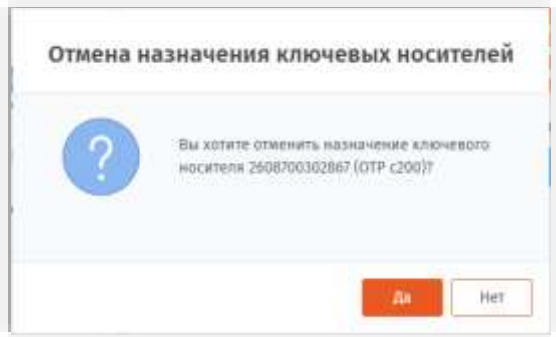


Рис. 102 –Окно подтверждение отмены назначения OTP-токена пользователю

2. Нажмите **Да**.
   Отобразится следующее окно для выбора ресурсной системы.

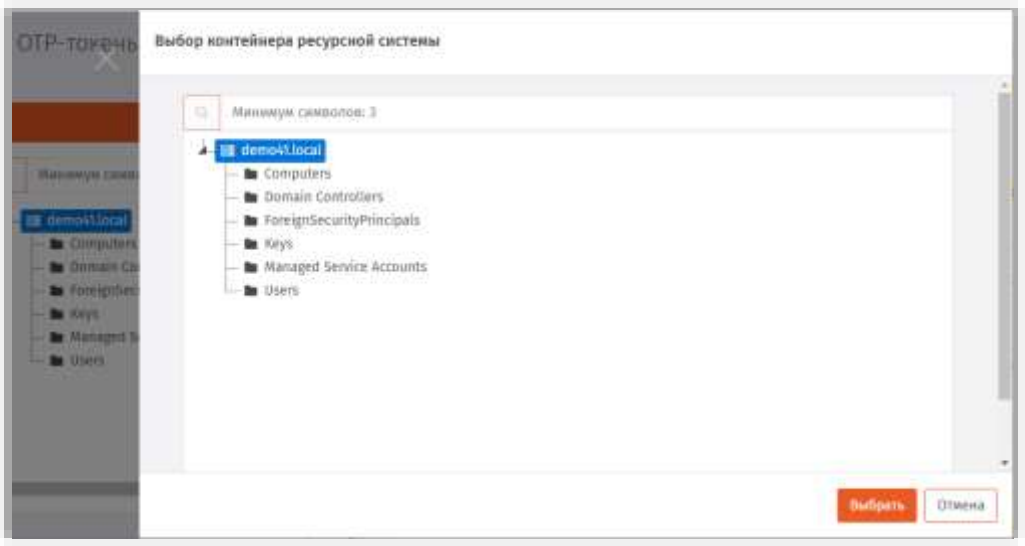


Рис. 103 – Окно выбора контейнера для привязки токена при отмене его назначения пользователю

3. Выберите контейнер для привязки к нему токена после отмены назначения и нажмите **Выбрать**.

В результате токен поменяет статус с *Назначен* на *Зарегистрирован*.

3.5.1.3 Выпуск аппаратных OTP-токенов

Чтобы выпустить для группы пользователей JMS аппаратные OTP-токены выполните следующие действия.

1. Импортируйте аппаратные токены, руководствуясь разделом «Импорт инвентарного файла», с. 73.
2. Выполните назначение аппаратных OTP-токенов пользователям, руководствуясь разделом «Назначение / отмена назначения аппаратного OTP-токена», с. 77.
3. Создайте профиль выпуска аппаратных OTP-токенов, руководствуясь разделом «Настройка профиля выпуска аппаратных OTP-токенов», с. 158, и выполните его привязку к

соответствующему контейнеру ресурсной системы, руководствуясь разделом «Привязка профилей», с. 195.

4. Настройте для выпуска аппаратных OTP-токенов и запустите на выполнение соответствующий план обслуживания, руководствуясь разделами «План обслуживания жизненного цикла OTP-токенов», с. 281 и «Запуск и просмотр результатов планов обслуживания», с.274.
5. Выпущенные и готовые к использованию (статус *Используется*) экземпляры аппаратных OTP-токенов отобразятся в консоли управления JMS со значением *HardwareOTP* в поле **Тип модели** (Рис. 104).

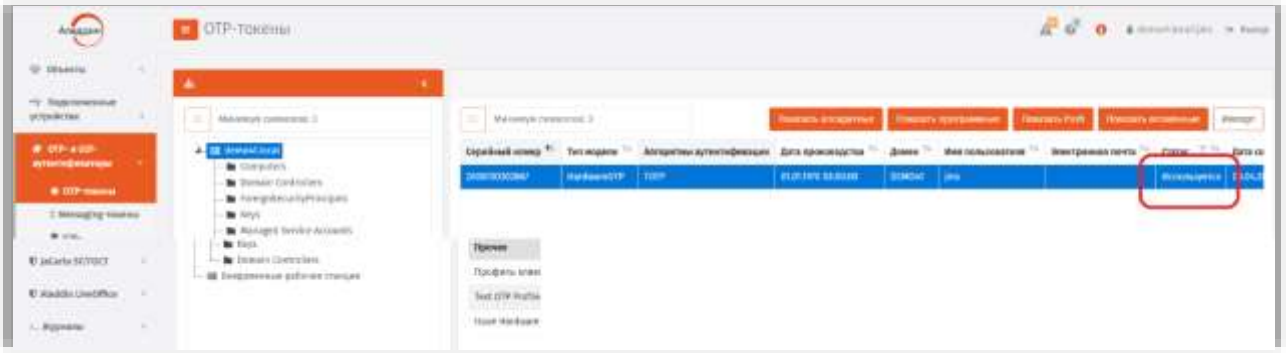


Рис. 104 – Отображение выпущенного экземпляра аппаратного OTP-токена

6. Пользователи, для которых были выпущены токены, требующие указания PIN-кода для аутентификации (см. параметр **Режим аутентификации** в профиле выпуска аппаратных OTP-токенов), получат на свой электронный адрес сообщение, содержащее PIN-код для OTP.

Примечание. Для оповещения пользователей по электронной почте об установке или смене PIN-кода для аппаратных OTP-токенов должны быть выполнены следующие условия:

1. У пользователей, зарегистрированных в JMS, для которых выпускаются токены, в ресурсной системе (например FreeIPA) должен быть настроен адрес электронной почты.
2. С помощью консольного агента в JMS должен быть настроен транспортный почтовый сервис (команда Aladdin.EAP.Agent.Terminal smtp configure, подробнее см. руководство по установке и настройке JMS [2]).

3.5.1.4 Выпуск программных OTP-токенов (мобильное приложение Aladdin 2FA)

Важно! Для корректного выпуска программных OTP-токенов должны быть выполнены следующие условия:

1. У пользователей, зарегистрированных в JMS, для которых выпускаются токены, в ресурсной системе (например FreeIPA) должен быть настроен адрес электронной почты.
2. С помощью консольного агента в JMS должен быть настроен транспортный почтовый сервис (команда Aladdin.EAP.Agent.Terminal smtp configure, подробнее см. руководство по установке и настройке JMS [2]).

Чтобы выпустить для группы пользователей JMS программные OTP-токены для мобильного приложения Aladdin 2FA компании Аладдин (или для аналогичных мобильных приложений других поставщиков), выполните следующие действия.

1. Создайте профиль выпуска программных OTP-токенов, руководствуясь разделом «Настройка профиля выпуска программных OTP-токенов», с. 164.
2. Настройте для выпуска программных OTP-токенов и запустите на выполнение соответствующий план обслуживания, руководствуясь разделами «План обслуживания жизненного цикла OTP-токенов», с. 281 и «Запуск и просмотр результатов планов обслуживания», с.274.

3. Выпущенные и готовые к использованию (статус *Используется*) экземпляры программных OTP-токенов отобразятся в консоли управления JMS со значением *SoftwareOTP* в поле **Модель (**Рис. 105**)**.

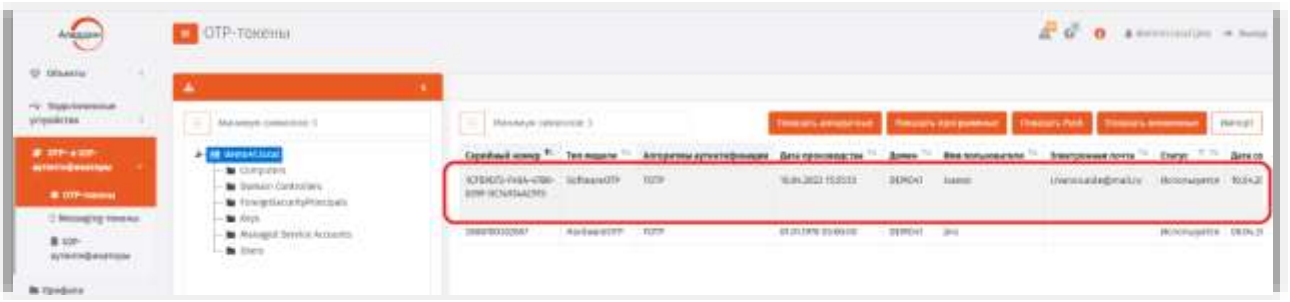


Рис. 105 – Отображение выпущенного экземпляра программного OTP-токена

4. Пользователи, для которых были выпущены токены получат на свой электронный адрес сообщение, содержащее PIN-код для OTP и QR-код (Рис. 106).

Рис. 106 - сообщение, содержащее PIN-код для OTP и QR-код

4. Пользователь с помощью своего мобильного устройства, на котором установлено необходимое приложение (например, мобильное приложение Aladdin 2FA компании Аладдин), должен отсканировать QR-код, после чего он сможет генерировать значения OTP.

3.5.1.5 Установка и изменение PIN-кода для OTP

Важно! Для обеспечения возможности установки или изменения PIN-кода у OTP-токена, он должен быть выпущен на основе профиля (см. разделы «Настройка профиля выпуска аппаратных OTP-токенов», с. 158, «Настройка профиля выпуска программных OTP-токенов» с. 164), у которого в поле **Режим аутентификации** установлено одно из значений, включающее в себя PIN-код (например *OTP PIN-код + OTP* или *Доменный пароль + OTP PIN-код + OTP*).

Чтобы установить или изменить PIN-код для OTP выбранного токена, выполните следующие действия.

1. В консоли управления JMS выберите токен, PIN-код для OTP которого вы хотите изменить, и нажмите на нем правой кнопкой мыши (Рис. 107).

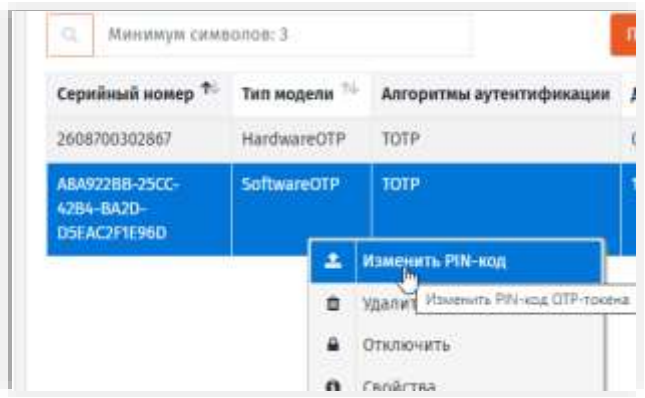


Рис. 107 – Установка или изменение PIN-кода для OTP

2. Выберите **Изменить PIN-код**.
Отобразится следующее окно.

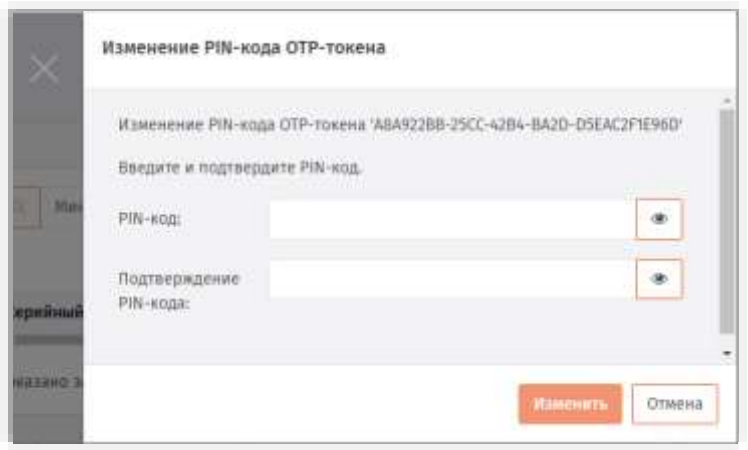


Рис. 108 – Установка или изменение PIN-кода для OTP

3. Введите значение нового PIN-кода для OTP в полях **PIN-код** и **Подтверждение PIN-кода**.
4. Нажмите **Изменить**.
При успешной установке/изменении PIN-кода для OTP отобразится соответствующее сообщение (Рис. 109). При этом пользователю будет отправлено уведомление по электронной почте об установке / смене PIN-кода.

Примечание. Для оповещения по электронной почте об установке или смене PIN-кода для аппаратных OTP-токенов у пользователей в ресурсной (например FreeIPA) должен быть настроен адрес электронной почты, а также с помощью в консольного агента в JMS должен быть настроен транспортный почтовый сервис (команда Aladdin.EAP.Agent.Terminal smtp configure, подробнее см. руководство по установке и настройке JMS [2].).

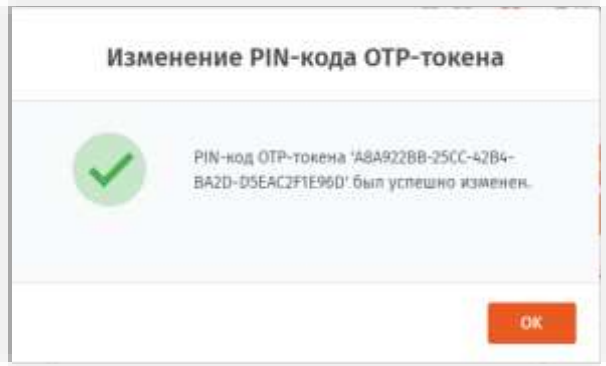


Рис. 109 – Установка или изменение PIN-кода для OTP

5. Нажмите **OK** для завершения процедуры.

3.5.1.6 Включение и отключение OTP-токена

Чтобы включить или отключить возможность использования OTP-токена, выполните следующие действия.

С OTP-токеном невозможно выполнить операции включения/отключения, если он не был выпущен (не имеет статуса *Используется*). О выпуске OTP-токенов см. в разделах «Выпуск аппаратных OTP-токенов», с. 79 и «Выпуск программных OTP-токенов (мобильное приложение Aladdin 2FA)», с. 80.

1. В консоли управления JMS выберите OTP-токен, возможность использования которого вы хотите включить или отключить.
2. Нажмите на выбранном токене правой кнопкой мыши и в зависимости от нужного действия в контекстном меню выберите **Включить** или **Отключить**.
   Отобразится диалоговое окно подтверждения действия.
3. Нажмите **Да** для продолжения.
   Новый статус OTP-токена (*Используется* или *Отключен*) отобразится в столбце **Статус** в правой консоли управления JMS (см. рис. 110 ниже).

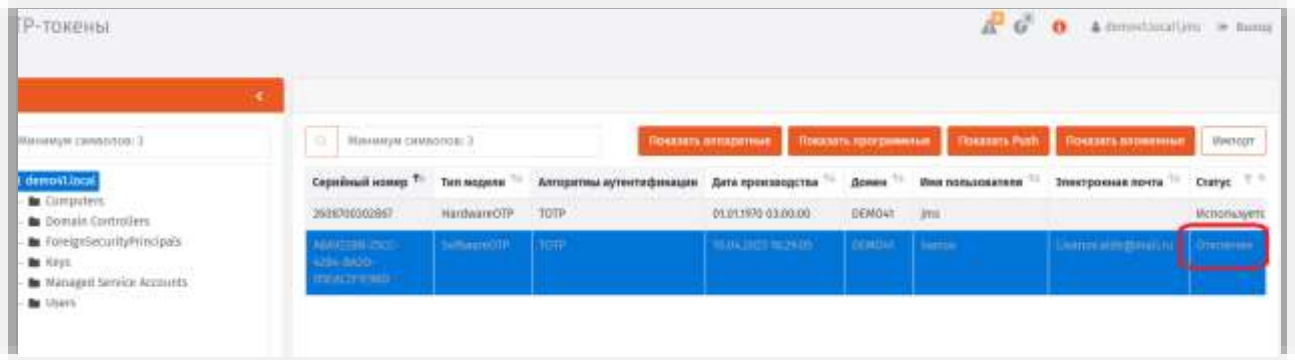


*Рис. 110 – Текущий статус OTP-токена отображается в столбце **Статус***

3.5.1.7 Синхронизация значений OTP (только для токенов HOTP)

Настоящий раздел относится только OTP-токенам (аппаратным и программным), функционирующим в соответствии со спецификацией RFC 4226 (HOTP).

Примечание. Тип спецификации выбирается в **Параметрах выпуска** профиля выпуска соответствующих токенов, в поле **Алгоритм**.

Синхронизацию значений OTP следует выполнять в следующих случаях:

- при вводе OTP-токена в эксплуатацию, перед передачей его пользователю;
- если пользователь сгенерировал большее число одноразовых паролей, чем указано в настройке **Окно аутентификации** профиля выпуска OTP-токена соответствующего типа (см. разделы «Настройка профиля выпуска аппаратных OTP-токенов», с. 158 и «Настройка профиля выпуска программных OTP-токенов», с. 164).

Чтобы синхронизировать OTP-токен с JMS, выполните следующие действия.

1. В консоли управления JMS выберите OTP-токен, который вы хотите синхронизировать с JMS.
2. Нажмите на выбранном токене правой кнопкой мыши и в контекстном меню выберите **Синхронизация**.
   Отобразится следующее окно.

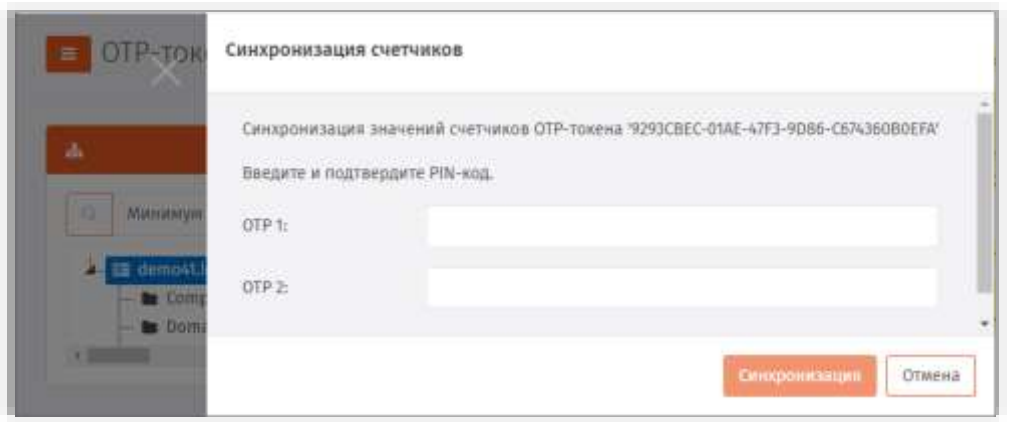


Рис. 111 – Синхронизация OTP-токена

3. С помощью синхронизируемого OTP-токена сгенерируйте значение OTP (или проинструктируйте пользователя сгенерировать значением OTP и сообщить его вам) и введите его в поле **OTP 1**.
4. С помощью синхронизируемого OTP-токена сгенерируйте следующее значение OTP (или проинструктируйте пользователя сгенерировать значением OTP и сообщить его вам) и введите его в поле **OTP 2**.
5. Нажмите **Синхронизировать**.
   При успешной синхронизации отобразится следующее сообщение.
6. Нажмите **ОК** для завершения процедуры.

3.5.1.8 Просмотр и редактирование свойств OTP-токена

Чтобы просмотреть или отредактировать свойства OTP-токена, выполните следующие действия.

1. В консоли управления JMS выберите OTP-токен, свойства которого вы хотите просмотреть или редактировать.
2. Нажмите на нем правой кнопкой мыши и в контекстном меню выберите **Свойства**.

Отобразится следующее окно.

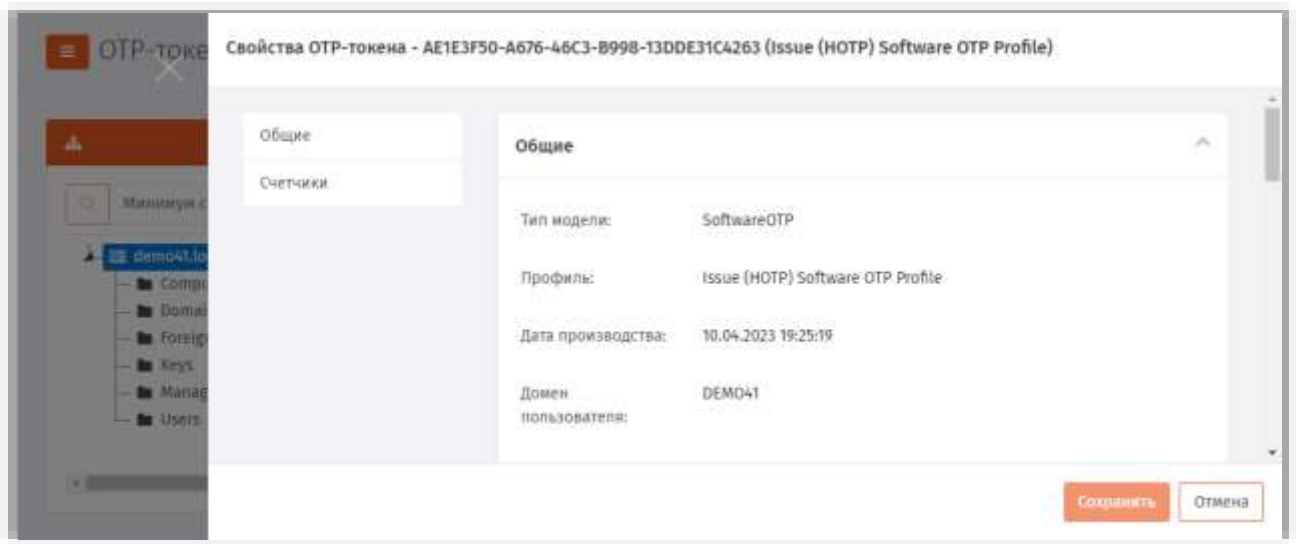


*Рис. 112 – Вкладка **Общие** свойств OTP-токена*

3. На вкладке отображаются нередактируемые поля в соответствии с табл. 6.

Табл. 6 – Общие параметры OTP-токена

Поле	Описание
Тип модели	Тип OTP-токена (программный/аппаратный). Возможные варианты: • **SoftwareOTP** • **HardwareOTP**
Профиль	Имя профиля, по которому был выпущен данный OTP-токен
Дата производства	Отображает дату производства OTP-токена.
Домен пользователя	Отображает домен, в котором зарегистрирован пользователь OTP-токена.
Имя пользователя	Отображает имя пользователя OTP-токена.
Email пользователя	Отображает адрес электронной почты, на который пользователю будут приходить уведомления. **Примечание.** Адрес e-mail пользователя берется из учетной записи пользователя в той ресурсной системе (например FreeIPA), из которой данная учётная запись была зарегистрирована (импортирована) в JMS. Настройка рассылки осуществляется с помощью в консольного агента в JMS (команда Aladdin.EAP.Agent.Terminal smtp configure, подробнее см. руководство по установке и настройке JMS [2])
FQDN	Отображение полного имени пользователя в FQDN-нотации.
UPN	Отображение полного имени пользователя в UPN-нотации.

Поле	Описание
Статус	Отображает текущий статус OTP-токена. Возможны следующие значения: • **Зарегистрирован** • **Назначен** • **Используется** • **Отключен**
Дата создания	Отображает дату и время внесения сведений об OTP-токене в базу данных JMS.
Дата изменения	Отображает дату и время последних изменений в состоянии OTP-токена (например, дату включения или выключения возможности использования OTP-токена).
Максимальное количество попыток аутентификации	Отображает число попыток аутентификации, установленное в параметре *MaxAuthFailCount* конфигурационного файла *BusinessLogic.json*, загружаемого с помощью команды консольного агента JAS – *AladdinJAS.Agent.Terminal config upload* (подробнее см. руководство по установке и настройке сервера JAS [3], раздел «Приложение 2. Справочник команд консольного агента AladdinJAS.Agent.Terminal»)
Оставшееся количество попыток аутентификации	Число попыток аутентификации (максимальное число попыток за вычетом использованных попыток).

4. Перейдите на вкладку **Счетчики**.
   В зависимости от типа OTP-токена окно примет следующий вид.

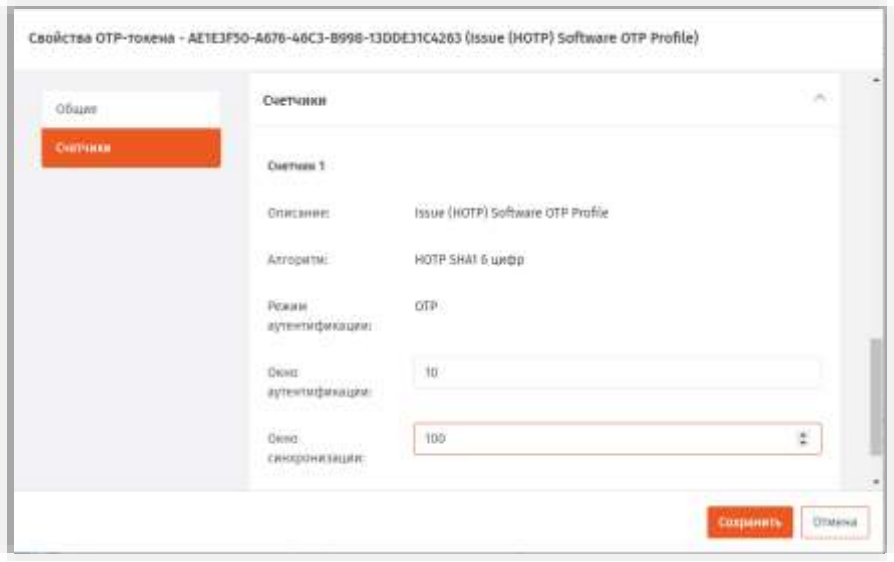


*Рис. 113 – Вкладка **Счетчики** окна свойств OTP-токена с алгоритмом генерации HOTP*

*Рис. 114 – Вкладка **Счетчики** окна свойств OTP-токена с алгоритмом генерации TOTP*

5. Выполните настройки, руководствуясь табл. 7 ниже.

Табл. 7 – Дополнительные параметры OTP-токена

Настройка/поле	Описание
Описание	Отображает описание выбранного OTP-токена, задается в профиле выпуска OTP-токенов (см. Табл. 40, с. 159). Неизменяемое поле.
Алгоритм	Отображает алгоритм формирования одноразовых паролей, используемый на OTP-токене. Задается в профиле выпуска OTP-токенов (см. Табл. 40, с. 159). Неизменяемое поле.
Текущее значение (только для токенов с алгоритмом HOTP)	Значение счетчика, используемое алгоритмом формирования одноразовых паролей для вычисления следующего значения OTP. Неизменяемое поле.
Режим аутентификации	Отображает режим аутентификации. Задается в профиле выпуска OTP-токенов. (см. Табл. 40, с. 159) Неизменяемое поле.
Окно аутентификации **Окно синхронизации** (только для токенов с алгоритмом HOTP)	Описание параметров приведено в Табл. 42, с. 162. Параметры позволяют выполнить индивидуальную настройку для отдельного токена (после выпуска токена со значениями параметров, определенных в профиле выпуска).
Интервал действия пароля (с) **Начальное значение**	Описание параметров приведено в Табл. 45, с. 168. Неизменяемые поля.

Настройка/поле	Описание
(только для токенов с алгоритмом TOTP)	
Количество временных интервалов, просматриваемых назад **Количество временных интервалов, просматриваемых вперед** (только для токенов с алгоритмом TOTP)	Описание параметров приведено в Табл. 45, с. 168. Параметры позволяют выполнить индивидуальную настройку для отдельного токена (после выпуска токена со значениями параметров, определенных в профиле выпуска).

6. Нажмите **Сохранить**, чтобы сохранить изменения.

3.5.1.9 Удаление сведений об OTP-токене

В случае утери или компрометации OTP-токена сведения о нём следует удалить из базы данных JMS, чтобы исключить возможность использования злоумышленником этого OTP-токена.

Чтобы удалить сведения об OTP-токене из базы данных JMS, выполните следующие действия.

1. В консоли управления JMS выберите OTP-токен, сведения о котором вы хотите удалить.
2. Нажмите на нём правой кнопкой мыши и в контекстном меню выберите **Удалить**.
3. Отобразится диалоговое окно подтверждения выбора.
4. Нажмите **Да** для завершения процедуры.

3.5.2 Операции с Messaging-токенами

Messaging-токен – это один из типов аутентификаторов на базе механизма OTP, поддерживаемых сервером JMS. Messaging-токен – это виртуальный объект, который регистрируется в JMS с привязкой к пользователю и осуществляет процедуру передачи значения OTP на мобильный телефон пользователя посредством службы SMS оператора связи по запросу внешней интегрируемой с JMS прикладной системы. Управление Messaging-токенами осуществляется в разделе **OTP- и U2F-аутентификаторы -> Messaging-токены** консоли управления JMS.

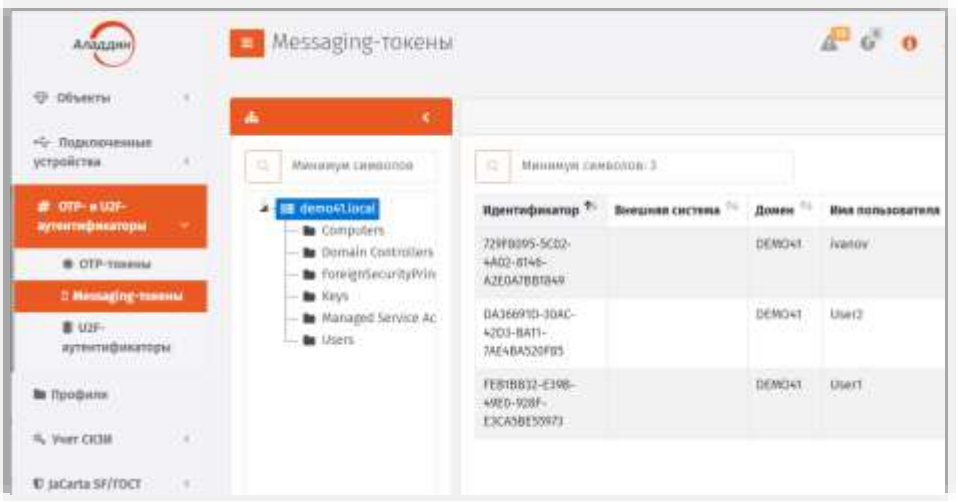


Рис. 115 – Раздел управления Messaging-токенами в консоли управления JMS

3.5.2.1 Выпуск messaging-токенов

Важно! Для корректного выпуска программных OTP-токенов должны быть выполнены следующие условия:

1. У пользователей, зарегистрированных в JMS, для которых выпускаются токены, в ресурсной системе (например FreeIPA) должен быть указан номер телефона, на который будут присылаться сообщения с OTP, подробнее см. описание параметра **Атрибут с номером телефона**, Табл. 47, с. 173.
2. С помощью консольного агента JAS должен быть настроен транспортный сервис для отправки SMS-сообщений пользователям (команда *AladdinJAS.Agent.Terminal config upload -n <json-файл с конфигурацией нотификации>*, подробнее см. руководство по установке и настройке сервера JAS [3], раздел «Приложение 2. Справочник команд консольного агента AladdinJAS.Agent.Terminal»).

Чтобы выпустить для группы пользователей JMS messaging-токены выполните следующие действия.

1. Создайте профиль выпуска messaging-токенов, руководствуясь разделом «Настройка профиля выпуска Messaging-токенов», с. 171, и выполните его привязку к соответствующему контейнеру ресурсной системы, руководствуясь разделом «Привязка профилей», с. 195.
2. Настройте для выпуска messaging-токенов и запустите на выполнение соответствующий план обслуживания, руководствуясь разделами «План обслуживания жизненного цикла OTP-токенов», с. 281 (проверьте факт включения задачи «Обслуживание Messaging-токенов») и «Запуск и просмотр результатов планов обслуживания», с.274.
3. Выпущенные и готовые к использованию (статус *Используется*) экземпляры messaging-токенов отобразятся в консоли управления (Рис. 115, выше).

3.5.2.2 Управление PIN-кодом для Messaging-токена

Установка и изменение PIN-кода для Messaging-токенов выполняется в консоли управления в разделе **OTP- и U2F-аутентификаторы -> Messaging-токены** так же, как и для OTP-токенов (см. раздел «Установка и изменение PIN-кода для OTP», с. 82).

3.5.2.3 Включение и отключение Messaging-токена

Операции включения и отключения возможности использования Messaging-токенов выполняются в консоли управления в разделе **OTP- и U2F-аутентификаторы -> Messaging-токены** так же, как и аналогичные операции для OTP-токенов (см. раздел «Включение и отключение OTP-токена», с. 83).

3.5.2.4 Просмотр свойств Messaging-токена

Чтобы просмотреть свойства Messaging-токена, выполните следующие действия.

1. В консоли управления JMS в разделе **OTP- и U2F-аутентификаторы -> Messaging-токены** выберите токен, сведения о котором вы хотите получить.
2. Нажмите на нём правой кнопкой мыши и выберите **Свойства**.

Отобразится следующее окно.

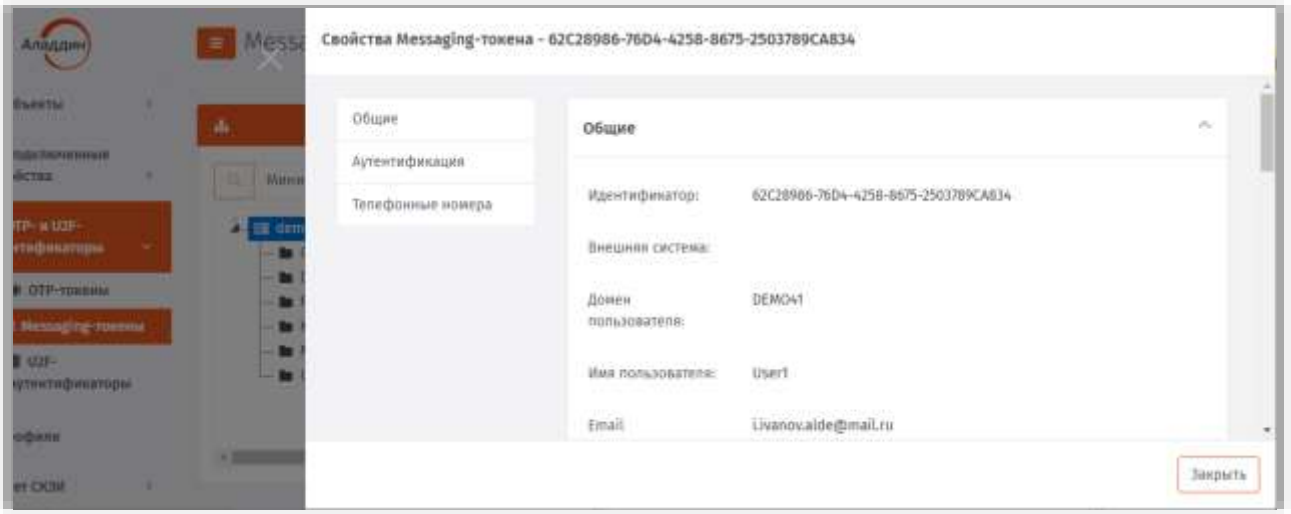


*Рис. 116 – Вкладка **Общие** свойств Messaging-токена*

3. Окно содержит параметры, описанные в Табл. 8.

Табл. 8 – Просмотр общих свойств Messaging-токена

Поле	Описание
Идентификатор	Отображает автоматически генерируемый идентификатор messaging-токена в JMS
Внешняя система	Отображает идентификатор внешней системы, для которой осуществляется аутентификация пользователя посредством Messaging-токена. Устанавливается в профиле выпуска Messaging-токенов, параметр **Внешняя система**, см. Табл. 47, с. 173.
Домен пользователя	Отображает домен, к которому принадлежит пользователь.
Имя пользователя	Отображает имя пользователя messaging-токена.
Email пользователя	Отображает адрес электронной почты пользователя.
FQDN	Отображает полное имя пользователя в FQDN-нотации.
UPN	Отображает полное имя пользователя в UPN-нотации.
Статус	Отображает текущий статус OTP-токена. Возможны следующие значения: • **Используется** • **Отключен**
Дата регистрации	Отображает дату и время выпуска messaging-токена.
Дата изменения	Отображает дату и время последних изменений в состоянии messaging-токена (например дату отключения или дату включения, см. раздел «Включение и отключение Messaging-токена», с. 89).

4. Перейдите на вкладку **Аутентификация**.

Окно примет следующий вид.

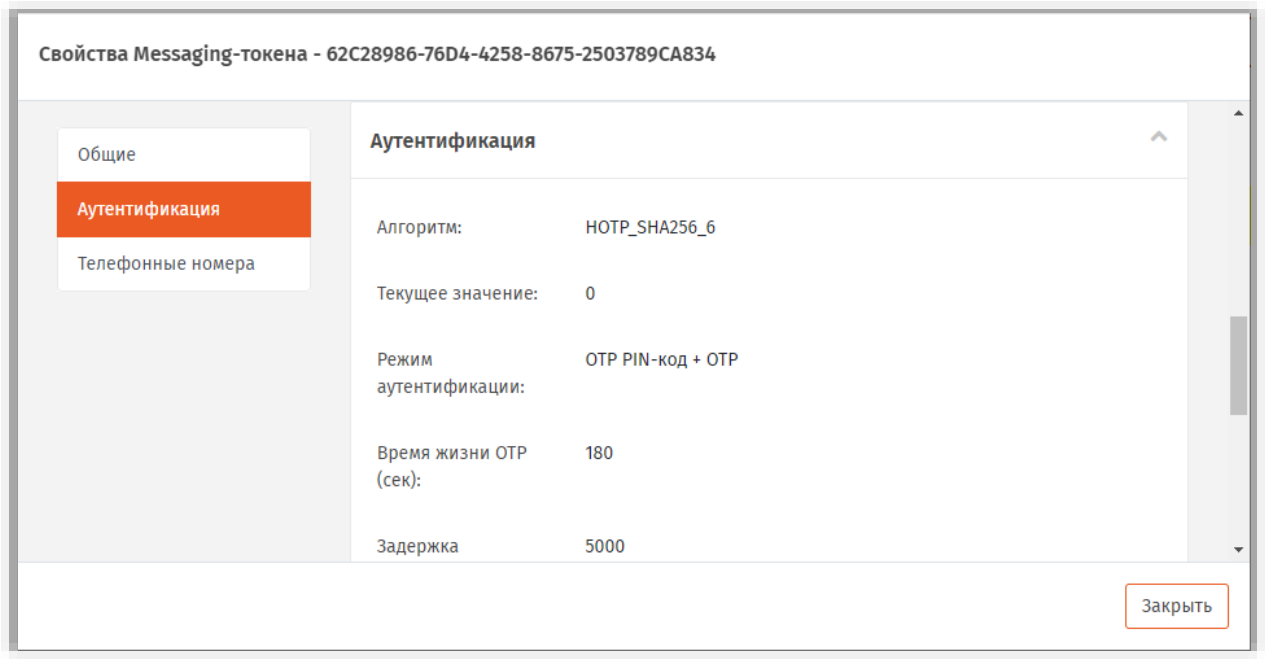


*Рис. 117 – Вкладка **Аутентификация** окна свойств Messaging-токена*

5. Окно содержит параметры токена, описанные в Табл. 9.

Табл. 9 – Параметры аутентификационной информации Messaging-токена

Настройка/поле	Описание
Алгоритм	Отображает алгоритм генерации одноразового пароля аутентификации (OTP). (Задается профилем выпуска messaging-токенов, см. Табл. 47, с. 173)
Текущее значение	Отображает значение счетчика, используемое алгоритмом формирования одноразовых паролей для вычисления следующего значения OTP
Настройки: • **Режим аутентификации** • **Время жизни OTP (с)** • **Задержка генерации OTP (мс)** • **Количество повторов аутентификации**	В полях отображаются значения настроек, выполненных в соответствии с профилем выпуска messaging-токенов, см. Табл. 47, с. 173

6. Перейдите на вкладку **Телефонные номера**.
На вкладке отображаются телефонные номера, абонента, к которому привязан данный токен в соответствии с параметром профиля выпуска Messaging-токенов **Атрибут с номером телефона** (см. Табл. 47, с. 173).
7. По окончании просмотра свойств токена нажмите **Закрыть.**

3.5.2.5 Удаление сведений о Messaging-токене

В случае прекращения необходимости аутентификации с использованием Messaging-токена сведения о нём следует удалить из базы данных JMS, чтобы исключить возможность использования злоумышленником этого аутентификатора. Удаление сведений о Messaging-токенах из JMS выполняется в консоли управления в разделе **OTP- и U2F-аутентификаторы -> Messaging-токены** так же, как и удаление сведений об OTP-токенах (см. раздел «Удаление сведений об OTP-токене», с. 88).

3.5.3 Операции с U2F-аутентификаторами

В JMS *U2F-аутентификатором* называется регистрационная информация (включает в себя дескриптор ресурсного закрытого ключа, ресурсный открытый ключ, аттестационный сертификат, счетчик аутентификаций), подлежащая хранению на U2F-сервере согласно спецификациям U2F альянса FIDO (см. веб-ресурс [**2**], с.).

Регистрация U2F-аутентификатора происходит автоматически при обработке соответствующего запроса от интегрируемой с сервером JAS внешней прикладной системы, к которой в свою очередь выполняет обращение пользователь из клиентского приложения, инициируя необходимое действие (регистрацию или аутентификацию) с помощью принадлежащего ему U2F-устройства.

Регистрация и аутентификация пользователя осуществляется в соответствии протоколом U2F, при этом сервер JAS выполняет роль U2F-сервера согласно спецификациям FIDO.

Консоль управления JMS позволяет выполнять операции с U2F-аутентификаторами в разделе **OTP- и U2F-аутентификаторы -> U2F-аутентификаторы** (Рис. 118).

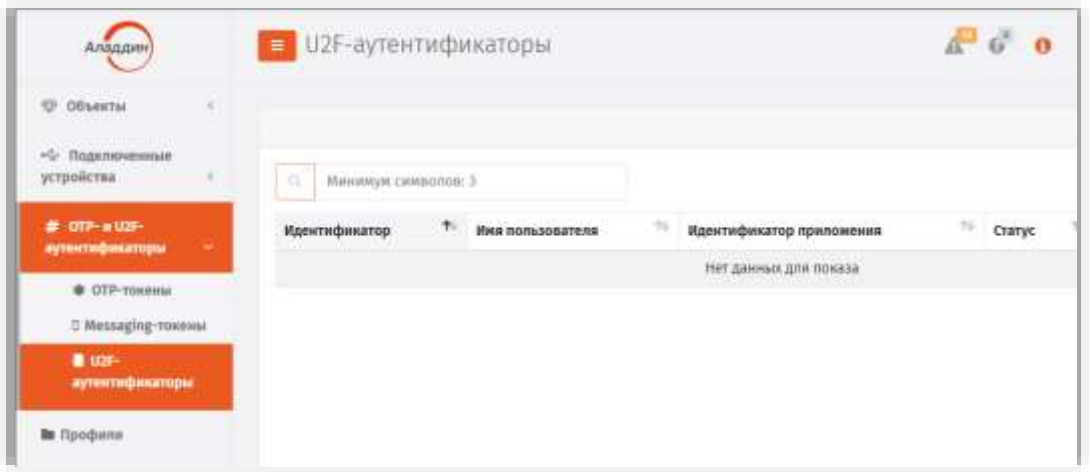


Рис. 118 – Раздел управления U2F-аутентификаторами в консоли управления JMS

3.5.3.1 Включение и отключение U2F-аутентификатора

Операции включения и отключения возможности использования U2F-аутентификаторов выполняются в консоли управления в разделе **OTP- и U2F-аутентификаторы -> U2F-**

аутентификаторы так же, как и аналогичные операции для OTP-токенов (см. раздел «Включение и отключение OTP-токена», с. 83).

3.5.3.2 Просмотр и редактирование свойств U2F-аутентификатора

Чтобы просмотреть или отредактировать свойства U2F-аутентификатора, выполните следующие действия.

1. В консоли управления JMS в разделе **OTP- и U2F-аутентификаторы -> U2F-аутентификаторы** выберите аутентификатор, свойства которого вы хотите просмотреть или отредактировать.
2. Нажмите на нём правой кнопкой мыши и выберите **Свойства**.
3. Отображаемые параметры описаны в Табл. 10.

Табл. 10 – Просмотр общих свойств U2F-аутентификатора

Поле	Описание
Идентификатор приложения	Имя приложения, от которого был получен запрос на регистрацию данного U2F-аутентификатора
Имя пользователя	Имя пользователя, которому принадлежит U2F-аутентификатор
Статус	Отображает текущий статус аутентификатора. Доступны следующие значения: • **Включен**; • **Отключен**
Дата создания	Отображает дату и время внесения сведений об аутентификаторе в базу данных JMS
Дата изменения	Отображает дату и время последних изменений в состоянии аутентификатора (например, дату включения или выключения возможности его использования).

4. Перейдите на вкладку **Аутентификация**.
5. Выполните настройки, руководствуясь Табл. 11.

Табл. 11 – Параметры аутентификационной информации U2F-аутентификатора

Настройка/поле	Описание
Значение счетчика	Значение счетчика аутентификаций, сохраняемое на стороне U2F-сервера согласно спецификациям протокола U2F. Неизменяемое поле.
Настройки по умолчанию	Если флажок установлен, для аутентификации пользователей будут применяться настройки U2 по умолчанию (секция *Секция U2fSettings* файла *BusinessLogic.json*), установленные с помощью консольного агента JAS (команда *Aladdin.JAS.Agent.Terminal config upload -b <json-файл с конфигурацией бизнес-логики>*, подробнее см. руководство по установке и настройке сервера JAS [3], раздел «Приложение 2. Справочник команд консольного агента AladdinJAS.Agent.Terminal»). Снятие этого флажка позволяет переопределить следующие настройки по умолчанию для выбранного U2F-аутентификатора: • Максимальное количество одновременных аутентификаций по токену; • Максимальное время аутентификации (мс)

Настройка/поле	Описание
Максимальное количество одновременных аутентификаций по токену	Максимальное количество одновременных аутентификаций по данному U2F-аутентификатору. **Примечание.** При создании аутентификатора параметр принимает значение по умолчанию, задаваемое параметре *MaxConcurrentAutentications* конфигурации бизнес-логики сервера JAS, установленной с помощью консольного агента JAS (команда *AladdinJAS.Agent.Terminal config upload -b <json-файл с конфигурацией бизнес-логики>*, подробнее см. руководство по установке и настройке сервера JAS [3], раздел «Приложение 2. Справочник команд консольного агента AladdinJAS.Agent.Terminal»)
Максимальное время аутентификации (мс)	Максимальное время (в миллисекундах), в течение которого начатая процедура аутентификации может быть завершена успешно. Если в течение данного времени начатая процедура аутентификации не завершилась, то она считается устаревшей и заканчивается с ошибкой (аутентификация не выполняется). Сообщение об ошибке записывается в *журнал аутентификации*. **Примечание.** При создании аутентификатора параметр принимает значение по умолчанию, задаваемое параметре *AutenticationTimeoutMsec* конфигурации бизнес-логики сервера JAS, установленной с помощью консольного агента JAS (команда *AladdinJAS.Agent.Terminal config upload -b <json-файл с конфигурацией бизнес-логики>*, подробнее см. руководство по установке и настройке сервера JAS [3], раздел «Приложение 2. Справочник команд консольного агента AladdinJAS.Agent.Terminal»)
Сертификат	Нажмите **Посмотреть**, для того чтобы отобразить окно с параметрами аттестационного сертификата U2F-устройства
• **Кем выдан** • **Кому выдан** • **Срок действия с** • **Срок действия по** • **Серийный номер**	Параметры аттестационного сертификата U2F-устройства. Неизменяемые поля.

б. Нажмите **ОК**, чтобы сохранить изменения.

3.5.3.3 Удаление сведений о U2F-аутентификаторе

В случае прекращения необходимости аутентификации с использованием U2F-аутентификатора сведения о нём следует удалить из базы данных JMS, чтобы исключить возможность его использования злоумышленником. Удаление сведений о U2F-аутентификаторах из JMS выполняется в консоли управления в разделе **OTP- и U2F-аутентификаторы -> U2F-аутентификаторы** так же, как и удаление сведений об OTP-токенах (см. раздел «Удаление сведений об OTP-токене», с. 88).

3.6 Настройка профилей JMS

Профили JMS классифицируются в соответствии с группами, перечисленными в табл. 12.

Табл. 12 – Профили JMS

Группа профилей JMS	Типы профилей в группе
Профили выпуска электронных ключей	**Выпуск ключевых носителей** - позволяет настроить общие параметры выпуска электронных ключей (а также задать необходимость инициализации электронных ключей при выпуске). Настройки профиля данного типа (на примере встроенного профиля по умолчанию) приведены в пункте «Настройка профиля выпуска электронных ключей», с. 97.
Профили настроек клиентского агента	**Настройки клиентского агента** – позволяет настроить параметры работы клиентского агента JMS, как то: возможность самостоятельного выпуска электронных ключей, параметры синхронизации электронных ключей, а также позволяет ограничить действия на стороне клиента. Настройка профиля данного типа приведена в пункте «Настройка профиля клиентского агента», с. 101.
Профили инициализации электронных ключей	• **Инициализация eToken Pro (Java) / JaCarta PKI (с обратной совместимостью)** – позволяет настроить параметры инициализации электронных ключей eToken PRO (Java), eToken NG-Flash (Java), eToken NG-OTP (Java) (без поддержки OTP), JaCarta PKI (с функцией обратной совместимости с продуктами компании Aladdin) - см. « eToken Pro (Java) / JaCarta PRO », с. 105; • **Инициализация JaCarta PKI** - позволяет настроить параметры инициализации электронных ключей JaCarta PKI, JaCarta PKI/Flash, JaCarta PKI/BIO (без использования биометрической аутентификации пользователя) – см. «JaCarta PKI», с. 111; Необходимость инициализации электронного ключа задается профилем типа **Выпуск ключевых носителей**. Если необходимость инициализации не задана, то профиль группы инициализации настраивать необязательно.
Профили коннекторов	• **Выпуска сертификатов –УЦ Microsoft CA** – позволяет настроить параметры выпуска сертификатов в центре сертификации Microsoft (см. «Настройки профиля выпуска сертификатов в центре сертификации Microsoft», с. 124); • **Выпуска сертификатов –УЦ DogTag** – позволяет настроить параметры выпуска сертификатов в удостоверяющем центре DogTag (см. «Настройки профиля выпуска сертификатов в УЦ DogTag», с. 138);
Профили внешних объектов	**Внешние объекты** – позволяет настроить процедуру взятия под управление внешних объектов (сертификатов), выпущенных без использования эксплуатируемого экземпляра системы JMS,например, выпущенных до развертывания JMS или с помощью сторонних УЦ. Подробнее см. в разделе «Взятие под управление JMS электронных ключей », с. 305

Для успешного выпуска электронных ключей после создания и настройки профилей необходимо выполнить привязку этих профилей к пользователям JMS (см. «Привязка профилей», с. 195).

3.6.1 Общие операции с профилями

Общее управление профилям осуществляется в разделе **Профили** Консоли управления JMS (Рис. 119).

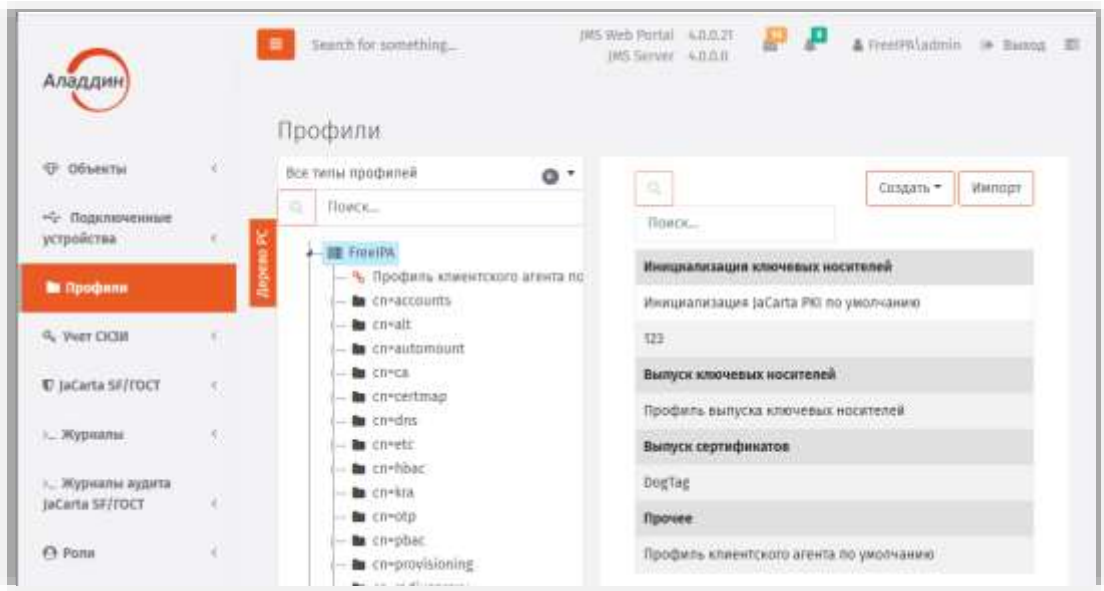
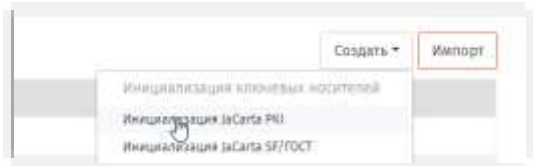
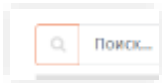


*Рис. 119 – Общий вид раздела **Профили** Консоли управления JMS*

Общая информации по управлению профилями содержится в Табл. 13.

Табл. 13 – Общие операции с профилями

Операция	Описание
Создать	Для создания профиля нажмите кнопку Создать  и выберите строку с названием раздела (например **Инициализация JaCarta PKI**). Подробно процедура создания профиля описано в разделах, посвященным соответствующим типам профилей
Копировать	Для копирования профиля выберите его в таблице профилей и по нажатию правой кнопкой мыши выберите **Копировать**.
Удалить	Для удаления профиля выберите его в таблице профилей и на верхней панели нажмите **Удалить**. **Важно!** Удаление *профиля выпуска сертификата* является событием, по которому обрабатываются **параметры отзыва** сертификата для всех выпущенных ранее по этому профилю электронных ключей. Подробнее смотри разделы: • «Настройки профиля выпуска сертификатов в УЦ DogTag», с. 138); • «Настройки профиля выпуска сертификатов в центре сертификации Microsoft», с. 124. Удаленные *профили выпуска сертификата* сохраняются в системе
Свойства	Операция служит для просмотра или редактирования свойств профилей.

Операция	Описание
Экспорт	См. раздел «Экспорт/импорт профилей», с. 201
Импорт	См. раздел «Экспорт/импорт профилей», с. 201
 (поиск профиля)	Для нахождения профиля в строке поиска введите фрагмент его имени и нажмите на клавиатуре клавишу **Ввод**. Профили будут отфильтрованы по введенному фрагменту имени.

3.6.2 Настройка профиля выпуска электронных ключей

7. В консоли управления JMS перейдите в раздел **Профили**.
8. Выполните одно из следующих действий:

   – чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Выпуск ключевых носителей**.
   – чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

   Отобразится следующее окно.

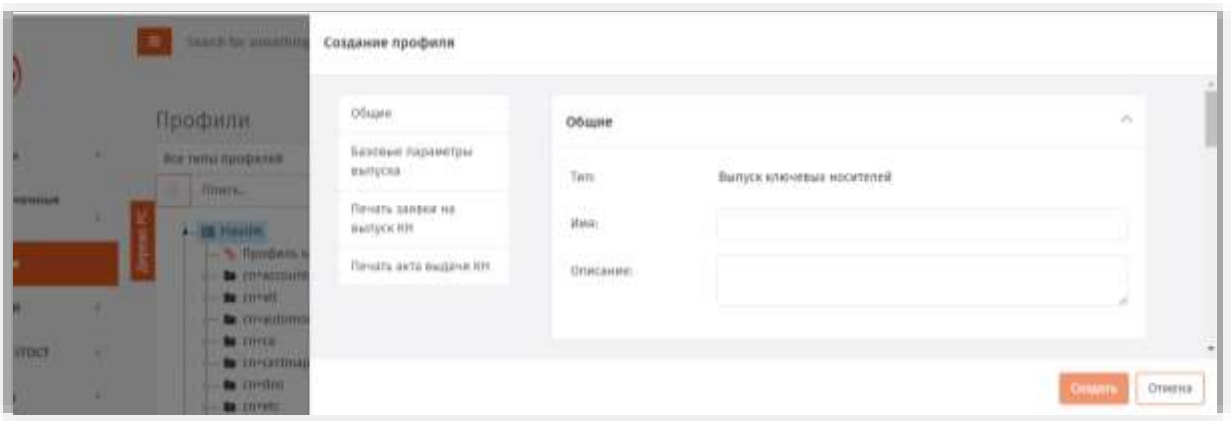


*Рис. 120 – Вкладка **Общие***

9. В соответствующих полях введите (или отредактируйте) имя и описание профиля, после чего переходите на вкладку **Параметры (**Рис. 121**)**.

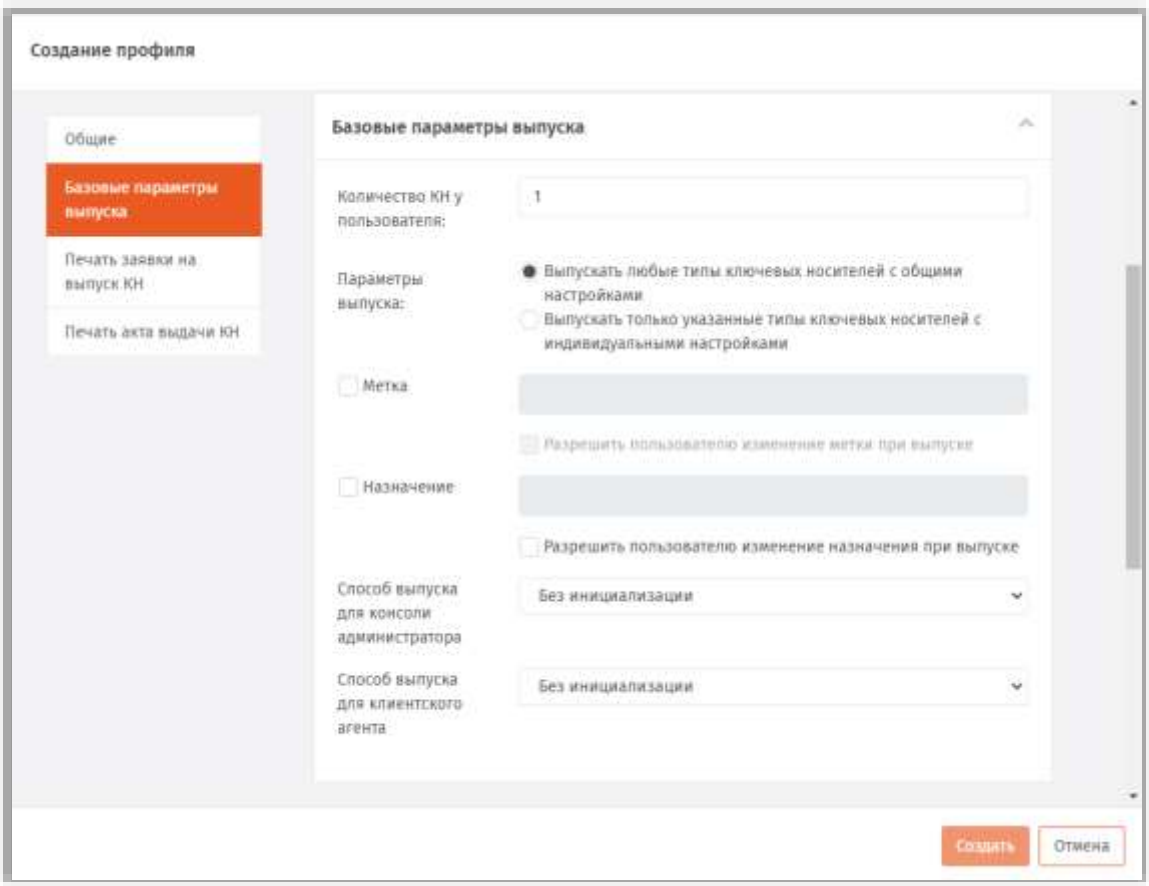


*Рис. 121 – Вкладка **Базовые параметры выпуска***

10. Выполните настройку, руководствуясь Табл. 14.

Табл. 14 – Параметры выпуска электронных ключей

Настройка	Описание
Количество КН у пользователя	В поле следует указать максимальное количество электронных ключей, которое можно выпустить для одного пользователя
Выпускать любые типы ключевых носителей с общими настройками	Данная опция устанавливает, что для всех выпускаемых типов электронных ключей будет применяться один общий профиль выпуска. Чтобы выполнить настройку, щелкните на ссылке **Настроить** напротив пункта.
Выпускать только указанные типы ключевых носителей с индивидуальными настройками	Данная опция позволяет задать индивидуальные настройки для кажого типа выпускаемого электронного ключа. При выборе опции добавляется кнопка **Выбрать комбинации апплетов**. Нажмите её, отметьте нужные апплеты (перечислены ниже), нажмите кнопку **Выбрать** и выполните настройку каждого апплета. Перечень доступных приложений (апплетов): • **PKI** - электронные ключи JaCarta с приложением PKI; • **PKI + ГОСТ** - электронные ключи JaCarta с приложениями PKI и ГОСТ;

Настройка	Описание
	• **PRO (Java) / PKI (с обратной совместимостью)** - электронные ключи eToken PRO (Java), eToken NG-Flash (Java), eToken NG-OTP (Java) (без поддержки OTP), а также электронные ключи JaCarta с приложением PKI (с обратной совместимостью); • **PRO (Java) / PKI (с обратной совместимостью) + PKI** - электронные ключи eToken PRO (Java), а также электронные ключи JaCarta с приложениями PKI (с обратной совместимостью) и PKI;  В некоторых случаях электронные ключи eToken ГОСТ также имеют функциональность электронных ключей eToken PRO (Java) - о наличии такой функциональности уточняйте в технической поддержке «Аладдин Р. Д.» • **ГОСТ 2**– электронные ключи JaCarta ГОСТ 2, а также электронные ключи JaCarta с приложением ГОСТ 2; • **ГОСТ 2 + SF** – электронные ключи JaCarta SF/ГОСТ
Метка	Позволяет задать метку выпускаемого электронного ключа. В случае установки флага (**Метка**) вы можете ввести значение метки вручную или воспользоваться кнопкой справочником (раскрывающимся списком). В последнем случае, вы можете выбрать шаблон, по которому будет формироваться метка: • **$AccountName** – имя учетной записи пользователя, для которого выпускается электронный ключ; • **$FullName** – полное имя учетной записи пользователя, для которого выпускается электронный ключ; • **$Description** – описание пользователя, для которого выпускается электронный ключ; • **$Department** – подразделение пользователя, для которого выпускается электронный ключ; • **$Mail** – адрес электронной почты пользователя, для которого выпускается электронный ключ. В случае если флаг **Метка** не установлен, то при выпуске электронного ключа без инициализации то значение метки приложения в нем будет оставлено без изменений; если выпуск осуществляется с инициализацией, то будет установлено значение метки по умолчанию.
Разрешить пользователю изменение метки при выпуске	Позволяет разрешить или запретить изменение метки электронного ключа в процессе самостоятельного выпуска пользователем.  Возможность самостоятельного выпуска должна быть включена в профиле клиентского агента (подробнее см. «Настройка профиля клиентского агента», с. 101).
Назначение	Позволяет задать назначение выпускаемого электронного ключа В случае установки флага (**Назначение**) вы можете ввести текстовое описание назначения (например, «Доступ к учетной записи»). В случае если флаг **Назначение** не установлен, то при выпуске электронного ключа в качестве «назначения» будет установлено название приложения, локализованное в соответствии с языковыми настройками интерфейса компонента JMS Server
Разрешить пользователю изменение назначения при выпуске	Позволяет разрешить или запретить менять описание назначения электронного ключа в процессе самостоятельного выпуска пользователем.

Настройка	Описание
Способ выпуска для консоли администратора	Позволяет выбрать, будет ли произведена инициализация в процессе выпуска электронного ключа с использованием консоли управления JMS. Если вы планируете взять под контроль JMS электронные ключи, выпущенные до установки и настройки JMS (см. «Взятие под управление JMS электронных ключей », с. 305), вам следует выбрать пункт **Без инициализации**. В противном случае все существующие объекты в памяти электронного ключа будут удалены.
Способ выпуска для клиентского агента	Позволяет выбрать, будет ли произведена инициализация в процессе самостоятельного выпуска электронного ключа пользователем. **Примечания:** 1. Возможность самостоятельного выпуска должна быть включена в профиле клиентского агента (подробнее см. «Настройка профиля клиентского агента», с. 101). 2. Если вы планируете взять под контроль JMS электронные ключи, выпущенные до установки и настройки JMS (см. ««Взятие под управление JMS электронных ключей », с. 305), вам следует выбрать пункт **Без инициализации**. В противном случае все существующие объекты в памяти электронного ключа будут удалены.

Примечание. Если электронный ключ содержит несколько апплетов (приложений), то в соответствующей секции типа электронного ключа будет несколько вкладок (Рис. 122). Каждая вкладка соответствует апплету (приложению) в памяти электронного ключа. В этом случае необходимо выполнить настройку для каждого из этих апплетов (приложений).

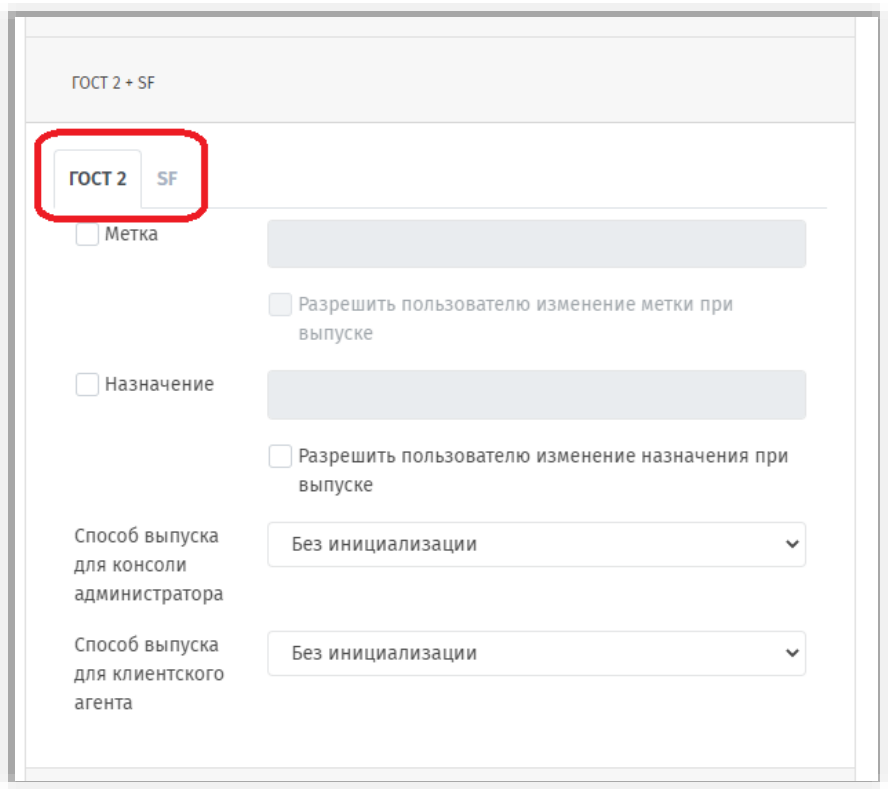


Рис. 122 – Окно настройки параметров выпуска электронных ключей с несколькими приложениями

11. При необходимости, выполните настройку печати документов (вкладки **Печать заявки на выпуск КН** и **Печать акта выдачи КН**) при выпуске электронного ключа (подробнее о

настройке шаблона печатной формы см. «Настройка параметров печати при выпуске объектов JMS», с. 201).

12. По окончании всех настроек нажмите кнопку **Создать** (Рис. 121, с. 98) или **Сохранить** (при редактировании профиля), чтобы сохранить изменения.

3.6.3 Настройка профиля клиентского агента

Профиль клиентского агента определяет, какие операции с электронными ключами, назначенными пользователю или подключенными к компьютеру, доступны пользователю при открытии сеанса работы с JMS из клиента (функция **Открыть сессию** в клиенте JMS).

Важно! В случае если профиль клиентского агента не привязан к учетной записи пользователя (см. «Привязка профилей», с. 195), в клиенте JMS при открытии сеанса пользователя:

- будет недоступно действие **Выпуск** для подключенных электронных ключей, которые еще не выпущены;
- будут недоступны действия **Заменить** и **Отключить** для всех электронных ключей, назначенных пользователю. (В текущей версии клиента JMS в процессе выполнения замены или отключения электронного ключа выдается окно предупреждения с соответствующим сообщением об ошибке).

Для создания/настройки профиля клиентского агента выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Профили**.
2. Выполните одно из следующих действий:

   – чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Настройки клиентского агента**.
   – чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

3. В полях **Имя** и **Описание** введите название и описание профиля соответственно (либо отредактируйте существующие), после чего перейдите на вкладку **Самостоятельный выпуск**.
4. Выполните настройку, руководствуясь табл. 15.

Табл. 15 – Настройка параметров самостоятельного выпуска

Секция	Настройка	Описание
Настройки самостоятельного выпуска ключевых носителей	**Для незарегистрированных КН**	Настройка самостоятельного выпуска пользователями электронных ключей, не зарегистрированных в JMS. Доступны следующие варианты: • **Запрещен** – пользователи не могут самостоятельно выпускать электронные ключи, не зарегистрированные в JMS; • **Разрешен вручную** – пользователи на свое имя могут вручную выпускать электронные ключи, не зарегистрированные в JMS (см. документ «Руководство пользователя», [1]); • **Разрешен автоматически** – выпуск незарегистрированного электронного ключа на имя пользователя, вошедшего в систему, произойдет автоматически после подсоединения этого электронного ключа к компьютеру.
	Для зарегистрированных КН	Настройка самостоятельного выпуска пользователями электронных ключей, зарегистрированных в JMS, но не назначенных конкретным пользователям. Доступны следующие варианты: • **Запрещен** – пользователи не могут самостоятельно выпускать электронные ключи, зарегистрированные в JMS;

Секция	Настройка	Описание
		• **Разрешен вручную** – пользователи могут вручную выпускать электронные ключи, на свое имя, если эти электронные ключи зарегистрированы в JMS (см. документ «Руководство пользователя», [1]); • **Разрешен автоматически** – выпуск зарегистрированного электронного ключа на имя пользователя, вошедшего в систему, произойдет автоматически после подсоединения электронного ключа к компьютеру.
	Для назначенных КН	Настройка самостоятельного выпуска пользователями электронных ключей, зарегистрированных в JMS и назначенных конкретным пользователям. Доступны следующие варианты: • **Запрещен** – пользователи не могут самостоятельно выпускать назначенные им электронные ключи; • **Разрешен вручную** – пользователи могут вручную выпустить назначенные им электронные ключи (см. документ «Руководство пользователя», [1]); • **Разрешен автоматически** – выпуск назначенного пользователю электронного ключа произойдет автоматически после подсоединения этого электронного ключа к компьютеру.
Настройки самостоятельного выпуска КН – СКЗИ Секция доступна только при подключении лицензии на право использования СКЗИ (см. «Учет СКЗИ», с. 208)	**Разрешить выпуск КН, являющихся СКЗИ**	Включение настройки позволит пользователям самостоятельно выпускать электронные ключи, являющиеся СКЗИ, с помощью клиентского агента JMS.
Настройки выпуска с восстановлением данных	**Разрешить самостоятельный выпуск с восстановлением данных из резервной копии**	Используя клиент JMS, пользователи смогут выпускать электронные ключи в режиме восстановления данных.

Примечание. При изменении настроек профиля клиентского агента, в частности в опциях, разрешающих/запрещающих самостоятельный выпуск электронных ключей, для вступления в силу данных настроек на стороне клиента (а также в приложении JWA Tray на клиентской стороне) в течение его текущего сеанса работы, следует последовательно закрыть, а затем снова открыть сеанс пользователя.

5. Перейдите на вкладку **Синхронизация**.
6. Выполните необходимые настройки, руководствуясь табл. 16.

Табл. 16 – Настройки автоматической синхронизации

Секция	Настройка	Описание
Запускать проверку синхронизации при возникновении событий	**Старт клиентского агента**	Синхронизация запускается при запуске клиентского агента JMS. **Примечание.** В текущей версии JMS настройка не действует: синхронизация электронных ключей во время

Секция	Настройка	Описание
		старта клиентского агента при установке флага не производится.
	Подключение ключевого носителя	Синхронизация запускается при подсоединении к компьютеру электронного ключа.
	По расписанию	Синхронизация проводится по графику, описанному в секции **Настройки расписания синхронизации**.
	Разблокировка пользовательской сессии	Синхронизация производится по факту разблокировки пользовательского сеанса Windows.
Дополнительные настройки синхронизации клиентского агента	**Разрешать синхронизацию для отключенного носителя**	Позволяет применять синхронизацию к электронным ключам, действие которых было приостановлено.
	Разрешать синхронизацию для отозванного носителя	Позволяет применять синхронизацию к электронным ключам, которые были отозваны.
Настройки расписания синхронизации	**Обычная синхронизация каждые (минут)**	Временной интервал, по истечении которого клиент JMS проверяет необходимость синхронизации – при условии, что предыдущая синхронизация прошла успешно. Настройка активна только в том случае, если в секции **Запускать проверку синхронизации при возникновении событий** включена настройка **По расписанию**.
	Ускоренная синхронизация каждые (минут)	Временной интервал, по истечении которого клиент JMS проверяет необходимость синхронизации – при условии, что предыдущая синхронизация завершилась с ошибками (например, с электронного ключа не были удалены данные, которые необходимо было удалить). Настройка активна только в том случае, если в секции **Запускать проверку синхронизации при возникновении событий** включена настройка **По расписанию**.
	Количество повторов неудачной синхронизации (раз)	Количество повторов синхронизации по ускоренному таймауту, после которых попытки синхронизации возвращается в режим обычного таймаута. Настройка активна только в том случае, если в секции **Запускать проверку синхронизации при возникновении событий** включена настройка **По расписанию**.
Ограничения синхронизации	**Разрешать выпуск объектов при синхронизации**	Позволяет выпускать записывать объекты в память электронного ключа во время синхронизации.

Секция	Настройка	Описание
	Разрешать обновление объектов при синхронизации	Позволяет обновлять объекты в памяти электронных ключей во время синхронизации.
	Разрешать удаление объектов при синхронизации	Позволяет удалять объекты из памяти электронных ключей во время синхронизации.

7. Перейдите на вкладку **Ограничения по работе с КН**.
8. Выполните настройку, руководствуясь табл. 17.

Табл. 17 – Ограничения по работе с электронными ключами

Секция	Настройка	Описание
Работа с ключевыми носителями	**Разрешать замену**	Если настройка включена, пользователи смогут самостоятельно производить процедуру замены электронного ключа. В противном случае в клиенте JMS опция **Замена** в виде ссылки не будет отражаться в доступных действиях по отношению к электронным ключам.
	Разрешать отключение	Если настройка включена, пользователи смогут самостоятельно отключать возможность использования своего электронного ключа. В противном случае в клиенте JMS опция **Отключить** в виде ссылки не будет отражаться в доступных действиях по отношению к электронным ключам.
	Разрешать сообщение об утере\поломке	Если настройка включена, пользователи смогут отзывать свои электронные ключи по причине утери или поломки электронного ключа. В противном случае в клиенте JMS опция **Сообщить об утере/поломке** в виде ссылки не будет отражаться в доступных действиях по отношению к электронным ключам.
	Разрешать разблокировку	Если настройка включена, пользователи смогут инициировать процедуру разблокировки электронного ключа.

Секция	Настройка	Описание
		В противном случае в клиенте JMS опция **Разблокировать <*Название приложения*>** в виде ссылки не будет отражаться в доступных действиях по отношению к электронным ключам.
Настройки автоматической разблокировки	**Разрешать автоматическую разблокировку**	Если настройка включена, после запуска соответствующей процедуры пользователь сможет разблокировать заблокированный электронный ключ без участия администратора. Настройка активна, только если включена настройка **Разрешать разблокировку**.
Подключение скрытых дисков	**Разрешить подключение скрытых дисков**	Настройка доступна только для электронных ключей JaCarta SF/ГОСТ. Включите настройку, если в клиентском приложении JMS необходимо разрешить монтирование скрытых дисков RW и CD-ROM.

9. Перейдите на вкладку **Смена PIN-кода**.
10. При необходимости отредактируйте следующие настройки:

10.1. **Время, отводимое пользователю для смены PIN-кода с момента установки опции** – позволяет задать время, которое будет предоставлено пользователю на смену PIN-кода с момента включения соответствующей настройки;
10.2. **Периодичность напоминания о необходимости смены PIN-кода до истечения срока** – позволяет задать интервал в минутах, через который пользователю будет отображаться предупреждение о необходимости смены PIN-кода электронного ключа до истечения срока действия этого PIN-кода;
10.3. **Периодичность напоминания о необходимости смены PIN-кода после истечения срока** – позволяет задать интервал в минутах, через который пользователю будет отображаться предупреждение о необходимости смены PIN-кода электронного ключа после истечения срока действия этого PIN-кода.

11. Нажмите **OK**, чтобы сохранить изменения.

3.6.4 Настройки параметров инициализации

3.6.4.1 eToken Pro (Java) / JaCarta PRO

Примечание. Тип профиля **Инициализация eToken Pro (Java) / JaCarta PRO** по умолчанию не отображается в консоли управления JMS. Для того, чтобы профиль начал отображаться следует включить в JMS поддержку ЭК eToken Pro (Java) / JaCarta PRO (приложение/апплет ProJava). Подробно процедура включения поддержки приложений ЭК (апплетов) описана в руководстве по настройке и установке [2], раздел «Добавление поддержки моделей ЭК / профилей в JMS».

1. В консоли управления JMS перейдите в раздел **Профили**.
2. Выполните одно из следующих действий:

– чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Инициализация eToken Pro (Java) / JaCarta PRO**.

– чтобы изменить существующий профиль, выберите этот профиль (например, **Инициализация eToken Pro (Java) / JaCarta PRO по умолчанию**) в центральной части окна консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

Отобразится страница следующего вида

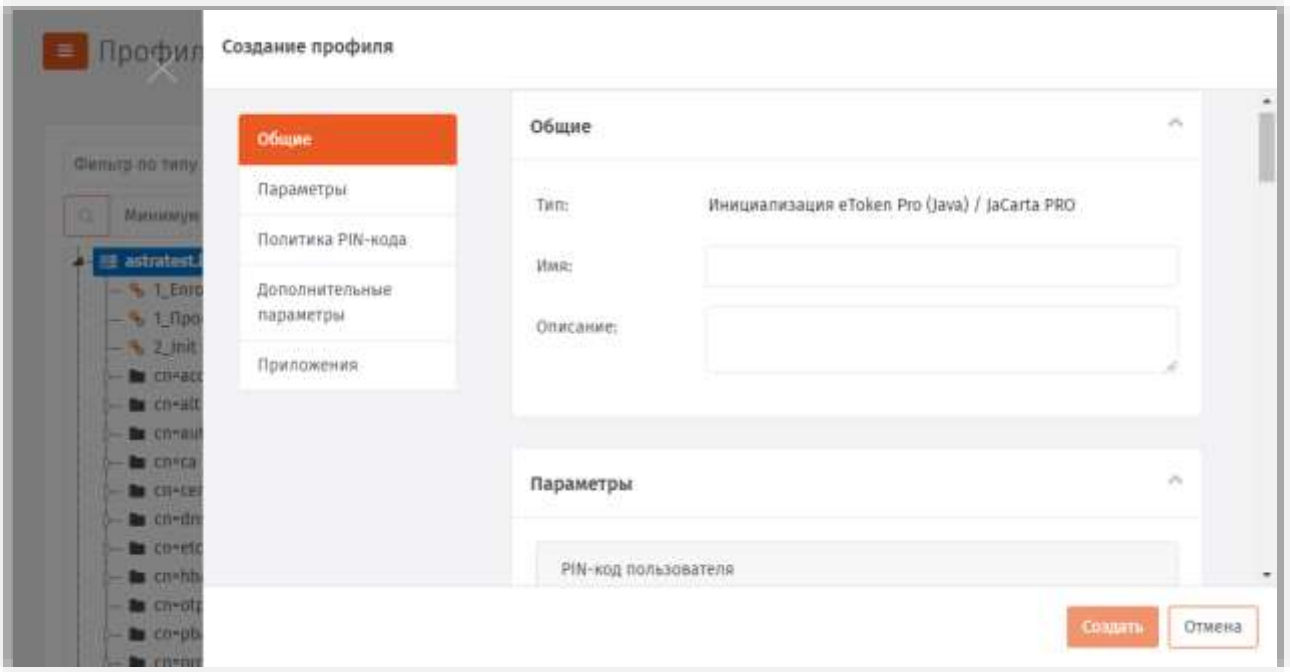


*Рис. 123 – Вкладка **Общие** свойств профиля инициализации*

3. В полях **Имя** и **Описание** введите (или отредактируйте) название и описание профиля соответственно, после чего перейдите на вкладку **Параметры**.
Отобразится страница следующего вида.

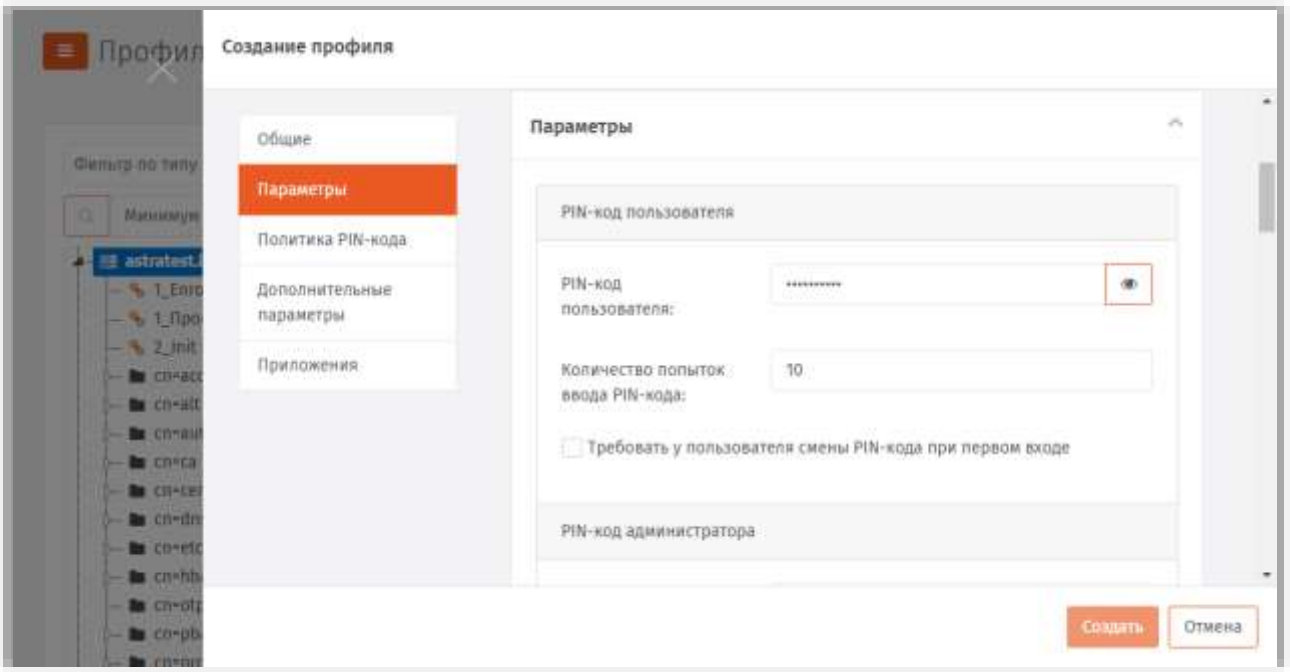


*Рис. 124 – Вкладка **Параметры** свойств профиля инициализации*

4. Выполните необходимые настройки, руководствуясь табл. 18.

Табл. 18 - Настройка параметров инициализации электронных ключей

Секция	Настройка	Описание
PIN-код пользователя	**PIN-код пользователя**	Позволяет задать PIN-код пользователя электронного ключа по умолчанию.
	Количество попыток ввода PIN-кода	Позволяет задать максимальное число последовательных неверных вводов PIN-кода пользователя электронного ключа, по достижении которого доступ по PIN-коду пользователя блокируется.
	Требовать у пользователя смены PIN-кода при первом входе	Если флаг установлен, пользователь должен будет сменить PIN-код пользователя электронного ключа при первом использовании.
PIN-код администратора	**Способ установки PIN-кода**	Позволяет задать способ формирования первоначального значения PIN-кода администратора электронного ключа. Список содержит следующие пункты: • **Использовать фиксированный** – позволяет задать PIN-код администратора электронного ключа по умолчанию (значение задается в поле **PIN-код администратора**); • **Генерировать случайный** – позволяет сгенерировать случайный PIN-код администратора электронного ключа при выпуске (в этом случае можно задать длину случайного PIN-кода с помощью настройки **Длина случайного PIN-кода**);
	PIN-код администратора	Позволяет задать PIN-код администратора электронного ключа. (Поле активно, только если в списке **Способ установки PIN-кода** выбран пункт **Использовать фиксированный**).
	Длина случайного PIN-кода	Позволяет задать длину случайного PIN-кода администратора электронного ключа. (Настройка активна, только если в списке **Способ установки PIN-кода** выбран пункт **Генерировать случайный**).
	Количество попыток ввода PIN-кода	Позволяет задать максимальное число последовательных неверных попыток ввода PIN-код администратора электронного ключа, по достижении которого доступ на уровне администратора к электронному ключу будет заблокирован.

5. Перейдите на вкладку **Политика PIN-кода**.

Отобразится страница следующего вида.

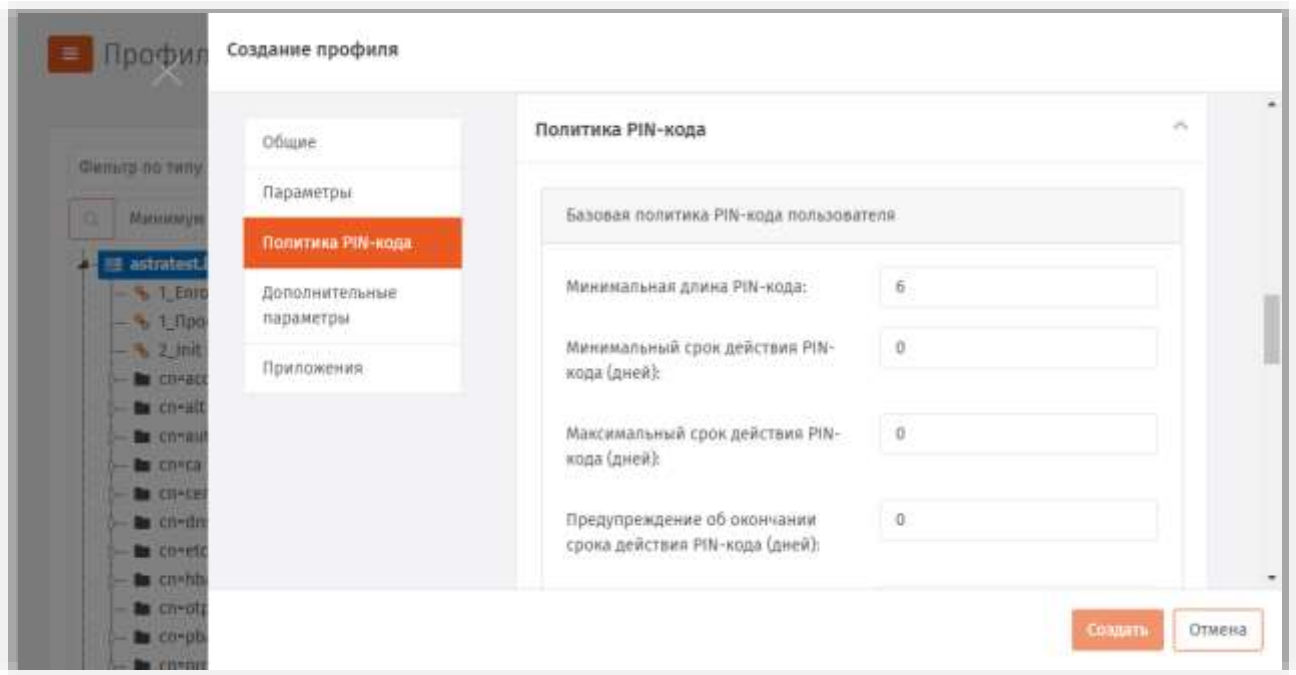


*Рис. 125 – Вкладка **Политика PIN-кода** свойств профиля инициализации*

Б. Выполните необходимые настройки, руководствуясь табл. 19.

Табл. 19 – Настройка параметров PIN-кода пользователя электронного ключа

Секция	Настройка	Описание
Базовая политика PIN-кода пользователя	**Минимальная длина PIN-кода**	Минимальная длина PIN-кода пользователя электронного ключа.
	Минимальный срок действия PIN-кода	Минимальный срок действия PIN-кода пользователя электронного ключа (в днях).
	Максимальный срок действия PIN-кода	Максимальный срок действия PIN-кода пользователя электронного ключа (в днях). По достижении этого срока пользователь должен будет сменить PIN-код пользователя электронного ключа.
	Предупреждение об окончании срока действия PIN-кода	Число дней до истечения срока действия PIN-кода пользователя электронного ключа, за которое пользователю будет отображаться предупреждение о необходимости смены PIN-кода пользователя.
	Помнить X последних PIN-кодов пользователя	Число ранее использованных PIN-кодов пользователя электронного ключа, которые нельзя использовать в качестве нового PIN-кода пользователя электронного ключа.

Секция	Настройка	Описание
Расширенная политика PIN-кода пользователя	**Включить расширенную проверку качества PIN-кода**	Позволяет установить дополнительные параметры безопасности PIN-кода пользователя электронного ключа.
	Числовые символы	Настройка активна, только если отмечен пункт **Включить расширенную проверку качества PIN-кода**. Позволяет настроить параметры использования цифр в PIN-коде. Список содержит следующие пункты: • **Не проверять** – наличие или отсутствие цифр в PIN-коде не влияет на успешность его создания; • **Запрещены** – нельзя использовать в PIN-коде цифры; • **Обязательны** – цифры в PIN-коде обязательны.
	Символы в верхнем регистре	Настройка активна, только если отмечен пункт **Включить расширенную проверку качества PIN-кода**. Позволяет настроить параметры использования букв верхнего регистра в PIN-коде. Список содержит следующие пункты: • **Не проверять** – наличие или отсутствие букв верхнего регистра в PIN-коде не влияет на успешность его создания; • **Запрещены** – нельзя использовать в PIN-коде буквы верхнего регистра; • **Обязательны** – буквы верхнего регистра в PIN-коде обязательны.
	Символы в нижнем регистре	Настройка активна, только если отмечен пункт **Включить расширенную проверку качества PIN-кода**. Позволяет настроить параметры использования букв нижнего регистра в PIN-коде. Список содержит следующие пункты: • **Не проверять** – наличие или отсутствие букв нижнего регистра в PIN-коде не влияет на успешность его создания; • **Запрещены** – нельзя использовать в PIN-коде буквы нижнего регистра; • **Обязательны** – буквы нижнего регистра в PIN-коде обязательны.
	Специальные символы	Настройка активна, только если отмечен пункт **Включить расширенную проверку качества PIN-кода**. Позволяет настроить параметры использования специальных символов (символов, не входящих в алфавитно-цифровой набор) в PIN-коде. Список содержит следующие пункты:

Секция	Настройка	Описание
		• **Не проверять** – наличие или отсутствие специальных символов в PIN-коде не влияет на успешность его создания; • **Запрещены** – нельзя использовать в PIN-коде специальные символы; • **Обязательны** – специальные символы в PIN-коде обязательны.
	Максимальное количество повторений символов	Настройка активна, только если отмечен пункт **Включить расширенную проверку качества PIN-кода**. Позволяет задать максимальное число идущих подряд одинаковых символов в PIN-коде.

7. Перейдите на вкладку **Дополнительные параметры**.
Отобразится страница следующего вида.

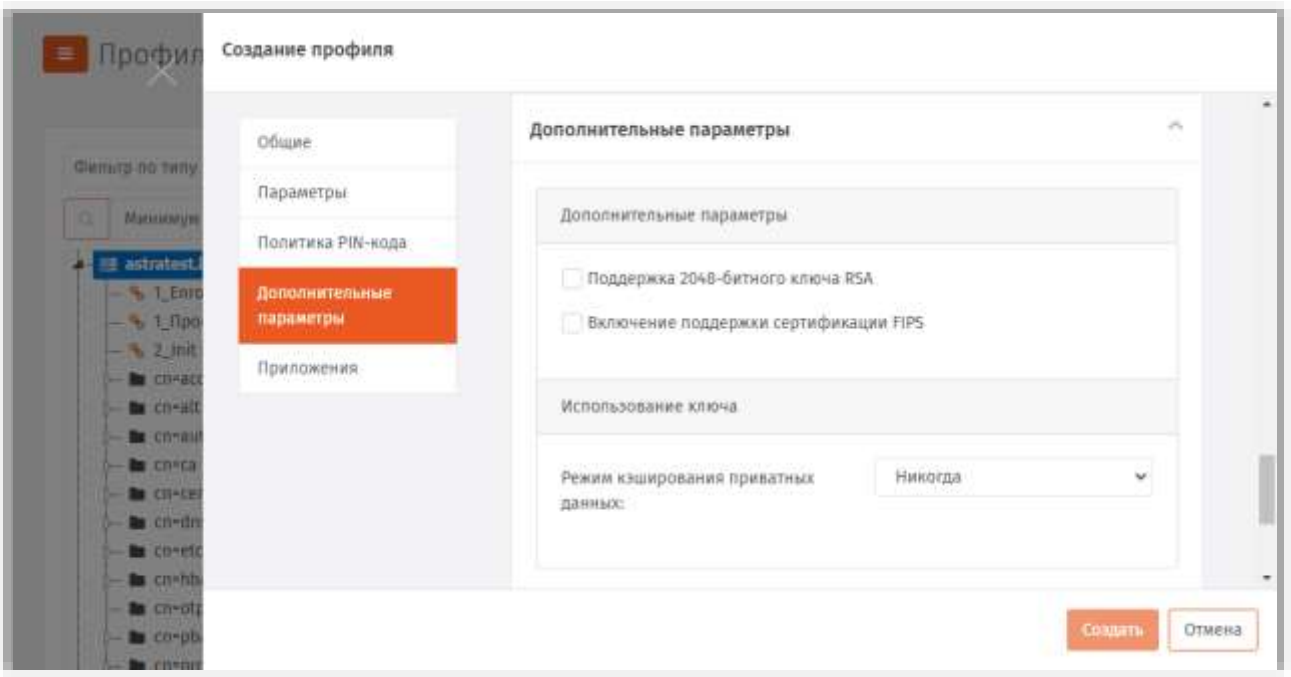


*Рис. 126 – Вкладка **Дополнительные параметры** свойств профиля инициализации*

8. Выполните необходимые настройки, руководствуясь табл. 20.

Табл. 20 – Настройка дополнительных параметров инициализации электронных ключей

Настройка	Описание
Поддержка 2048-битного ключа RSA	Установите этот флаг для поддержки 2048-битных ключей RSA.
Включение поддержки сертификации FIPS	Установите этот флаг для инициализации устройств в режиме соответствия стандарту FIPS. FIPS (Federal Information Processing Standards) – утвержденный правительством США набор стандартов, направленных на улучшение

Настройка	Описание
	управления и использования компьютерных и телекоммуникационных систем связи.
Режим кэширования приватных данных	Эта настройка определяет, когда личная информация (кроме закрытых ключей) может быть кэширована вне памяти электронного ключа. Список содержит следующие пункты: • **Никогда** - данные не кешируются; • **Всегда** - личные данные всегда кешируются; • **Только при активной сессии пользователя** - данные остаются в кеше с момента авторизации с помощью электронного ключа и до момента, пока сеанс авторизации не будет закрыт.

9. Перейдите на вкладку **Приложения**.
Отобразится страница следующего вида.

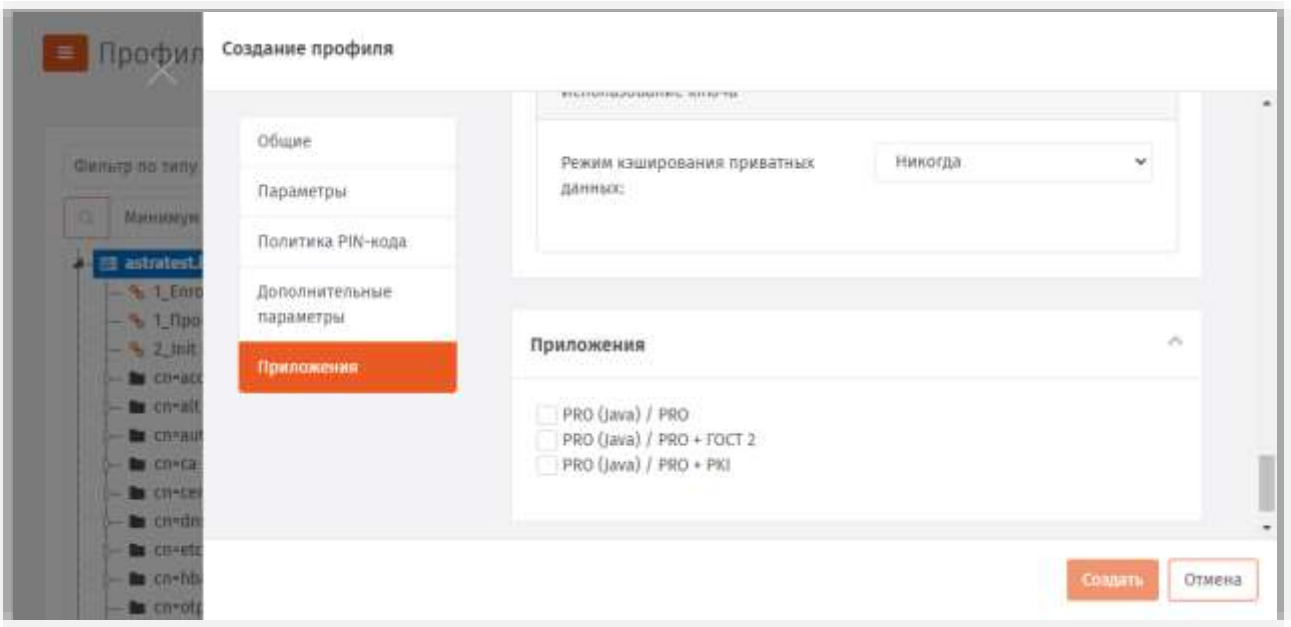


*Рис. 127 – Вкладка **Приложения** свойств профиля инициализации*

10. Отметьте нужные комбинации приложений
11. Нажмите **Создать** (или **Сохранить**, если редактировался ранее созданный профиль).

Изменения, внесенные в профиль, будут сохранены.

3.6.4.2 JaCarta PKI

12. В консоли управления JMS перейдите в раздел **Профили**.
13. Выполните одно из следующих действий:

- чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Инициализация JaCarta PKI**.
- чтобы изменить существующий профиль, выберите этот профиль (например, **Инициализация JaCarta PKI по умолчанию**) в центральной части окна консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

Отобразится следующее окно.

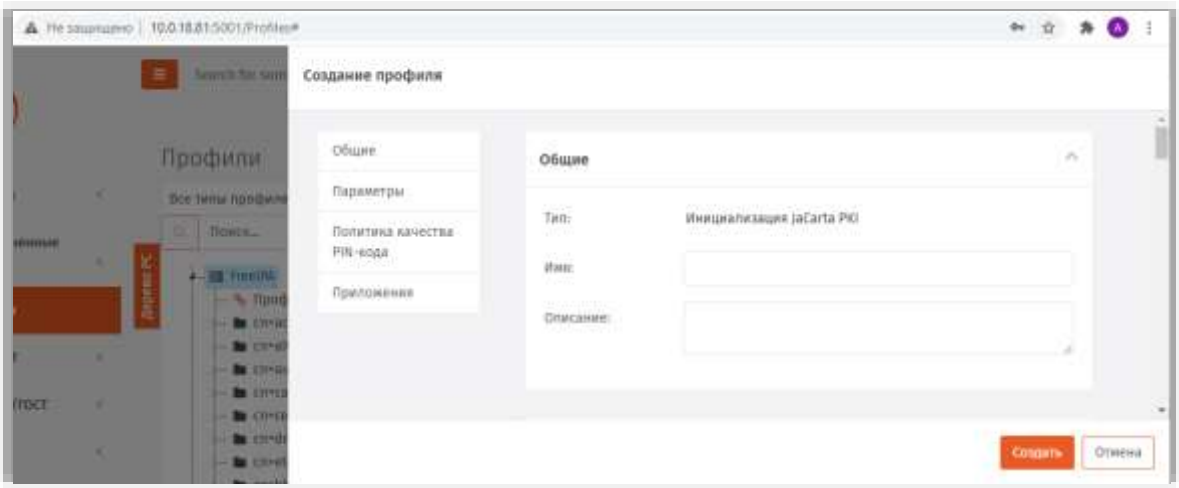


*Рис. 128 – Вкладка **Общие***

14. В соответствующих полях введите (или отредактируйте) имя и описание профиля, после чего переходите на вкладку **Параметры (**Рис. 129**)**.

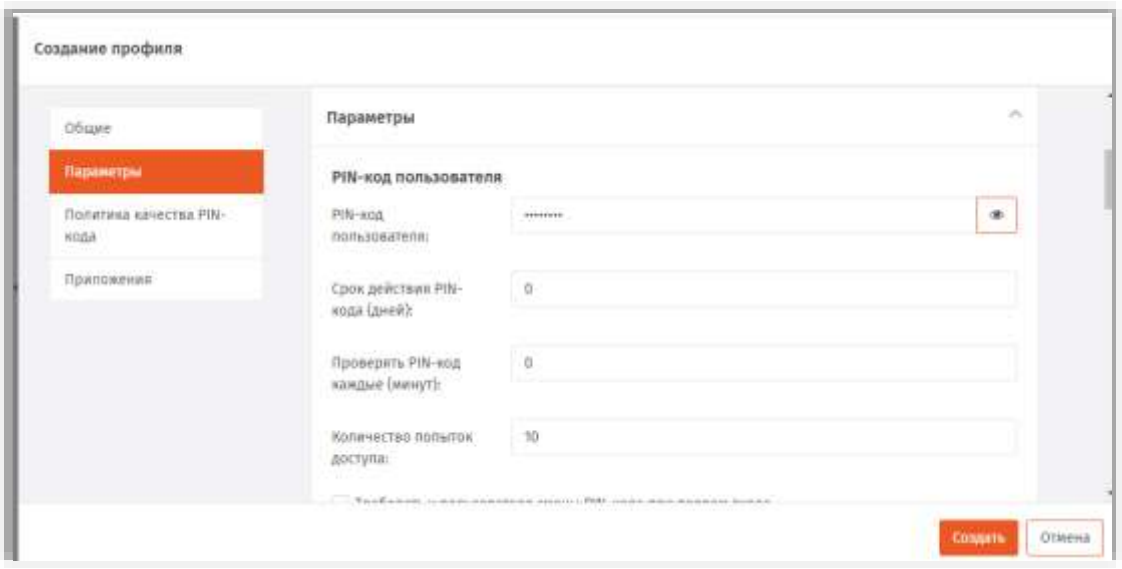


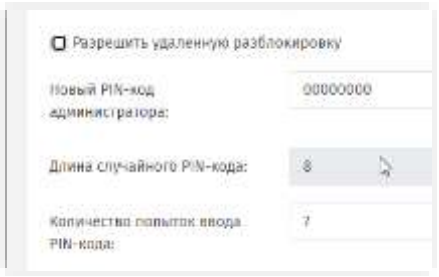
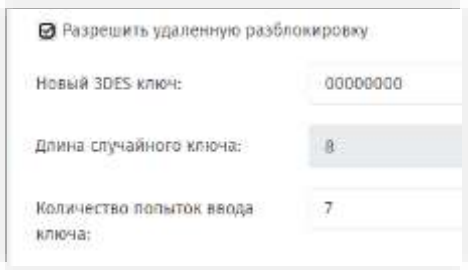
*Рис. 129 – Вкладка **Параметры***

15. Выполните настройку, руководствуясь табл. 21.

Табл. 21 - Настройка параметров инициализации

Настройка	Описание
Секция **PIN-код пользовател**	
PIN-код пользователя	Позволяет задать значение PIN-кода пользователя.
Срок действия PIN-кода (дней)	Число дней, спустя которое пользователь должен будет сменить PIN-код пользователя.

Настройка	Описание
Проверять PIN-код каждые (минут)	В течение какого времени (в минутах) PIN-код пользователя будет кешироваться на компьютере, к которому подсоединен электронный ключ. По истечении этого времени пользователь должен будет снова ввести PIN-код, чтобы подтвердить доступ.
Количество попыток доступа	Максимальное допустимое число последовательных попыток ввода неверного PIN-кода и/или неудачных попыток биометрической аутентификации, по достижении которого PIN-код и/или доступ по отпечатку пальца блокируется. Попытки неудачного доступа учитываются отдельно – для PIN-кода пользователя и для биометрической аутентификации.
Требовать у пользователя смены PIN-кода при первом входе	Установка этого флага обяжет пользователя сменить PIN-код пользователя при первом использовании электронного ключа.
Требовать у пользователя смены PIN-кода после разблокировки	Установка этого флага обяжет пользователя сменить PIN-код пользователя, после того как электронный ключ был разблокирован.
Секция **PIN-код администратора**	
Использовать текущий PIN-код администратора из профиля / Использовать текущий 3DES ключ из профиля	Позволяет использовать/не использовать при инициализации электронного ключа значение, заданное в поле **Текущий PIN-код администратора / Текущий 3DES-ключ** (ниже). Если этот флаг не установлен, то при инициализации электронного ключа будет использован дефолтный PIN-код администратора для данного приложения (установленный, например, на производстве), либо дефолтный 3DES-ключ (установленный в рамках эксплуатирующей организации). **Примечание.** При применении профиля к ренее инициализированному в JMS электронному ключу (т.е. при повторном его выпуске), даже если ключ был отозван и удален, значение данного флага будет игнорироваться, а для инициализации будет использоваться действующий PIN-код администратора / 3DES-ключ для данного электронного ключа, ранее сохраненный в БД JMS.
Текущий PIN-код администратора / Текущий 3DES ключ	Значение PIN-кода администратора /3DES-ключа, установленное в настоящий момент в электронном ключе. Используется только при включенном флаге **Использовать текущий PIN-код администратора из профиля / Использовать текущий 3DES ключ из профиля**
Способ установки PIN-кода	Позволяет выбрать способ формирования PIN-кода администратора / 3DES-ключа: • **Использовать фиксированный** – позволяет задать фиксированный PIN-код администратора /3DES-ключа, значение которого следует указать в поле **PIN-код администратора/3DES ключ**; • **Генерировать случайный** – при выборе этого пункта в процесс инициализации будет сгенерирован случайный PIN-код администратора / 3DES-ключа; количество символов случайного PIN-кода задается в поле **Длина случайного PIN-кода / Длина случайного ключа**.
Разрешить удаленную разблокировку	Установка этого флага позволяет удаленно (например, с помощью клиента JMS) разблокировать пользовательские PIN-коды электронных ключей в режиме **Запрос-Ответ**. (Возможность удаленной разблокировки биометрической аутентификации не предусмотрена.) В этом случае вместо PIN-кода администратора должен быть задан ключ 3DES. При установке этого флага соответствующим образом меняются настройки (см. изображения ниже).

Настройка	Описание
	• Флаг не установлен  • Флаг установлен 
Новый PIN-код администратора / Новый 3DES ключ	Позволяет задать произвольный PIN-код администратора (если был выбран фиксированный способ установки и флаг **Разрешить удаленную разблокировку** не был установлен). ИЛИ Позволяет задать ключ 3DES, который будет использоваться в качестве PIN-кода администратора (если был выбран фиксированный способ установки и флаг **Разрешить удаленную разблокировку** установлен).
Длина случайного PIN-кода / Длина случайного ключа	Позволяет задать длину случайного PIN-кода администратора (или ключа 3DES), если в настройке **Способ установки PIN-кода** был выбран пункт **Генерировать случайный**.
Количество попыток ввода PIN-кода / Количество попыток ввода ключа	Максимальное число попыток ввода неверного PIN-кода администратора (или максимальное число попыток применения неверного ключа 3DES), по достижении которого PIN-код администратора (ключ 3DES) на электронном ключе блокируется.

16. Перейдите на вкладку **Политика качества PIN-кода** (Рис. 130).

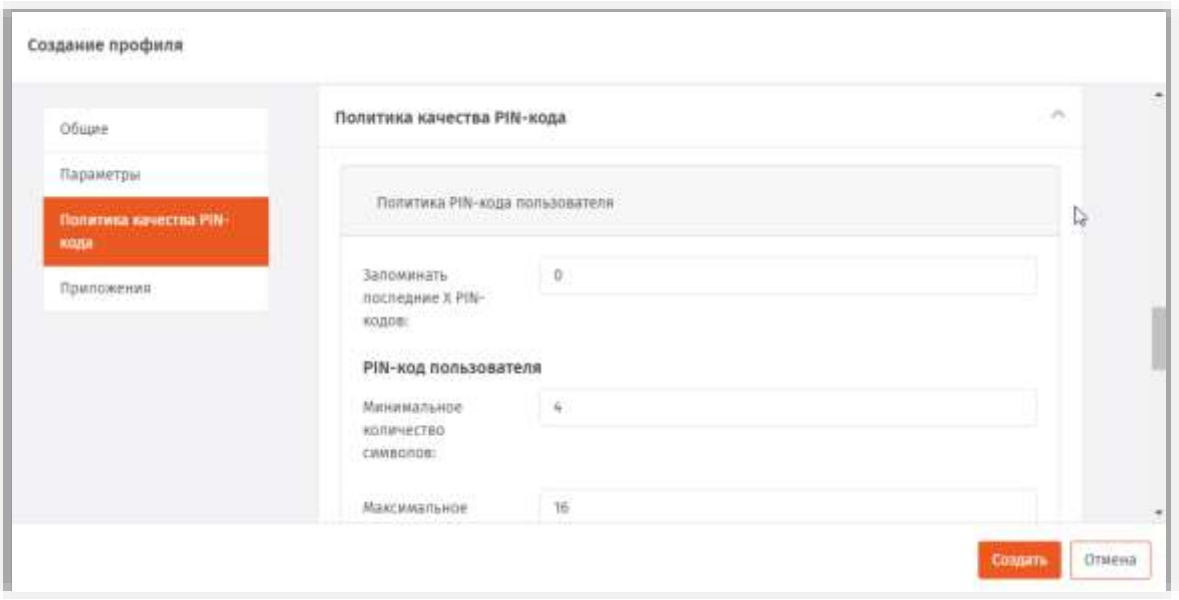


*Рис. 130 – Вкладка **Политика качества PIN-кода***

17. Эта вкладка позволяет настроить качество PIN-кодов, используемых с электронными ключами, которые будут инициализированы с настраиваемым профилем.
18. Выполните настройку, руководствуясь табл. 22.

Табл. 22 – Политики качества PIN-кодов

Настройка	Описание
Выбор секции **Политика PIN-кода пользователя / Политика PIN-кода администратора** (последовательно выберите и настройте политику сначала для PIN-кода пользователя, затем для PIN-кода администратора)	
Запоминать последние X PIN-кодов	Позволяет задать число использованных подряд ранее PIN-кодов, которые пользователь не сможет использовать при назначении нового PIN-кода. **Примечание.** Нулевое значение параметра означает отключение проверки, т.е. предыдущие значения PIN-кода будут игнорироваться.
Секция **PIN-кода пользователя / PIN-кода администратора** (в зависимости от выбора первой секции)	
Минимальное количество символов	Позволяет задать минимальное необходимое число символов в PIN-коде.
Максимальное количество символов	Позволяет задать максимальное возможное число символов в PIN-коде.
Секция **Минимальное количество символов** (задает качество PIN-кода)	
Символы алфавита	Позволяет задать минимальное необходимое число символов алфавита в PIN-коде.

Настройка	Описание
Символы в верхнем регистре	Позволяет задать минимальное необходимое число символов в верхнем регистре в PIN-коде.
Символы в нижнем регистре	Позволяет задать минимальное необходимое число символов в нижнем регистре в PIN-коде.
Числовые символы	Позволяет задать минимальное необходимое число цифр в PIN-коде.
Специальные символы	Позволяет задать минимальное необходимое число специальных символов (не алфавитно-цифровых) в PIN-коде.
Максимальное количество повторений символов	Определяет максимальное допустимое число одинаковых символов в PIN-коде.

19. Перейдите на вкладку **Приложения (**Рис. 131**)**.

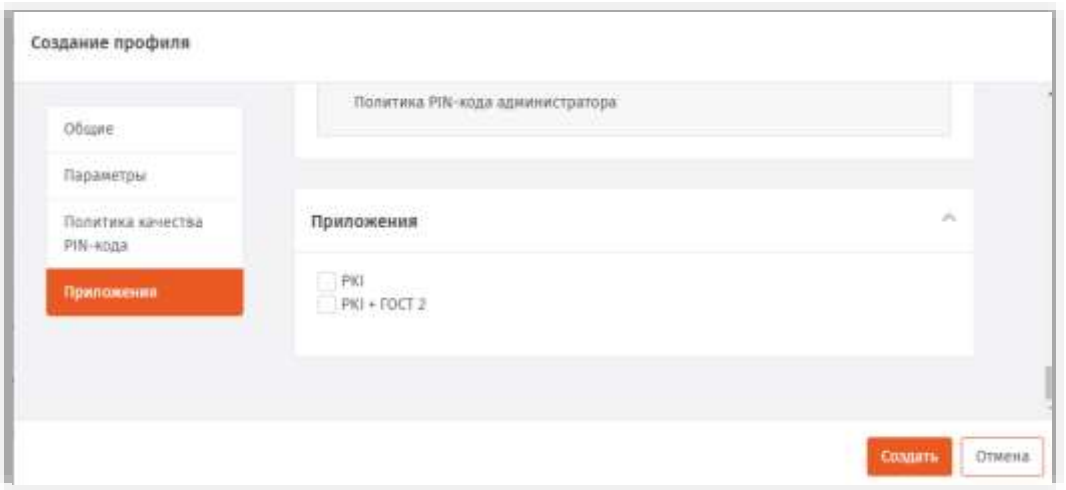


*Рис. 131 – Вкладка **Приложения***

20. Отметьте нужные комбинации приложений.
21. Нажмите **Создать** (или **Сохранить**, если редактировался ранее созданный профиль).

Изменения, внесенные в профиль, будут сохранены.

3.6.4.3 DataStore

Примечание. Тип профиля **Инициализация DataStore** по умолчанию не отображается в консоли управления JMS. Для того, чтобы профиль начал отображаться следует включить в JMS поддержку ЭК **DataStore** (приложение/апплет Storage). Подробно процедура включения поддержки приложений/апплетов ЭК описана в руководстве по настройке и установке [2], раздел «Добавление поддержки моделей ЭК / профилей в JMS».

В консоли управления JMS перейдите в раздел **Профили**.

1. Выполните одно из следующих действий:

   – чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Инициализация DataStore**.

– чтобы изменить существующий профиль, выберите этот профиль (например, **Инициализация DataStore по умолчанию**) в центральной части окна консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

Отобразится страница следующего вида

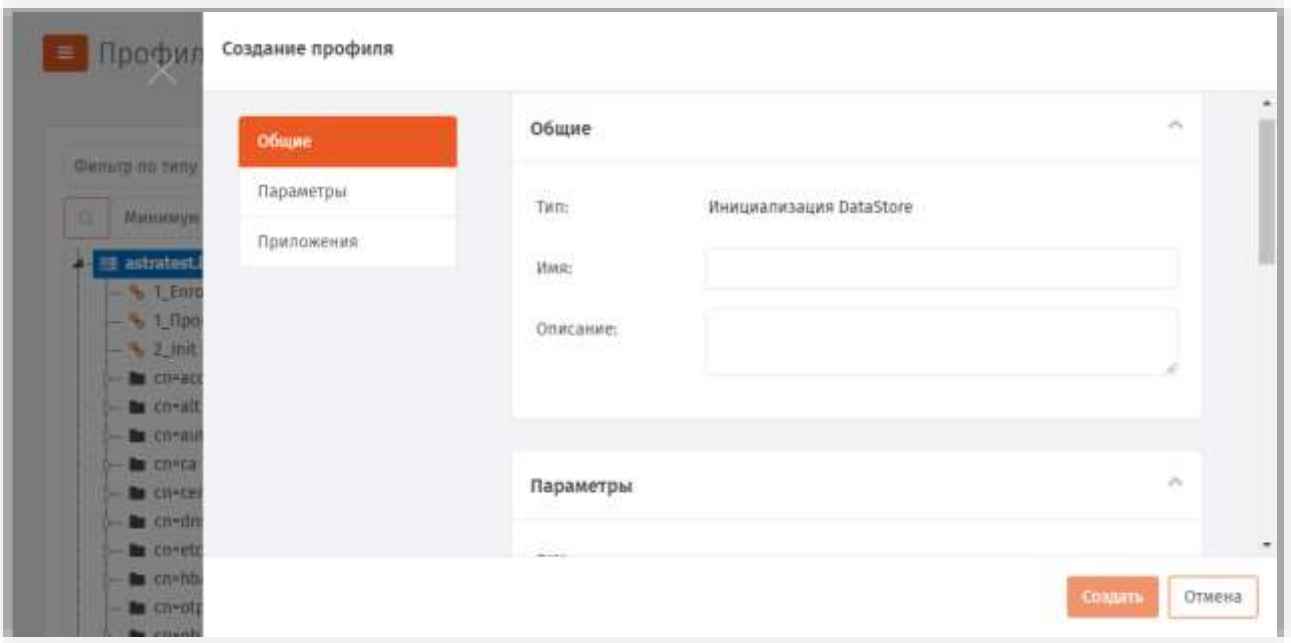


*Рис. 132 – Вкладка **Общие** свойств профиля инициализации*

2. В соответствующих полях введите (или отредактируйте) имя и описание профиля, после чего переходите на вкладку **Параметры**.
Отобразится страница следующего вида

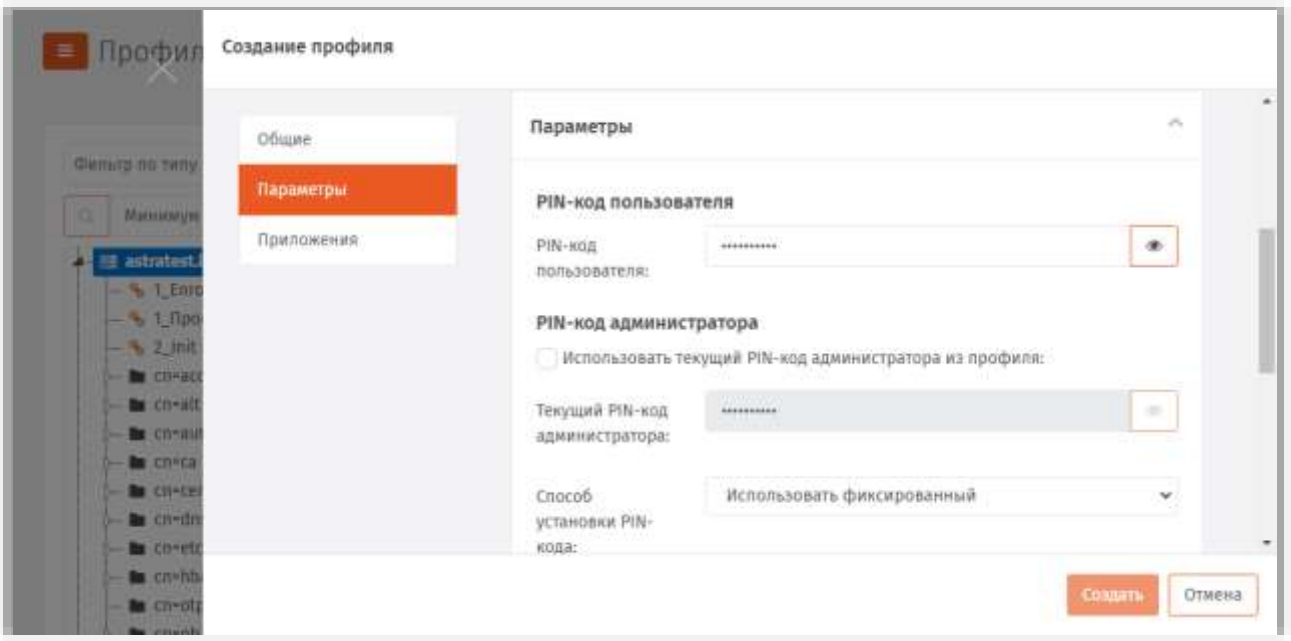


*Рис. 133 – Вкладка **Параметры** свойств профиля инициализации*

3. Выполните настройку, руководствуясь табл. 23.

Табл. 23 – Настройка параметров инициализации

Секция	Настройка	Описание
PIN-код пользователя	**PIN-код пользователя**	Позволяет задать значение PIN-кода пользователя.
PIN-код администратора	**Использовать текущий PIN-код администратора из профиля**	В случае установки данного флага при *первой* инициализации электронного ключа (т.е. в результате первой его регистрации в JMS с выпуском) будет использован PIN-код, указанный в поле **Текущий PIN-код администратора** (ниже). В противном случае (флаг не установлен) будет использован дефолтный PIN-код администратора для данного *приложения* (установлен в JMS по умолчанию, недоступен администратору для настройки). **Примечание.** При применении профиля к ренее инициализированному в JMS электронному ключу (т.е. при повторном его выпуске), даже если ключ был отозван и удален, значение данного флага (**Использовать текущий PIN-...**) будет игнорироваться, а для инициализации будет использоваться действующий PIN-код администратора для данного электронного ключа, ранее сохраненный в БД JMS.
	Текущий PIN-код администратора	Поле позволяет указать текущий PIN-код администратора в электронном ключе. Используется при включенном флаге **Использовать текущий PIN-код администратора из профиля**
	Способ установки PIN-кода	Позволяет выбрать способ формирования PIN-кода администратора. Доступны следующие варианты: • **Использовать фиксированный** – если выбран этот пункт, задайте значение PIN-кода администратора в поле PIN-код администратора; • **Генерировать случайный** – в процессе инициализации будет создан случайный PIN-код администратора; укажите длину случайного PIN-кода в поле **Длина случайного PIN-кода**.
	Новый PIN-код администратора	Если в списке **Способ установки PIN-кода** был выбран пункт **Использовать фиксированный**, это поле позволяет задать новый PIN-код администратора.
	Длина случайного PIN-кода	Позволяет задать длину случайного PIN-кода администратора, если в списке **Способ установки PIN-кода** был выбран пункт **Генерировать случайный**.

4. Переходите на вкладку **Приложения**.

Отобразится страница следующего вида

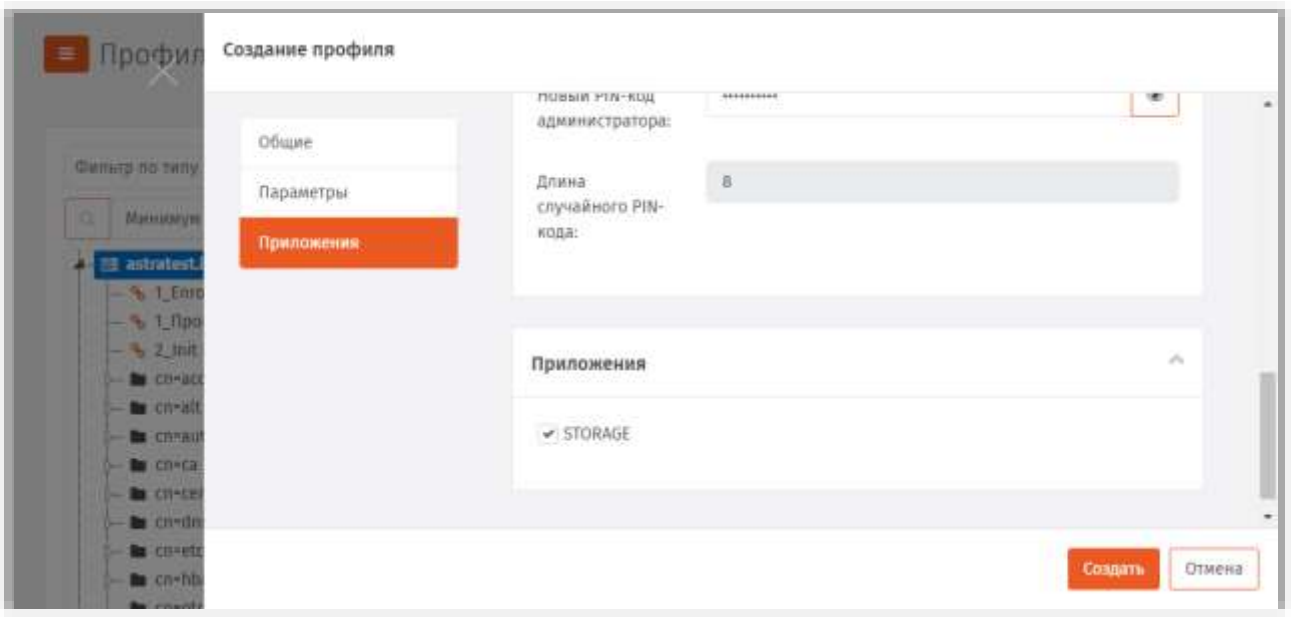


*Рис. 134 – Вкладка **Приложения** свойств профиля инициализации*

5. Отметьте нужные комбинации приложений.
6. Нажмите **Создать** (или **Сохранить**, если редактировался ранее созданный профиль).

Изменения, внесенные в профиль, будут сохранены.

3.6.4.4 JaCarta SF/ГОСТ

Примечание. Перед созданием профилей для выпуска электронных ключей JaCarta SF/ГОСТ следует с помощью утилиты «Программа Главного Администратора» (из комплекта поставки ключей данного типа) создать ключевой контейнер администратора доступа (файл с расширением .kka) для его использования в процедуре создания профиля в JMS, либо убедиться, что нужный kka-контейнер уже импортирован в JMS (см. «Импорт/экспорт контейнеров JaCarta SF/ГОСТ», с 187).

1. В консоли управления JMS перейдите в раздел **Профили**.
2. Выполните одно из следующих действий:

   – чтобы создать новый профиль, нажмите **Создать**, выберите тип профиля **Инициализация JaCarta SF/ГОСТ**.
   – чтобы изменить существующий профиль, выберите этот профиль (например, **Инициализация JaCarta SF/ГОСТ по умолчанию**) в центральной части окна консоли управления JMS, после чего по нажатию на нём правой кнопкой мыши выберите **Свойства**.

Отобразится страница следующего вида.

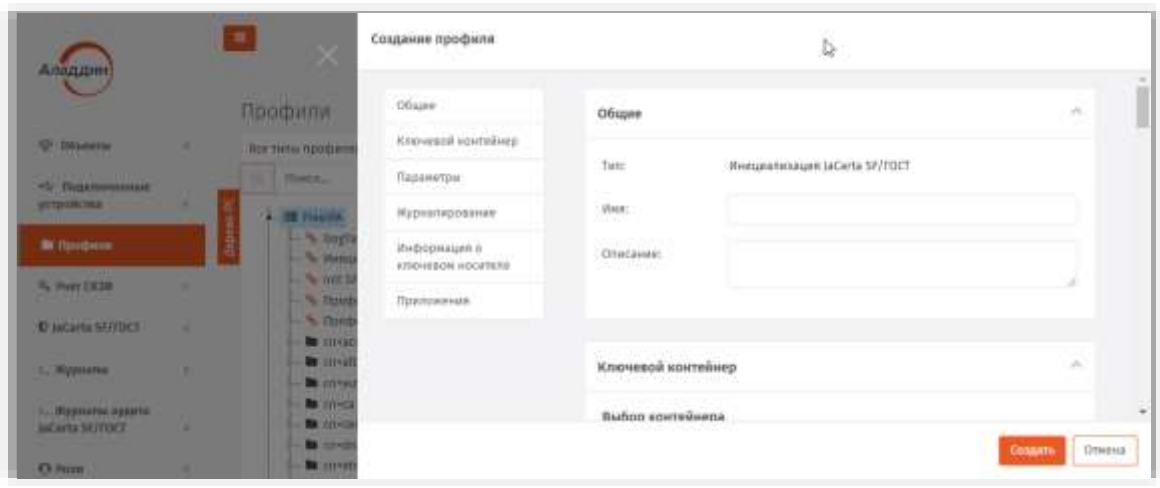


*Рис. 135 – Вкладка **Общие***

3. На вкладке **Общие** в соответствующих полях введите (или отредактируйте) имя и описание профиля.

3.6.4.4.1 Вкладка Ключевой контейнер

4. Перейдите на вкладку **Ключевой контейнер:**

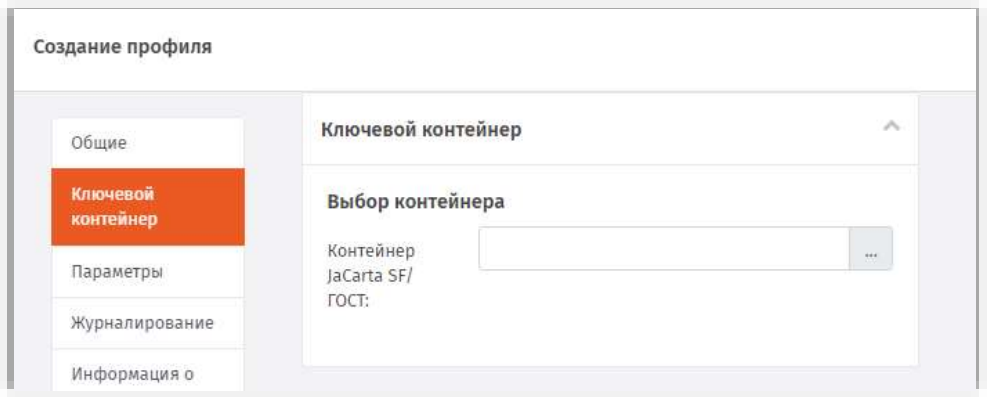


*Рис. 136 – Вкладка **Ключевой контейнер***

5. В поле **Контейнер JaCarta SF/ГОСТ** нажмите три точки (…), выберите необходимый контейнер и нажмите **Выбрать**, или импортируйте соответствующий контейнер из файла, нажав **Импорт** (подробнее импорт контейнера JaCarta SF/ГОСТ описан в разделе «Импорт/экспорт контейнеров JaCarta SF/ГОСТ», с. 187).

3.6.4.4.2 Вкладка Параметры

6. Перейдите на вкладку **Параметры**.

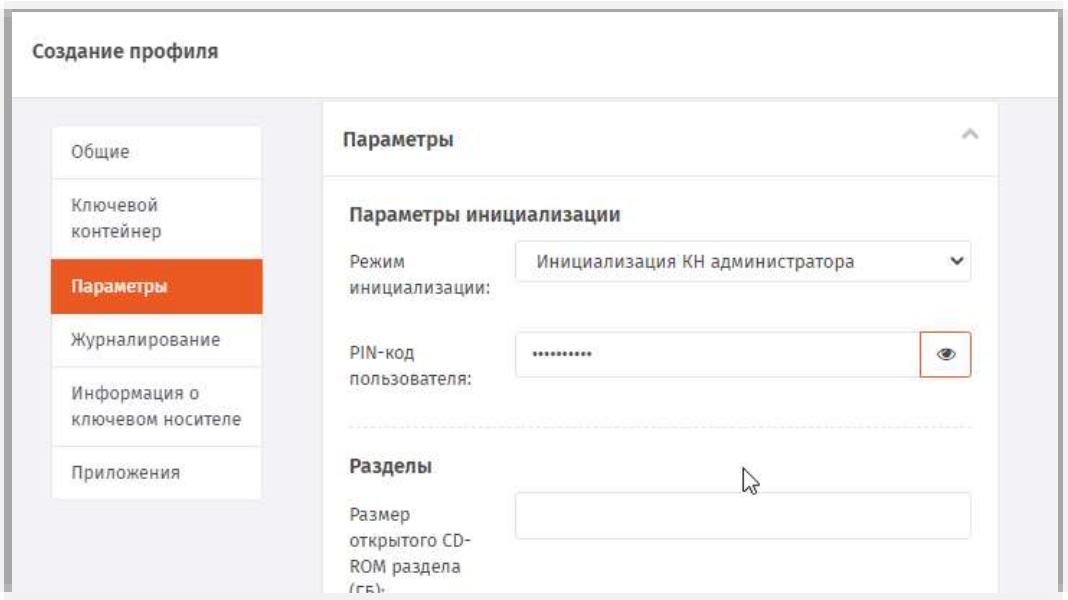


*Рис. 137 – Вкладка **Параметры***

7. Выполните настройки, руководствуясь Табл. 24.

Табл. 24 – Настройка параметров профиля инициализации JaCarta SF

Настройка	Описание
Секция **Параметры инициализации**	
Режим инициализации	Настройка определяет тип электронного носителя (ЭН) который будет получен после инициализации электронного ключа JaCarta SF/ГОСТ. Возможные значения: • **Инициализация КН администратора** – электронный ключ будет инициализирован как *ЭН администратора доступа* • **Инициализация КН пользователя** – электронный ключ будет инициализирован как *ЭН пользователя*
PIN-код пользователя	Установите PIN-код пользователя приложения SF. Значение PIN-кода пользователя должно соответствовать парольной политике (требование к длине пароля и использования определенных категорий символов), установленной в секции **Безопасность** (ниже). Значение по умолчанию: 1234567890
Секция **Разделы**	
Важно! Настройки в данной секции устанавливают реальные размеры соответствующих разделов, которые могут отличаться от размеров разделов, указанных контейнере JaCarta SF/ГОСТ **Примечание.** Размер скрытого RW-раздела электронного ключа JaCarta SF/ГОСТ определяется как общий объем флеш-памяти данного электронного ключа за вычетом объема перечисленных ниже разделов.	
Размер открытого CD-ROM раздела (ГБ)	Установите размер открытого раздела CD-ROM электронного ключа JaCarta SF/ГОСТ. Если раздел создавать не нужно, то следует указать значение 0 (ноль).

Настройка	Описание
Размер скрытого CD-ROM раздела (ГБ)	Установите размер скрытого раздела CD-ROM электронного ключа JaCarta SF/ГОСТ. Если раздел создавать не нужно, то следует указать значение 0 (ноль).
Размер открытого RW-раздела (ГБ)	Установите размер открытого RW-раздела CD-ROM электронного ключа JaCarta SF/ГОСТ. Если раздел создавать не нужно, то следует указать значение 0 (ноль).
Алгоритм шифрования	Выберите алгоритм шифрования для скрытых разделов. Доступные значения: • **ГОСТ 28147-89** • **Ускоренный ГОСТ 28147-89**
Форматировать RW-разделы	Настройка определяет необходимость форматирования RW-разделов ЭН
Настройки, относящиеся к RW-разделам ЭН. Данные настройки доступны при условии, что установлен флаг **Форматировать RW-разделы** (выше)	
Файловая система открытого раздела	Настройка доступна при условии установки флага **Форматировать RW-разделы** (выше) Выберите тип файловой системы для монтирования в открытом разделе ЭН. Доступные значения: • **FAT32** • **NTFS**
Метка открытого раздела	При необходимости установите метку открытого RW-раздела
Файловая система скрытого раздела	Выберите тип файловой системы для монтирования в скрытом разделе ЭН. Доступные значения: • **FAT32** • **NTFS** **Примечание.** Поле недоступно в случае если в поле **Режим инициализации** (выше) установлено значение **Инициализация КН администратора**.
Метка скрытого раздела	При необходимости установите метку скрытого RW-раздела **Примечание.** Поле недоступно в случае если в поле **Режим инициализации** (выше) установлено значение **Инициализация КН администратора**.
Секция **Безопасность**	
Минимальная длина ПИН-кода	Укажите минимальную длину PIN-кода приложения SF. Значение по умолчанию: **6**
Ограничения алфавита	При помощи настроек установите какие типы символов допускается использовать при создании PIN-кода приложения: • **Строчные символы** • **Прописные символы** • **Цифровые символы** (установлены по умолчанию) • **Специальные символы**

3.6.4.4.3 Вкладка Журналирование

8. Перейдите на вкладку **Журналирование**.

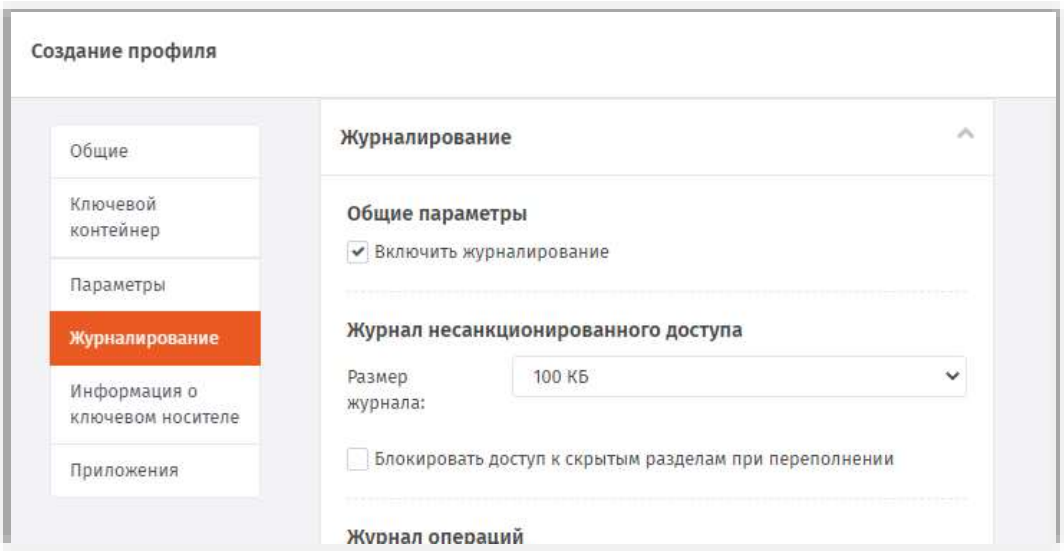


*Рис. 138 – Вкладка **Журналирование***

9. Выполните настройки, руководствуясь Табл. 25.

Табл. 25 – Настройка параметров журналирования ЭН

Настройка	Описание
Секция **Общие параметры**	
Включить журналирование	При установке флага в ЭН будет включена система регистрации событий Флаг установлен по умолчанию
Секция **Журнал несанкционированного доступа**	
Размер журнала	Укажите размер журнала
Блокировать доступ к скрытым разделам при переполнении	Установите флаг, если необходимо блокировать работу со скрытыми разделами при переполнении журнала
Секция **Журнал операций**	
Размер журнала	Укажите размер журнала
Блокировать доступ к скрытым разделам при переполнении	Установите флаг, если необходимо блокировать работу со скрытыми разделами при переполнении журнала
Секция **Журнал событий безопасности**	
Размер журнала	Укажите размер журнала

Настройка	Описание
Блокировать доступ к скрытым разделам при переполнении	Установите флаг, если необходимо блокировать работу со скрытыми разделами при переполнении журнала

3.6.4.4.4 Вкладка Информация о КН

10. Перейдите на вкладку **Информация о ключевом носителе**.

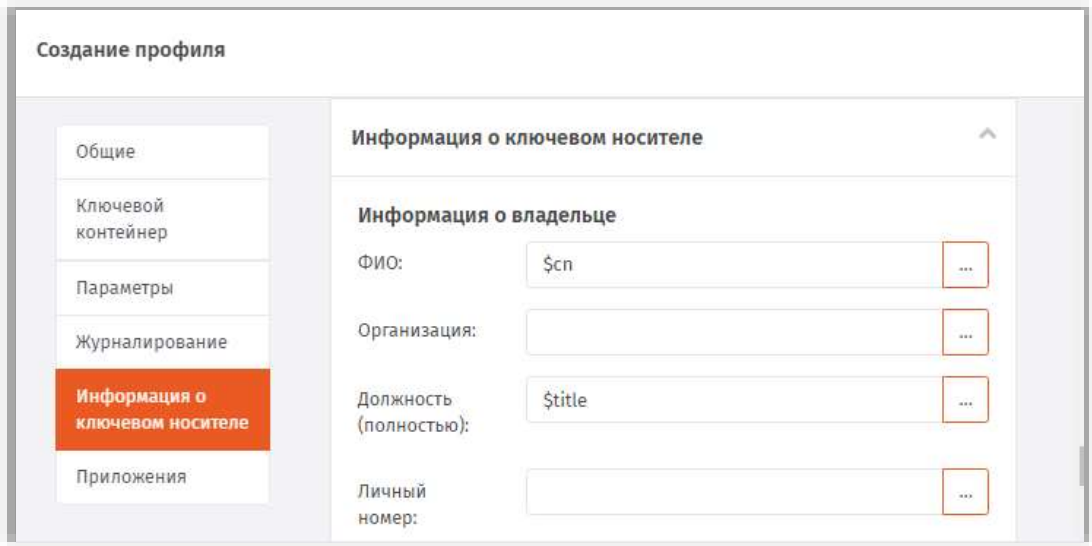


*Рис. 139 – Вкладка **Информацию о ключевом носителе***

11. Выполните настройки, руководствуясь Табл. 26.

Табл. 26 – Настройка информации о пользователе КН

Настройка	Описание
Секция **Информация о владельце**	
• **ФИО** • **Организация** • **Должность (полностью)** • **Личный номер**	Заполните поля. В качестве значений можно выбрать атрибуты пользователя соответствующей ресурсной системы (например, FreeIPA). Для этого нажмите «...» (три точки) и выберите необходимое значение. Данное значение будет подставлено автоматически во время инициализации приложения JaCarta SF.

3.6.4.4.5 Вкладка Приложения

12. Перейдите на вкладку **Приложения**.
13. Отметьте нужные комбинации приложений.
14. Нажмите **Создать** (или **Сохранить**, если редактировался ранее созданный профиль).

3.6.5 Настройки профиля выпуска сертификатов в центре сертификации Microsoft

1. В консоли управления JMS перейдите в раздел **Профили**.

2. Выполните одно из следующих действий:

   – чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Выпуск сертификатов - УЦ Microsoft CA**.
   – чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

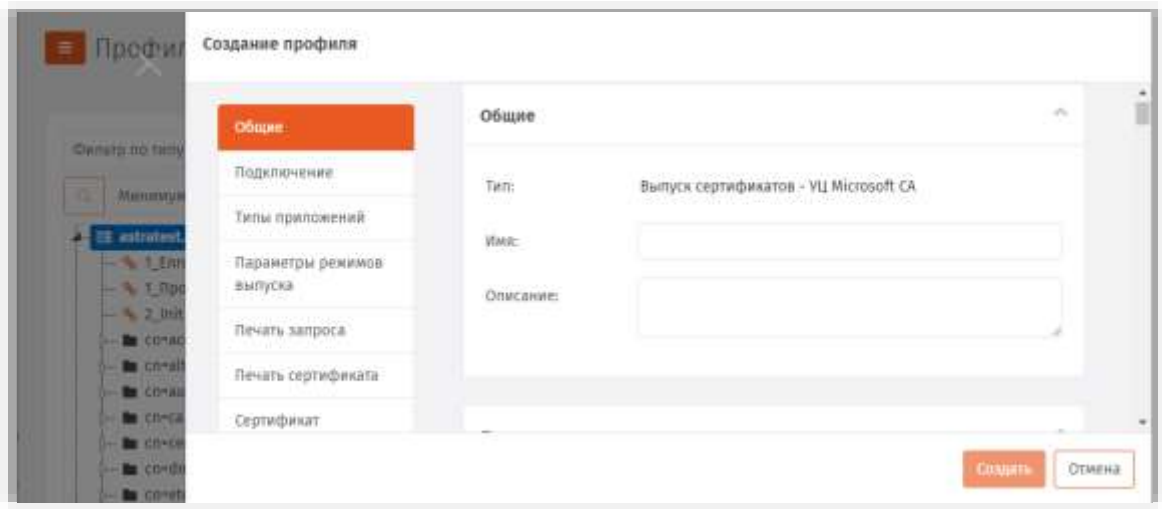


*Рис. 140 – Вкладка **Общие** профиля выпуска сертификатов*

3. В полях **Имя** и **Описание** введите (или отредактируйте) название и описание профиля соответственно.

3.6.5.1 Настройка параметров подключения

4. Перейдите на вкладку **Подключение**.
   Окно примет следующий вид.

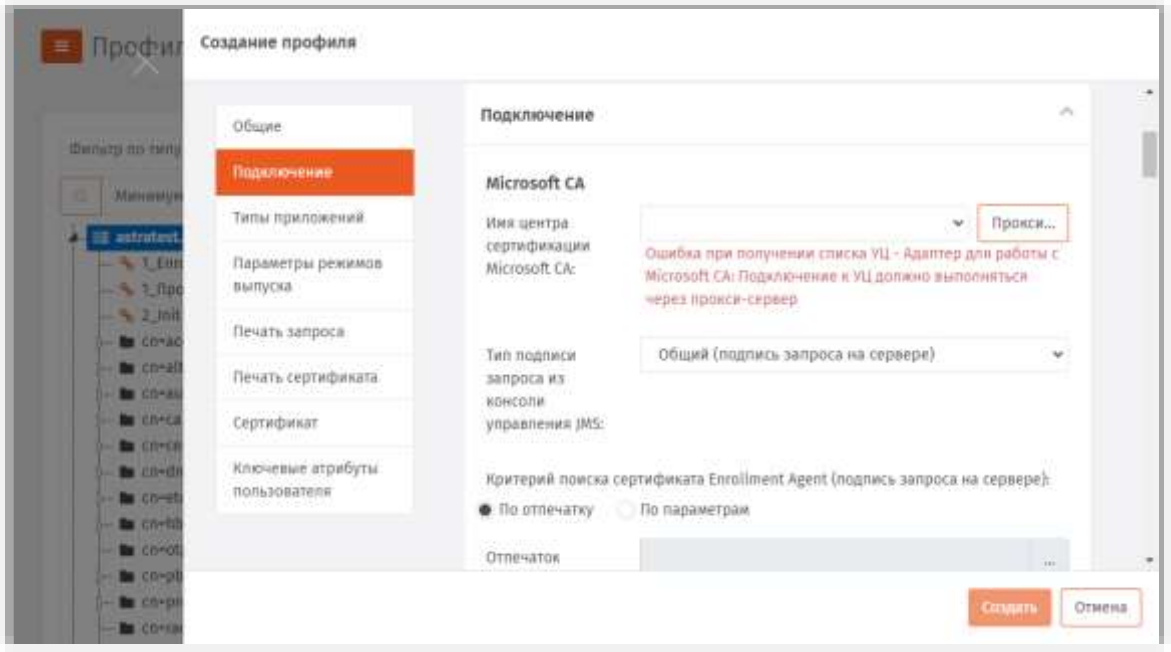


*Рис. 141 – Вкладка **Подключение** профиля выпуска сертификатов*

5. Выполните необходимые настройки, руководствуясь табл. 27.

Табл. 27 – Настройка параметров подключения к удостоверяющему центру

Секция	Настройка	Описание
Microsoft CA	**Имя центра сертификации Microsoft CA**	**Важно!** В текущей реализации JMS 4LX подключение к УЦ MSCA осуществляется через специально установленный web-API – Прокси-сервер для УЦ MSCA (подробнее об установке и настройке прокси-сервера см. в руководстве по установке [2], раздел «Установка Прокси-сервера для УЦ (Web API к УЦ)»). Нажмите кнопку **Прокси...** справа. В появившейся форме (Рис. 142, с. 128) выполните следующие настройки: • **Использовать прокси-сервер** – установите флаг для подключения через прокси-сервер • **Адрес прокси-сервера** – введите адрес Прокси-сервера для УЦ MSCA (например http://192.168.10.1:6610) **Примечание.** Номер порта должен соответствовать порту, указанному в параметре реестра **MSCAProxyWebApiAddresses** в настройках прокси-сервера (подробнее см. в руководстве по установке [2], раздел «Установка Прокси-сервера для УЦ (Web API к УЦ)»); • **Логин** – укажите имя доменного пользователя, принадлежащего доменной или локальной группе, указанной в параметре реестра **AuthorizeAsGroupMember** в настройках прокси-сервера (подробнее см. в руководстве по установке [2], раздел «Установка Прокси-сервера для УЦ (Web API к УЦ)»); • **Пароль** По выполнение подключения к прокси-серверу значение **Имя центра сертификации Microsoft CA** подставится автоматически
	Тип подписи запроса из консоли управления JMS	Позволяет выбрать субъект, который может быть агентом регистрации, при выпуске сертификата пользователя из консоли управления JMS. Доступны следующие варианты: • **Общий (подпись запроса на сервере)** – агентом регистрации выступает сервер JMS, соответствующий сертификат должен быть установлен в хранилище компьютера на сервере JMS (настройка является обязательной); **Примечание**. В случае если служба JMS запускается от имени учетной записи пользователя, то сертификат агента регистрации должен выпускаться на имя учетной записи данного пользователя и устанавливается в хранилище пользователя на сервере JMS. • **Частный (подпись запроса на клиенте)** – роль агента регистрации выполняет администратор JMS, сертификат агента регистрации должен быть установлен в хранилище пользователя на компьютере, с которого работает администратор JMS (из консоли управления JMS), или записан в память электронного ключа администратора JMS.

Секция	Настройка	Описание
	Критерии поиска сертификата Enrollment Agent (подпись запроса на сервере)	Настройка позволяет выбрать сертификат агента регистрации, выпущенный в хранилище компьютера сервера JMS. Выберите способ поиска сертификата агента регистрации: • **По отпечатку**; • **По параметрам**. После выбора способа поиска воспользуйтесь кнопкой  (Обзор), чтобы выбрать нужный сертификат, и подтвердите выбор, нажав **ОК**. **Примечания:** 1. Настройка не касается подписи запроса на сертификат из консоли управления JMS при выборе опции **Частный (подпись запроса на клиенте)**, см. выше. В этом случае администратору будут предложены на выбор все сертификаты из личного хранилища пользователя, от имени которого запущена консоль управления. 2. В случае настройки данного профиля для единичного сервера JMS (т.е. без кластера) следует выбирать способ поиска **По отпечатку**. В случае настройки профиля в кластерной конфигурации JMS следует использовать способ поиска **По параметрам**. Подробнее об особенностях режима выбора **По параметрам** см. в разделе «Порядок использования *режима* По параметрам при настройке выбора сертификата», с. 128. Порядок развертывания кластерной конфигурации приведен в соответствующем руководстве.
Шаблоны сертификатов	**Пользователь**	Выберите из списка опубликованный шаблон сертификата, который будет использоваться при самостоятельном (т.е. из клиента JMS) выпуске пользователями электронных ключей. Чтобы самостоятельно запрашивать сертификаты пользователи должны иметь разрешения: **Чтение** и **Заявка** для шаблона, по которому будут выпускаться сертификаты. Если вы планируете взять под контроль JMS электронные ключи, выпущенные до установки и настройки JMS, шаблон сертификата, выбранный в этой настройке, должен совпадать с шаблоном сертификата, использованным ранее для выпуска электронного ключа.
	Администратор	Выберите из списка опубликованный шаблон сертификата, который будет использоваться при выпуске электронных ключей администратором (т.е. из консоли управления JMS) для пользователей. **Примечания:** 1. Если вы планируете взять под контроль JMS электронные ключи, выпущенные до установки и настройки JMS, шаблон сертификата, выбранный в этой настройке, должен совпадать с шаблоном сертификата, использованным ранее для выпуска электронного ключа.

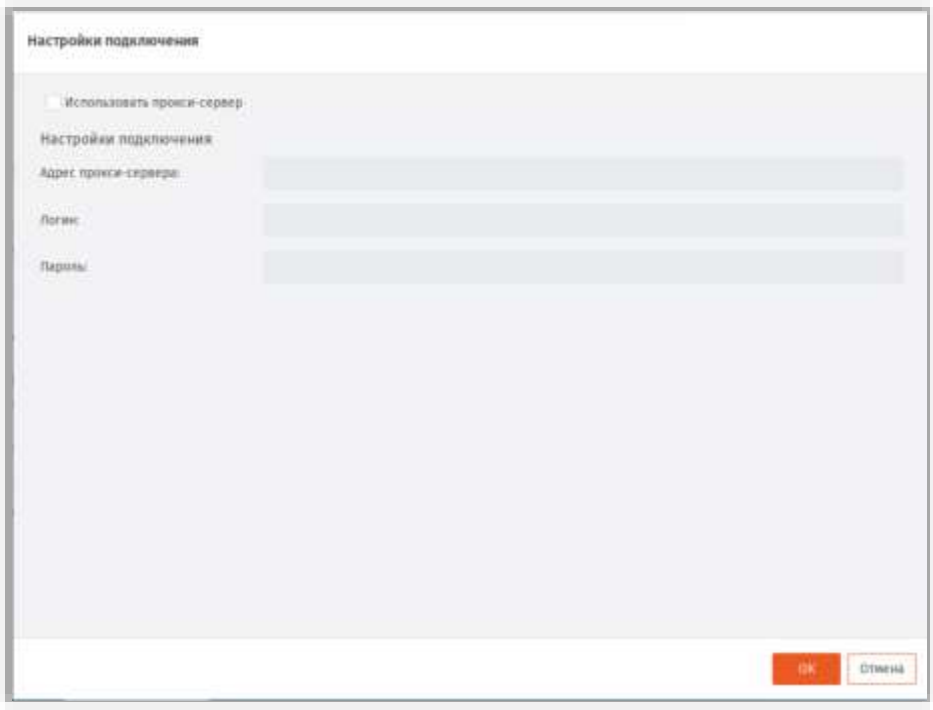


Рис. 142 – Настройки подключения к Прокси-серверу для УЦ MSCA

3.6.5.2 Порядок использования режима *По параметрам* при настройке выбора сертификата

Режим **По параметрам** позволяет выбирать не жестко заданный сертификат (как в случае **По отпечатку**), а произвольный, удовлетворяющий двум критериям отбора: имени удостоверяющего центра (поле **Кем выдан**) и идентификатору расширенного назначения ключа (поле **Улучшенный ключ**). Настройка параметра осуществляется путем выбора одного из сертификатов (кнопка обзора ...), который должен служить образцом для установки значений двух указанных выше полей (критериев отбора).

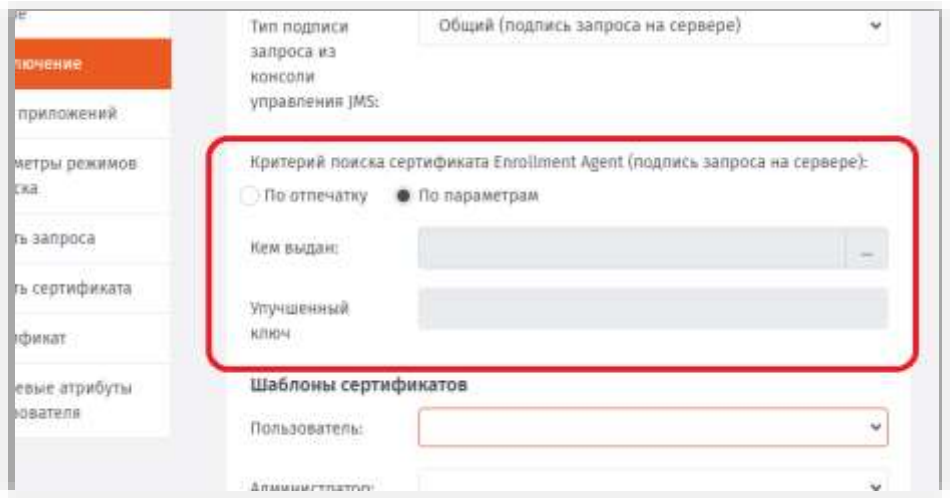


*Рис. 143 – Механизм поиска **По параметрам** на примере профиля выпуска сертификата MSCA*

Если в хранилище, в котором осуществляется поиск **По параметрам**, имеется несколько сертификатов, удовлетворяющих заданным критериям, то среди них будет выбран один из

действующих сертификатов. Если вы хотите гарантировать выбор единственного сертификата, то в соответствующем хранилище следует оставить только этот действующий сертификат, удовлетворяющий критериям отбора.

Режим **По параметрам** следует использовать *только* при настройке выбора сертификата Enrollment Agent (в профиле выпуска сертификата в MSCA) и *только* в кластерной конфигурации JMS, поскольку данный режим позволяет при обращении к произвольному узлу кластера использовать сертификат, выпущенный специально для данного узла и при этом удовлетворяющий заданным критериям отбора.

3.6.5.3 Настройки на вкладке Типы приложений

6. Перейдите на вкладку **Типы приложений**.
   Окно примет следующий вид.

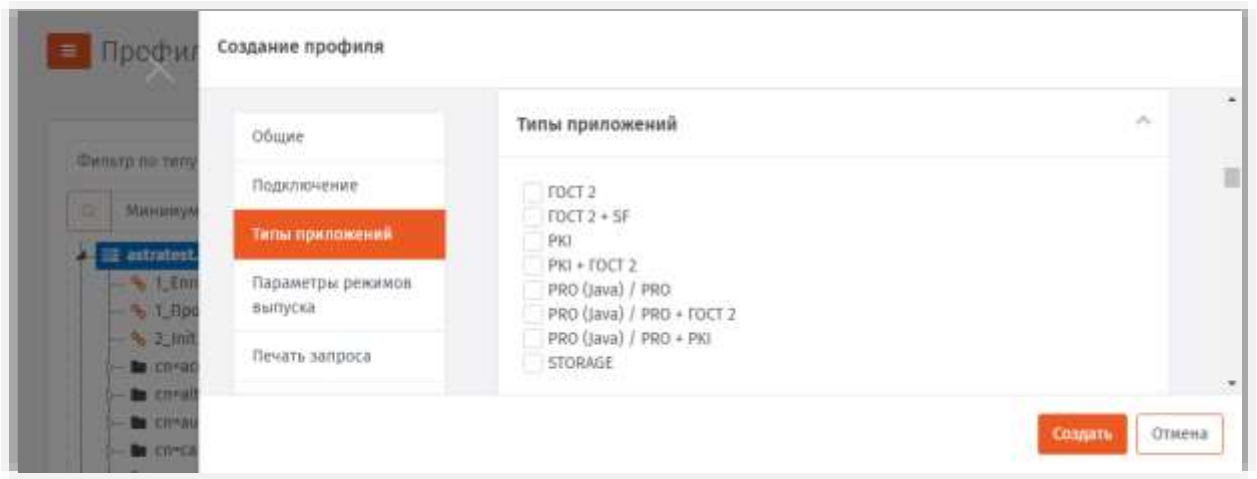


*Рис. 144 – Вкладка **Типы приложений***

7. Отметьте нужные комбинации приложений.

3.6.5.4 Настройка параметров режимов выпуска сертификатов

8. Перейдите на вкладку **Параметры режимов выпуска**.

Окно будет выглядеть следующим образом.

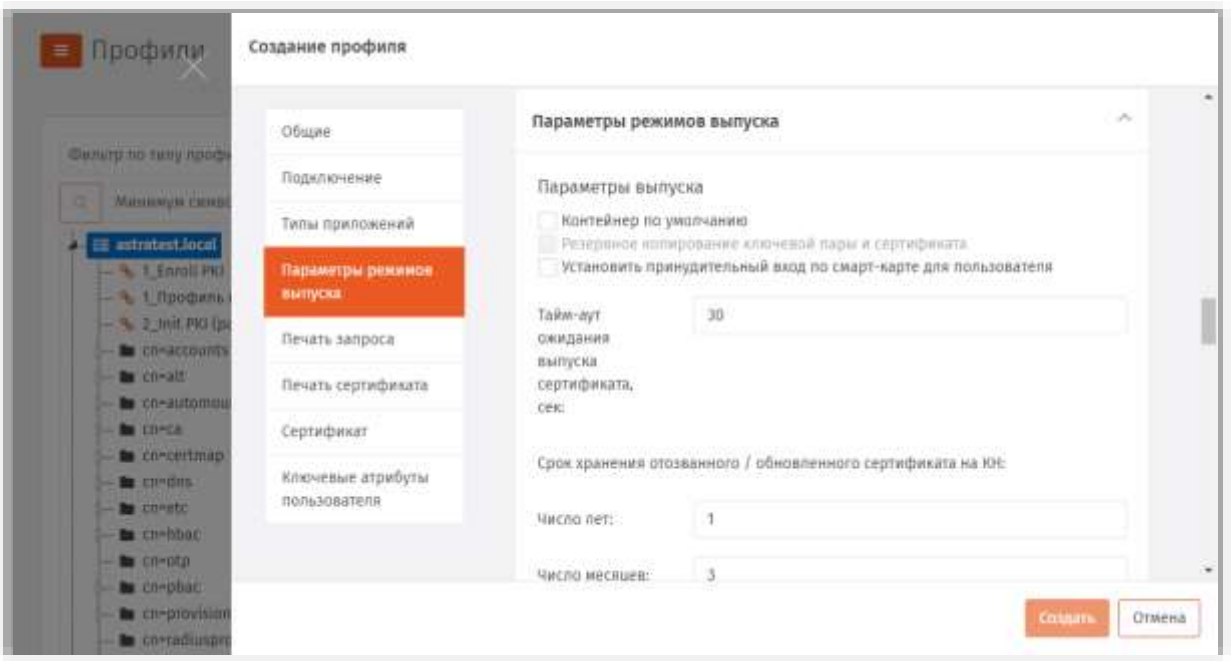


*Рис. 145 – Вкладка **Параметры режимов выпуска** профиля выпуска сертификатов*

9. Выполните необходимые настройки, руководствуясь табл. 28.

Табл. 28 – Настройка параметров выпуска сертификатов

Секция	Настройка	Описание
Параметры выпуска	**Контейнер по умолчанию**	Если этот флаг установлен, защищенный контейнер, создаваемый в памяти электронного ключа при выпуске, будет помечен в качестве контейнера по умолчанию. Настройка актуальна для Windows XP. При выполнении входа с использованием электронного ключа, если на электронном ключе более одного сертификата, система может считать только контейнер по умолчанию, остальные сертификаты игнорируются.
	Резервное копирование ключевой пары и сертификата	Если флаг установлен, при выпуске электронного ключа будет создаваться резервная копия ключевой пары и сертификата в БД JMS. Если внешними средствами с электронного ключа будет удалена ключевая пара с сертификатом, то при синхронизации данные будут восстановлены на электронном ключе с помощью резервной копии на сервере. **Примечание.** Доступность опции зависит от выбранного криптопровайдера (возможности данного криптопровайдера по экспорту ключевой пары и последующей записи ключевой пары из резервной копии в память электронного ключа заданного типа)
	Установить принудительный вход по	Если флаг установлен, пользователю, на имя которого выпускается электронный ключ, будут запрещены все

Секция	Настройка	Описание
	смарт-карте для пользователя	возможности входа в систему, кроме возможности входа с использованием смарт-карты.
	Тайм-аут ожидания выпуска сертификата, сек	Позволяет указать максимальную величину задержки (в секундах) при выпуске сертификата.
	Срок хранения отозванного/обновленного сертификата на КН	Позволяет задать время, в течение которого в памяти электронного ключа будет храниться отозванный или обновленный сертификат. При этом в консоли управления данный сертификат отображается с состоянием «Сохранен на КН». Срок хранения отсчитывается от момента выпуска сертификата. При превышении срока хранения сертификат удаляется из электронного ключа и из БД JMS Значение по умолчанию: 1 год и 3 месяца
Параметры отзыва	 **Важно!** Под событием «отзыв» в настройках данной секции подразумевается отзыв сертификата в JMS, который выполняется в следующих случаях: • при отзыве электронного ключа (см. «Отзыв ЭК/ЗНИ », с. 50); • при отмене привязки *профиля выпуска сертификата*, применявшегося к данному электронному ключу (см. «Привязка профилей», с. 195), в том числе и при удалении профиля; • при удалении сертификата средствами JMS (см. раздел «Операции с сертификатами», с. 26); • при отзыве сертификата (в состоянии «Выпущен на КН») на УЦ не средствами JMS (проверка отзыва сертификата обеспечивается при выполнении планов обслуживания).	
	Публиковать CRL после отзыва	Если флаг установлен, после отзыва в JMS электронного ключа/сертификата на сервере удостоверяющего центра будет публиковаться список отозванных сертификатов (CRL).
	Отзывать сертификат в УЦ	Если флаг установлен, то сертификат, выпущенный на электронном ключе, который был впоследствии отозван в JMS, будет также отозван в УЦ (центре сертификации Microsoft).
	Удалять ключевой контейнер отзываемого сертификата	Если флаг установлен, то при отзыве электронного ключа (или сертификата) из памяти электронного ключа будет удален ключевой контейнер, созданный при выпуске по данному профилю. (Электронный ключ для этого должен быть подсоединен к компьютеру во время процедуры отзыва или синхронизации). Если флаг не установлен, то при отзыве сертификат из электронного ключа не удаляется, а в консоли управления сертификат отображается с состоянием «Сохранен на КН».
Параметры обновления	**Обновлять сертификат с истекающим сроком действия**	Позволяет обновлять сертификат, срок действия которого скоро истечет.

Секция	Настройка	Описание
	Режим обновления	Позволяет выбрать режим обновления сертификатов с истекшим сроком действия. Доступны следующие настройки: • **Существующая ключевая пара** – для обновления сертификата будет использована существующая ключевая пара; • **Новая ключевая пара** – для обновления сертификата будет сгенерирована новая ключевая пара. Эта настройка активна, только если установлен флаг **Обновлять сертификат с истекшим сроком действия**.
	Количество дней до окончания срока действия	Позволяет указать, за сколько дней до истечения срока действия можно обновить сертификат. Эта настройка активна, только если установлен флаг **Обновлять сертификат с истекшим сроком действия**.
	Отзывать заменяемый сертификат в УЦ	Если этот флаг установлен, заменяемый сертификат будет отозван центром сертификации. Эта настройка активна, только если установлен флаг **Обновлять сертификат с истекшим сроком действия**.
	Удалять ключевой контейнер заменяемого сертификата	Если флаг установлен, то при замене сертификата из памяти электронного ключа будет удален ключевой контейнер (электронный ключ для этого должен быть подсоединен к компьютеру) заменяемого сертификата. Если флаг не установлен, то из электронного ключа сертификат не удаляется, а в консоли управления он отображается с состоянием «Сохранен на КН». Данный флаг доступен для изменения только при режиме обновления с новой ключевой парой (см. параметр **Режим обновления**) и произвольно генерируемом имени ключевого контейнера (см. описание вкладки **Ключевой контейнер**).

3.6.5.5 Настройка параметров ключевого контейнера

10. Перейдите к секции **Ключевой контейнер**.

Окно примет следующий вид.

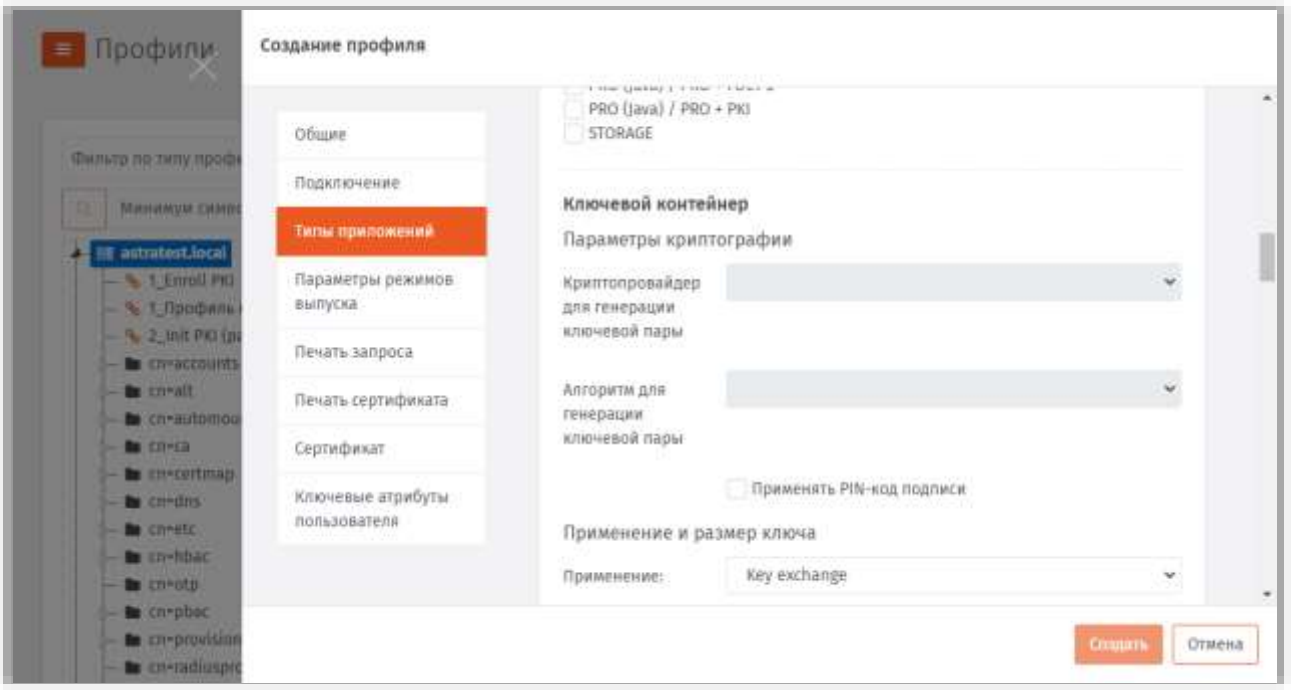


*Рис. 146 – Вкладка **Ключевой контейнер***

11. Выполните необходимые настройки, руководствуясь табл. 29.

Табл. 29 – Настройки ключевого контейнера

Секция	Настройка	Описание
Параметры криптографии	**Криптопровайдер для генерации ключевой пары**	Выберите в этом списке поставщика криптографии, с помощью которого будут формироваться ключевые пары. (Чтобы появиться в списке доступных соответствующий криптопровайдер должен быть установлен на сервере JMS.) **Примечание.** Список доступных поставщиков криптографии зависит от комбинации приложений, выбранных на вкладке **Приложения**. В случае если выбранные приложения не имеют общих поддерживающих их поставщиков криптографии, список будет пустым.

Секция	Настройка	Описание
	Алгоритм для генерации ключевой пары	Выберите алгоритм для генерации ключевой пары. Список алгоритмов зависит выбранного поставщика криптографии, например, в случае выбора *Aladdin GOST PKCS11 Cryptographic Provider* для приложения (на электронном ключе) *ГОСТ 2* появляется возможность выбора алгоритмов ГОСТ 34.10-2001 или ГОСТ 34.10-2012. **Примечания:** 1. Список доступных алгоритмов зависит от комбинации приложений, выбранных на вкладке **Приложения** и содержит только алгоритмы, поддерживаемые одновременно всеми выбранными приложениями. 2. Для выпуска сертификата открытого ключа, сгенерированного по алгоритму ГОСТ 34.10-2012 необходимо обеспечить, наличия на стороне УЦ поставщика криптографии с поддержкой данного алгоритма (например, КриптоПро CSP 4.0).
	Применять PIN-код подписи	При необходимости установите признак обязательности применения пользователем PIN-кода подписи. **Примечания:** 1. Настройка действует только в приложениях ГОСТ 2 на электронных ключах JaCarta. 2. Настройка применяется только к ключевому контейнеру (а значит и к закрытому ключу), созданному при выпуске данного электронного ключа. 3. При установке данного признака, в процессе выпуска электронного ключа у пользователя будет запрошен PIN-код подписи с целью его установки.
Применение и размер ключа, бит	**Key Exchange** (Обмен ключами)	Позволяет указать основное применение ключа.
	Digital Signature (Цифровая подпись)	
	Размер ключа	Укажите размер ключа (в битах), который будет формироваться на основе используемого профиля.
Ключевой контейнер **Имя контейнера**	**Сгенерировать произвольное имя**	Если выбран этот пункт, то для ключевых контейнеров, созданных на основе этого профиля, будет сгенерировано случайное имя.
	Использовать название профиля	Если выбран этот пункт, то для ключевых контейнеров, созданных на основе этого профиля, будет использоваться имя этого профиля. **Важно!** При установке данной опции убедитесь, что используемые в названии профиля символы и его синтаксис поддерживаются соответствующим криптопровайдером

Секция	Настройка	Описание
	Использовать существующий контейнер	Если выбран этот пункт, при выпуске электронных ключей ключевая пара будет записываться в существующий контейнер.
	Использовать указанное имя	Позволяет задать имя, которым будут названы ключевые контейнеры, выпущенные с использованием этого профиля. **Важно!** При задании имени контейнера вручную убедитесь, что используемые символы и синтаксис имени поддерживается соответствующим криптопровайдером

3.6.5.6 Настройка шаблонов полей сертификата

12. Перейдите на вкладку **Сертификат**.
Отобразится следующее окно.

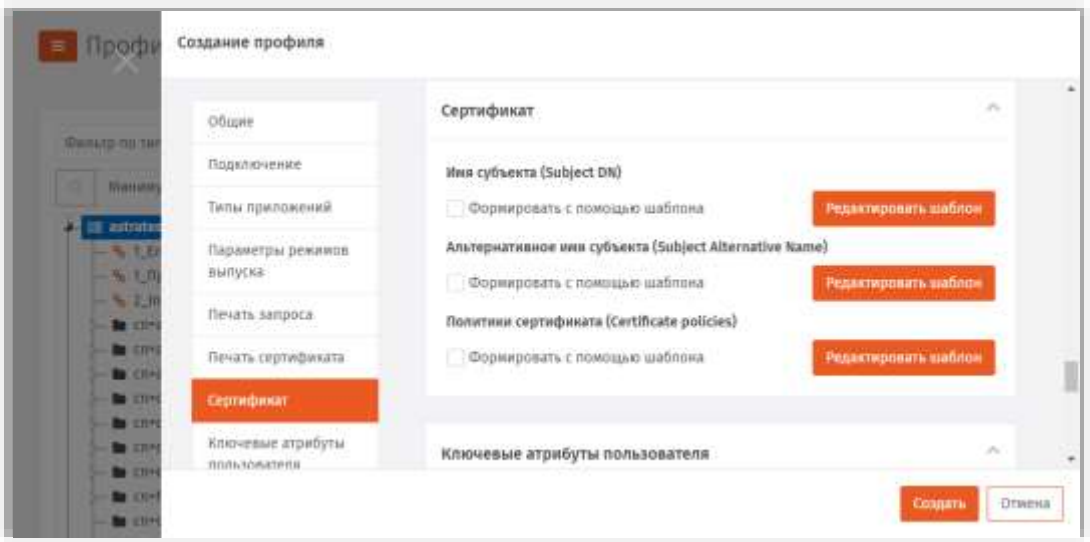


*Рис. 147 – Вкладка **Сертификат***

13. При необходимости отредактируйте поля сертификата (запроса на сертификат), который будет выпускаться на имя пользователей. Для этого выполните следующие действия:

13.1. В секции с названием нужного поля нажмите **Редактировать шаблон**;
13.2. Отредактируйте шаблон, руководствуясь сведениями, представленными в Табл. 30.
13.3. В окне редактирования шаблона нажмите **OK**, чтобы сохранить изменения.
13.4. В секции с названием нужного поля установите флаг **Формировать с помощью шаблона**.
13.5. При необходимости повторите действия для других полей.

Табл. 30 – Настройка шаблонов полей сертификата

Поле	Описание настроек шаблона
Имя субъекта (Subject DN)	Шаблон имеет следующие столбцы: • **OID** (первый столбец)– позволяет выбрать значение OID, которое будет использоваться в имени субъекта; • **Источник** (второй столбец)– содержит два пункта:

Поле	Описание настроек шаблона
	– **Атрибут пользователя** – в имени субъекта будут использоваться значения атрибутов зарегистрированных в JMS ресурсных систем (каталогов учетных записей), выбранные в столбцах **OID** и **Значение**; **Примечание.** При выборе атрибута необходимо следить за тем, чтобы он относился к той ресурсной системе (каталогу учетных записей), к которой впоследствии будет привязан данный профиль выпуска сертификата. – **Константа** – позволяет вручную ввести значения в столбцах **OID** и **Значение**. • **Значение** (третий столбец)– позволяет указать значение атрибута, которое будет использоваться в имени субъекта.
Альтернативное имя субъекта (Subject Alternative Name)	Шаблон имеет следующие столбцы: • **Выбор** (первый столбец)– позволяет отметить пункт, который будут включен в альтернативное имя субъекта; • **Имя** (второй столбец)– позволяет вручную задать имя атрибута, которое будет использоваться в альтернативном имени субъекта • **Источник** (третий столбец)– содержит два пункта: – **Атрибут пользователя** – в имени субъекта будут использоваться значения атрибутов зарегистрированных в JMS ресурсных систем (каталогов учетных записей), выбранные в столбцах **OID** и **Значение**; **Примечание.** При выборе атрибута необходимо следить за тем, чтобы он относился к той ресурсной системе (каталогу учетных записей), к которой впоследствии будет привязан данный профиль выпуска сертификата. – **Константа** – позволяет вручную ввести значения в столбце **Значение**. • **Значение** (четвертый столбец) – позволяет указать значение атрибута, которое будет использоваться в альтернативном имени субъекта. Также вы можете установить флаг **Критическое расширение**, чтобы сделать данное поле критически расширением.
Политики сертификата (Certificate Policies)	Позволяет установить путём выбора из предустановленного списка политики сертификата (с их названием и OID-идентификатором). Вы также можете установить флаг **Критическое расширение**, чтобы сделать данное поле критическим расширением.

3.6.5.7 Настройки на вкладке Ключевые атрибуты пользователя

14. Перейдите на вкладку **Ключевые атрибуты пользователя**.

Отобразится следующее окно.

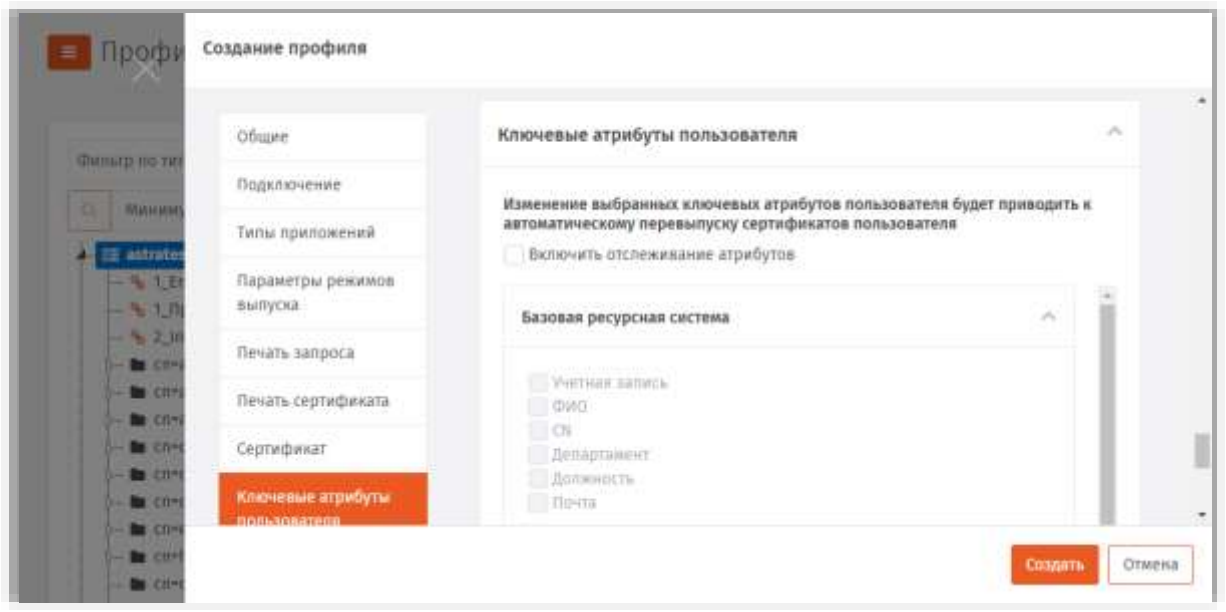


*Рис. 148 – Вкладка **Ключевые атрибуты пользователя***

15. На вкладке отображаются списки атрибутов, сгруппированных по ресурсным системам. При необходимости отметьте атрибуты пользователя, при изменении которых в ресурсной системе (внешнем каталоге учетных записей) в JMS должен быть автоматически перевыпущен сертификат пользователя в момент синхронизации его электронного ключа. Для этого выполните следующие действия:

15.1. Установите флаг **Включить отслеживание атрибутов**.
15.2. Выберите ресурсную систему (соответствующий список атрибутов).
15.3. Если все необходимые для отслеживания атрибуты располагаются в окне в отображаемой части списка, отметьте их.
15.4. В противном случае установите флаг **Показать все**, после чего раскроется список, в котором будут отражены все атрибуты пользователя из ресурсных систем, зарегистрированные в JMS. Отметьте среди них необходимые.

Примечания:

1. Отслеживание изменений в указанных на данной вкладке атрибутах пользователя реализуется при выполнении *плана обслуживания по умолчанию*, а именно задачи **Выявление рассинхронизации учетных записей из каталогов учетных записей**, см. раздел «План обслуживания по умолчанию», с. 288. Перевыпуску подлежат только сертификаты в приложении на электронном ключе, выпущенные по данному профилю. Перевыпуск сертификата (т.е. отзыв имеющегося и выпуск нового) происходит в момент синхронизации электронного ключа (см. раздел «Синхронизация ЭК/ЗНИ », с. 47).
2. **Базовая ресурсная система.** Под базовой ресурсной системой подразумевается ресурсная система, к которой будет привязан профиль для выпуска сертификатов пользователей. Таким образом перечень атрибутов, перечисленных в **Базовой ресурсной системе**, является универсальным для всех доступных в JMS ресурсных систем. Каждый атрибут из базового набора имеет отображение на соответствующий атрибут в каждой ресурсной системе (см. Табл. 31, ниже).
3. В случае если в списке ресурсных систем присутствует только **Базовая ресурсная система**, это означает, что в подключенных в JMS ресурсных системах при первоначальной настройке не было выбрано ни одного атрибута. В этом случае для выбора будут доступны только атрибуты из базового списка (Базовой ресурсной системы).
4. Для контроля изменения атрибутов допускается выбор ресурсной системы, которая будет привязана к первичной ресурсной системе. В случае изменения атрибута, выбранного в такой «привязанной» ресурсной системе, также будет производиться перевыпуск сертификата.

Табл. 31 – Схема отображения атрибутов внешних ресурсных систем на базовый список атрибутов JMS

Наименование поля в *Базовой ресурсной системе*	Имя поля в FreeIPA	Имя поля в КриптоПро УЦ 1.5	Имя поля в КриптоПро УЦ 2.0	Имя поля в JDS
Учетная запись	sAMAccountName	2.5.4.3 (CommonName)	DisplayName	AccountName
ФИО	displayName	2.5.4.3 (CommonName)	2.5.4.3 (CommonName)	FullName
CN	canonicalName	*(поле отсутствует)*	*(поле отсутствует)*	CN
Департамент	department	2.5.4.11 (OrgUnit)	2.5.4.11 (OrgUnit)	Department
Должность	title	2.5.4.12 (Title)	2.5.4.12 (Title)	Title
Почта	mail	1.2.840.113549.1.9.1 (EMail)	1.2.840.113549.1.9.1 (EMail)	Email

3.6.5.8 Прочие настройки профиля выпуска сертификатов

16. При необходимости, выполните настройку печати соответствующих документов (вкладки **Печать запроса** на сертификат и **Печать сертификата**). Подробнее о настройке **Шаблона печатной формы** см. в разделе «Настройка параметров печати при выпуске объектов JMS», с. 201.
17. Для сохранения профиля нажмите **Создать** (или **Сохранить**, если редактировался ранее созданный профиль).

3.6.6 Настройки профиля выпуска сертификатов в УЦ DogTag

1. В консоли управления JMS перейдите в раздел **Профили**.
2. Выполните одно из следующих действий:
   - чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Выпуск сертификатов - УЦ DogTag;**
   - чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.
3. В полях **Имя** и **Описание** введите (или отредактируйте) название и описание профиля соответственно.

3.6.6.1 Настройка параметров подключения

4. Перейдите на вкладку **Подключение**.
5. Выполните необходимые настройки, руководствуясь Табл. 32.

Табл. 32 – Настройка параметров подключения к удостоверяющему центру

Настройка	Описание
Секция **Настройка подключения**	
Адрес сервера FreeIPA	Укажите адрес удостоверяющего центра FreeIPA в формате: `http://<FQDN-адрес сервера FreeIPA/DogTag>` Например:

Настройка	Описание
	`http://freeipa.fqdn3.com`
Имя пользователя	Укажите имя пользователя (администратора FreeIPA), от имени которого будет осуществляться настройки в соответствии с настоящим профилем и его пароль.
Пароль	
Секция **Шаблоны сертификатов**	
Шаблон сертификата	Выберите из списка опубликованный шаблон сертификата, который будет использоваться при выпуске электронных ключей  Если вы планируете взять под контроль JMS электронные ключи, выпущенные до установки и настройки JMS, шаблон сертификата, выбранный в этой настройке, должен совпадать с шаблоном сертификата, использованным ранее для выпуска электронного ключа.

3.6.6.2 Настройки на вкладке Приложения

6. Перейдите на вкладку **Приложения**.
7. Отметьте нужные комбинации приложений.

3.6.6.3 Настройка параметров режимов выпуска сертификатов

8. Перейдите на вкладку **Параметры режимов выпуска**.
9. Выполните необходимые настройки, руководствуясь Табл. 33.

Табл. 33 – Настройка параметров выпуска сертификатов

Настройка	Описание
Секция **Параметры выпуска**	
Контейнер по умолчанию	Если этот флаг установлен, защищенный контейнер, создаваемый в памяти электронного ключа при выпуске, будет помечен в качестве контейнера по умолчанию. Настройка актуальна для Windows XP. При выполнении входа с использованием электронного ключа, если на электронном ключе более одного сертификата, система может считать только контейнер по умолчанию, остальные сертификаты игнорируются.
Резервное копирование ключевой пары и сертификата	Если флаг установлен, при выпуске электронного ключа будет создаваться резервная копия ключевой пары и сертификата в БД JMS. Если внешними средствами с электронного ключа будет удалена ключевая пара с сертификатом, то при синхронизации данные будут восстановлены на электронном ключе с помощью резервной копии на сервере.  **Примечание.** Доступность опции зависит от выбранного криптопровайдера (возможности данного криптопровайдера по экспорту ключевой пары и последующей записи ключевой пары из резервной копии в память электронного ключа заданного типа)

Настройка	Описание
Установить принудительный вход по смарт-карте для пользователей	Если флаг установлен, пользователю, на имя которого выпускается электронный ключ, будут запрещены все возможности входа в систему, кроме возможности входа с использованием смарт-карты.
Тайм-аут ожидания выпуска сертификата	Позволяет указать задержку при выпуске сертификата.
Срок хранения отозванного/обновленного сертификата на КН	Позволяет задать время, в течение которого в памяти электронного ключа будет храниться отозванный или обновленный сертификат. При этом в консоли управления данный сертификат отображается с состоянием «Сохранен на КН». Срок хранения отсчитывается от момента выпуска сертификата. При превышении срока хранения сертификат удаляется из электронного ключа и из БД JMS Значение по умолчанию: 1 год и 3 месяца
Секция **Параметры отзыва** **Важно!** Под событием «отзыв» в настройках данной секции подразумевается отзыв сертификата в JMS, который выполняется в следующих случаях: • при отзыве электронного ключа (см. «Отзыв ЭК/ЗНИ », с. 50); • при отмене привязки *профиля выпуска сертификата*, применявшегося к данному электронному ключу (см. «Привязка профилей», с. 195), в том числе и при удалении профиля; • при удалении сертификата средствами JMS (см. раздел «Операции с сертификатами», с. 26); • при отзыве сертификата (в состоянии «Выпущен на КН») на УЦ не средствами JMS (проверка отзыва сертификата обеспечивается при выполнении планов обслуживания).	
Публиковать CRL после отзыва	Если флаг установлен, после отзыва в JMS электронного ключа/сертификата на сервере удостоверяющего центра будет публиковаться список отозванных сертификатов (CRL).
Отзывать сертификат в УЦ	Если флаг установлен, то сертификат, выпущенный на электронном ключе, который был впоследствии отозван в JMS, будет также отозван в УЦ (центре сертификации Microsoft).
Удалять ключевой контейнер отзываемого сертификата	Если флаг установлен, то при отзыве электронного ключа (или сертификата) из памяти электронного ключа будет удален ключевой контейнер, созданный при выпуске по данному профилю. (Электронный ключ для этого должен быть подсоединен к компьютеру во время процедуры отзыва или синхронизации). Если флаг не установлен, то при отзыве сертификат из электронного ключа не удаляется, а в консоли управления сертификат отображается с состоянием «Сохранен на КН».
Секция **Параметры обновления**	
Обновлять сертификат с истекающим сроком действия	Позволяет обновлять сертификат, срок действия которого скоро истечет.
Режим обновления	Позволяет выбрать режим обновления сертификатов с истекшим сроком действия. Доступны следующие настройки: • **Существующая ключевая пара** – для обновления сертификата будет использована существующая ключевая пара;

Настройка	Описание
	• **Новая ключевая пара** – для обновления сертификата будет сгенерирована новая ключевая пара. Эта настройка активна, только если установлен флаг **Обновлять сертификат с истекшим сроком действия**.
Количество дней до окончания срока действия	Позволяет указать, за сколько дней до истечения срока действия можно обновить сертификат. Эта настройка активна, только если установлен флаг **Обновлять сертификат с истекшим сроком действия**.
Отзывать заменяемый сертификат в УЦ	Если этот флаг установлен, заменяемый сертификат будет отозван центром сертификации. Эта настройка активна, только если установлен флаг **Обновлять сертификат с истекшим сроком действия**.
Удалять ключевой контейнер заменяемого сертификата	Если флаг установлен, то при замене сертификата из памяти электронного ключа будет удален ключевой контейнер (электронный ключ для этого должен быть подсоединен к компьютеру) заменяемого сертификата. Если флаг не установлен, то из электронного ключа сертификат не удаляется, а в консоли управления он отображается с состоянием «Сохранен на КН». Данный флаг доступен для изменения только при режиме обновления с новой ключевой парой (см. параметр **Режим обновления**) и произвольно генерируемом имени ключевого контейнера (см. описание вкладки **Ключевой контейнер**).

3.6.6.4 Настройка параметров ключевого контейнера

10. Перейдите на вкладку **Ключевой контейнер**.
11. Выполните необходимые настройки, руководствуясь Табл. 34.

Табл. 34 – Настройки ключевого контейнера

Настройка	Описание
Секция **Параметры криптографии**	
Криптопровайдер для генерации ключевой пары	Выберите в этом списке поставщика криптографии, с помощью которого будут формироваться ключевые пары. (Чтобы появиться в списке доступных соответствующий криптопровайдер должен быть установлен на сервере JMS.) **Примечание.** Список доступных поставщиков криптографии зависит от комбинации приложений, выбранных на вкладке **Приложения**. В случае если выбранные приложения не имеют общих поддерживающих их поставщиков криптографии, список будет пустым.

Настройка	Описание
Алгоритм для генерации ключевой пары	Выберите алгоритм для генерации ключевой пары. Список алгоритмов зависит выбранного поставщика криптографии, например, в случае выбора *Aladdin GOST PKCS11 Cryptographic Provider* для приложения (на электронном ключе) *ГОСТ 2* появляется возможность выбора алгоритмов ГОСТ 34.10-2001 или ГОСТ 34.10-2012. **Примечания:** 1. Список доступных алгоритмов зависит от комбинации приложений, выбранных на вкладке **Приложения** и содержит только алгоритмы, поддерживаемые одновременно всеми выбранными приложениями. 2. Для выпуска сертификата открытого ключа, сгенерированного по алгоритму ГОСТ 34.10-2012 необходимо обеспечить, наличия на стороне УЦ поставщика криптографии с поддержкой данного алгоритма (например, КриптоПро CSP 4.0).
Применять PIN-код подписи	При необходимости установите признак обязательности применения пользователем PIN-кода подписи. **Примечания:** 1. Настройка действует только в приложениях ГОСТ 2 на электронных ключах JaCarta. 2. Настройка применяется только к ключевому контейнеру (а значит и к закрытому ключу), созданному при выпуске данного электронного ключа. 3. При установке данного признака, в процессе выпуска электронного ключа у пользователя будет запрошен PIN-код подписи с целью его установки.
Секция **Применение и размер ключа**	
Key Exchange (Обмен ключами)	Позволяет указать основное применение ключа.
Digital Signature (Цифровая подпись)	
Размер ключа	Укажите размер ключей, которые будут формироваться на основе используемого профиля.
Секция **Ключевой контейнер**	
Сгенерировать произвольное имя	Если выбран этот пункт, то для ключевых контейнеров, созданных на основе этого профиля, будет сгенерировано случайное имя.
Использовать название профиля	Если выбран этот пункт, то для ключевых контейнеров, созданных на основе этого профиля, будет использоваться имя этого профиля. **Важно!** При установке данной опции убедитесь, что используемые в названии профиля символы и его синтаксис поддерживаются соответствующим криптопровайдером
Использовать существующий контейнер	Если выбран этот пункт, при выпуске электронных ключей ключевая пара будет записываться в существующий контейнер.

Настройка	Описание
Использовать указанное имя	Позволяет задать имя, которым будут названы ключевые контейнеры, выпущенные с использованием этого профиля.  **Важно!** При задании имени контейнера вручную убедитесь, что используемые символы и синтаксис имени поддерживается соответствующим криптопровайдером

3.6.6.5 Настройки на вкладке Ключевые атрибуты

12. Перейдите на вкладку **Ключевые атрибуты**.
13. На вкладке отображаются раскрывающиеся списки атрибутов, сгруппированных по ресурсным системам. При необходимости отметьте атрибуты пользователя, при изменении которых в ресурсной системе (внешнем каталоге учетных записей) в JMS должен быть автоматически перевыпущен сертификат пользователя в момент синхронизации его электронного ключа. Для этого выполните следующие действия:

13.1. Установите флаг **Включить отслеживание атрибутов**.
13.2. Выберите ресурсную систему, чтобы раскрылся соответствующий список атрибутов.
13.3. Если все необходимые для отслеживания атрибуты располагаются в окне в отображаемой части списка, отметьте их.
13.4. В противном случае установите флаг **Показать все атрибуты**, после чего заново раскройте список, в котором будут отражены все атрибуты пользователя из ресурсных систем, зарегистрированные в JMS. Отметьте среди них необходимые.

Примечания:

1. Отслеживание изменений в указанных на данной вкладке атрибутах пользователя реализуется при выполнении *плана обслуживания по умолчанию*, а именно задачи **Выявление рассинхронизации учетных записей из каталогов учетных записей**, см. раздел «План обслуживания по умолчанию», с. 288. Перевыпуску подлежат только сертификаты в приложении на электронном ключе, выпущенные по данному профилю. Перевыпуск сертификата (т.е. отзыв имеющегося и выпуск нового) происходит в момент синхронизации электронного ключа (см. раздел «Синхронизация ЭК/ЗНИ », с. 47).
2. **Базовая ресурсная система.** Под базовой ресурсной системой подразумевается ресурсная система, к которой будет привязан профиль для выпуска сертификатов пользователей. Таким образом перечень атрибутов, перечисленных в **Базовой ресурсной системе**, является универсальным для всех доступных в JMS ресурсных систем. Каждый атрибут из базового набора имеет отображение на соответствующий атрибут в каждой ресурсной системе (см. Табл. 35, ниже).
3. В случае если в списке ресурсных систем присутствует только **Базовая ресурсная система**, это означает, что в подключенных в JMS ресурсных системах при первоначальной настройке не было выбрано ни одного атрибута. В этом случае для выбора будут доступны только атрибуты из базового списка (Базовой ресурсной системы).
4. Для контроля изменения атрибутов допускается выбор ресурсной системы, которая будет привязана к первичной ресурсной системе. В случае изменения атрибута, выбранного в такой «привязанной» ресурсной системе, также будет производиться перевыпуск сертификата.

Табл. 35 – Схема отображения атрибутов внешних ресурсных систем на базовый список атрибутов JMS

Наименование поля в *Базовой ресурсной системе*	Имя поля в FreeIPA	Имя поля в КриптоПро УЦ 1.5	Имя поля в КриптоПро УЦ 2.0	Имя поля в JDS
Учетная запись	sAMAccountName	2.5.4.3 (CommonName)	DisplayName	AccountName
ФИО	displayName	2.5.4.3 (CommonName)	2.5.4.3 (CommonName)	FullName
Департамент	department	2.5.4.11 (OrgUnit)	2.5.4.11 (OrgUnit)	Department
Должность	title	2.5.4.12 (Title)	2.5.4.12 (Title)	Title

Почта	mail	1.2.840.113549.1.9.1 (EMail)	1.2.840.113549.1.9.1 (EMail)	Email
Внешний ID	objectSid	UserID	UserID	UID
CN	canonicalName	*(поле отсутствует)*	*(поле отсутствует)*	CN
Описание	description	*(поле отсутствует)*	*(поле отсутствует)*	Description

3.6.6.6 Прочие настройки профиля выпуска сертификатов

14. При необходимости, выполните настройку печати соответствующих документов (вкладки **Печать запроса** на сертификат и **Печать сертификата**). Подробнее о настройке **Шаблона печатной формы** см. в разделе «Настройка параметров печати при выпуске объектов JMS», с. 201.
15. Для сохранения профиля нажмите **Создать** (или **Сохранить**, если редактировался ранее созданный профиль).

3.6.7 Настройки профиля для выпуска сертификатов в режиме офлайн

Профиль **Выпуск сертификатов (режим офлайн)** становится доступен в консоли управления JMS после установки специального компонента JMS «Коннектор к Offline Certification Authority», позволяющего выпускать сертификаты пользователей в аккредитованных удостоверяющих центрах, не имеющих сетевого подключения к телекоммуникационным сетям общего пользования.

Для начала работы с профилем **Выпуск сертификатов (режим офлайн)** выполните следующие действия.

16. В консоли управления JMS перейдите в раздел **Профили**.
17. Выполните одно из следующих действий:

- чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Выпуск сертификатов (режим офлайн)**.
- чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

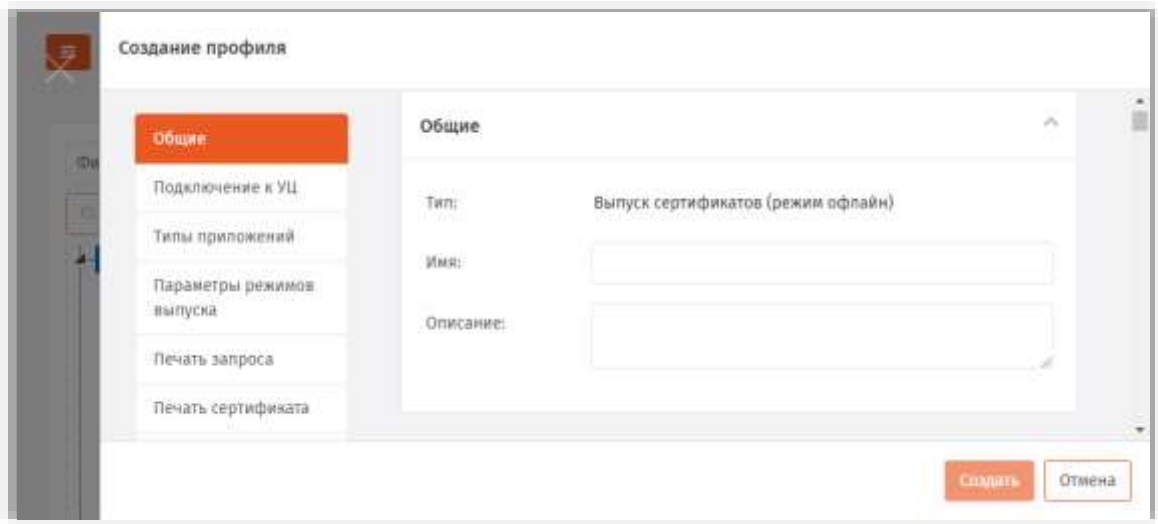


*Рис. 149 – Вкладка **Общие** профиля выпуска сертификатов*

18. В полях **Имя** и **Описание** введите (или отредактируйте) название и описание профиля соответственно.

3.6.7.1 Настройка параметров подключения к УЦ

19. Перейдите на вкладку **Подключение к УЦ**.
Окно примет следующий вид.

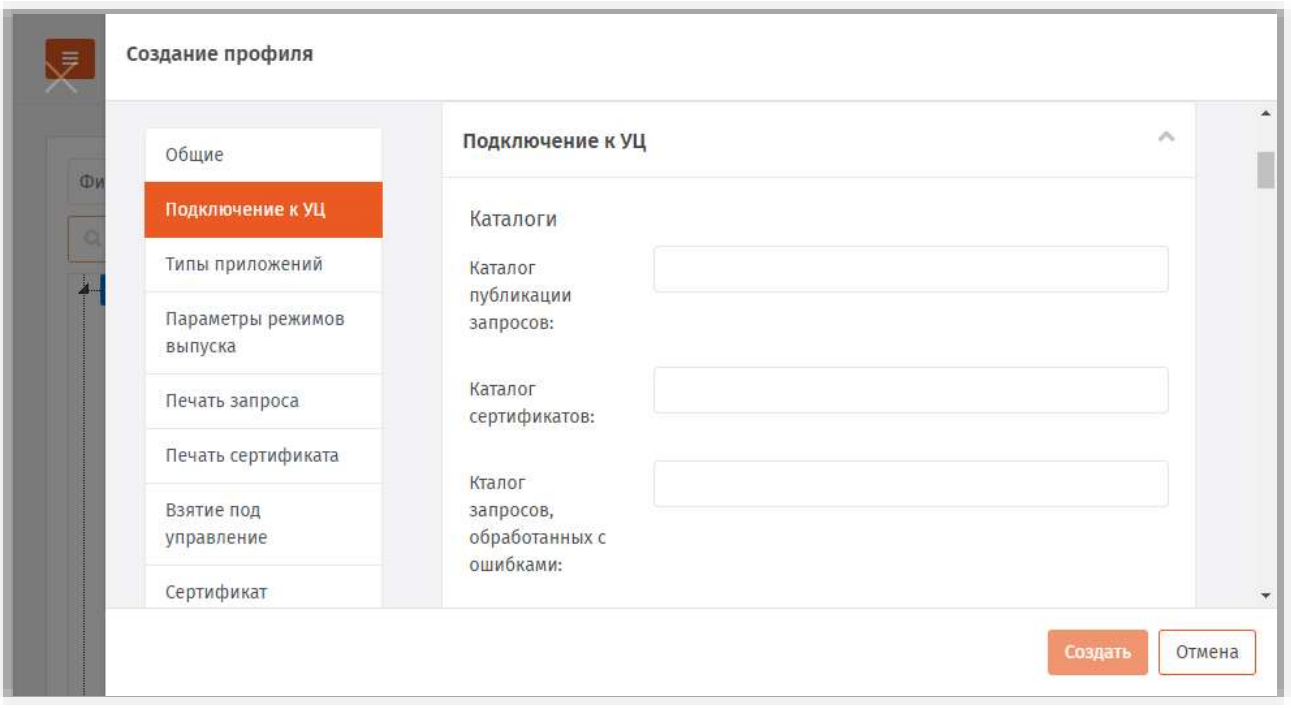


*Рис. 150 – Вкладка **Подключение к УЦ** профиля выпуска сертификатов*

20. Выполните необходимые настройки, руководствуясь Табл. 36.

Табл. 36 – Настройка параметров подключения к удостоверяющему центру

Настройка	Описание
Секция **Каталоги**	
Каталог публикации запросов	Укажите локальную или сетевую папку, в которую должны сохраняться запросы на сертификат. **Примечание.** Сервер JMS должен иметь права на запись, изменения и чтения для данной папки.
Каталог сертификатов	Укажите локальную или сетевую папку, в которой при попытке синхронизации КН со стороны JMS будет происходить поиск готовых сертификатов (заполняется со стороны УЦ). **Примечание.** Сервер JMS должен иметь права на запись, изменения и чтения для данной папки.

Настройка	Описание
Каталог запросов, обработанных с ошибками	Укажите локальную или сетевую папку, в которую должны помещаться (со стороны УЦ) запросы на сертификат, которые были отклонены.  **Примечание.** Сервер JMS должен иметь права на запись, изменения и чтения для данной папки.
Секция **Очистка каталогов**	
Удалять обработанные сертификаты из каталога	Установите флаг, если сертификаты после их успешной обработки (выпуска на КН в момент синхронизации последнего) должны быть удалены.
Удалять обработанные запросы из каталога	Установите флаг, если необходимо удалять запросы на сертификаты после успешной обработки полученных по ним сертификатов (выпуска на КН) из соответствующей папки.
Удалять запросы с ошибками из каталога после обработки	Установите флаг, если необходимо удалять отклоненные запросы на сертификат в случае, если данные отклоненные запросы были обработаны (по факту получения отказа в выпуске сертификата пользователю было выслано уведомление, ключевая пара удалена из памяти электронного ключа).
Секция **Именование запросов на сертификат**	
Генерировать случайное имя (GUID)	Выберите данную опцию, если для идентификации запроса необходимо использовать случайно сгенерированный идентификатор (GUID)
Использовать шаблон	Выберите данную опцию, если для идентификации запроса необходимо сформировать его имя с помощью шаблона, формируемого в поле **Шаблон**. Для создания шаблона последовательно выберите в поле **Макропеременные** несколько или все выпадающие значения. Для выбора доступны значения: • %AccountName% — Имя аккаунта; • %FullName% — Полное имя пользователя; • %Mail% — Почтовый адрес; • %Date% — Текущая дата (ДД-ММ-ГГГГ); • %Time% — Текущее время (ЧЧ-ММ-СС). Выбранные переменные будут подставлены в шаблон.
Секция **Расширение кодировки**	
Формат	Выберите формат, в котором должны сохраняться в папку запросы на сертификаты. В текущей версии JMS доступны следующие форматы: • .p10 (DER) • .p10 (Base 64) • .cmc (Base 64) • .req (DER) • .req (Base 64) • .pem (Base 64) • .der (DER) • .dat (Base 64) • .csr (Base 64)

Настройка	Описание
Добавлять заголовок	В случае если в поле **Формат** выбрана кодировка *Base64*, то для данной кодировки доступна возможность добавления заголовка в тело запроса на сертификат. При установке флага, такой заголовок будет добавлен

3.6.7.2 Настройки на вкладке Типы приложений

21. Перейдите на вкладку **Типы приложений**, выполните настройки по аналогии с настройкой вкладки **Типы приложений** профиля выпуска сертификатов в центре сертификации Microsoft (см. раздел «Настройки на вкладке Типы приложений», с. 129).

3.6.7.3 Настройка параметров режимов выпуска сертификатов

22. Перейдите на вкладку **Параметры режимов выпуска**.
Окно будет выглядеть следующим образом.

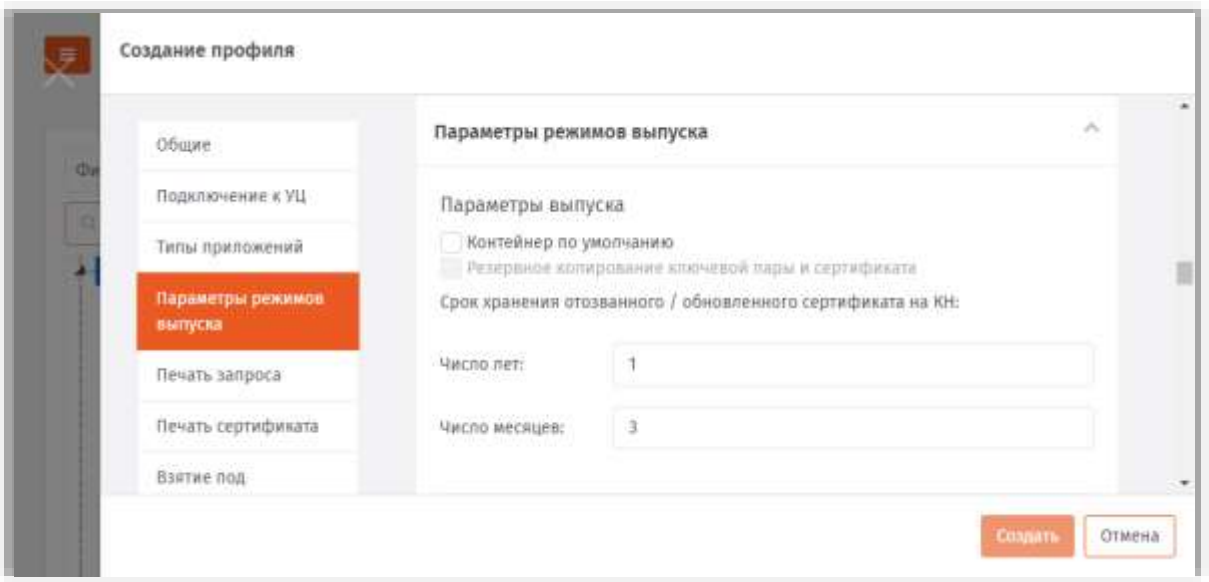


*Рис. 151 – Вкладка **Параметры режимов выпуска** профиля выпуска сертификатов*

23. Выполните необходимые настройки, руководствуясь Табл. 37.

Табл. 37 – Настройка параметров выпуска сертификатов

Секция	Настройка	Описание
Параметры выпуска	**Контейнер по умолчанию**	Если этот флаг установлен, защищенный контейнер, создаваемый в памяти электронного ключа при выпуске, будет помечен в качестве контейнера по умолчанию. Настройка актуальна для Windows XP. При выполнении входа с использованием электронного ключа, если на электронном ключе более одного сертификата, система может считать только контейнер по умолчанию, остальные сертификаты игнорируются.

Секция	Настройка	Описание
	Резервное копирование ключевой пары и сертификата	Если флаг установлен, при выпуске электронного ключа будет создаваться резервная копия ключевой пары и сертификата в БД JMS. Если внешними средствами с электронного ключа будет удалена ключевая пара с сертификатом, то при синхронизации данные будут восстановлены на электронном ключе с помощью резервной копии на сервере. **Примечание.** Доступность опции зависит от выбранного криптопровайдера (возможности данного криптопровайдера по экспорту ключевой пары и последующей записи ключевой пары из резервной копии в память электронного ключа заданного типа)
	Срок хранения отозванного/обновленного сертификата на КН	Позволяет задать время, в течение которого в памяти электронного ключа будет храниться отозванный или обновленный сертификат. При этом в консоли управления данный сертификат отображается с состоянием «Сохранен на КН». Срок хранения отсчитывается от момента выпуска сертификата. При превышении срока хранения сертификат удаляется из электронного ключа и из БД JMS Значение по умолчанию: 1 год и 3 месяца
Параметры отзыва	**Важно!** Под событием «отзыв» в настройках данной секции подразумевается отзыв сертификата в JMS, который выполняется в следующих случаях: • при отзыве электронного ключа (см. «Отзыв ЭК/ЗНИ », с. 50); • при отмене привязки *профиля выпуска сертификата*, применявшегося к данному электронному ключу (см. «Привязка профилей», с. 195), в том числе и при удалении профиля.	
	Удалять ключевой контейнер отзываемого сертификата	Если флаг установлен, то при отзыве электронного ключа (или сертификата) из памяти электронного ключа будет удален ключевой контейнер, созданный при выпуске по данному профилю. (Электронный ключ для этого должен быть подсоединен к компьютеру во время процедуры отзыва или синхронизации). Если флаг не установлен, то при отзыве сертификат из электронного ключа не удаляется, а в консоли управления сертификат отображается с состоянием «Сохранен на КН».
Параметры обновления	**Обновлять сертификат с истекающим сроком действия**	Позволяет обновлять сертификат, срок действия которого скоро истечет.
	Режим обновления	Позволяет выбрать режим обновления сертификатов с истекшим сроком действия. Доступны следующие настройки: • **Новая ключевая пара** – для обновления сертификата будет сгенерирована новая ключевая пара. Эта настройка активна, только если установлен флаг **Обновлять сертификат с истекшим сроком действия**.

Секция	Настройка	Описание
	Количество дней до окончания срока действия	Позволяет указать, за сколько дней до истечения срока действия можно обновить сертификат. Эта настройка активна, только если установлен флаг **Обновлять сертификат с истекшим сроком действия**.

3.6.7.4 Настройка параметров ключевого контейнера

24. Перейдите в секцию **Ключевой контейнер** выполните настройки по аналогии с настройкой параметров секции **Ключевой контейнер** профиля выпуска сертификатов в центре сертификации Microsoft (см. раздел «Настройка параметров ключевого контейнера», с. 132).

3.6.7.5 Настройка шаблонов полей сертификата

25. Перейдите на вкладку **Сертификат**.
Отобразится следующее окно.

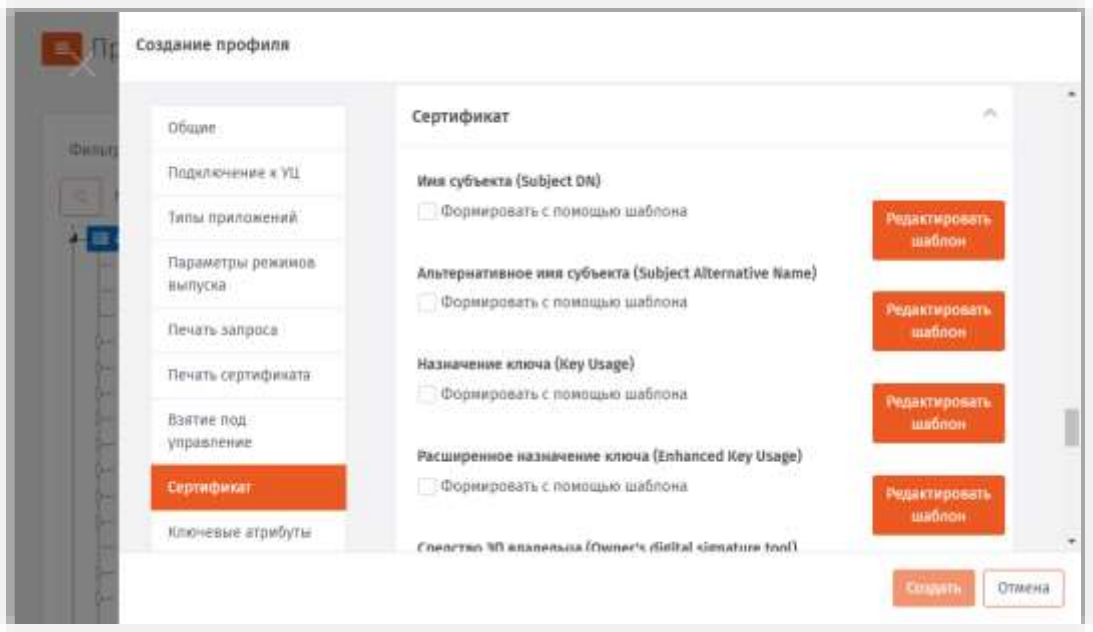


*Рис. 152 – Вкладка **Сертификат***

26. При необходимости отредактируйте поля сертификата (запроса на сертификат), который будет выпускаться на имя пользователей. Для этого выполните следующие действия:

26.1. В секции с названием нужного поля нажмите **Редактировать шаблон**;
26.2. Отредактируйте шаблон, руководствуясь сведениями, представленными в Табл. 38, с. 150.
26.3. В окне редактирования шаблона нажмите **ОК**, чтобы сохранить изменения.
26.4. В секции с названием нужного поля установите флаг **Формировать с помощью шаблона**.
26.5. При необходимости повторите действия для других полей.

Табл. 38 – Настройка шаблонов полей сертификата

Поле	Описание настроек шаблона
Имя субъекта (Subject DN)	Шаблон имеет следующие столбцы: • **OID** – позволяет выбрать значение OID, которое будет использоваться в имени субъекта; • **Источник** – содержит два пункта: – **Атрибут пользователя** – в имени субъекта будут использоваться значения из КриптоПро УЦ, выбранные в столбцах **OID** и **Значение**; – **Константа** – позволяет вручную ввести значения в столбцах **OID** и **Значение**. • **Значение** – позволяет указать значение атрибута, которое будет использоваться в имени субъекта.
Альтернативное имя субъекта (Subject Alternative Name)	Шаблон имеет следующие столбцы: • **Выбор** – позволяет отметить пункт, который будут включен в альтернативное имя субъекта; • **Имя** – позволяет вручную задать имя атрибута, которое будет использоваться в альтернативном имени субъекта • **Источник** – содержит два пункта: – **Атрибут пользователя** – в имени субъекта будут использоваться значения из КриптоПро УЦ, выбранные в столбце **Значение**; – **Константа** – позволяет вручную ввести значения в столбце **Значение**. • **Значение** – позволяет указать значение атрибута, которое будет использоваться в альтернативном имени субъекта. Также вы можете установить флаг **Критическое расширение**, чтобы сделать данное поле критически расширением.
Назначение ключа (Key Usage)	Позволяет выбрать назначение ключа, доступны следующие пункты: • **Цифровая подпись (Digital Signature)**; • **Подтверждение подлинности (Non Repudiation)**; • **Шифрование ключей (Key Encipherment)**; • **Шифрование данных (Data Encipherment)**; • **Согласование ключей (Key agreement)**; • **Подписание сертификатов (Certificate signing)**; • **Подписание списка отзыва сертификатов (CRL signing)**; • **Только шифрование (Encipher Only)** – доступно, только если выбран пункт **Согласование ключей (Key agreement)**; • **Только расшифрование (Decipher Only)** - доступно, только если выбран пункт **Согласование ключей (Key agreement)**.
Расширенное использование ключа (Enhanced Key Usage)	Позволяет задать в списке варианты расширенного использования ключа. Вы также можете установить флаг **Критическое расширение**, чтобы сделать данное поле критическим расширением.

Поле	Описание настроек шаблона
Средство ЭП владельца (Owner's digital signature tool)	Позволяет ввести название средства электронной подписи владельца электронного ключа. Вы также можете установить флаг **Критическое расширение**, чтобы сделать данное поле критическим расширением.
Политики сертификата (Certificate Policies)	Позволяет ввести названия политик сертификата. Вы также можете установить флаг **Критическое расширение**, чтобы сделать данное поле критическим расширением.

3.6.7.6 Настройки на вкладке Ключевые атрибуты

27. Перейдите на вкладку **Ключевые атрибуты**, выполните настройки по аналогии с настройкой параметров на вкладке **Ключевые атрибуты** профиля выпуска сертификатов в центре сертификации Microsoft (см. раздел «Настройки на вкладке Ключевые атрибуты», с. 136).

3.6.7.7 Прочие настройки профиля выпуска сертификатов

28. При необходимости, выполните настройку печати соответствующих документов (вкладки **Печать запроса** на сертификат и **Печать сертификата**). Подробнее о настройке **Шаблона печатной формы** см. в разделе «Настройка параметров печати при выпуске объектов JMS», с. 201.
29. Нажмите **ОК**, чтобы сохранить изменения.

3.6.8 Создание и настройка профиля Внешние объекты

1. В консоли управления JMS перейдите в раздел **Профили**.
2. Выполните одно из следующих действий:

   – чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Внешние объект** (Рис. 153);
   – чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

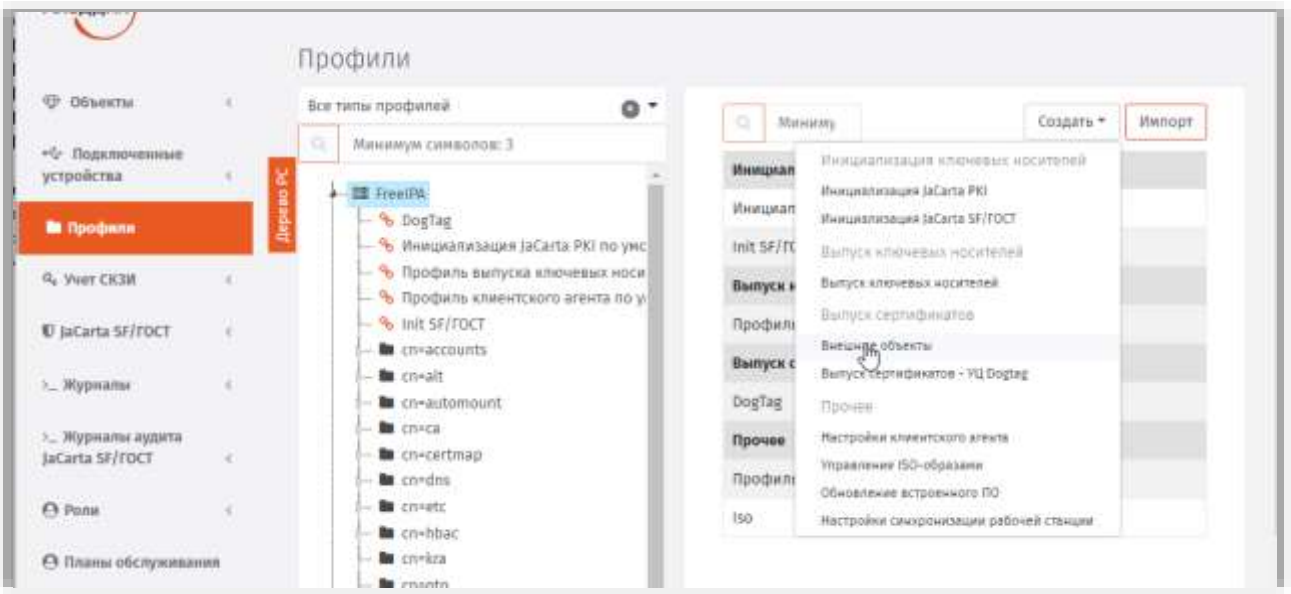


Рис. 153 – Создание профиля внешнего объекта

3. В полях **Имя** и **Описание** введите (или отредактируйте) название и описание профиля соответственно.
4. На вкладке **Общие** и заполните поле **Имя:**

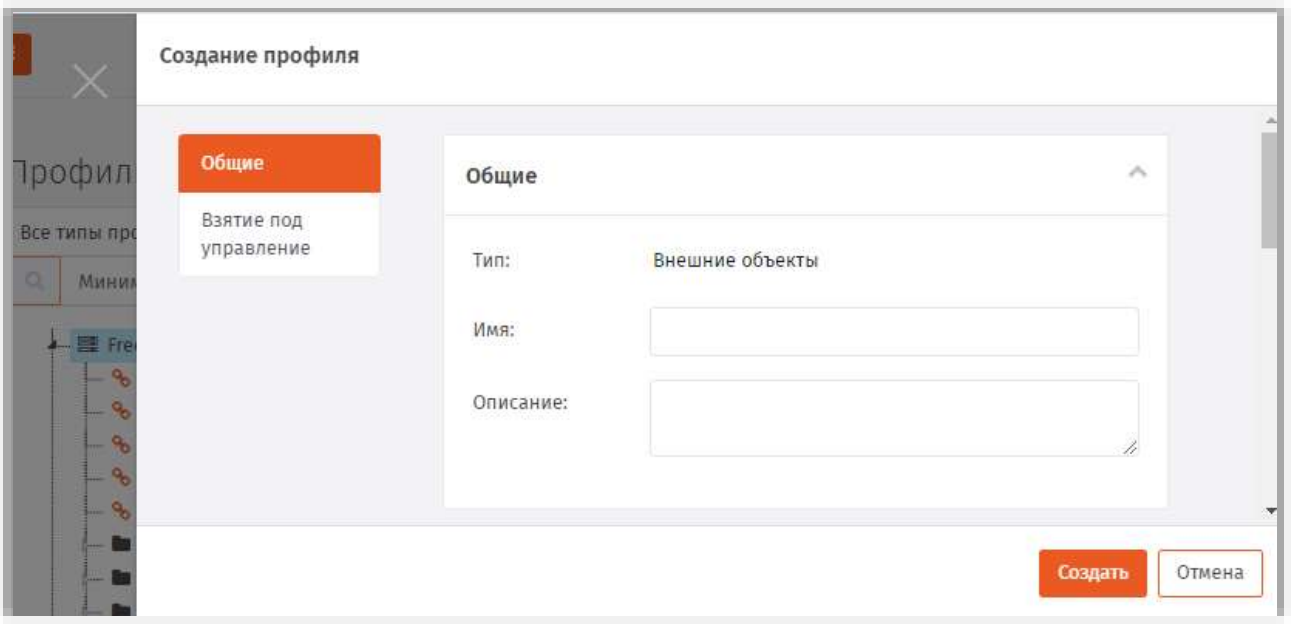


Рис. 154 – Вкладка Общие на странице Создание профиля

5. Перейдите на вкладку **Взятие под управление.**

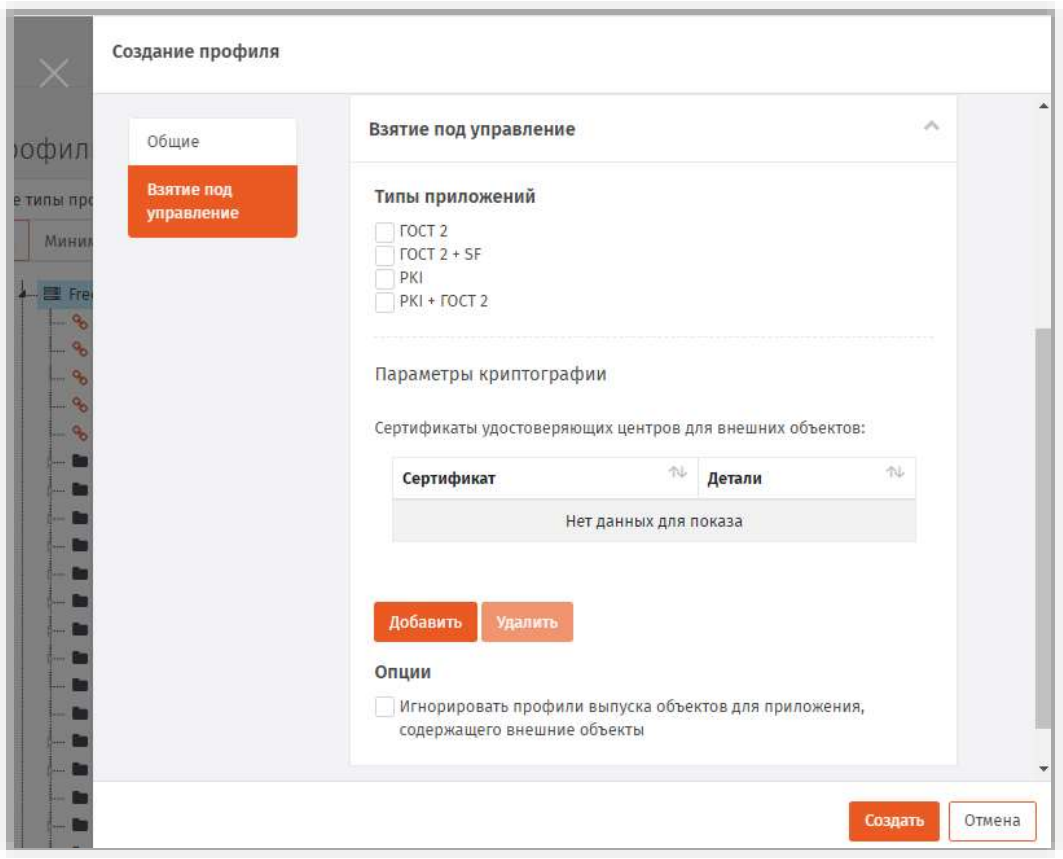


*Рис. 155 – Вкладка **Взятие под управление***

6. Отметьте нужные приложения (типы электронных ключей) или их комбинации, в которых следует проверять на наличие внешних объектов (сертификатов).

Примечание. При выборе комбинации приложений необходимо согласовать такую комбинацию с настройками в секции **Параметры криптографии** таким образом, чтобы у всех выбранных приложений имелся хотя бы один общий поставщик криптографии, поддерживаемый данными приложениями (как на Рис. 156). Если у выбранных типов приложений не будет общих поддерживающих криптопрова йдеров, то в секции отобразится соответствующее сообщение (*«Нет доступных криптопровайдеров для выбранной комбинации апплетов»*).

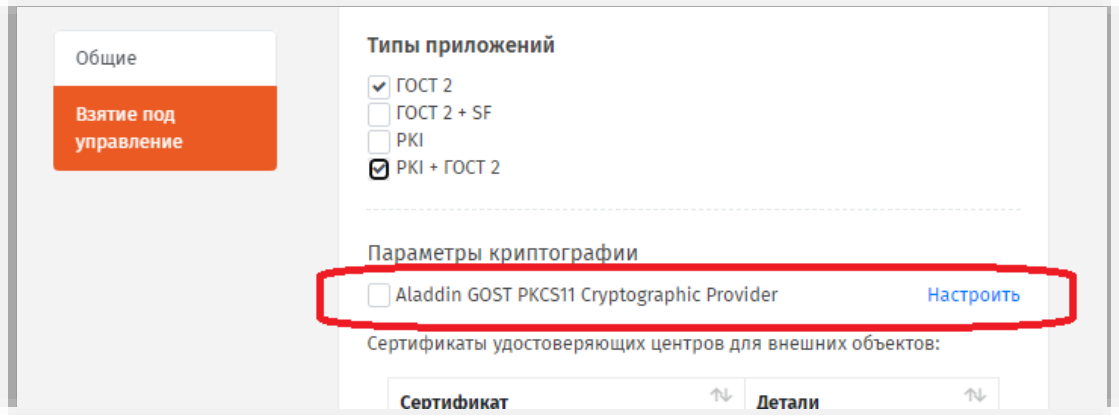


Рис. 156 – Общий криптоарофайдер у двух выбранных типов приложений

7. В секции (таблице) **Сертификаты удостоверяющих центров для внешних объектов** (Рис. 155, выше) загрузите список сертификатов УЦ, которые могут быть необходимы для дополнительной фильтрации сертификатов (т.е. регистрации в качестве внешних объектов только тех сертификатов, которые были выпущены данными УЦ). Для этого нажмите **Добавить** и в окне выбора файлов добавьте необходимые файлы сертификатов. (Для удаления сертификата из таблицы, выберите сертификат в таблице и нажмите **Удалить**). Добавление сертификатов УЦ не является обязательным действием.

Примечание. Чтобы отбор сертификатов для их регистрации в качестве внешних объектов по признаку их выпуска указанным УЦ сработал корректно, необходимо предварительно сохранить на сервер JMS сертификат корневого УЦ и цепочку сертификатов УЦ (см. раздел «Регистрация в JMS сертификатов сторонних УЦ (внешних объектов)», с. 306).

8. Опция **Игнорировать профили выпуска объектов для приложения, содержащего внешние объекты** при ее выборе позволяет не выпускать сертификаты DogTag и т.п. для записи в те приложения электронного ключа, которые содержат внешние объекты.
9. После добавления сертификатов УЦ следует выполнить настройку отмеченных криптопровайдеров. Для этого в секции **Параметры криптографии** напротив соответствующего криптопровайдера нажмите **Настроить** (Рис. 156, выше).
10. Откроется страница настройки работы с сертификатами УЦ, ассоциированными с данным криптопровайдером:

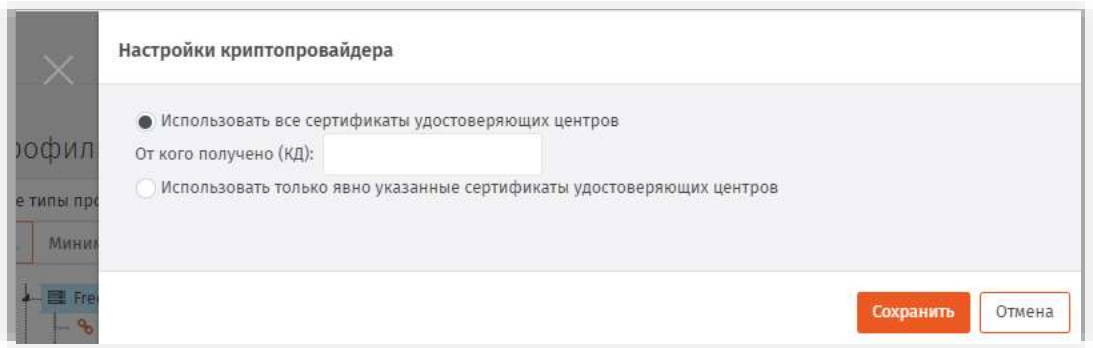


*Рис. 157 – Страница **Настройки криптопровайдера***

11. Выполните необходимые настройки, руководствуясь Табл. 39.

Табл. 39 – Настройка отбора внешних объектов по выпускающим УЦ

Настройка	Описание
Использовать все сертификаты удостоверяющих центров	При выборе данной опции в качестве внешних объектов в JMS будут зарегистрированы все сертификаты на электронном ключе (при условии успешной проверки их подписей), выпущенные УЦ, чьи сертификаты были добавлены на вкладке **Взятие под управление**
От кого получено (КД)	Наименование организции, от которой получен сертификат, регистрируемый в JMS в качестве внешнего объекта. Значение поля используется в нормативных документах СКЗИ. (Необязательное поле) **Примечание.** Поле доступно только в настройках криптопровайдеров российских производителей
Использовать только явно указанные сертификаты удостоверяющих центров	При выборе данной опции в качестве внешних объектов в JMS будут зарегистрированы только сертификаты (при условии успешной проверки их подписей), выпущенные удостоверяющими центрами, чьи сертификаты будут отмечены в нижележащем списке. При этом для каждого сертификата УЦ в столбце **От кого получено (КД)** можно заполнить наименование организации, от которой получен сертификат, регистрируемый в JMS в качестве внешнего объекта. (Столбец доступен только в настройках криптопровайдеров российских производителей)

12. После настройки всех криптопровайдеров в окне настройки профиля нажмите **Сохранить** (Рис. 155, выше) и переходите к привязке профиля (подробнее см. раздел «Привязка профилей», с. 195).

Важно! Регистрация сертификата в качестве внешнего объекта на основании настроенного профиля производится в соответствии с описанием из раздела «Процедура автоматической регистрации внешних объектов», ниже.

3.6.8.1 Процедура автоматической регистрации внешних объектов

Регистрация внешних объектов (сертификатов) осуществляется в автоматическом режиме в процессе выпуска (синхронизации) электронного ключа в соответствии с подключенным профилем типа **Внешние объекты**. Если на электронном ключе находится сертификат, выпущенный сторонним УЦ, и у пользователя электронного ключа подключен профиль внешних объектов, применимый для приложения на данном электронном ключе, то распознавание данного сертификата и его регистрация в качестве внешнего объекта происходит в следующем порядке:

1. Выбирается первый поставщик криптографии, отмеченный в настройках профиля внешних объектов (вкладка **Взятие под управление**);
2. Выполняется попытка распознавания сертификата данным поставщиком криптографии.
3. Если сертификат был распознан поставщиком криптографии, то проверяется, не выпущен ли данный сертификат одним из УЦ, выбранным в настройках данного поставщика криптографии.

3.1. Если список сертификатов УЦ для данного поставщика криптографии пуст, то сертификат регистрируется в JMS как внешний объект.

3.2. В противном случае проверяется подпись сертификата на электронном ключе (с помощью сертификата УЦ с проверкой цепочки сертификатов), при этом игнорируются срок действия сертификата и списки отзыва сертификатов.

3.2.1. При положительном результате проверки данный сертификат на электронном ключе регистрируется как внешний объект.
3.2.2. В противном случае данный сертификат игнорируется.

4. Если сертификат не был распознан поставщиком криптографии, то он игнорируется.
5. Если поставщиков криптографии больше не осталось, процедура завершается.
6. В противном случае, выбирается следующий поставщик криптографии и выполняется шаг. 2.

3.6.9 Профиль настройки синхронизации рабочей станции

Важно! В текущей версии JMS настройки профиля действуют только для вкладки **Открытие сессии пользователя** (настройка **Открывать сессию под текущей доменной учётной записью**). Настройки остальных вкладок не реализованы.

Примечание. Вступление в силу данного профиля на рабочей станции наступает либо при его автоматической загрузке (выполняется раз в сутки), либо при перезагрузке рабочей станции с установленным клиентским агентом JMS.

Для создания / редактирования профиля выполните следующие действия

1. В консоли управления JMS перейдите в раздел **Профили**.
2. Выполните одно из следующих действий:

   – чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Настройки синхронизации рабочих станций** (Рис. 153);
   – чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

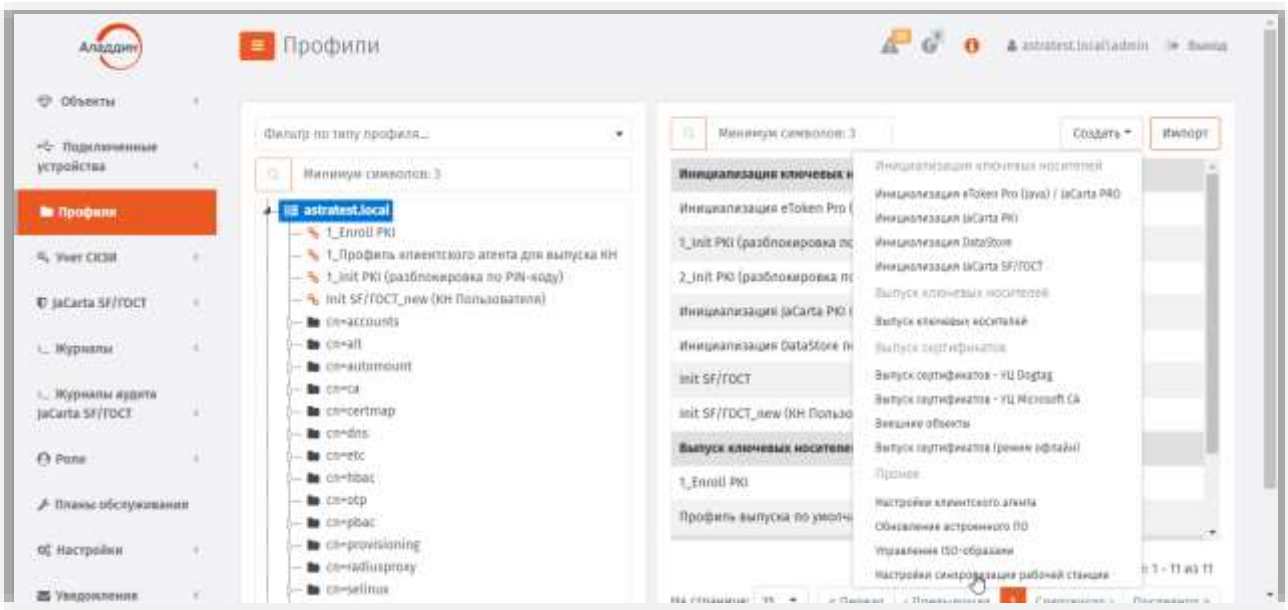


Рис. 158 – Создание профиля настройки синхронизации рабочей станции

3. Отобразится страница следующего вида.

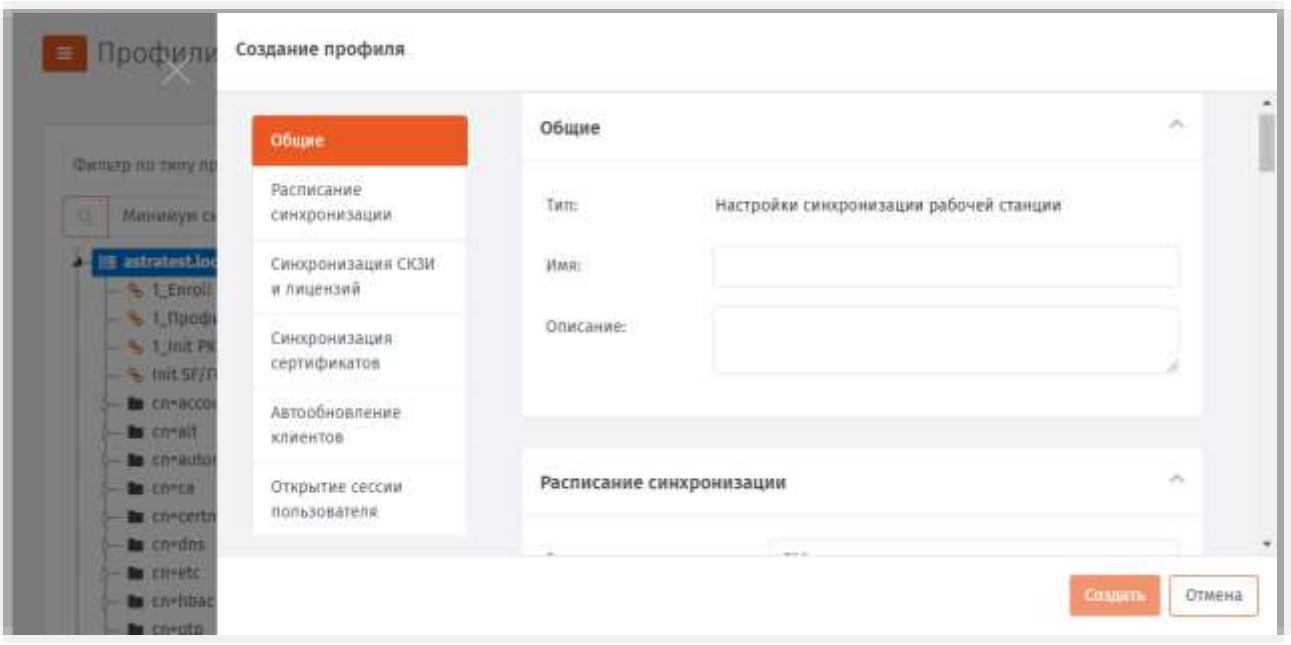


Рис. 159 – Вкладка Общие на странице Создание профиля

4. В полях **Имя** и **Описание** введите (или отредактируйте) название и описание профиля соответственно.
5. Перейдите на вкладку **Открытие сессии пользователя**.
   Страница примет следующий вид.

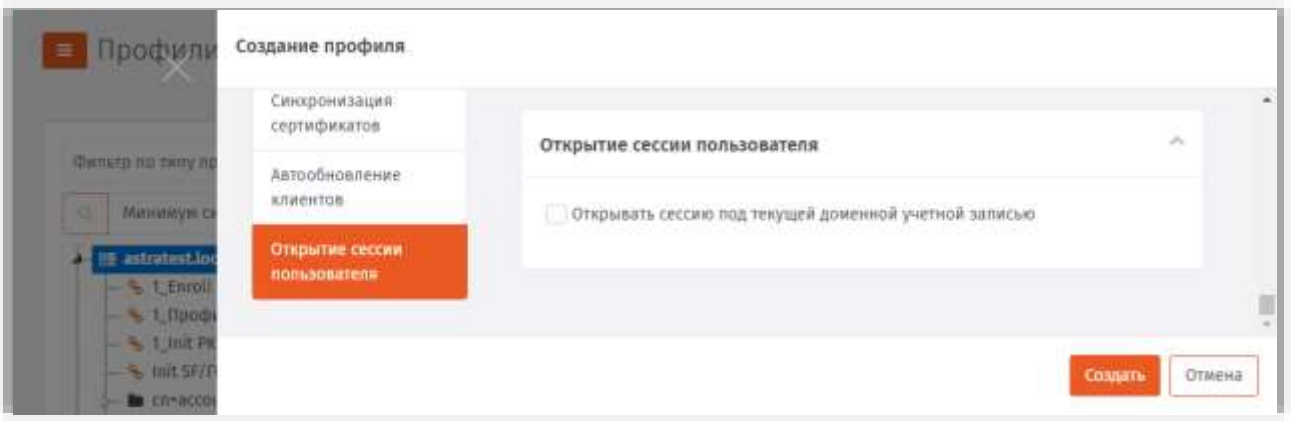


*Рис. 160 – Вкладка **Открытие сессии пользователя***

6. Установите флаг **Открывать сессию под текущей доменной учетной записью**, если при запуске приложения *JWA Tray* (подробнее о приложении см. в руководстве по установке [2] и руководстве пользователя [1]) следует выполнить автоматическую аутентификацию пользователя (*Вход в JMS*) от имени учетной записи пользователя, открывшего сеанс работы с ОС Astra Linux.
7. Для завершения редактирования/создания профиля нажмите **Создать**.

3.6.10 Настройка профиля выпуска аппаратных OTP-токенов

1. В консоли управления JMS перейдите в раздел **Профили**.
2. Выполните одно из следующих действий:

   – чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Прочее -> Выпуск аппаратных OTP-токенов**.
   – чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

   Отобразится следующее окно.

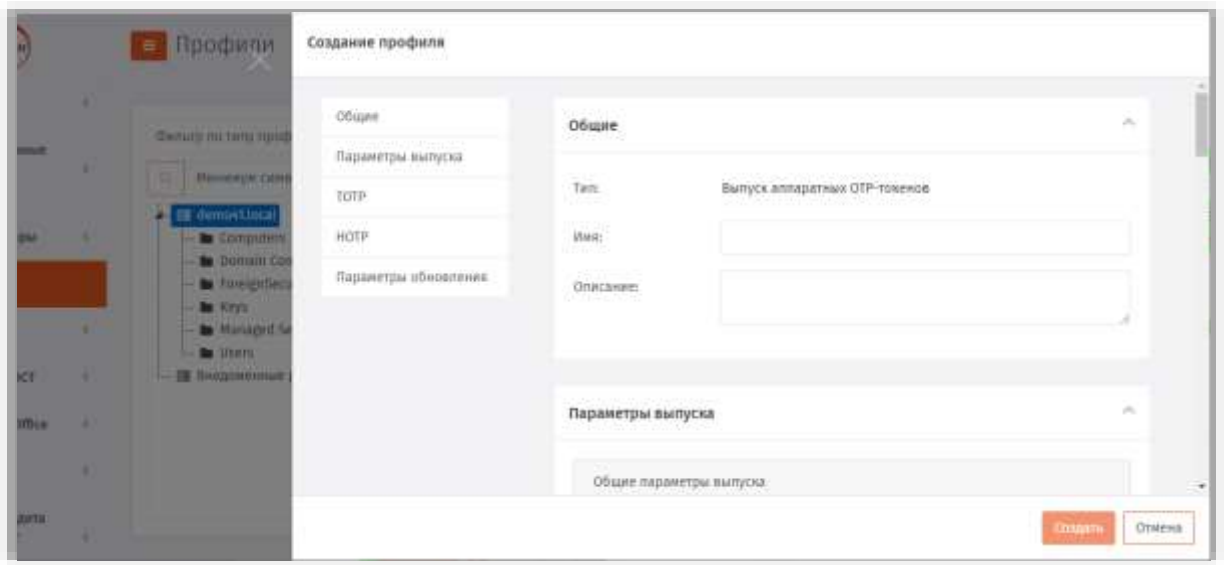


*Рис. 161 – Вкладка **Общие***

3. В соответствующих полях введите (или отредактируйте) имя и описание профиля, после чего переходите на вкладку **Параметры выпуска (**Рис. 162**)**.

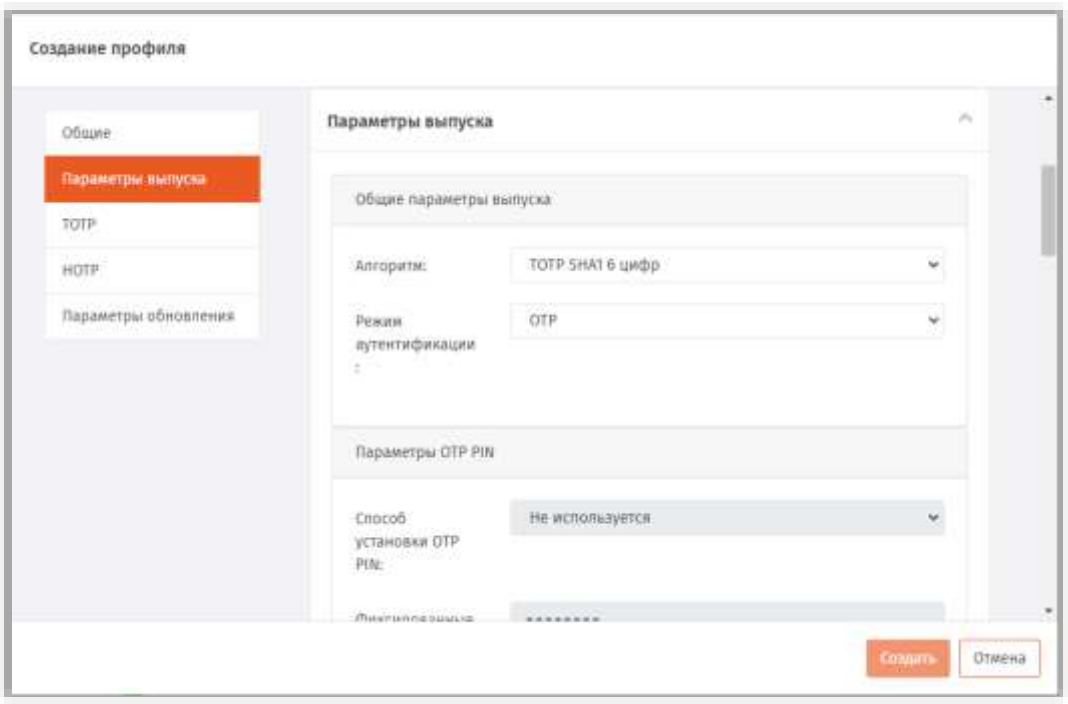


*Рис. 162 – Вкладка **Параметры выпуска***

4. Выполните настройки, руководствуясь Табл. 40.

Табл. 40 – Параметры выпуска аппаратных OTP-токенов

Настройка	Описание
	<секция> **Общие параметры выпуска**
Алгоритм	Параметр позволяет выбрать тип алгоритма генерации OTP-пароля: • для случая *если создаваемый профиль* предназначен для выпуска токенов только с алгоритмом **HOTP**-генерации одноразового пароля: – **HOTP SHA1 6 цифр** – генерация OTP по RFC 4226 с использование хэш-функции SHA1, результирующий пароль длиной 6 цифр; – **HOTP SHA256 6 цифр** – RFC 4226, хэш SHA256, результирующий пароль длиной 6 цифр; – **HOTP SHA256 7 цифр** –пароль длиной 7 цифр; – **HOTP SHA256 8 цифр** – пароль длиной 8 цифр. • для случая *если создаваемый профиль* предназначен для выпуска токенов только с алгоритмом **TOTP**-генерации одноразового пароля: – **TOTP SHA1 6 цифр** – генерация OTP по RFC 6238 с использование хэш-функции SHA1, результирующий пароль длиной 6 цифр; – **TOTP SHA256 6 цифр** – генерация OTP по RFC 6238 с использование хэш-SHA-256, результирующий пароль длиной 6 цифр; – **TOTP SHA256 7 цифр** –пароль длиной 7 цифр; – **TOTP SHA256 8 цифр** –пароль длиной 8 цифр; – **TOTP SHA512 6 цифр** – генерация OTP по RFC 6238 с использование хэш-SHA-5126, результирующий пароль длиной 6 цифр; – **TOTP SHA512 7 цифр** –пароль длиной 7 цифр; – **TOTP SHA512 8 цифр** –пароль длиной 8 цифр

Настройка	Описание
	Примечание. Обратите внимание, что создаваемый экземпляр профиля может быть предназначен для выпуска только одного типа аппаратных токенов: либо TOTP, либо HOTP.
Режим аутентификации	Параметр позволяет выбрать, какие данные должны будут предоставить пользователи для успешной аутентификации. Доступны следующие варианты: • **OTP** – для аутентификации в поле пароля пользователь должен ввести значение одноразового пароля; • **OTP PIN-код + OTP** – для аутентификации в поле пароля пользователь одной строкой должен ввести PIN-код для OTP и значение одноразового пароля; • **Доменный пароль + OTP** - для аутентификации в поле пароля пользователь одной строкой должен ввести пароль от своего доменного профиля и значение одноразового пароля; • **Доменный пароль + OTP PIN-код + OTP** - для аутентификации в поле пароля пользователь одной строкой должен ввести пароль от своего доменного профиля, PIN-код для OTP и значение одноразового пароля. **Важно!** При выборе режима аутентификации (т.е. при добавлении к OTP требования ввода PIN-кода и/или доменного пароля) следует убедиться, что данные настройки согласованы с настройками модуля JWM (см. параметры **Запрашивать OTP-PIN-код** и **Запрашивать доменный пароль** в секции **Настройки OTP**). В случае если настройки профиля будут рассинхронизированы с JWM по данным параметрам, при аутентификации пользователя в личном кабинете на JWM будет возникать ошибка.
<секция> **Параметры OTP PIN** **Примечание.** Параметры секции доступны для настройки при включении опции **OTP PIN-код + OTP** в параметре **Режим аутентификации** (выше)	
Способ установки OTP PIN	Параметр позволяет выбрать способ установки PIN-кода, используемого для аутентификации в дополнение к OTP-паролю: • **Не используется** – выберите, если режим аутентификации не предусматривает дополнительного PIN-кода (значение «OTP» в поле **Режим аутентификации**) • **Фиксированное значение** – значение дополнительного PIN-кода задается в явном виде в поле **Фиксированный OTP PIN**, ниже (значение PIN-кода будет единое для всех выпускаемых токенов); • **Случайное значение**[1] [1] **Важно!** В текущей версии продукта параметр не используется. При установке настройки **Случайное значение** пользователь не сможет аутентифицироваться в системе.
Фиксированный OTP PIN	В случае если в поле **Способ установки OTP PIN** было выбрано **Фиксированное значение**, введите значение дополнительного PIN-кода в явном виде. **Примечание**. При установке PIN-кода в поле **Фиксированное значение OTP PIN**, указанное значение следует организационными методами (сообщив лично или разослав по доступным каналам связи: e-mail, SMS и др.) довести до пользователей, для которых выпущены данные аппаратные OTP-токены.

Настройка	Описание
	При работе с таким аппаратным OTP-токеном пользователь имеет возможность в личном кабинете JWM сменить централизованно установленный PIN-код на персональный.
Длина случайного OTP PIN (мин)	В случае если в поле **Способ установки OTP PIN** был выбрано **Случайное значение**, установите минимальную (**мин**) и максимальную (**макс**) длину PIN-кода, генерируемого автоматически
Длина случайного OTP PIN (макс)	
Количество цифр в OTP PIN	Параметры сложности автоматически генерируемого PIN-кода. **Примечание**. Суммарное число символов указанных типов не должно превышать общую длину пароля (см. поле **Длина случайного OTP PIN**)
Количество строчных букв в OPT PIN	
Количество прописных букв в OPT PIN	
Количество спецсимволов в OPT PIN	

5. В случае, если в поле **Алгоритм** было выбрано одно из значений, начинающееся с **TOTP...**, выберите вкладку **TOTP**, в противном случае перейдите к шагу 7, с. 162 (настройки на вкладке **HOTP**).
   Окно примет следующий вид.

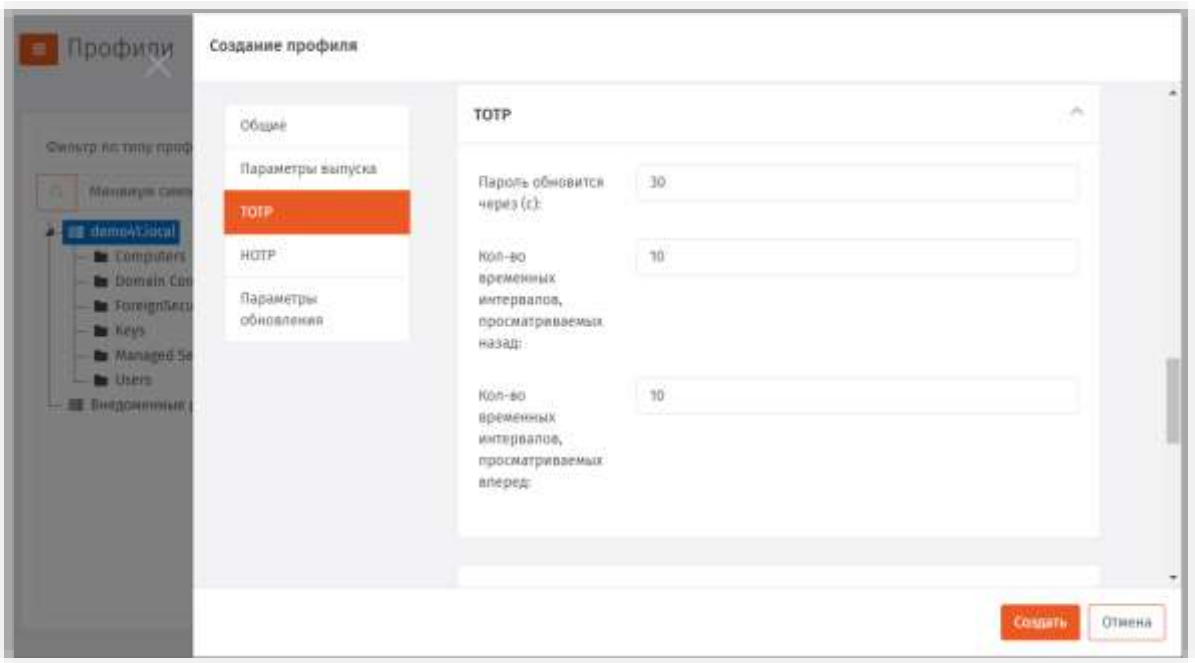


*Рис. 163 – Вкладка **TOTP***

6. Выполните настройки, руководствуясь Табл. 41.

Табл. 41 – Параметры выпуска TOTP-токенов

Настройка	Описание
Пароль обновится через (с)	Интервал времени (в секундах), в течение которого действителен одноразовый пароль

Настройка	Описание
	Значение по умолчанию: **30**
Кол-во временных интервалов, просматриваемых назад	Диапазон времени (измеряется в числе **Интервалов действия пароля**, см. выше), отсчитываемый назад от текущего момента времени. На указанном диапазоне проверяется действительность значения одноразового пароля. Значение по умолчанию: **10** **Примечание.** Подробнее протокол валидации пароля описывается в RFC 6238. Параметры **Кол-во временных интервалов, просматриваемых назад** и **Кол-во временных интервалов, просматриваемых вперед** задают так называемое "окно синхронизации".
Кол-во временных интервалов, просматриваемых вперед	Диапазон времени (измеряется в числе **Интервалов действия пароля**, см. выше), отсчитываемый вперед от текущего момента времени. На указанном диапазоне проверяется действительность значения одноразового пароля. Значение по умолчанию: **10**

7. Выберите вкладку **HOTP**.
   Окно примет следующий вид.

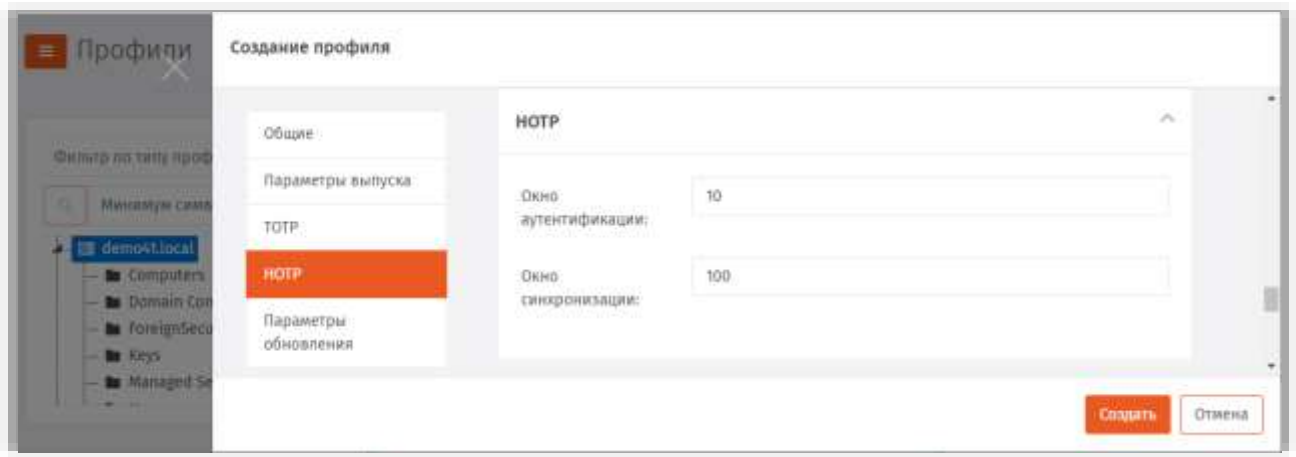


*Рис. 164 – Вкладка **HOTP***

8. Выполните настройки, руководствуясь Табл. 42.

Табл. 42 – Параметры выпуска HOTP-токенов

Настройка	Описание
Окно аутентификации	Максимальное количество одноразовых паролей, проверяемых подряд при аутентификации. Диапазон значений OTP, которые будут проверяться во время аутентификации пользователя, если предъявленное пользователем значением OTP не будет совпадать с очередным ожидаемым значением. (Количество допустимых «пустых» нажатий.) Значение по умолчанию: **10**
Окно синхронизации	Максимальное количество одноразовых паролей, проверяемых подряд при синхронизации OTP-счетчиков.

Настройка	Описание
	Диапазон пар значений OTP, который будет проверяться, в случае если OTP не совпадает ни с одним значением из диапазона **Окно аутентификации**. В этом случае при синхронизации OTP-токена необходимо предъявить два правильных значения OTP подряд. Значение по умолчанию: **100**

9. Выберите вкладку **Параметры обновления**.
Окно примет следующий вид.

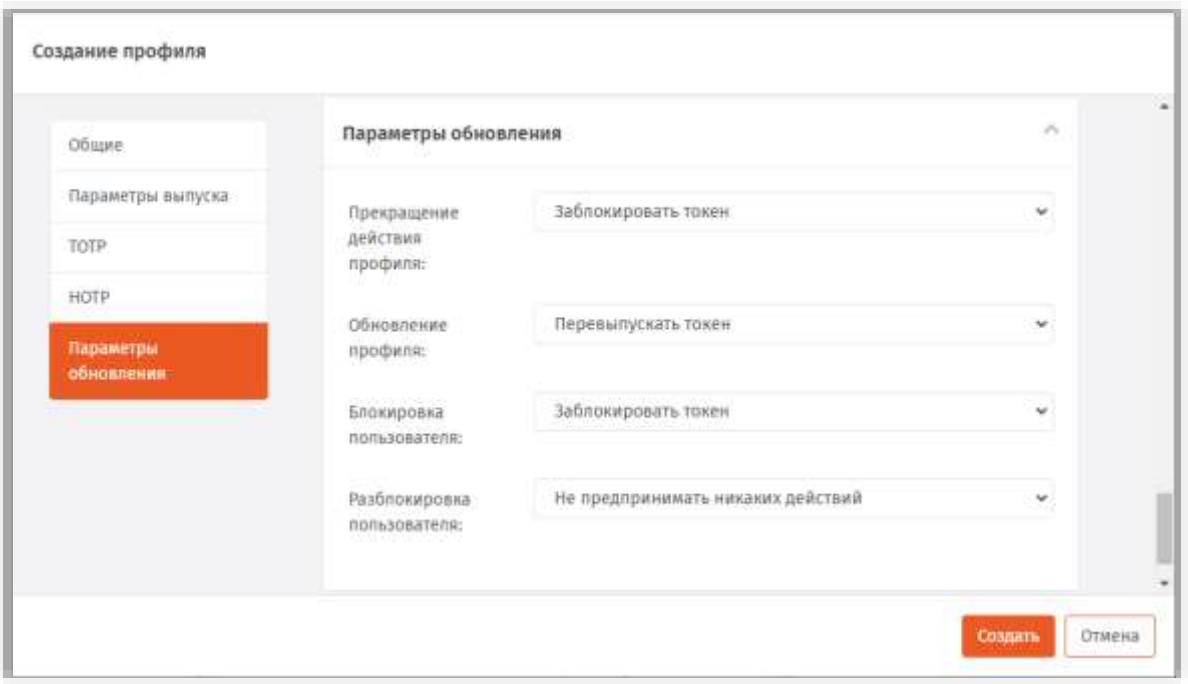


*Рис. 165 – Вкладка **Параметры обновления***

10. Выполните настройки, руководствуясь Табл. 43.

Табл. 43 – Параметры обновления профиля

Настройка	Описание
Прекращение действия профиля	Параметр определяет действия, которые необходимо предпринять с OTP-токенами, выпускавшимися по данному профилю, в случае удаления или прекращения привязки профиля к контейнеру, которому принадлежат данные токены. Доступные значения: • **Заблокировать токен** – при прекращении действия профиля токен должен быть автоматически заблокирован в JMS; • **Удалить токен** – при прекращении действия профиля токен должен быть автоматически удален из JMS; • **Не предпринимать никаких действий** Значение по умолчанию: **Заблокировать токен**

Настройка	Описание
Обновление профиля	Параметр определяет действия, которые необходимо предпринять с OTP-токенами, выпускавшимися по данному профилю, в случае изменения параметров профиля. Доступные значения: • **Перевыпустить токен** – при изменении параметров профиля все выпущенные на его основе токены должны быть автоматически перевыпущены с применением обновленных параметров профиля • **Не предпринимать никаких действий** Значение по умолчанию: **Перевыпустить токен** **Примечание.** В текущей версии продукта установка значения **Не предпринимать никаких действий** означает, что изменение настроек OTP-токена не вступят в силу после сохранения профиля и выполнения плана обслуживания (за исключением случая, когда токен с прежними настройками был предварительно удалён). Вступление в силу изменений в профиле возможно только при выборе значения **Перевыпустить токен**.
Блокировка пользователя	Параметр определяет действия, которые необходимо предпринять с OTP-токеном, выпускавшимся по данному профилю, в случае если его владелец (пользователь) был заблокирован в JMS. Доступные значения: • **Заблокировать токен** – при блокировке пользователя токен должен быть автоматически заблокирован в JMS; • **Не предпринимать никаких действий** Значение по умолчанию: **Заблокировать токен**
Разблокировка пользователя	Параметр определяет действия, которые необходимо предпринять с OTP-токеном, выпускавшимся по данному профилю, в случае если его владелец (пользователь) был разблокирован в JMS. Доступные значения: • **Разблокировать токен** – при разблокировке пользователя токен должен быть автоматически разблокирован в JMS; • **Не предпринимать никаких действий** Значение по умолчанию: **Не предпринимать никаких действий**

11. По окончании всех настроек нажмите кнопку **Создать** (Рис. 165, с. 163) или **Сохранить** (при редактировании профиля), чтобы сохранить изменения.

3.6.11 Настройка профиля выпуска программных OTP-токенов

12. В консоли управления JMS перейдите в раздел **Профили**.
13. Выполните одно из следующих действий:

- чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Прочее -> Выпуск программных OTP-токенов**.

– чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

Отобразится следующее окно.

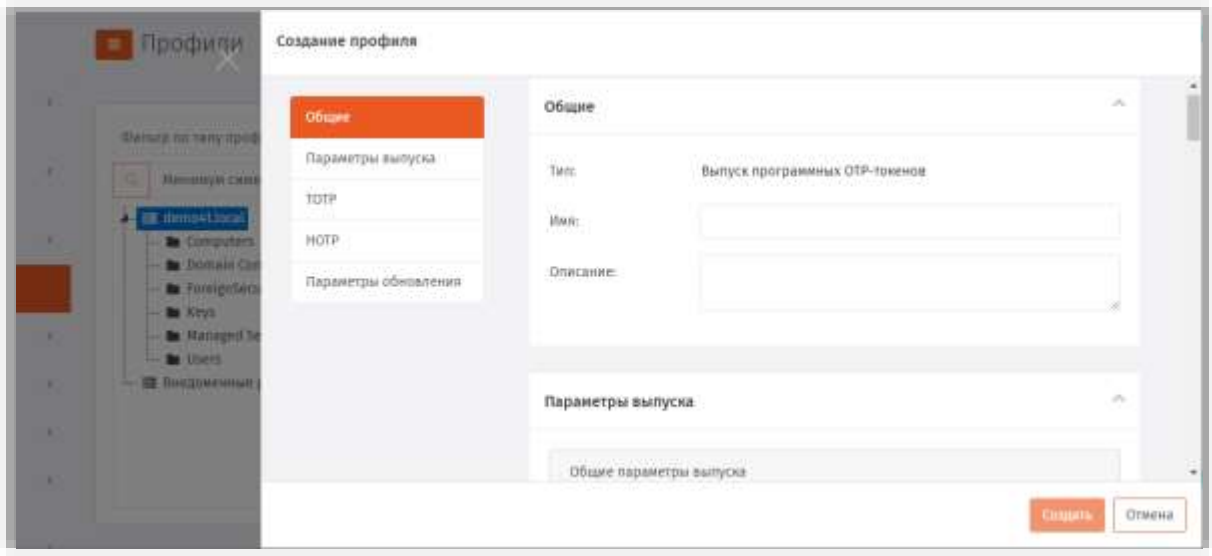


*Рис. 166 – Вкладка **Общие***

14. В соответствующих полях введите (или отредактируйте) имя и описание профиля.

Примечание. В поле **Имя** следует ввести информативное и понятное конечному пользователю название профиля, отображающее назначение OTP-токена, который будет применяться пользователем для аутентификации в определенной информационной системе, например *OTP-токен для входа в Систему XYZ*.

Данное имя будет отображаться в пользовательском интерфейсе (в личном кабинете пользователя) JWM-портала.

После редактирование полей на вкладке **Общие** переходите на вкладку **Параметры выпуска (**Рис. 167**)**.

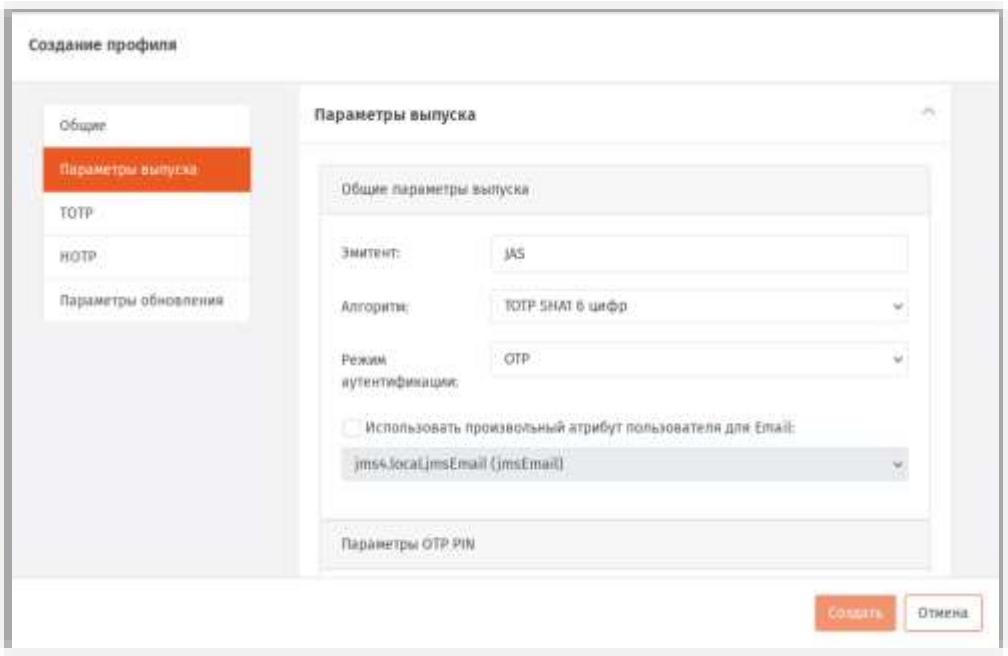


*Рис. 167 – Вкладка **Параметры выпуска***

15. Выполните настройки, руководствуясь Табл. 44.

Табл. 44 – Параметры выпуска программных OTP-токенов

Настройка	Описание
	<секция> **Общие параметры выпуска**
Эмитент	Введите в этом поле название вашего сайта или организации.
Алгоритм	Параметр позволяет выбрать тип алгоритма генерации OTP-пароля: • для случая *если создаваемый профиль* предназначен для выпуска токенов только с алгоритмом **HOTP**-генерации одноразового пароля: – **HOTP SHA1 6 цифр** – генерация OTP по RFC 4226 с использование хэш-функции SHA1, результирующий пароль длиной 6 цифр; – **HOTP SHA256 6 цифр** – RFC 4226, хэш SHA256, результирующий пароль длиной 6 цифр; – **HOTP SHA256 7 цифр** –пароль длиной 7 цифр; – **HOTP SHA256 8 цифр** – пароль длиной 8 цифр; • для случая *если создаваемый профиль* предназначен для выпуска токенов только с алгоритмом **TOTP**-генерации одноразового пароля: – **TOTP SHA1 6 цифр** – генерация OTP по RFC 6238 с использование хэш-функции SHA1, результирующий пароль длиной 6 цифр; – **TOTP SHA256 6 цифр** – генерация OTP по RFC 6238 с использование хэш-функции SHA256, результирующий пароль длиной 6 цифр; – **TOTP SHA256 7 цифр** –пароль длиной 7 цифр; – **TOTP SHA256 8 цифр** –пароль длиной 8 цифр; – **TOTP SHA512 6 цифр** – генерация OTP по RFC 6238 с использование хэш-функции SHA512, результирующий пароль длиной 6 цифр; – **TOTP SHA512 7 цифр** –пароль длиной 7 цифр; – **TOTP SHA512 8 цифр** –пароль длиной 8 цифр.

Настройка	Описание
	Примечание. Обратите внимание, что создаваемый экземпляр профиля может быть предназначен для выпуска только одного типа программных токенов: либо TOTP, либо HOTP.
Режим аутентификации	Выполните настройку по аналогии с настройкой параметра для выпуска аппаратных OTP-токенов (см. Табл. 40, с. 159)
Использовать произвольный атрибут пользователя для Email:	Установите флаг, если необходимо определить специальный атрибут в любой из подключенных в JMS ресурсных систем, в котором будет содержаться адрес электронной почты пользователя для передачи на него активационной информации OTP-аутентификатора. **Примечание.** Чтобы проверить, в каком атрибуте ресурсной системы хранится адрес электронной почты, можно воспользоваться вкладкой **Учетные записи** свойств пользователя, пролистав поле **Атрибуты учетной записи**.
<секция> **Параметры OTP PIN**	
Способ установки OTP PIN **Фиксированный OTP PIN** **Длина случайного OTP PIN (мин)** **Длина случайного OTP PIN (макс)** **Количество цифр в OTP PIN** **Количество строчных букв в OPT PIN** **Количество прописных букв в OPT PIN** **Количество спецсимволов в OPT PIN**	В данных полях формы выполните настройки по аналогии с настройками **Параметров выпуска** в аппаратных OTP-токенов (см. Табл. 40, с. 159)
<секция> **Передача OTP-секрета**	
Способ передачи OTP-секрета	Выберите способ передачи OTP-секрета: • **Базовый** – OTP-секрет генерируется сервером JMS и отправляется в виде QR-кода на почтовый адрес владельца OTP-токена без дополнительной защиты. QR-код может быть использован, например, в мобильном приложении Aladdin 2FA компании Аладдин. • **Защищенный** -- OTP-секрет будет сгенерирован сторонним веб-сервисом безопасной передачи OTP-секрета для защиты от кражи QR-кода и его повторного использования. OTP-секрет может быть дополнительно защищен PIN-кодом. QR-код должен быть использован в специальном приложении (комплексное решение Aladdin 2FA Service) **Примечание.** При выборе способа **Защищенный** следует выполнить дополнительные настройки в серверном агенте JMS, вкладка **Настройки JAS** -> ссылка **Настройки подключения к JAS** -> секция **Веб-сервис безопасной передачи OTP-секрета**, подробнее см . руководство по установке и настройке JMS [2].

Настройка	Описание
Время жизни тикета. Если не указано - время жизни не ограничено	Настройка для ограничения срока жизни OTP-секрета (настройка доступна при выборе способа передачи OTP-секрета **Защищённый**, выше). Значение по умолчанию – 3 дня. Если *время жизни тикета* не задано, то срок действия OTP-секрета не ограничен.
Способ передачи QR-кода	Установите канал/каналы, по которому QR-код будет передан пользователю: • **E-mail** – в почтовый ящик пользователя; • **JMS Web Manager** – непосредственно в интерфейсе личного кабинета пользователя (посредством сервера JWM)
Тема email сообщения	Укажите тему письма, которое будет содержать активационную информацию для OTP-аутентификатора

16. В случае, если в поле **Алгоритм** было выбран алгоритм по спецификации *TOTP*, выберите вкладку **TOTP** (в противном случае перейдите к шагу 18, с. 169 – настройки на вкладке **HOTP**).
Окно примет следующий вид.

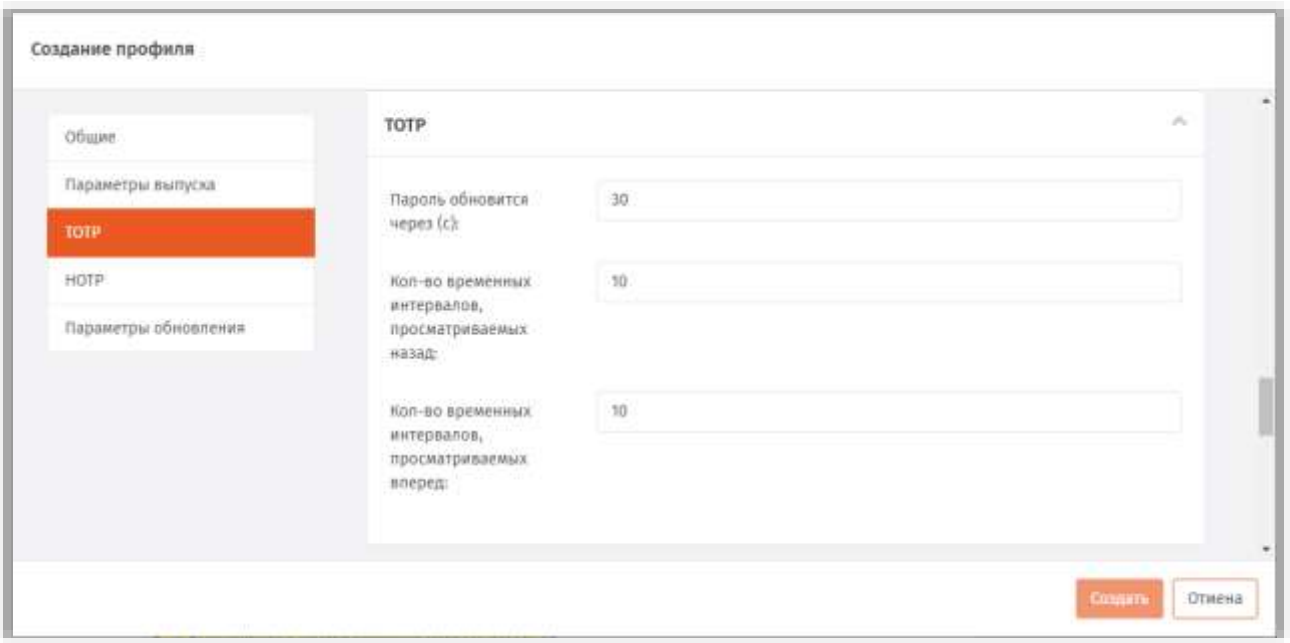


*Рис. 168 – Вкладка **TOTP***

17. Выполните настройки, руководствуясь Табл. 45.

Табл. 45 – Параметры выпуска программных TOTP-токенов

Настройка	Описание
Пароль обновится через (с)	Интервал времени (в секундах), в течение которого действителен одноразовый пароль. Значение по умолчанию: **30**

Настройка	Описание
Кол-во временных интервалов, просматриваемых назад	Диапазон времени (измеряется в числе интервалов, определяемых параметром **Пароль обновится через (с)**, см. выше), отсчитываемый назад от текущего момента времени. На указанном диапазоне проверяется действительность значения одноразового пароля. Значение по умолчанию: **10**
Кол-во временных интервалов, просматриваемых вперед	Диапазон времени (измеряется в числе интервалов, определяемых параметром **Пароль обновится через (с)**, см. выше), отсчитываемый вперед от текущего момента времени. На указанном диапазоне проверяется действительность значения одноразового пароля. Значение по умолчанию: **10**

18. Выберите вкладку **HOTP**.
    Окно примет следующий вид.

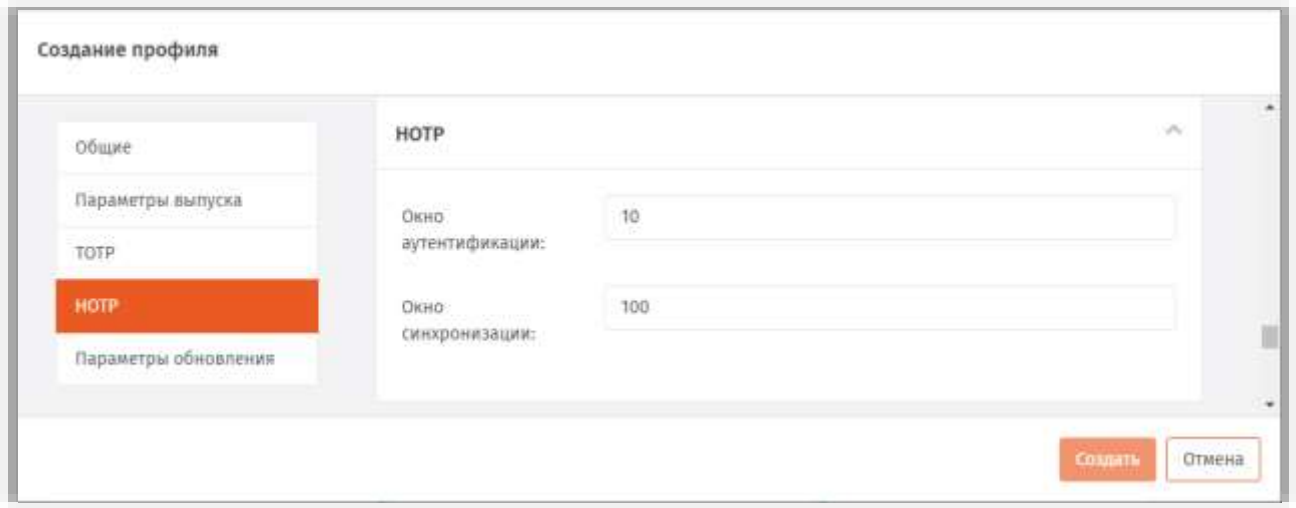


*Рис. 169 – Вкладка **HOTP***

19. Выполните настройки, руководствуясь Табл. 42, с. 162.
20. Выберите вкладку **Параметры обновления**.

Окно примет следующий вид.

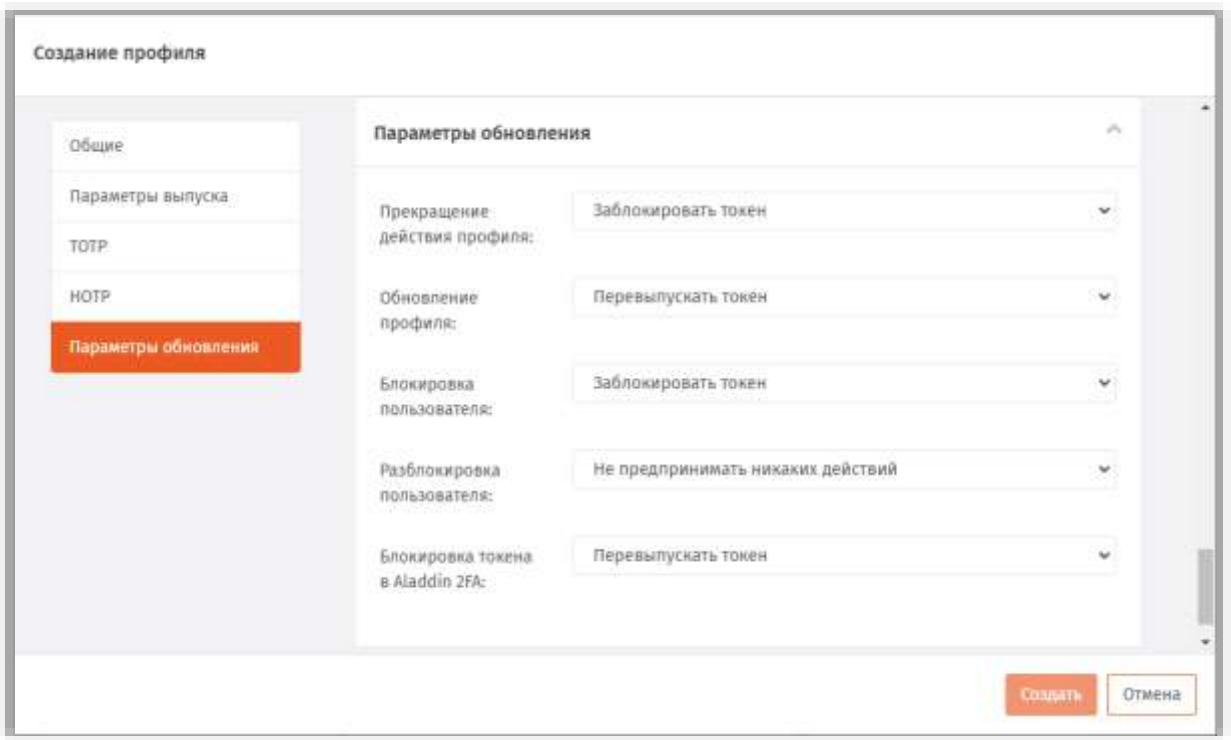


*Рис. 170 – Вкладка **Параметры обновления***

21. Выполните настройки, руководствуясь Табл. 46.

Табл. 46 – Параметры обновления профиля

Настройка	Описание
Прекращение действия профиля **Обновление профиля** **Блокировка пользователя** **Разблокировка пользователя**	Для данных параметров выполните настройки, руководствуясь Табл. 43, с. 163.
Блокировка токена в Aladdin 2FA	Параметр определяет действия, которые необходимо предпринять с OTP-токеном, выпускавшимся по данному профилю, в случае если токен был заблокирован в системе Aladdin 2FA. Доступные значения: • **Перевыпустить токен** – при блокировке токена в A2FA он должен быть перевыпущен в JMS (данная опция позволяет автоматически перевыпускать токен, если истекло время жизни «тикета» (т.е. одноразовой ссылки), значение которого по умолчанию 3 дня); • **Заблокировать токен** – при блокировке токена в A2FA он должен быть автоматически заблокирован в JMS. Значение по умолчанию: **Перевыпустить токен** **Примечание.** Действия, предлагаемые в данном параметре, реализуются в ходе выполнения задачи **Обслуживание программных OTP-токенов** плана обслуживания жизненного цикла OTP-токенов (см. раздел

Настройка	Описание
	«План обслуживания жизненного цикла OTP-токенов», с. 281). Для того чтобы данная задача корректно обработала токены, заблокированные в A2FA, следует также включить выполнение задачи **Получение статусов программных OTP-токенов с сервиса Aladdin 2FA** в том же плане обслуживания.

22. По окончании всех настроек нажмите кнопку **Создать** (Рис. 170, с. 170) или **Сохранить** (при редактировании профиля), чтобы сохранить изменения.

Примечание. При сохранении профиля выполняется проверка на завершённость других настроек, необходимых для успешного выпуска для пользователей OTP-токенов. При появлении предупреждения об отсутствии настройки SMTP-транспорта (Рис. 171) выполните соответствующую настройку в консольном агенте JMS (команда Aladdin.EAP.Agent.Terminal smtp configure, подробнее см. руководство по установке и настройке JMS [2].

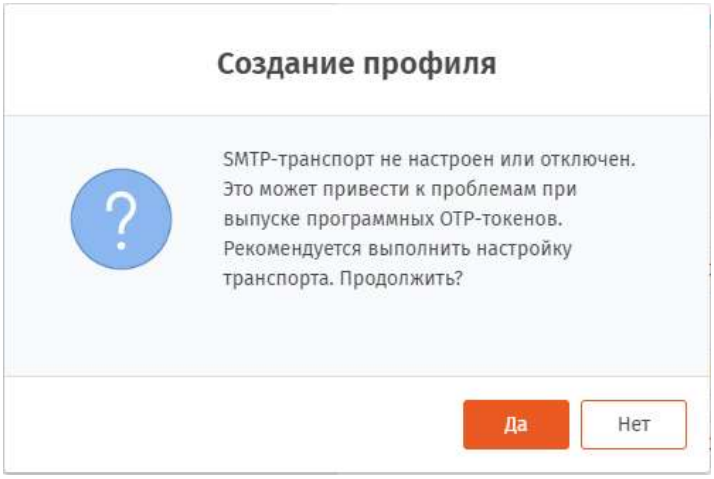


Рис. 171 – Предупреждение о необходимости включить и настроить SMTP-транспорт

3.6.12 Настройка профиля выпуска Messaging-токенов

1. В консоли управления JMS перейдите в раздел **Профили**.
2. Выполните одно из следующих действий:

   – чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Прочее -> Выпуск Messaging-токенов**.
   – чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

Отобразится следующее окно.

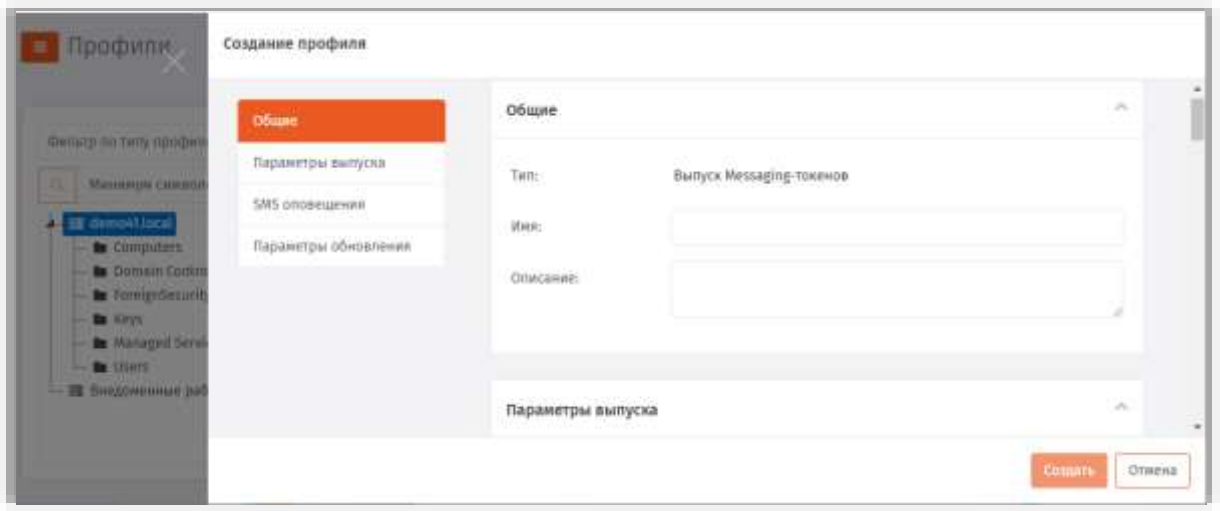


*Рис. 172 – Вкладка **Общие***

3. В соответствующих полях введите (или отредактируйте) имя и описание профиля.

Примечание. В поле **Имя** следует ввести информативное и понятное конечному пользователю название профиля, отображающее назначение Messaging-токена, который будет применяться пользователем для аутентификации в определенной информационной системе, например *Messaging-токен для входа в Систему XYZ*.

Данное имя будет отображаться в пользовательском интерфейсе (в личном кабинете пользователя) JWM-портала.

После редактирование полей на вкладке **Общие** переходите на вкладку **Параметры выпуска (**Рис. 173**)**.

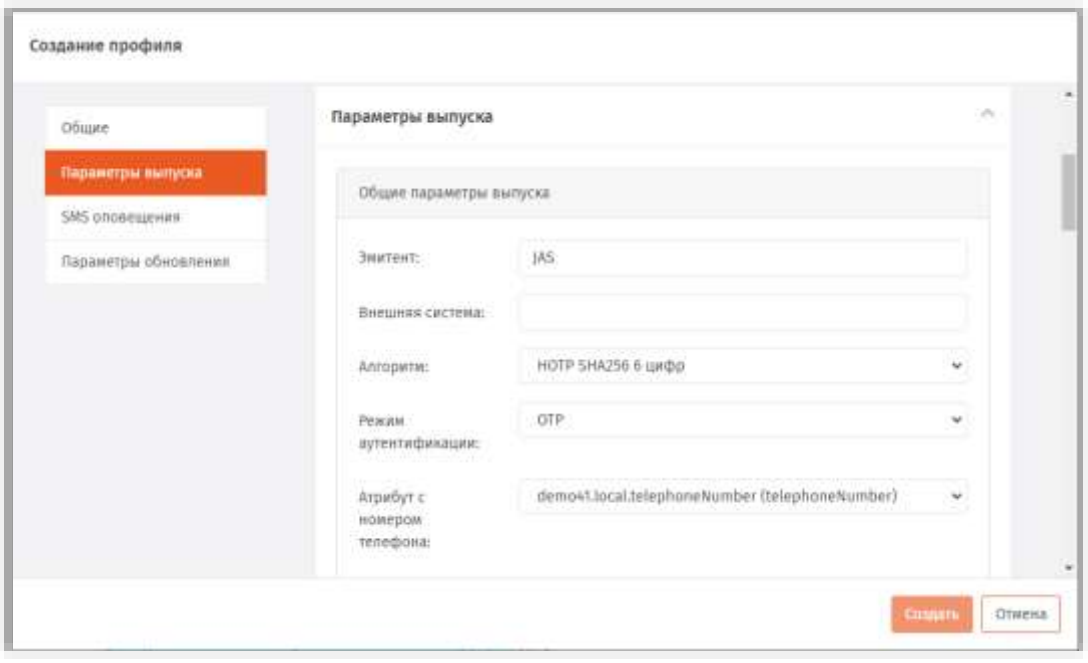


*Рис. 173 – Вкладка **Параметры выпуска***

4. Выполните настройки, руководствуясь Табл. 47.

Табл. 47 – Параметры выпуска Messaging-токенов

Настройка	Описание
	<секция> **Общие параметры выпуска**
Эмитент	Введите в этом поле название вашего сайта или организации.
Внешняя система	Идентификатор внешней системы, для которой осуществляется аутентификация пользователя посредством Messaging-токена. **Важно!** Один пользователь не может иметь более одного Messaging-токена для одной внешней системы. Это означает, что при привязке профиля к пользователю (контейнеру пользователя) нужно убедиться, что к данному контейнеру в настоящий момент не привязан другой профиль выпуска Messaging-токенов с тем же идентификатором внешней системы. В противном случае на этапе выпуска токена возникнет ошибка (отображается в отчете о выполнения плана обслуживания). **Примечание.** Данный идентификатор прописывается также на стороне интегрируемой системы. Например в случае интеграции с JAS-плагином ADFS данный идентификатор прописывается в параметре **MessagingSystemId** (см. [**3**], раздел «Настройка JAS-плагина для AD FS») Аналогичным образом, в случае интеграции с JAS-плагином NPS данный идентификатор следует задать в его настройках (см. [**3**], раздел «Настройка JAS-плагина для NPS»). При использовании Messaging-otp для JWM данная настройка прописывается в поле **Внешняя система** секции **Настройки Messaging**. При настройке Messaging-аутентификации через API данный идентификатор следует сообщить разработчикам, выполняющим данную интеграцию.
Алгоритм	Алгоритм генерации одноразового пароля аутентификации (OTP). Допустимые значения: • **HOTP SHA1 6 цифр** – генерация OTP по RFC 4226 с использование хэш-функции SHA1, результирующий пароль длиной 6 цифр; • **HOTP SHA256 6 цифр** — RFC 4226, хэш SHA256, результирующий пароль длиной 6 цифр; • **HOTP SHA256 7 цифр** —пароль длиной 7 цифр; • **HOTP SHA256 8 цифр** — пароль длиной 8 цифр.
Режим аутентификации	Параметр позволяет выбрать, какие данные должны будут предоставить пользователи для успешной аутентификации. Доступны следующие варианты: • **OTP** – для аутентификации в поле пароля пользователь должен ввести значение одноразового пароля; • **OTP PIN-код + OTP** – для аутентификации в поле пароля пользователь одной строкой должен ввести PIN-код для OTP и значение одноразового пароля; • **Доменный пароль + OTP** - для аутентификации в поле пароля пользователь одной строкой должен ввести пароль от своего доменного профиля и значение одноразового пароля; • **Доменный пароль + OTP PIN-код + OTP** - для аутентификации в поле пароля пользователь одной строкой должен ввести пароль от своего доменного профиля, PIN-код для OTP и значение одноразового пароля. **Важно!** При выборе режима аутентификации (т.е. при добавлении к OTP требования ввода PIN-кода и/или доменного пароля) следует убедиться, что

Настройка	Описание
	данные настройки согласованы с настройками модуля JWM (см. параметры **Запрашивать OTP-PIN**-код и **Запрашивать доменный пароль** в секции **Настройки OTP**). В случае если настройки профиля будут рассинхронизированы с JWM по данным параметрам, при аутентификации пользователя в личном кабинете на JWM будет возникать ошибка.
Атрибут с номером телефона	Выберите атрибут в любой из подключенных в JMS ресурсных систем, в котором будет содержаться номер телефона пользователя для передачи на него одноразового пароля и других оповещений в рамках работы со своим messaging-токеном.  **Примечание.** 1. Чтобы проверить, в каком атрибуте ресурсной системы хранится номер мобильного телефона, можно воспользоваться вкладкой **Учетные записи** свойств пользователя, пролистав поле **Атрибуты учетной записи**. 2. Атрибут может содержать одновременно несколько номеров телефонов (данная возможность реализуется средствами самой ресурсной системы).
<секция> **Параметры OTP**	
Время жизни OTP (с)	Промежуток времени (в секундах), в течение которого производятся попытки отправки сообщения с OTP (паролем) и время, в течение которого данный OTP действителен. Значение по умолчанию: **180**
Задержка генерации OTP (мс)	Определяет, через какое время (в миллисекундах) с момента генерации предыдущего пароля OTP разрешается запрашивать следующий. Значение по умолчанию: **5000**
Кол-во повторов аутентификации	Количество *дополнительных* (к первой) попыток аутентификации, т.е. ввода одноразового пароля. Например, если в поле указано 3, то общее количество попыток составит 1+3. Значение по умолчанию: **3**
<секция> **Параметры OTP PIN**  **Примечание.** Параметры секции доступны для настройки при включении опции **OTP PIN-код + OTP** в параметре **Режим аутентификации** (выше)	
• **Способ установки OTP PIN** • **Фиксированный OTP PIN** • **Длина случайного OTP PIN (мин)** • **Длина случайного OTP PIN (макс)** • **Количество цифр в OTP PIN** • **Количество строчных букв в OPT PIN**	Выполните настройки по аналогии настройками **Параметров выпуска** в профиле выпуска аппаратных OTP-токенов (см. Табл. 40, с. 159).

Настройка	Описание
• **Количество прописных букв в OPT PIN** • **Количество спецсимволов в OPT PIN**	

5. Выберите вкладку **SMS-оповещения**.
Окно примет следующий вид.

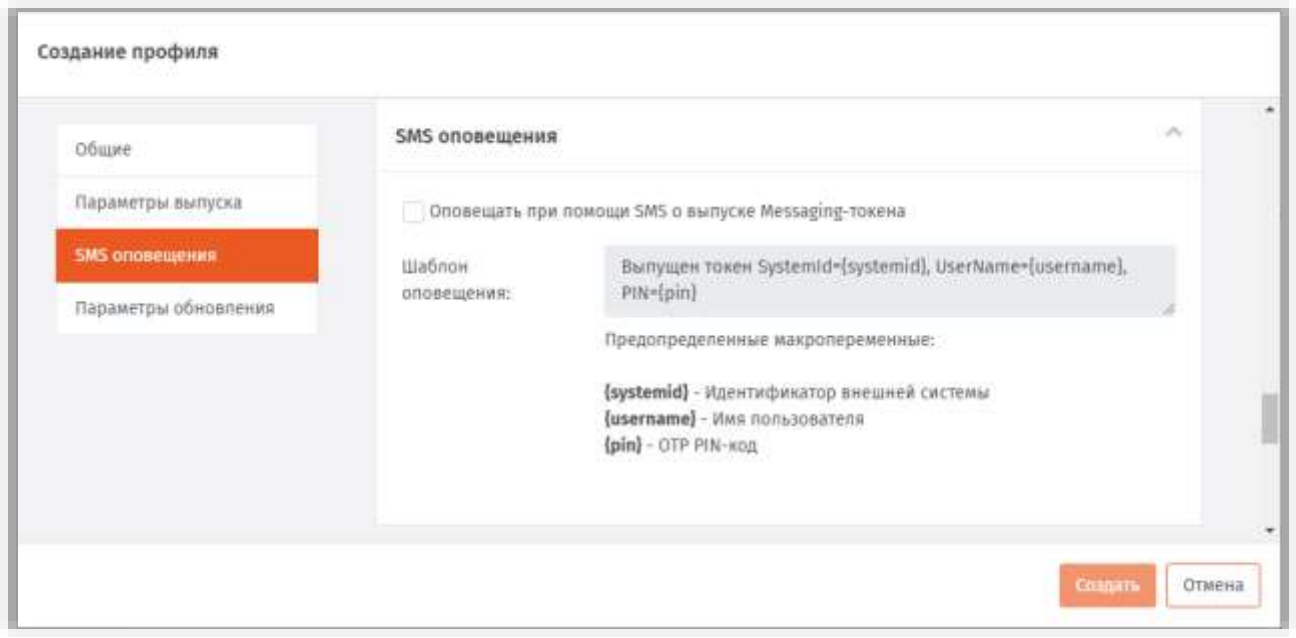


*Рис. 174 – Вкладка **SMS оповещения***

6. Выполните настройки, руководствуясь Табл. 48.

Табл. 48 – Настройки SMS оповещений

Настройка	Описание
Оповещать при помощи SMS при выпуске Messaging-токена	Установите флажок в том случае, если пользователя необходимо оповестить по SMS о факте выпуска для него Messaging-токена
Шаблон оповещения	В случае если оповещение о выпуске токена включено, можно отредактировать шаблон такого оповещения для всех пользователей, для которых будет выпущен токен по данному профилю. Шаблон содержит

Настройка	Описание
	зарезервированные переменные, которые будут заменены при отправке данного оповещения: • **{systemid}** – идентификатор внешней системы; • **{username}** – имя пользователя; • **{pin}** – значение добавочного PIN-кода (OTP PIN), следует указать, только если OTP PIN был определен на вкладке **Параметры выпуска**. Шаблон сообщения по умолчанию: *Выпущен токен SystemId={systemid}, UserName={username}, PIN ={pin}*

7. Выберите вкладку **Параметры обновления**.
Окно примет следующий вид.

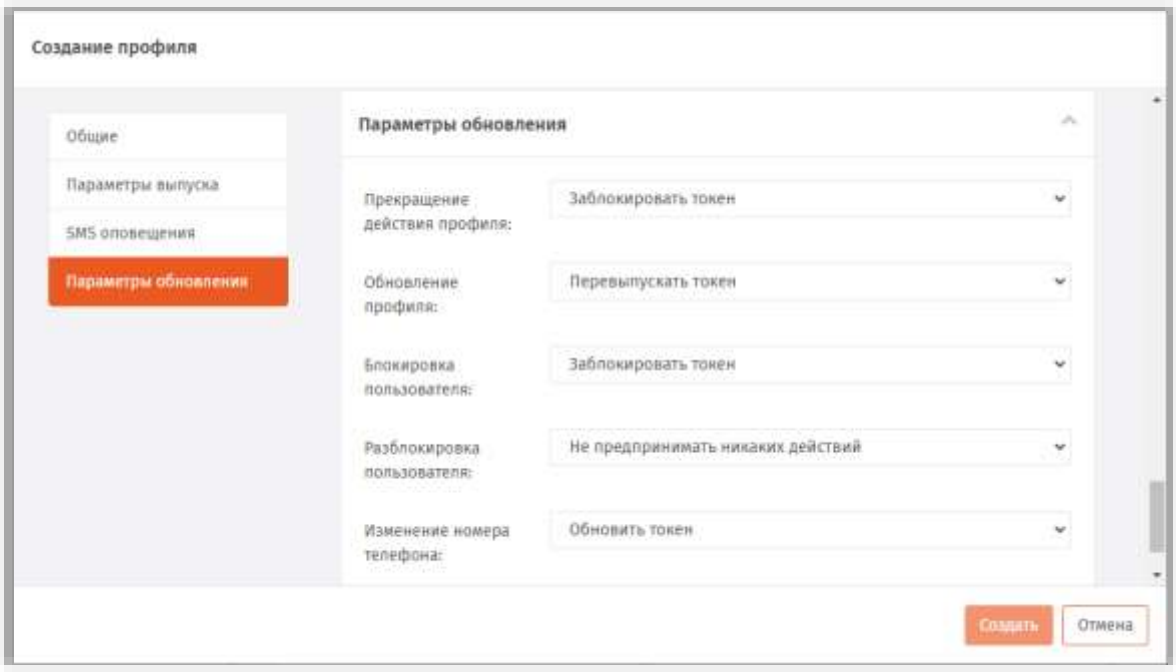


*Рис. 175 – Вкладка **Параметры обновления***

8. Выполните настройки, руководствуясь Табл. 49.

Табл. 49 – Настройки параметров обновления

Настройка	Описание
Прекращение действия профиля **Обновление профиля** **Блокировка пользователя** **Разблокировка пользователя**	Выполните настройки по аналогии настройками **Параметров обновления** в профиле выпуска аппаратных OTP-токенов (см. Табл. 43, с. 163).
Изменение номера телефона	Параметр определяет действия, которые необходимо предпринять с Messaging-токеном, выпускавшимся по данному профилю, в случае изменения номера телефона, указанного в **Атрибуте с номером телефона** (см. Табл. 47, с 173) данного пользователя.

Настройка	Описание
	Доступные значения: • **Заблокировать токен** – при изменении номера телефона пользователя токен должен быть автоматически заблокирован в JMS; • **Обновить токен** – при изменении номера телефона пользователя токен должен быть автоматически обновлен в БД JMS;  **Примечание.** Обновление номера в БД JMS происходит в результате последовательно отработки **Плана обслуживания по умолчанию** (задача *Выявление рассинхронизации учетных записей*, выявляет изменения данных пользователя в ресурсной системе, в частности, значение телефонного номера см. «План обслуживания по умолчанию»", с.288) и **Плана обслуживания жизненного цикла OTP-токенов** (задача *Синхронизация номеров телефонов Messaging-токенов*, см. раздел «План обслуживания жизненного цикла OTP-токенов»", с.281) • **Не предпринимать никаких действий** Значение по умолчанию: **Обновить токен**

9. По окончании всех настроек нажмите кнопку **Создать** (Рис. 175, с. 176) или **Сохранить** (при редактировании профиля), чтобы сохранить изменения.

3.6.13 Настройка профиля выпуска Push OTP-токенов

Push OTP-токен – это виртуальный токен с использованием Push-технологии, обеспечивающей протокол аутентификации с персонально аутентифицированного доверенного устройства, не требующей от пользователя ввода аутентификационной информации.

 **Примечание.** Для обеспечения функционирования Push OTP-токенов следует выполнить дополнительные настройки в серверном агенте JMS, вкладка **Настройки JAS** -> ссылка **Настройки подключения к JAS** -> секция **Веб-сервис безопасной передачи OTP-секрета**, подробнее см . руководство по установке и настройке JMS [2].

Для настройки профиля выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Профили**.
2. Выполните одно из следующих действий:
   - чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Прочее -> Выпуск Push OTP-токенов**.
   - чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

Отобразится следующее окно.

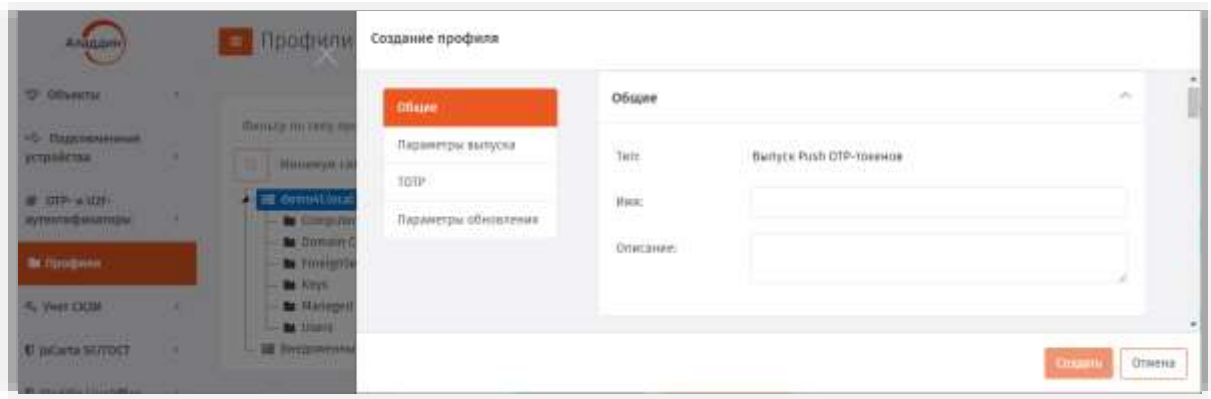


*Рис. 176 – Вкладка **Общие***

3. В соответствующих полях введите (или отредактируйте) имя и описание профиля.

Примечание. В поле **Имя** следует ввести информативное и понятное конечному пользователю название профиля, отображающее назначение OTP-токена, который будет применяться пользователем для аутентификации в определенной информационной системе, например *Push OTP-токен для входа в Систему XYZ*.

Данное имя будет отображаться в пользовательском интерфейсе (в личном кабинете пользователя) JWM-портала.

После редактирование полей на вкладке **Общие** переходите на вкладку **Параметры выпуска (**Рис. 177**)**.

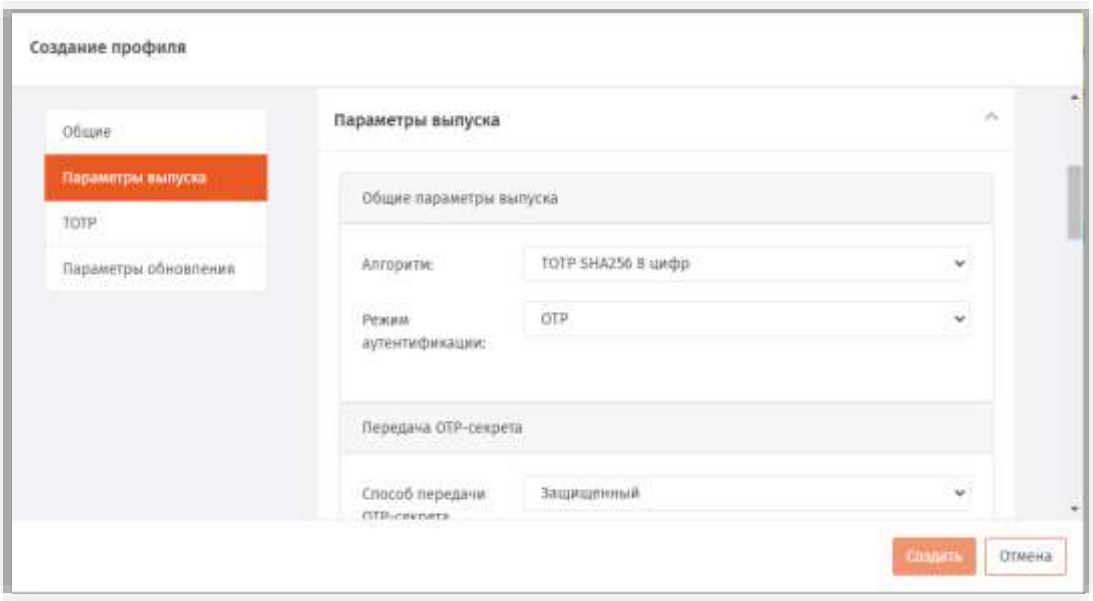


*Рис. 177 – Вкладка **Параметры выпуска***

4. Выполните настройки, руководствуясь Табл. 50.

Табл. 50 – Параметры выпуска Push OTP-токенов

Настройка	Описание
<секция> **Общие параметры выпуска**	
Алгоритм **Режим аутентификации**	Нередактируемые поля
<секция> **Передача OTP-секрета**	
Способ передачи OTP-секрета	Нередактируемое поле Значение: *Защищенный*
Время жизни тикета. Если не указано - время жизни не ограничено	Настройка для ограничения срока жизни OTP-секрета. Значение по умолчанию – 3 дня. Если *время жизни тикета* не задано, то срок действия OTP-секрета не ограничен.
Способ передачи QR-кода	Параметр для указания того, по каким каналам следует передать QR-код для инициализации токена в мобильном приложении пользователя. Доступные значения (должно быть выбрано хотя бы одно): • **E-mail** – передача QR-кода на адрес электронной почты пользователя; • **JMS Web Manager** – передача QR-кода осуществляется непосредственно на web-страницу личного кабинета пользователя в JWM-портале. При этом для отображения QR-кода пользователю необходимо нажать на его мнемоническое обозначение (см. рис. ниже)  **Важно!** При указании значения **E-mail** следует убедиться в наличии следующих настроек: 1. У пользователей, для которых выпускаются Push-токены, в ресурсной системе Active Directory настроен адрес электронной почты. 2. В консольном агенте JMS должен быть настроен транспортный почтовый сервис (команда Aladdin.EAP.Agent.Terminal smtp configure, подробнее см. руководство по установке и настройке JMS [2]).

5. Выберите вкладку **TOTP**.

Окно примет следующий вид.

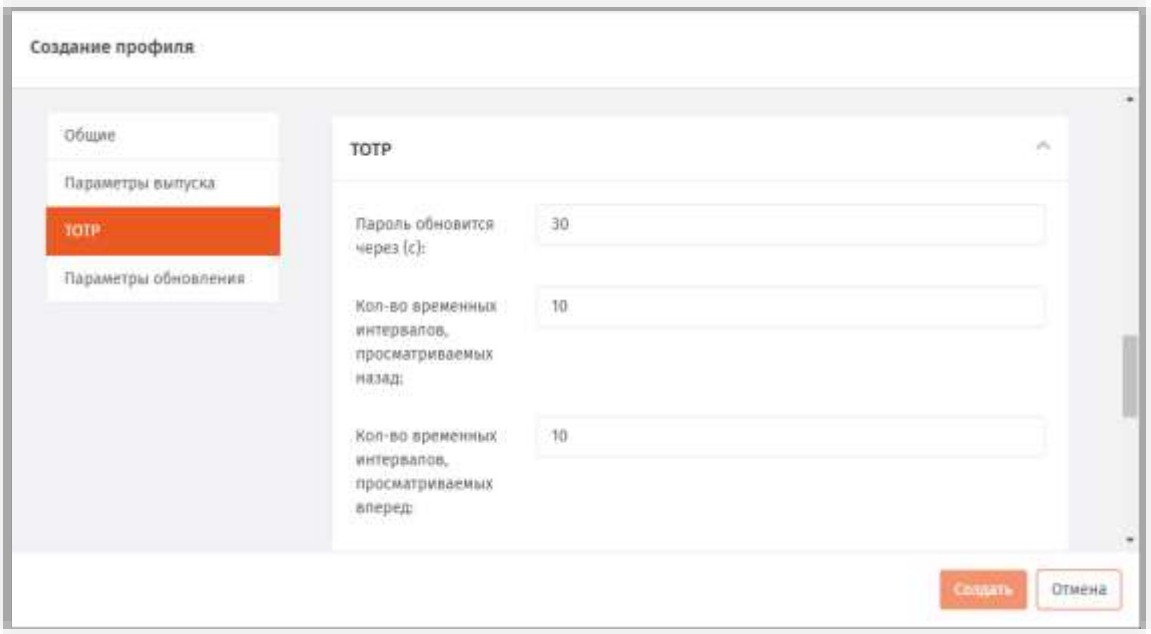


*Рис. 178 – Вкладка **TOTP***

6. Выполните настройки, руководствуясь Табл. 45, с. 168.
7. Выберите вкладку **Параметры обновления**.
   Окно примет следующий вид.

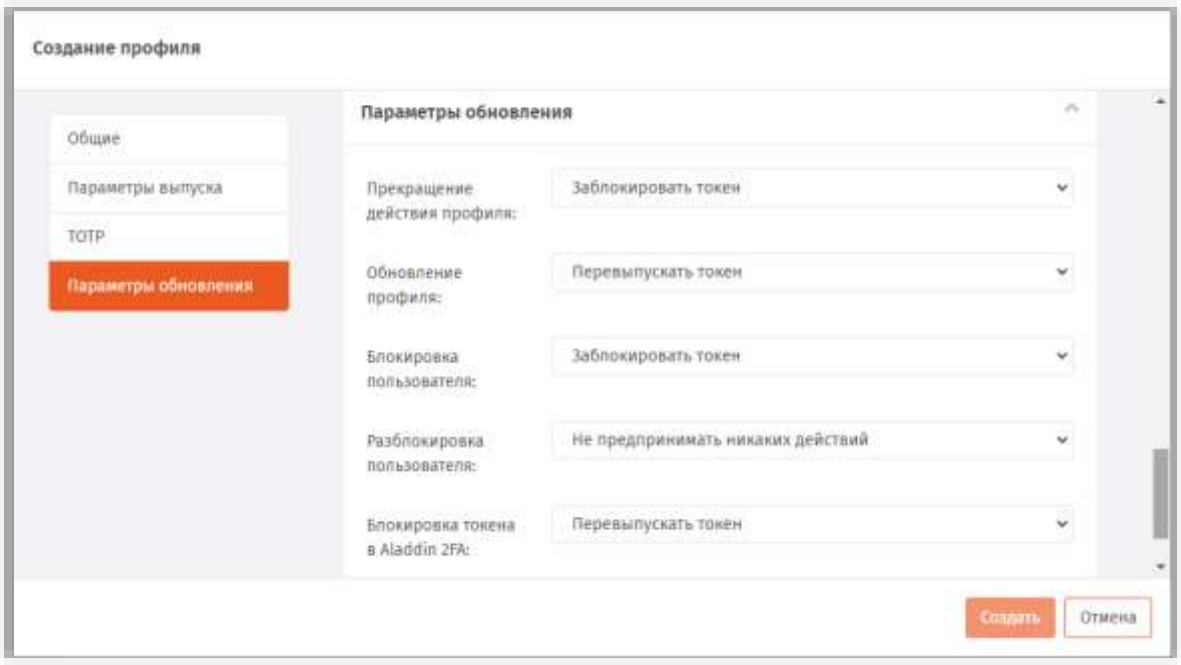


*Рис. 179 – Вкладка **Параметры обновления***

8. Выполните настройки, руководствуясь Табл. 51.

Табл. 51 – Параметры обновления профиля

Настройка	Описание
Прекращение действия профиля **Обновление профиля** **Блокировка пользователя** **Разблокировка пользователя**	Для данных параметров выполните настройки, руководствуясь Табл. 43, с. 163.
Блокировка токена в Aladdin 2FA	Параметр определяет действия, которые необходимо предпринять с PUSH OTP-токеном, выпускавшимся по данному профилю, в случае если токен был заблокирован в системе Aladdin 2FA. Доступные значения: • **Перевыпустить токен** – при блокировке токена в A2FA он должен быть перевыпущен в JMS (данная опция позволяет автоматически перевыпускать токен, если истекло время жизни «тикета» (т.е. одноразовой ссылки), значение которого по умолчанию 3 дня); • **Заблокировать токен** – при блокировке токена в A2FA он должен быть автоматически заблокирован в JMS. Значение по умолчанию: **Перевыпустить токен** **Примечание.** Действия, предлагаемые в данном параметре, реализуются в ходе выполнения задачи **Обслуживание PUSH OTP-токенов** плана обслуживания жизненного цикла OTP-токенов (см. раздел «План обслуживания жизненного цикла OTP-токенов», с. 281). Для того чтобы данная задача корректно обработала токены, заблокированные в A2FA, следует также включить выполнение задачи **Получение статусов PUSH OTP-токенов с сервиса Aladdin 2FA** в том же плане обслуживания

9. По окончании всех настроек нажмите кнопку **Создать** (Рис. 179, выше) или **Сохранить** (при редактировании профиля), чтобы сохранить изменения.

Примечание. При сохранении профиля выполняется проверка на завершённость других настроек, необходимых для успешного выпуска для пользователей Push OTP-токенов.

1. При появлении предупреждения об отсутствии настройки Веб-сервиса безопасной передачи OTP-секрета (Рис. 180) выполните соответствующую настройку в консольном агенте JMS (команда Aladdin.EAP.Agent.Terminal a2fa configure, подробнее см. руководство по установке и настройке JMS [2].
2. При появлении предупреждения об отсутствии настройки SMTP-транспорта (Рис. 171) выполните соответствующую настройку в консольном агенте JMS (команда Aladdin.EAP.Agent.Terminal smtp configure, подробнее см. руководство по установке и настройке JMS [2].

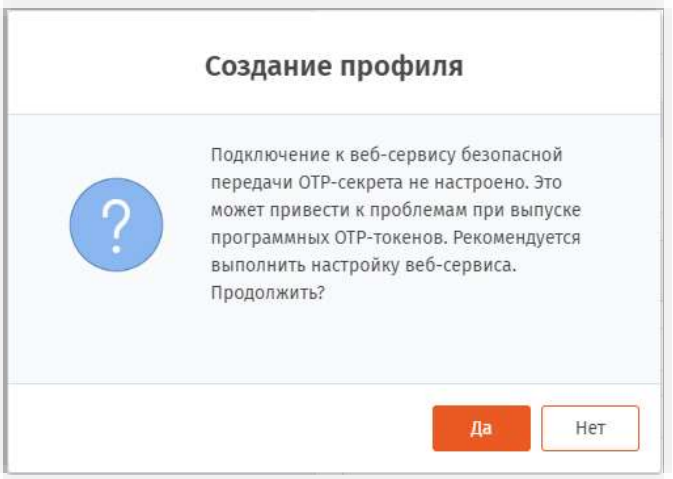


Рис. 180 – Предупреждение о необходимости настроить веб-сервис безопасной передачи OTP-секрета

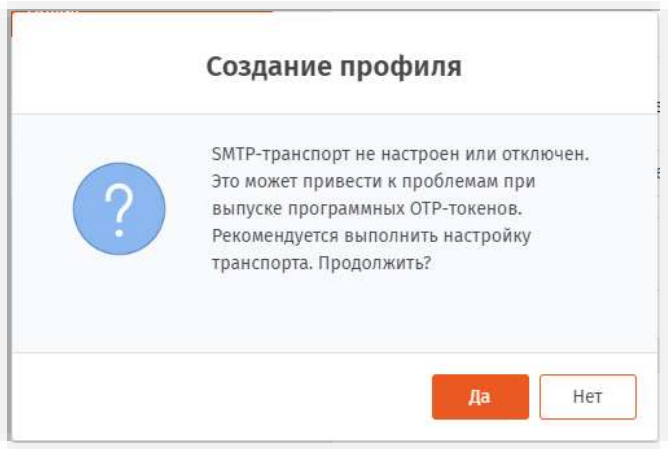


Рис. 181 – Предупреждение о необходимости включить и настроить SMTP-транспорт

3.6.14 Профиль управления ISO-образами JaCarta SF/ГОСТ

Для создания или настройки профиля записи ISO-образов JaCarta SF/ГОСТ выполните следующие действия:

1. В консоли управления JMS перейдите в раздел **Профили**
2. Выполните одно из следующих действий:

   – чтобы создать новый профиль, нажмите **Создать**, выберите тип профиля **Управление ISO-образами**.
   – чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию на нём правой кнопкой мыши выберите **Свойства**.

Отобразится страница следующего вида.

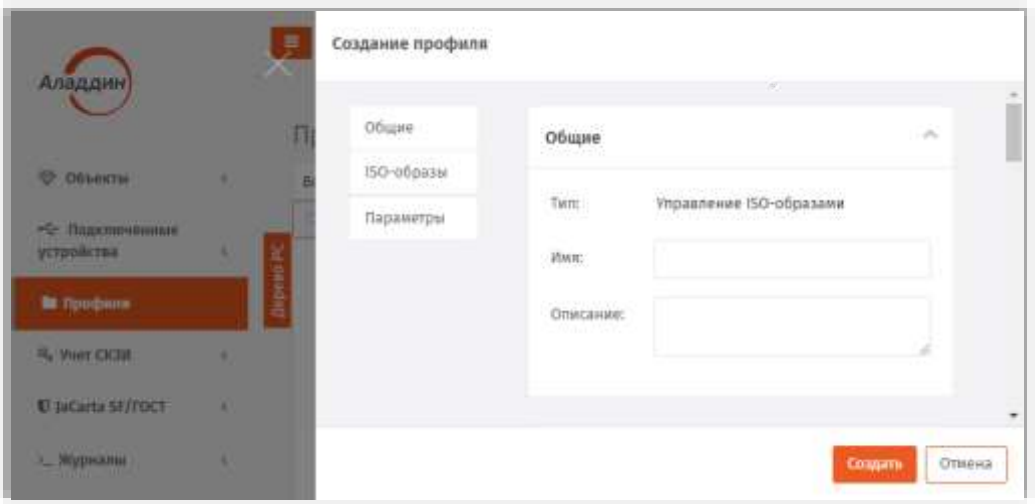


*Рис. 182 – Вкладка **Общие***

3. На вкладке **Общие** в соответствующих полях введите (или отредактируйте) имя и описание профиля.
4. Перейдите на вкладку **ISO Образы**.

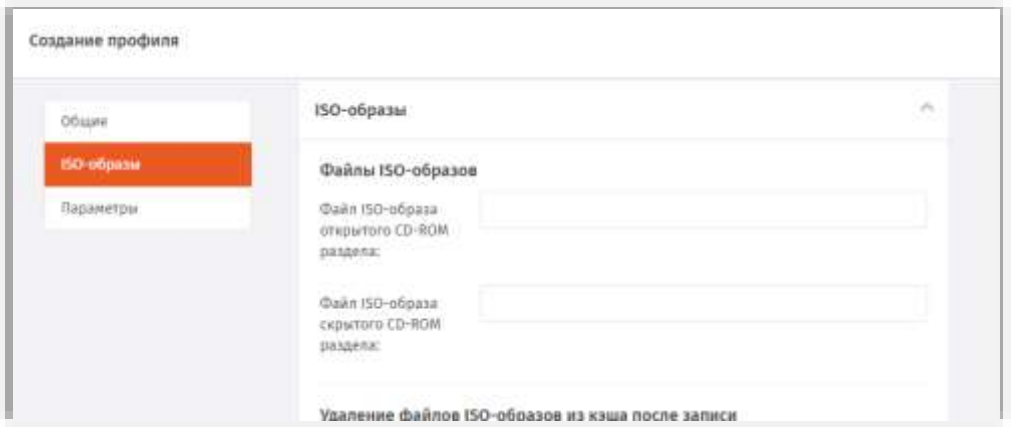


*Рис. 183 – Вкладка **ISO-образы***

5. Выполните настройку, руководствуясь Табл. 52.

Табл. 52 – Параметры записи ISO-образов JaCarta SF/ГОСТ

Пункт	Описание
Секция **Файл ISO-образа открытого раздела**	
Файл ISO-образа открытого CD-ROM раздела	Укажите полный сетевой путь к файлу ISO-образа открытого CD-ROM раздела. **Примечание.** Сетевой путь к файлу должен быть доступен для всех рабочих станций и консолей управления, используемых в развернутой системе JMS

Пункт	Описание
Файл ISO-образа скрытого CD-ROM раздела	То же для ISO-образа скрытого раздела.
Секция **Удаление файлов ISO-образов из кэша после записи**	
Консоль Управления JMS	При установке флага ISO-образы разделов CD-ROM будут удалены из кэша компьютера с установленной консолью управления JMS. Флаг установлен по умолчанию
Клиент JMS	При установке флага ISO-образы разделов CD-ROM будут удалены из кэша компьютера с установленным клиентом JMS. Флаг установлен по умолчанию.

6. Перейдите на вкладку **Параметры**.
7. Выполните необходимые настройки, руководствуясь Табл. 53.

Табл. 53 – Параметры записи ISO-образов JaCarta SF/ГОСТ

Пункт	Описание
Секция **Параметры обновления**	
Разрешить обновление средствами клиента JMS	Установите флаг в случае, если необходимо предоставить возможность пользователям обновлять ISO-образы в ЭН, подключенных к компьютеру, при работе из клиента JMS.
Блокировать ключевой носитель в случае отказа от обновления после указанной даты	Установите флаг в случае, если необходимо заблокировать ЭН JaCarta SF/ГОСТ при отказе от обновления после даты, указанной в поле **Последний день обновления**
Последний день обновления	Выберите дату, если установлен признак блокировки
Блокировать ключевой носитель в случае отказа от обновления при превышении количества подключений скрытых разделов	Установите флаг в случае, если необходимо заблокировать ЭН JaCarta SF/ГОСТ с устаревшим ISO-образом по счетчику подключений скрытых разделов (указывается в числовом поле). Значение по умолчанию: **10** (подключений скрытых разделов)
Очищать ISO-образ после отвязки профиля	Установите флаг в случае, если необходимо удалить ISO-образ с ЭН JaCarta SF/ГОСТ после того, как привязка профиля к контейнеру пользователя будет отменена.
Секция **Запрос на подтверждение операции**	
Консоль управления JMS	При установленном флаге, перед обновлением ISO-образов в консоли управления JMS будет выполнен запрос на разрешение пользователем операции.
Клиент JMS	При установленном флаге перед обновлением ISO-образов в клиенте JMS будет выполнен запрос на разрешение пользователем операции.

8. Нажмите **Создать** (или **Сохранить**, если редактировался ранее созданный профиль).

3.6.15 Профиль обновления встроенного ПО JaCarta SF/ГОСТ

Для создания или настройки профиля обновления встроенного ПО JaCarta SF/ГОСТ выполните следующие действия:

1. В консоли управления JMS перейдите в раздел **Профили**.
2. Выполните одно из следующих действий:

   – чтобы создать новый профиль, нажмите **Создать**, выберите тип профиля **Обновление встроенного ПО**.
   – чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию на нём правой кнопкой мыши выберите **Свойства**.

   Отобразится страница следующего вида.

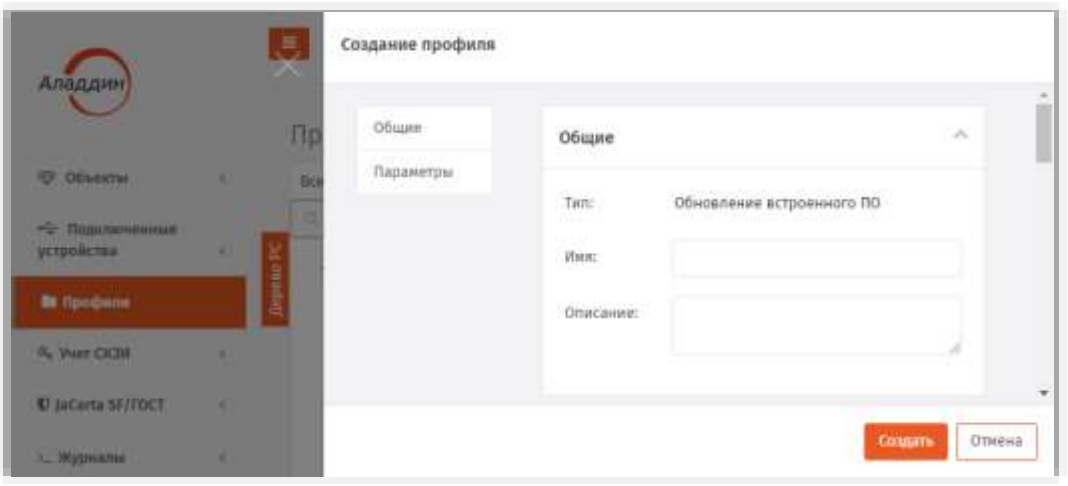


*Рис. 184 – Вкладка **Общие***

3. На вкладке **Общие** в соответствующих полях введите (или отредактируйте) имя и описание профиля.

4. Перейдите на вкладку **Параметры**.

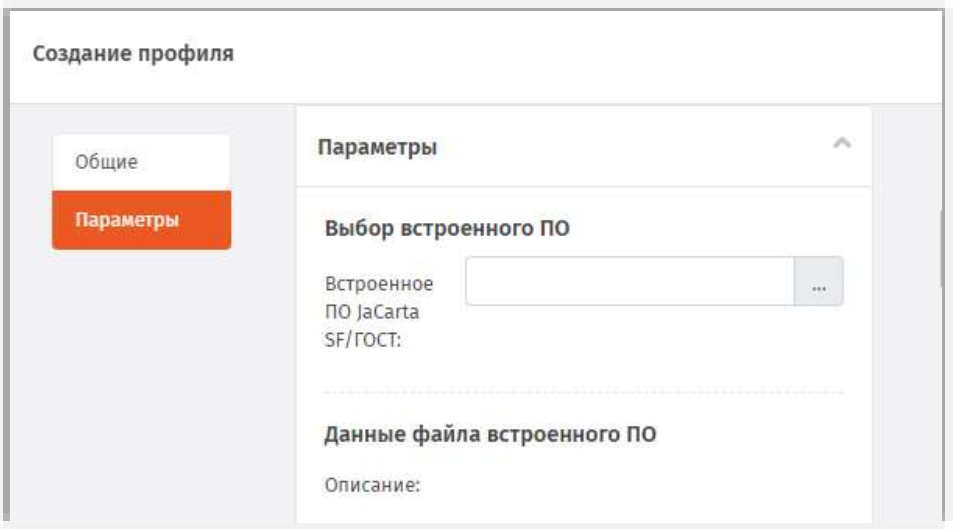


*Рис. 185 – Вкладка **Параметры***

5. Выполните настройку, руководствуясь Табл. 54.

Табл. 54 – Параметры обновления встроенного ПО JaCarta SF/ГОСТ

Пункт	Описание
Секция **Выбор встроенного ПО**	
Встроенное ПО JaCarta SF/ГОСТ	Нажмите три точки (...) и в отрывшемся списке выберите необходимую учетную запись файла обновления, ранее зарегистрированного в JMS (для получения актуального списка нажмите на **Обновить**). В случае если необходимое обновление в раскрывающемся списке отсутствует, добавьте его из файла, нажав **Зарегистрировать** (настройки выполняются по аналогии с настройками, изложенными в разделе «Регистрация обновлений встроенного ПО JaCarta SF/ГОСТ», с. 190).
Секция **Данные файла встроенного ПО**	
Описание	Описание пакета обновления встроенного ПО JaCarta SF/ГОСТ. Нередактируемое поле (заполняется автоматически).
Обновлять с версий	Список версий встроенного ПО JaCarta SF/ГОСТ, установленных в подключаемом ЭН, которые (и только они) требуют обновления**.** Нередактируемое поле (заполняется автоматически).
Обновлять по версию	Версия встроенного ПО, на которое будет осуществляться обновление. Нередактируемое поле (заполняется автоматически).
Секция **Параметры обновления**	
Разрешить обновление средствами клиента JMS	Установите флаг в случае, если необходимо предоставить возможность пользователям обновлять встроенное ПО JaCarta SF/ГОСТ в ЭН, подключенных к компьютеру, на которых установлен клиент JMS.

Пункт	Описание
Блокировать ключевой носитель в случае отказа от обновления после указанной даты	Установите флаг в случае, если необходимо заблокировать ЭН JaCarta SF/ГОСТ при отказе от обновления после даты, указанной в поле **Последний день обновления**
Последний день обновления	Выберите дату, если установлен признак блокировки
Блокировать ключевой носитель со старой версией встроенного ПО при превышении количества подключений скрытых разделов	Установите флаг в случае, если необходимо заблокировать ЭН JaCarta SF/ГОСТ с устаревшей прошивкой по счетчику подключений скрытых разделов (указывается в поле числовом поле **Количество подключений скрытых разделов до блокировки**, ниже). Значение по умолчанию: **10** (подключений скрытых разделов)
Количество подключений скрытых разделов до блокировки	Укажите число подключений срытых разделов, после которых следует заблокировать ЭН в случае, если пользователь откажется от обновления встроенного ПО
Предупреждение о переинициализации носителя после обновления	В случае если после обновления прошивки в ЭН требуется его переинициализация, установите данный флаг.  **Примечание.** Информация о необходимости переинициализации ЭН после обновления в нем встроенного ПО содержится в сопроводительной документации к данному файлу обновления встроенного ПО.
Переинициализировать носитель автоматически после обновления	Установите флаг, если перенициализация ЭН должна выполняться автоматически.

6. Нажмите **Создать** (или **Сохранить**, если редактировался ранее созданный профиль).

3.6.16 Импорт/экспорт контейнеров JaCarta SF/ГОСТ (kka-контейнеров)

Контейнеры JaCarta SF/ГОСТ (kka-контейнеры) или *ключевые контейнеры администратора доступа* служат для инициализации работы с ЗНИ (в заводской документации – ЭН, электронными носителями) JaCarta SF/ГОСТ, определяют механизм доступа к скрытым разделам данных ЗНИ и содержат другую служебную информацию. Для доступа к данным в контейнере требуется знание PIN-кода (пароля) данного контейнера. (Подробное описание см. в документации из комплекта поставки ЭН JaCarta SF/ГОСТ).

Контейнеры .kka необходимы для выпуска и синхронизации ЗНИ JaCarta SF/ГОСТ. Данные контейнеры создаются с помощью ПО из комплекта поставки ЗНИ JaCarta SF/ГОСТ.

Для добавления или создания учетной записи с kka-контейнером выполните следующие действия:

1. В консоли управления JMS перейдите в раздел **JaCarta SF/ГОСТ -> Контейнеры JaCarta SF/ГОСТ**.

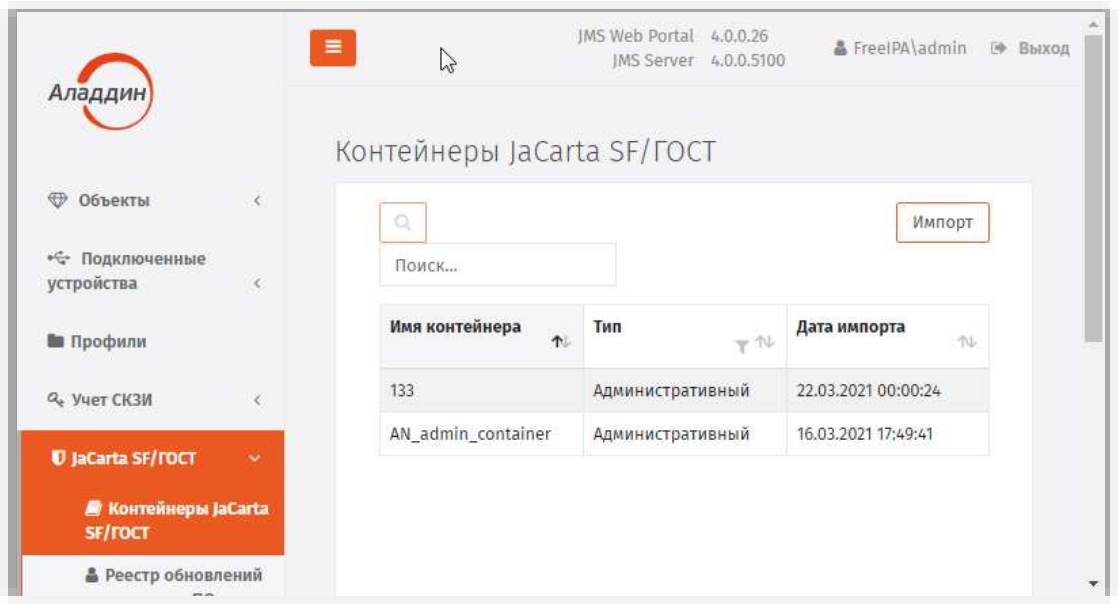


*Рис. 186 – Раздел **JaCarta SF/ГОСТ -> Контейнеры JaCarta SF/ГОСТ** консоли управления JMS*

2. Выполните одно из следующих действий:

- если вы хотите добавить новую учетную запись с контейнером JaCarta SF/ГОСТ, справа вверху нажмите **Импорт**, откроется страница импорта контейнера (Рис. 187);
- если вы хотите отредактировать существующую учетную запись с контейнером JaCarta SF/ГОСТ, в центральной части окна консоли управления JMS отметьте эту учетную запись, нажмите правой кнопкой мыши и в меню действий выберите **Свойства**.

Примечание. Если вы открыли уже зарегистрированную в JMS учетную запись контейнера, то для редактирования будет доступно только поле **Имя**.

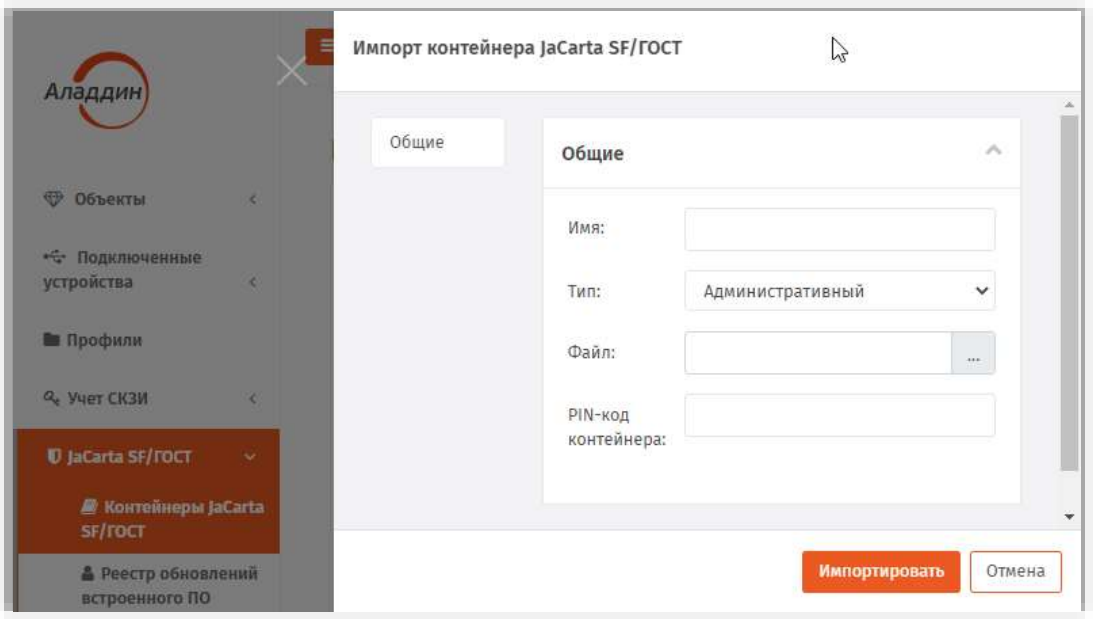


Рис. 187 – Страница импорта контейнера JaCarta SF/ГОСТ

3. Для импорта контейнера выполните необходимые действия, руководствуясь Табл. 55.

Табл. 55 – Параметры учетной записи контейнера JaCarta SF/ГОСТ

Пункт	Описание
Имя	Введите имя учетной записи контейнера, которое будет использоваться для обозначения данного контейнера в профилях, в которых он задействуется.
Тип	Из раскрывающегося списка выберите тип контейнера: • **Административный** – для импорта административного контейнера JaCarta SF/ГОСТ (в документации из комплекта ПО обозначается как *ключевой контейнер для ЭН администратора доступа*);
Файл	Нажмите на три точки «**...**» и в диалоге выберите файл с расширением **kka.** **Примечание.** Контейнеры JaCarta SF/ГОСТ создаются при помощи программного обеспечения из комплекта поставки электронных ключей JaCarta SF/ГОСТ. При этом в соответствии с документацией JaCarta SF/ГОСТ данные контейнеры имеют следующие названия: • «ключевой контейнер ЭН администратора доступа» (контейнер JaCarta SF/ГОСТ, используемый для инициализации административных электронных ключей JaCarta SF/ГОСТ. Тип: **Административный**);
PIN-код контейнера	Введите PIN-код контейнера JaCarta SF/ГОСТ, указанного в поле Файл. **Примечание.** PIN-код контейнера JaCarta SF/ГОСТ задается при создании последнего с помощью ПО из комплекта поставки JaCarta SF/ГОСТ. Заблаговременно узнайте PIN-код у администратора безопасности, создававшего данный контейнер.

4. Нажмите кнопку **Импортировать** в случае импортирования контейнера JaCarta SF/ГОСТ, либо **Сохранить** в случае редактирования ранее созданной учетной записи соответствующего контейнера.

Примечание. После сохранения контейнера в режиме редактирования (т.е. после нажатия на кнопку **Сохранить**) для выхода со страницы редактирования контейнера следует закрыть данную страницу (Рис. 188).

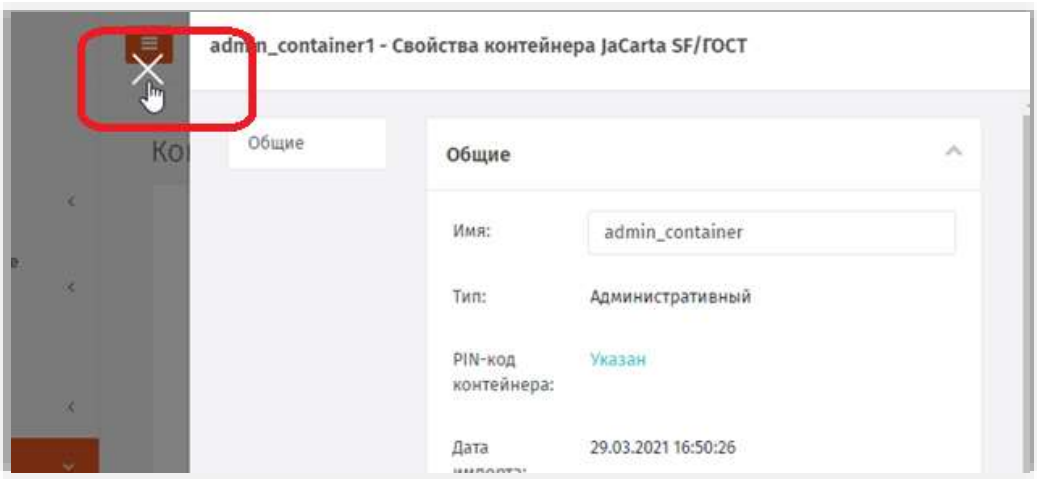


Рис. 188 – Закрытие страницы редактирования контейнера JaCarta SF/ГОСТ

Для экспорта контейнера JaCarta SF/ГОСТ, ранее импортированного в JMS, в разделе **JaCarta SF/ГОСТ** -> **Контейнеры JaCarta SF/ГОСТ** выберите в центральной части экрана необходимую учётную запись контейнера, нажмите на ней правой кнопкой мыши и выберите пункт **Экспорт.** Файл контейнера будет записан в папку, назначенную по умолчанию для загрузок (для скачанных файлов) используемого web-браузера.

Для экспорта контейнера JaCarta SF/ГОСТ пользователю JMS должно быть предоставлено право на операцию «JaCarta SF/ГОСТ – Контейнеры: Экспорт»

3.6.17 Регистрация обновлений встроенного ПО JaCarta SF/ГОСТ

В JMS имеется возможность добавлять в БД файлы обновления встроенного ПО (прошивки) электронных ключей (ЭН) JaCarta SF/ГОСТ, и в дальнейшем управлять данными файлами.

Для создания учетной записи с файлом обновления встроенного ПО JaCarta SF/ГОСТ выполните следующие действия:

5. В консоли управления JMS перейдите в раздел **JaCarta SF/ГОСТ -> Реестр обновлений встроенного ПО JaCarta SF/ГОСТ**.

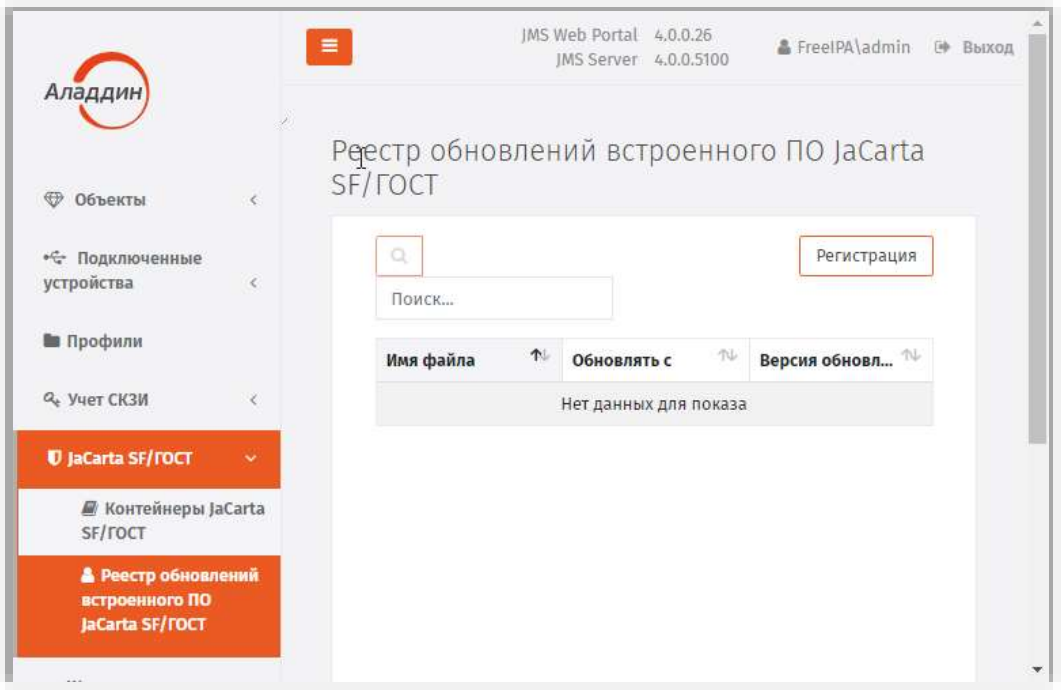


*Рис. 189 – Раздел **JaCarta SF/ГОСТ** -> **Реестр обновления встроенного ПО JaCarta SF/ГОСТ** консоли управления JMS*

б. Выполните одно из следующих действий:

- если вы хотите добавить новую учетную запись с файлом обновления встроенного ПО JaCarta SF/ГОСТ, справа вверху нажмите **Регистрация**, откроется страница регистрации обновления встроенного ПО (Рис. 190);
- если вы хотите отредактировать существующую учетную запись с файлом обновления встроенного ПО JaCarta SF/ГОСТ, в центральной части окна консоли управления JMS отметьте эту учетную запись, нажмите правой кнопкой мыши и в меню действий выберите **Свойства**.

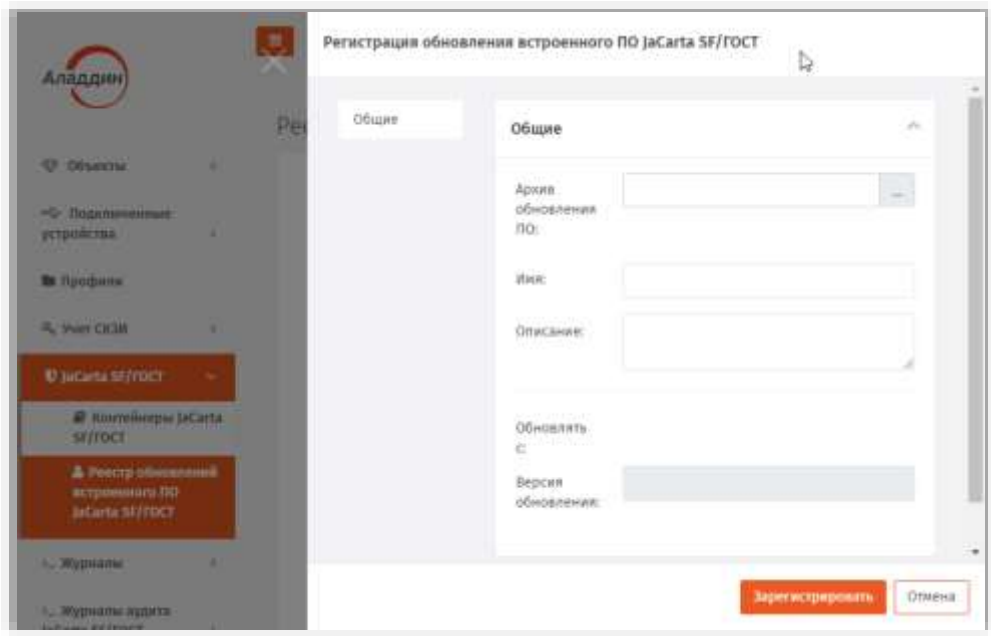


Рис. 190 – Страница регистрации обновления встроенного ПО JaCarta SF/ГОСТ

7. Для регистрации файла обновления встроенного ПО выполните необходимые действия, руководствуясь Табл. 56.

Табл. 56 – Параметры учетной записи файла обновления встроенного ПО JaCarta SF/ГОСТ

Пункт	Описание
Архив обновления ПО	Нажмите на три точки «**...**» и в диалоге выберите zip-файл обновлением встроенного ПО
Имя	Имя пакета обновления встроенного ПО в ЭН JaCarta SF/ГОСТ. Заполняется автоматически (может быть отредактировано).
Описание	Описание пакета обновления встроенного ПО JaCarta SF/ГОСТ. Заполняется автоматически (может быть отредактировано).
Обновлять с	Список версий встроенного ПО JaCarta SF/ГОСТ, установленных в подключаемом ЭН, которые (и только они) требуют обновления с помощью файла, указанного в поле **Архив обновления ПО.** Нередактируемое поле (заполняется автоматически).
Дата создания	Дата создания файла обновления встроенного ПО JaCarta SF/ГОСТ. Нередактируемое поле (заполняется автоматически).
Версия обновления	Версия регистрируемого обновления. Нередактируемое поле (заполняется автоматически).

8. Нажмите **Зарегистрировать** в случае регистрации файла обновления встроенного ПО JaCarta SF/ГОСТ, либо **Сохранить** в случае редактирования учетной записи ранее зарегистрированного файла обновления.

После регистрации новая учетная запись отобразится в реестре обновлений встроенного ПО JaCarta SF/ГОСТ:

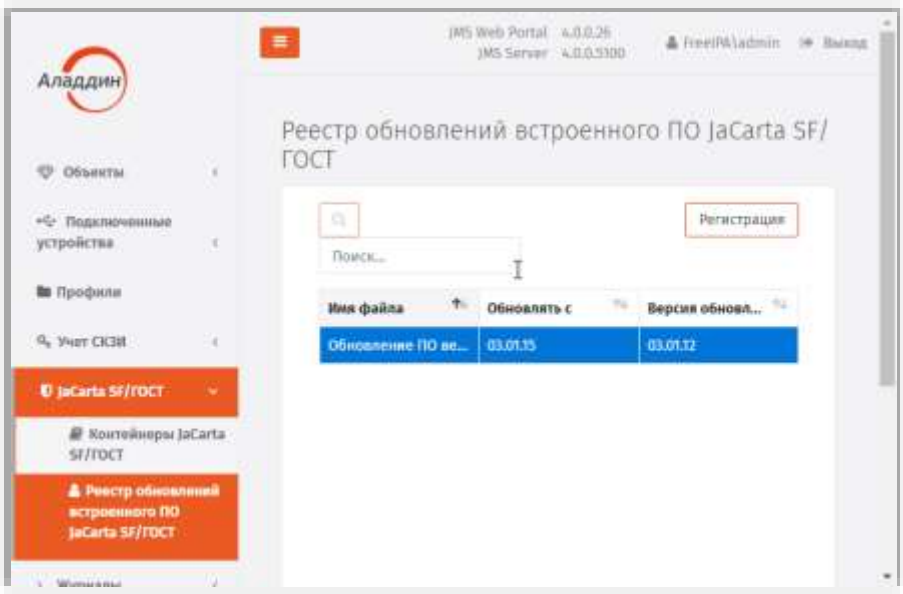


Рис. 191 – Учетная запись в реестре обновлений встроенного ПО JaCarta SF/ГОСТ

3.6.18 Настройка профиля доступа в личный кабинет JWM

Примечание. Профили **Доступ в личный кабинет** становятся доступны в консоли управления JMS после установки расширения *JWM-коннектор для JMS* (подробнее см. руководство по установке и настройке [2], раздел «JWM-коннектор для JMS») на компьютере, где развернуто приложение *Консоль управления JMS*.

Профиль **Доступ в личный кабинет** предназначен для массовой настройки свойств пользователей, на которых распространяется действие данного профиля (благодаря механизмам привязки профилей и фильтрации пользователей на основе **Глобальных групп**.)

Заданные в профиле права пользователей по отношению к объектам доступа из их личного кабинета на портале JWM будут занесены в личные настройки пользователей после выполнения **Плана обслуживания настроек личного кабинета** (см. раздел «План обслуживания настроек личного кабинета», с. 287).

Права пользователей по отношению к объектам доступа из их личного кабинета на портале JWM можно найти в свойствах пользователя на вкладке **Личный кабинет**.

Важно! При привязке профиля **Доступ в личный кабинет** к контейнеру ресурсной системы нужно убедиться, что к одному контейнеру привязано не более одного профиля.

Для создания (или настройки) профиля выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Профили**.
2. Выполните одно из следующих действий:

   – чтобы создать новый профиль, нажмите **Создать** выберите тип профиля **Прочее -> Доступ в личный кабинет**.
   – чтобы изменить существующий профиль, выберите этот профиль на правой панели в консоли управления JMS, после чего по нажатию правой кнопкой мыши выберите **Свойства**.

Отобразится следующее окно.

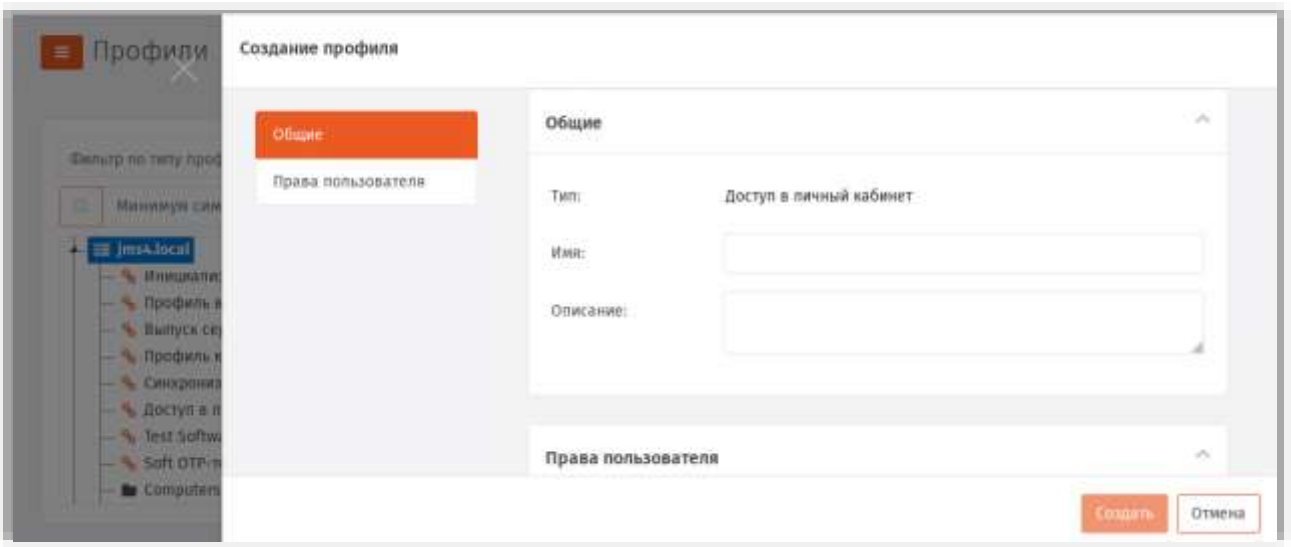


*Рис. 192 – Вкладка **Общие***

3. В соответствующих полях введите (или отредактируйте) имя и описание профиля.
После редактирование полей на вкладке **Общие** переходите на вкладку **Права пользователя**.

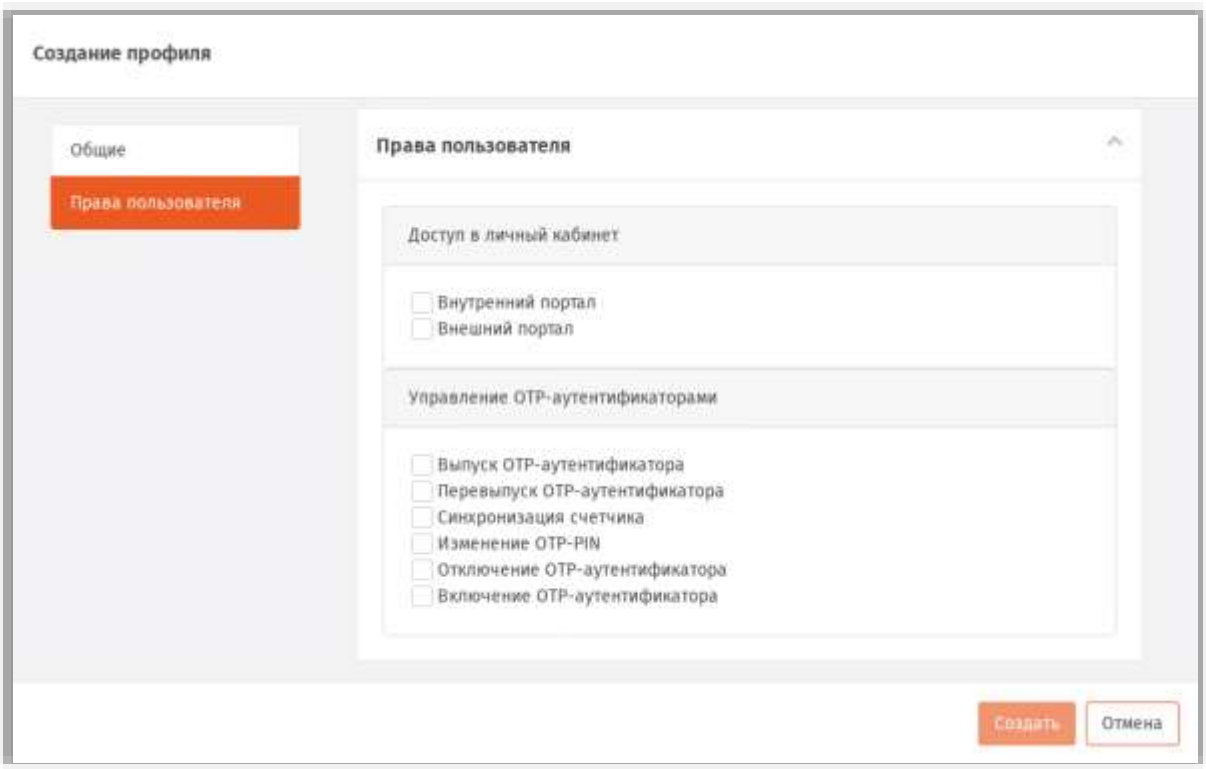


*Рис. 193 – Вкладка **Права пользователя***

4. Выполните настройки, руководствуясь Табл. 57.

Табл. 57 – Права пользователей по отношению к объектам личного кабинета на портале JWM

Настройка	Описание
<секция> **Доступ в личный кабинет**	
Внутренний портал	Установите флаг, если пользователю необходимо предоставить право аутентификации в личном кабинете на внутреннем портале JWM
Внешний портал	Установите флаг, если пользователю необходимо предоставить право аутентификации в личном кабинете на внешнем портале JWM
<секция> **Управление OTP-аутентификаторами** (в настоящей секции под OTP-аутентификаторами подразумеваются программный OTP-, Messaging- и A2FA Push-токены)	
Выпуск OTP-аутентификатора	Установите флаг, если пользователю следует разрешить самостоятельный выпуск OTP-аутентификатора
Перевыпуск OTP-аутентификатора	Установите флаг, если пользователю следует разрешить самостоятельный перевыпуск OTP-аутентификатора
Синхронизация счётчика	Установите флаг, если пользователю следует разрешить самостоятельную синхронизацию счетчиков в OTP-аутентификаторе и БД JAS
Изменение OTP-PIN	Установите флаг, если пользователю следует разрешить самостоятельную смену (установку) PIN-кода для OTP
Отключение OTP-аутентификатора	Установите флаг, если пользователю следует разрешить самостоятельную блокировку своего OTP-аутентификатора
Включение OTP-аутентификатора	Установите флаг, если пользователю следует разрешить самостоятельную разблокировку своего OTP-аутентификатора

По окончании всех настроек нажмите кнопку **Создать** (Рис. 193, выше) или **Сохранить** (при редактировании профиля), чтобы сохранить изменения.

3.6.19 Привязка профилей

Для выпуска электронных ключей после настройки профилей необходимо привязать эти профили к пользователям, на имя которых электронные ключи будут выпускаться.

Чтобы привязать созданные профили к пользователям, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Профили**.

2. В центральной панели отметьте контейнер, содержащий пользователей, к которым вы хотите привязать настроенные профили (например, контейнер **FreeIPA**), нажмите на нем правой кнопкой мыши и в появившемся меню выберите **+ Привязать профиль:**

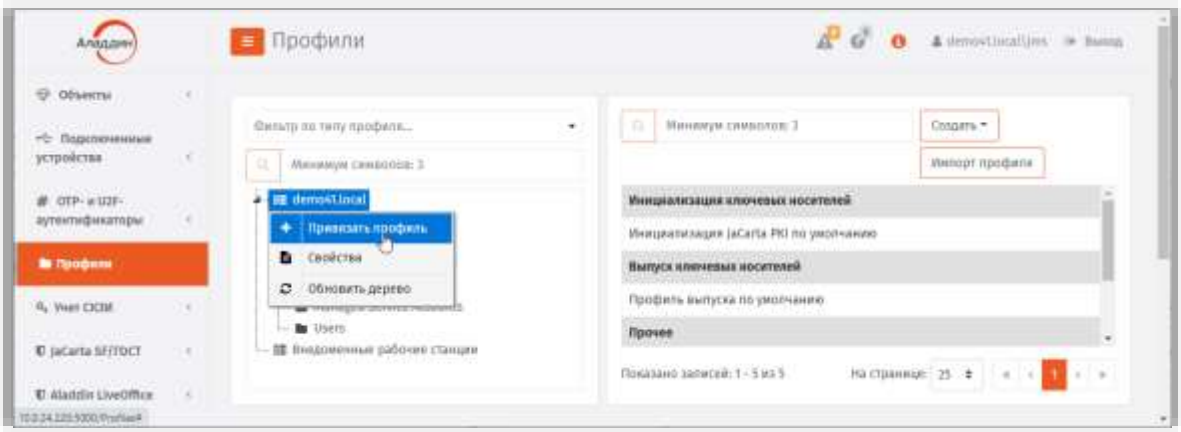


Рис. 194 – Выбор контейнера для привязки профиля

3. Откроется перечень профилей.

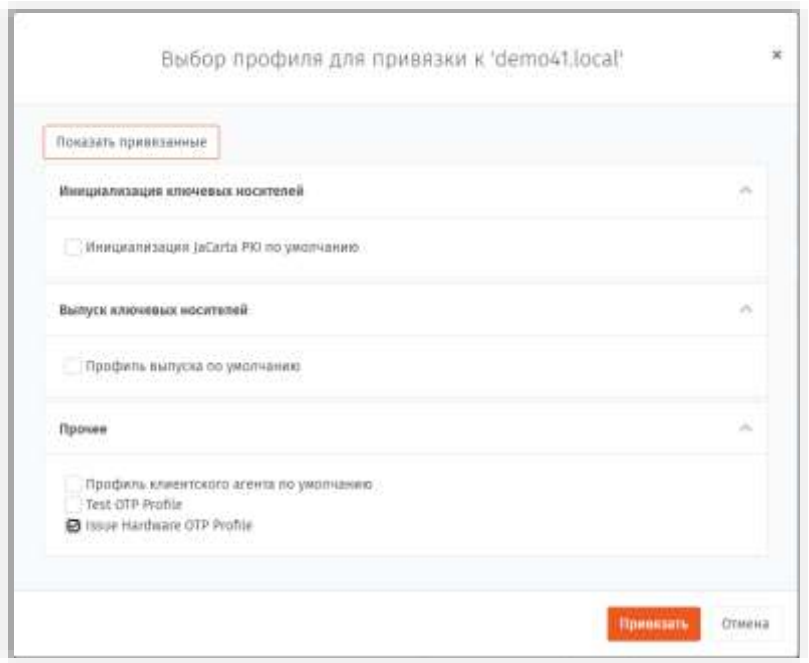


Рис. 195 – Выбор профилей для привязки к контейнеру

4. Отметьте профили, которые вы хотите привязать к выбранному контейнеру, и нажмите **Привязать**. Отобразится окно запроса на подтверждение привязки:

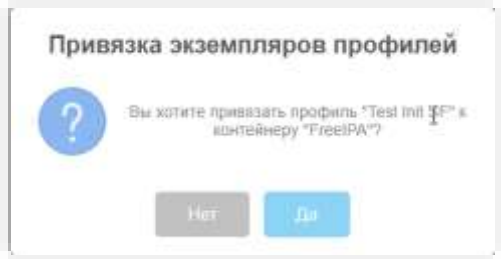


Рис. 196 – Окно запроса на подтверждение привязки профиля

5. Для привязки профиля нажмите Да.

Список привязок отобразится на центральной панели с контейнерами ресурсной системы:

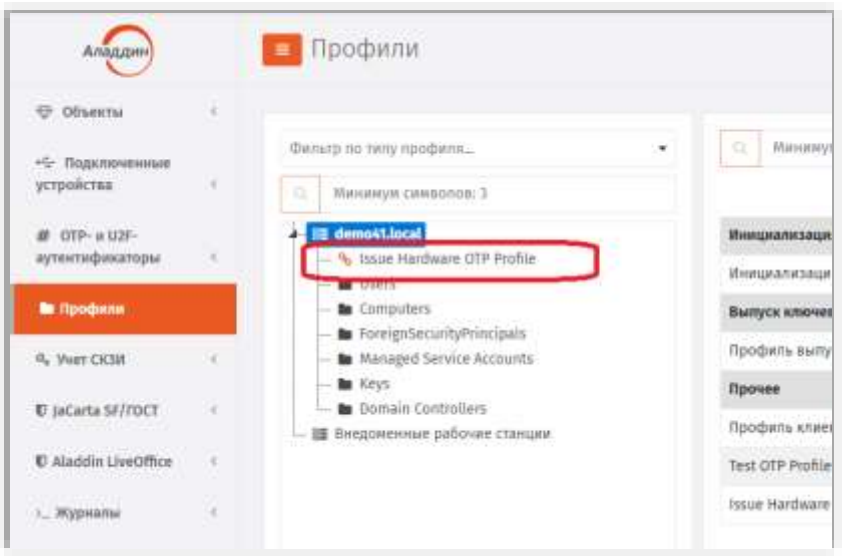


Рис. 197 – Результат привязки профилей к контейнеру ресурсной системы

Примечание. Привязку профилей можно также выполнить методом «перетаскивания мышью» профилей из правой панели на панель с деревом ресурсной системы.

Для отмены привязки профиля к контейнеру выполните следующие действия.

1. Выберите необходимую привязку профиля в центральной части окна.
2. Нажмите на ней правой кнопкой мыши и выберите пункт **–Отменить привязку**.

С примерами порядка настройки и привязки профилей можно ознакомиться в разделе «Примеры настроек профилей», с. 203.

3.6.20 Ограничение действия профилей через группы домена/глобальные группы JMS

Чтобы распространить действие привязки профиля только на определенных пользователей выбранного контейнера ресурсной системы (а также на определенные рабочие станции),

используя группы домена (или ресурсной системы, такой как FreeIPA или Active Directory) или глобальные группы JMS, выполните следующие действия.

Если вы планируете ограничить действие привязки профиля за счет глобальных групп JMS, такие группы предварительно нужно создать (см. «Глобальные группы JMS», с. 261).

1. В консоли управления JMS перейдите в раздел **Профили**.
   Окно консоли будет выглядеть следующим образом.

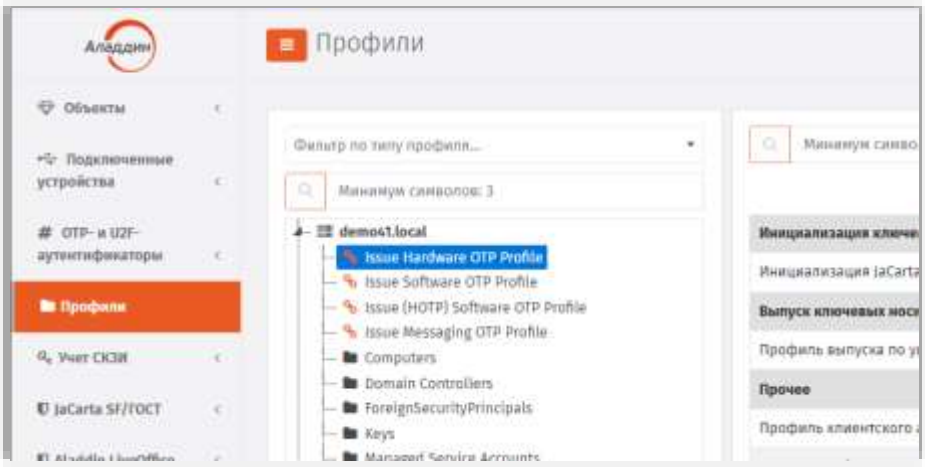


Рис. 198 – Привязки профилей

2. В центральной части окна отметьте привязку, действие которой необходимо ограничить глобальной группой, нажмите на ней правой кнопкой и выберите **Свойства**.
   Отобразится окно следующего вида.

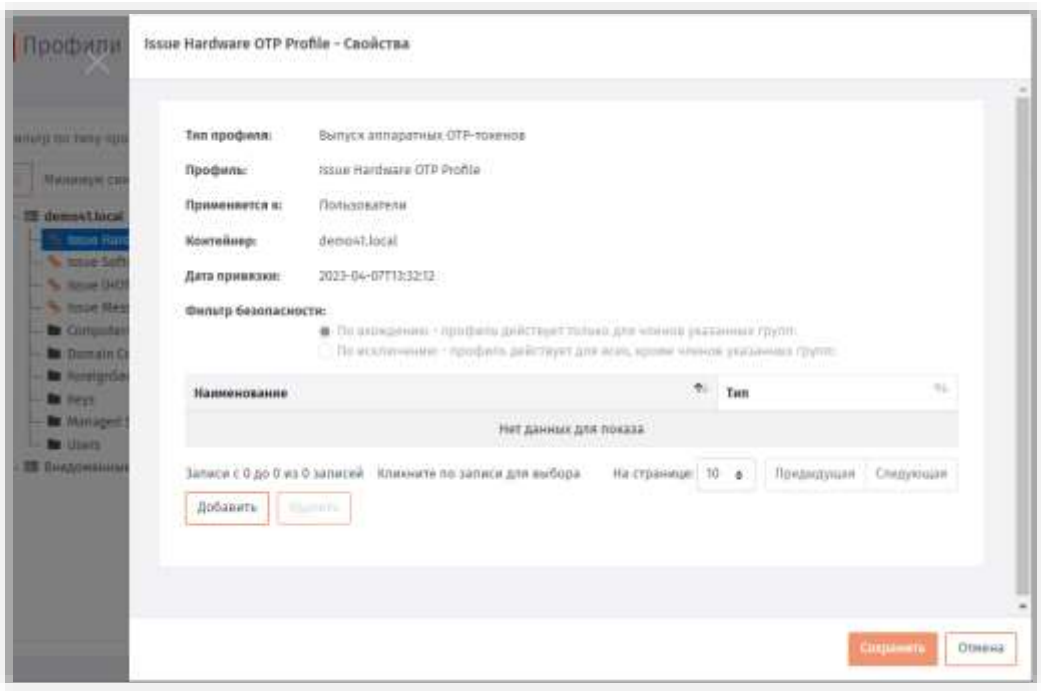


Рис. 199 – Свойства привязки профиля

3. В секции **Фильтр безопасности** нажмите **Добавить**.

Отобразится окно следующего вида.

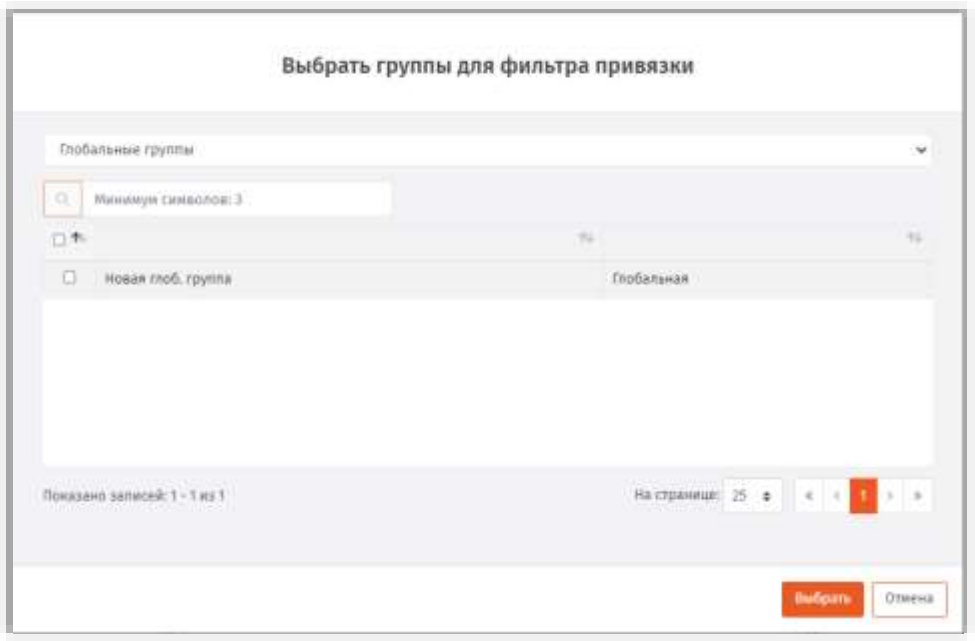


Рис. 200 – Окно выбора групп для фильтра привязки

4. В верхнем поле выберите тип групп для фильтрации (**Глобальные группы** или группы домена ресурсной системы, Рис. 201). По умолчанию выбраны **Глобальные группы**.

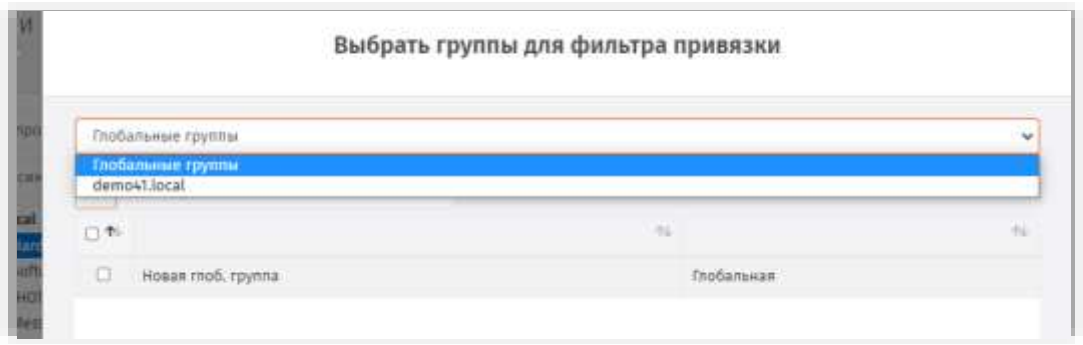


Рис. 201 – Выбор типа группы для фильтрации

5. При выборе фильтра по глобальным группам отобразится соответствующее окно (по умолчанию, Рис. 200). Выберите в нем необходимые группы и нажмите **Выбрать**.
6. При необходимости добавить доменные группы, в верхнем поле выберите домен (ресурсную систему, Рис. 201).

Отобразится окно следующего вида

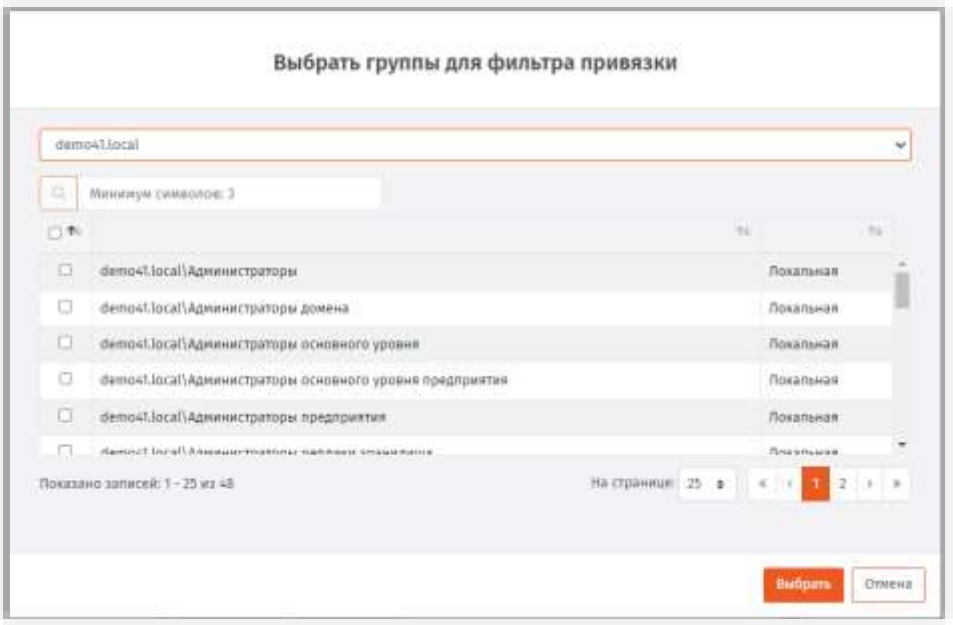


Рис. 202 – Окно выбора доменных (локальных) групп

7. Отметьте доменную (локальную) группу (группы), которой вы хотите ограничить область действия привязки профиля, после чего нажмите **Выбрать**.
8. Выбранные группы отобразятся в списке **Фильтр безопасности (**Рис. 203**)**.

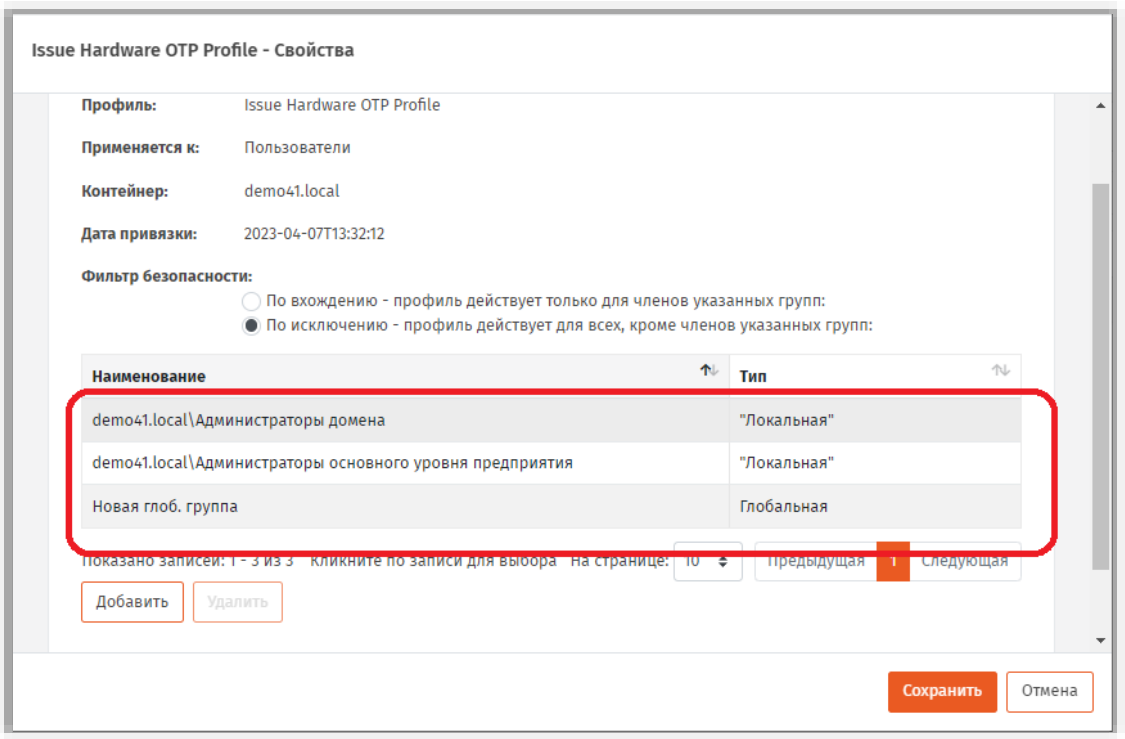


Рис. 203 – Окно выбора доменных (локальных) групп

9. В секции **Фильтр безопасности** выберите один из двух пунктов:
   - **По вхождению – профиль действует только для членов указанных групп**;

- **По исключению – профиль действует для всех, кроме членов указанных групп**.

10. Повторите необходимые действия, если необходимо создать фильтр с использованием других групп JMS.
11. Нажмите **Сохранить**, чтобы сохранить изменения и закрыть окно.

3.6.21 Наследование профилей

В JMS контейнеры (например, cn=accounts) ресурсных систем (например, FreeIPA) наделены настраиваемым признаком наследования профилей. *Наследование профилей* вложенным контейнером означает, что действие профилей, привязанных к вышестоящему контейнеру, переносится на данный вложенный контейнер. По умолчанию наследование профилей в JMS разрешено во всех контейнерах.

Для того чтобы запретить/разрешить наследование профилей у контейнера, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Профили**.
2. На центральной панели с деревом ресурсной системы выберите необходимый контейнер, нажмите правой кнопкой мыши и выберите **Запретить наследование** (в случае запрета) или **Разрешить наследование** (в случае разрешения).
3. В окне подтверждения действия нажмите **Да**.

После запрета/разрешения наследования профилей изменения отразятся в полях **Наследование** и **Унаследованные профили** свойств контейнера (можно посмотреть, выбрав пункт **Свойства** по нажатию правой кнопкой мыши на контейнере).

3.6.22 Экспорт/импорт профилей

Чтобы экспортировать/импортировать профиль JMS, выполните следующие действия.

Экспорт профилей

1. В консоли управления JMS перейдите в раздел **Профили**.
2. В правой секции страницы выберите профиль, который нужно экспортировать, нажмите на нем правой кнопкой мыши и в контекстном меню выберите **Экспорт**.
3. В окне подтверждения действия нажмите **Да**.

XML-файл с параметрами экспортированного профиля будет записан в папку, назначенную по умолчанию для загрузок (для скачанных файлов) используемого web-браузера.

Импорт профилей

1. В консоли управления JMS перейдите в раздел **Профили**.
2. Справа вверху страницы нажмите **Импорт**.
3. В отобразившемся окне укажите путь к XML-файлу профиля и нажмите **Открыть**.
4. В окне сообщения об успешном импорте нажмите **ОК**.

Импортированный профиль отобразится в списке профилей в правой секции страницы.

3.6.23 Настройка параметров печати при выпуске объектов JMS

JMS позволяет настроить параметры печати документов, которые формируются при выпуске различных объектов в JMS (электронных ключей, ЗНИ и сертификатов). Настройка параметров печати осуществляется в свойствах профиля выпуска.


Существует возможность распечатать указанные в настройках профиля документы, как непосредственно в момент выпуска электронного ключа, так и по прошествии времени после выпуска электронного ключа (подробнее см. Акты и заявки).

В зависимости от профиля, в котором происходит настройка печати, возможна настройка параметров печати для следующих типов документов (см. табл. 58).

Табл. 58 – Параметры печати

Профиль	Тип документа
См. «Настройка профиля выпуска электронных ключей», с. 97.	• Заявка на выпуск КН; • Акт выдачи КН.
См. «Настройки профиля выпуска сертификатов в центре сертификации Microsoft», с. 124.	• Запрос на сертификат; • Сертификат.
См. «Настройки профиля выпуска сертификатов в УЦ DogTag», с. 138.	

Настройка параметров печати документов рассмотрена на примере вкладки **Печать запроса** на сертификат (см. «Настройка печати на примере вкладки Печать акта выдачи КН», ниже). Настройка параметров печати на вкладках **Печать заявки на выпуск КН**, **Печать акта выдачи КН** и **Печать сертификата** аналогична приведенному примеру.

3.6.23.1 Настройка печати на примере вкладки Печать акта выдачи КН

В настоящем разделе приводится типовой пример настроек печати на соответствующей вкладке профилей выпуска ЭК, ЗНИ и сертификатов.

Вкладка **Печать акта выдачи КН** выглядит следующим образом:

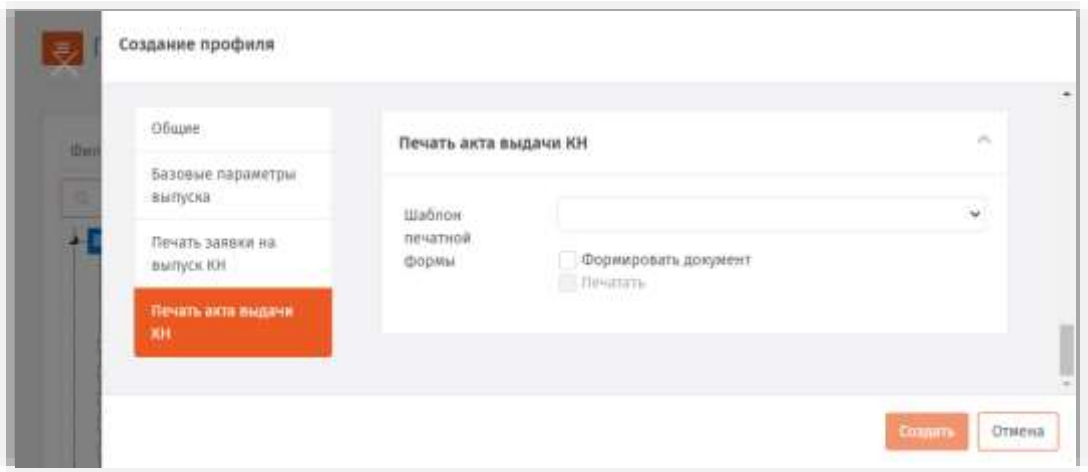


*Рис. 204 – Вкладка **Печать акта выдачи КН***

Чтобы настроить печать документов, связанных с выпуском электронных ключей, выполните следующие действия:

1. В поле **Шаблон печатной формы** выберите из раскрывающегося списка выберите шаблон печатной формы (например *Шаблон акта выдачи КН*), по которому будет создан и распечатан документ.

   О создании и настройке **Шаблона печатной формы** подробнее см. в разделе «Подсистема печати», с. 244.

2. Чтобы в процессе выпуска ключевого носителя/сертификата происходило формирование соответствующего документа следует установить флаг **Формировать документ** (Рис. 205, ниже). В случае если такой документ необходимо печатать в процессе выпуска, следует установить флаг **Печатать** (флаг становится активен только после выбора шаблона сертификата в поле Шаблон печатной формы).
   При установке флага **Печать** в процессе выполнения процедуры выпуска ключевого носителя/сертификата пользователю будет показано окно запроса на распечатку соответствующего документа. В противном случае (флаг **Печать** не установлен) документ будет сформирован и сохранен в БД JMS, после чего его можно распечатать из раздела Акты и заявки консоли управления JMS (см. раздел «Акты и заявки», с. 207)

Важно! Если флаг **Формировать документ** не установлен, то документ не будет сформирован в системе, т.е. его нельзя будет распечатать не только во время выпуска ключевого носителя/сертификата, но и позже.

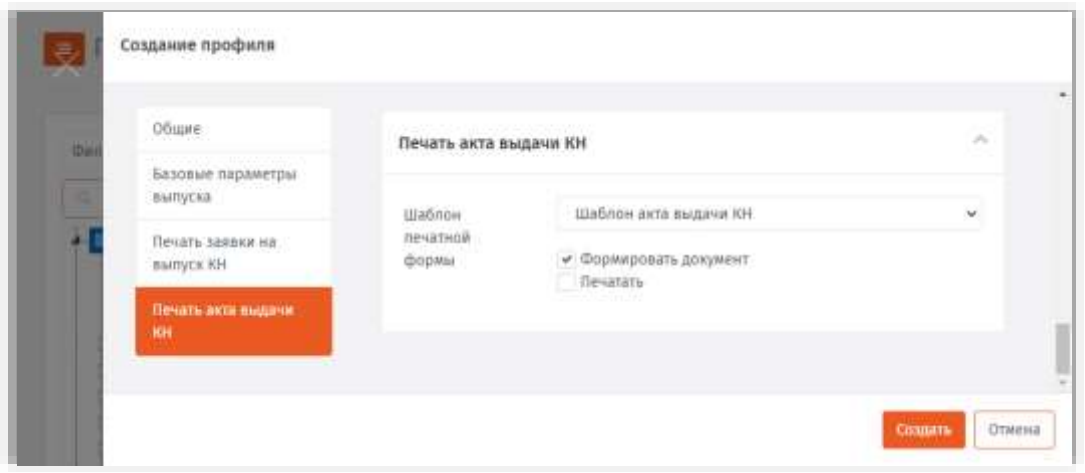


Рис. 205 – Пример корректной настройки печати документа

3.6.24 Примеры настроек профилей

Комплекс профилей, привязываемых в JMS к контейнеру (см. «Привязка профилей», с. 195), полностью определяет набор возможных действий в отношении ЭК/ЗНИ пользователя. Ниже представлены примеры действий для создания типовых наборов профилей и их настроек, которые необходимо выполнить, чтобы в JMS стали доступны основные операции с электронными ключами.

3.6.24.1 Профили для выпуска ЗНИ SF/ГОСТ из консоли управления JMS

Для выпуска ЗНИ SF/ГОСТ из консоли управления JMS необходимо выполнить привязку к пользователю (контейнеру пользователя в ресурсной системе) следующего набора профилей:

- *профиль выпуска ключевого носителя* (см. «Настройка профиля выпуска электронных ключей», с. 97); в настройках параметров выпуска (в профиле) нужно разрешить инициализацию в приложении SF (параметр **Способ выпуска для консоли администратора**).

  Примечание. В JMS к одному пользователю (контейнеру) не должно быть привязано более одного профиля выпуска ключевого носителя

- *профиль инициализации JaCarta SF/ГОСТ* (см. «Настройки параметров инициализации» -> «JaCarta SF/ГОСТ», с. 119).

В случае выпуска *ЭН пользователя* в профиле инициализации SF/ГОСТ на вкладке **Параметры** (см. «Вкладка Параметры», с. 120) в параметре **Режим инициализации** следует установить значение *Инициализация КН пользователя*

В случае выпуска *ЭН администратора доступа* в параметре **Режим инициализации** следует установить значение *Инициализация КН администратора*.

3.6.24.2 Профили для выпуска ЗНИ SF/ГОСТ из клиентского приложения JMS

Для того чтобы в клиенте JMS стал доступен выпуск ЗНИ SF/ГОСТ (ЭН Пользователя) следует настроить и привязать к пользователю (к его контейнеру) профили, указанные в разделе «Профили для выпуска ЗНИ SF/ГОСТ », выше. При этом в настройках параметров *профиля выпуска ключевого носителя* нужно разрешить инициализацию в приложении SF для клиента JMS (параметр **Способ выпуска для клиентского агента**).

Кроме того, необходимо создать (если он еще не создан) и привязать к пользователю *профиль клиентского агента*, а также настроить в нем параметры, разрешающие самостоятельный выпуск электронного ключа (см. «Настройка профиля клиентского агента», с. 101).

3.6.24.3 Профили для выпуска администратором электронного ключа с сертификатом

Для выпуска электронного ключа с сертификатом из консоли управления JMS необходимо выполнить привязку к пользователю (контейнеру пользователя в ресурсной системе) следующего набора профилей:

- *профиль выпуска ключевого носителя* (см. «Настройка профиля выпуска электронных ключей», с. 97);

  Примечание. В JMS к одному пользователю (контейнеру) не должно быть привязано более одного профиля выпуска ключевого носителя

- *профиль выпуска сертификата* (см. например «Настройки профиля выпуска сертификатов в УЦ DogTag», с. 138).

  Примечание. К одному пользователю (контейнеру) может быть привязано несколько профилей выпуска сертификата. Число выпускаемых сертификатов на электронном ключе будет равно числу таких привязанных профилей.

В случае если при выпуске электронного ключа требуется его очистка (инициализация) и установка заданных параметров аутентификации (PIN-кодов по умолчанию, парольной политики и др.), следует также:

- создать (если отсутствует) и привязать соответствующий *профиль инициализации ключевого носителя* (см. «Настройки параметров инициализации», с. 105)
- в *профиле выпуска ключевого носителя* в настройках параметров выпуска нужно разрешить инициализацию в соответствующем приложении (параметр **Способ выпуска для консоли администратора**).

3.6.24.4 Профили для выпуска пользователем электронного ключа с сертификатом

Для того чтобы в клиенте JMS стал доступен выпуск электронного ключа с сертификатом следует настроить и привязать к пользователю (к его учетной записи в JMS или контейнеру) профили, указанные в разделе «Профили для выпуска администратором электронного ключа с сертификатом», выше, с тем отличием, что в случае настройки *профиля инициализации ключевого носителя*, в *профиле выпуска ключевого носителя* в настройках параметров выпуска для того чтобы разрешить инициализацию в соответствующем приложении следует настраивать параметр **Способ выпуска для клиентского агента**.

Кроме того, необходимо создать (если он еще не создан) и привязать к пользователю *профиль клиентского агента*, а также настроить в нем параметры, разрешающие самостоятельный выпуск электронного ключа (см. «Настройка профиля клиентского агента», с. 101).

3.6.24.5 Порядок настройки самостоятельного выпуска пользователями OTP-аутентификатора

Настройка самостоятельного выпуска пользователями OTP-аутентификатора из личного кабинета JWM использует специальные механизмы JMS, которые требуют выполнения дополнительных действий, отличных от стандартных настроек при выпуске других объектов JMS.

Примечание. Под OTP-аутентификаторами подразумеваются программный OTP-, Messaging- и A2FA Push-токены.

Для настройки самостоятельного выпуска пользователями OTP-аутентификатора выполните следующие действия

1. Создайте профиль выпуска OTP-аутентификатора в зависимости от требуемого типа:
   - профиль выпуска программного OTP-токена (см. «Настройка профиля выпуска программных OTP-токенов», с. 164);
   - профиль выпуска Messaging-токена (см. «Настройка профиля выпуска Messaging-токенов», с. 171);
   - профиль выпуска Push OTP-токена (см. «Настройка профиля выпуска Push OTP-токенов», с. 177).
2. Создайте глобальную группу для пользователей, которым необходимо предоставить право на самостоятельный выпуск OTP (см. «Глобальные группы JMS», с. 261, группу можно оставить пустой, не добавляя в нее пользователей, подробнее см. далее)
3. Выполните привязку профиля (см. «Привязка профилей», с. 195).
4. Добавьте в привязку фильтр по глобальной группе, созданной на шаге 2 (создание фильтра см. в разделе «**Ограничение действия профилей через группы** домена/глобальные группы JMS», с. 197). Глобальную группу можно оставить пустой, поскольку специальный механизм индивидуального выпуска OTP-аутентификаторов будет заполнять эту группу автоматически.

   Примечание.

1. При отсутствии настройки фильтра по глобальной группе у пользователя не будет возможности отказаться от выпуска данного вида аутентификатора в момент, когда ему будет предоставлен список возможных аутентификаторов для выпуска.
2. Поскольку при использовании глобальной группы с профилями выпуска OTP-аутентификаторов такая группа может пополняться пользователями автоматически (в момент выпуска аутентификатора из Личного кабинета), это следует учитывать при настройке фильтра с помощью той же глобальной группы для привязки другого профиля (чтобы избежать неконтролируемого выпуска OTP-аутентификаторов при запуске плана обслуживания). В общем случае следует использовать отдельную глобальную группу для установки фильтра на каждый профиль выпуска OTP-аутентификатора.

5. Создайте профиль доступа в личный кабинет (см. «Настройка профиля доступа в личный кабинет JWM», с. 193).
6. Выполните привязку профиля (см. «Привязка профилей», с. 195) к тем пользователям, на которых распространяется право самостоятельного выпуска OTP-аутентификаторов.

Важно! При привязке профиля **Доступ в личный кабинет** к контейнеру ресурсной системы убедитесь, что к одному контейнеру привязано не более одного профиля.

7. Проверьте и при необходимости измените план обслуживания настроек личного кабинета (см. «**План обслуживания настроек личного кабинета**», с. 287) и запустите его на выполнение (см. раздел «Запуск и просмотр результатов планов обслуживания», с. 274). Результатом работы плана обслуживания будет настройка прав самостоятельного выпуска OTP-аутентификаторов в личном кабинете для всех пользователей, на которых распространяется действие *профиля доступа в личный кабинет*.

Примечание. Для того чтобы убедиться, что после завершения плана обслуживания конкретному пользователю разрешен доступ к соответствующему порталу и право на выпуск OTP-аутентификатора, откройте свойства пользователя и на вкладке **Личный кабинет** и проверьте, что установлены соответствующие настройки, как, например, на Рис. 206, ниже.

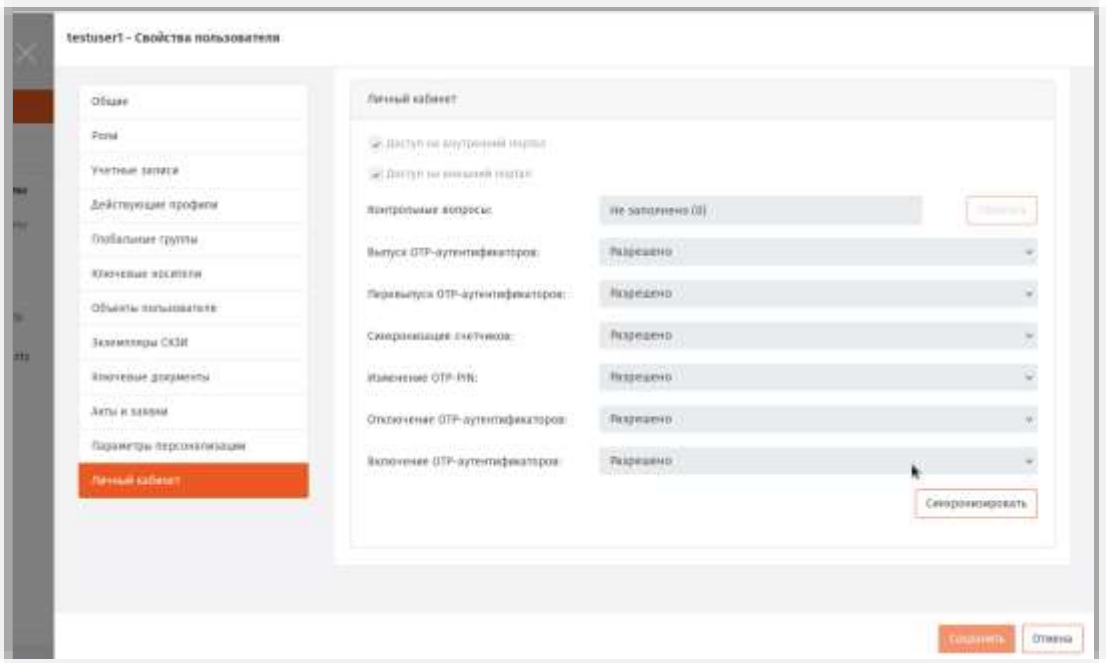


Рис. 206 –Пример разрешений пользователя в ЛК для самостоятельного выпуска OTP-аутентификатора

8. В настройках личного кабинета (раздел **Настройки личного кабинета** –> **Выпуск OTP-аутентификаторов**) у соответствующего профиля установите флаг **Разрешить выпуск через личный кабинет**.
9. В настройках личного кабинета (раздел **Настройки личного кабинета** –> **Аутентификация** консоли управления JMS) сделайте доступной соответствующую вкладку для аутентификации

пользователей, например **Вход по OTP** (для OTP- и Push-токенов) и/или **Вход по Messaging** (для Messaging-токенов), подробнее см. «Раздел Аутентификация», с. 321.

Проверку самостоятельного выпуска можно произвести из личного кабинета пользователя на портале JWM на вкладке **Устройства** в секции **Выпуск OTP-аутентификатора в JMS** (см. руководство пользователя [1]).

Примечание. В случае настройки аутентификации по Push OTP-токену во внешней системе с использование JAS-плагина NPS не забудьте выполнить дополнительную настройку параметров данного плагина в реестре (параметр *PushTokenAction=Pass*). Подробнее см. руководство по установке и настройке JAS [3], раздел «Настройка JAS-плагина для NPS».

3.6.24.6 Профили для отключения и замены пользователем ЭК / ЗНИ

Для того чтобы в клиенте JMS пользователю стало доступно *отключение* (временная блокировка в JMS) и замена ЭК/ЗНИ следует настроить и привязать к пользователю профили, указанные:

- для случая ЭК: в разделах «Профили для выпуска администратором электронного ключа с сертификатом» и «Профили для выпуска пользователем электронного ключа с сертификатом», выше.
- для случая ЗНИ: в разделах «Профили для выпуска ЗНИ SF/ГОСТ из консоли управления JMS» и «Профили для выпуска ЗНИ SF/ГОСТ из клиентского приложения JMS», с. 204.

Кроме того, в настройках профиля клиентского агента следует установить признаки **Разрешать отключение** и **Разрешать замену** на вкладке **Ограничения по работе с КН** (см. «Настройка профиля клиентского агента», с. 101).

3.7 Акты и заявки

В JMS существует возможность распечатать указанные в настройках профиля документы, формируемые при выпуске электронного ключа, не только в момент выпуска данного ключа, но и по прошествии времени после его выпуска.

Примечание. При печати документа возможен выбор другого шаблона для печати (если, например, были внесены правки в шаблон и требуется заново напечатать документ о выпуске электронного ключа по новому шаблону).

Для того чтобы распечатать документ после выпуска электронного ключа выполните следующие действия:

1. Перейдите на вкладку **Объекты -> Акты и заявки**, выберите нужный контейнер (например, *cn=accounts*, рис. Рис. 207). В случае если необходимо отображать документы, содержащиеся во вложенных контейнерах и нажмите **Показать вложенные**.

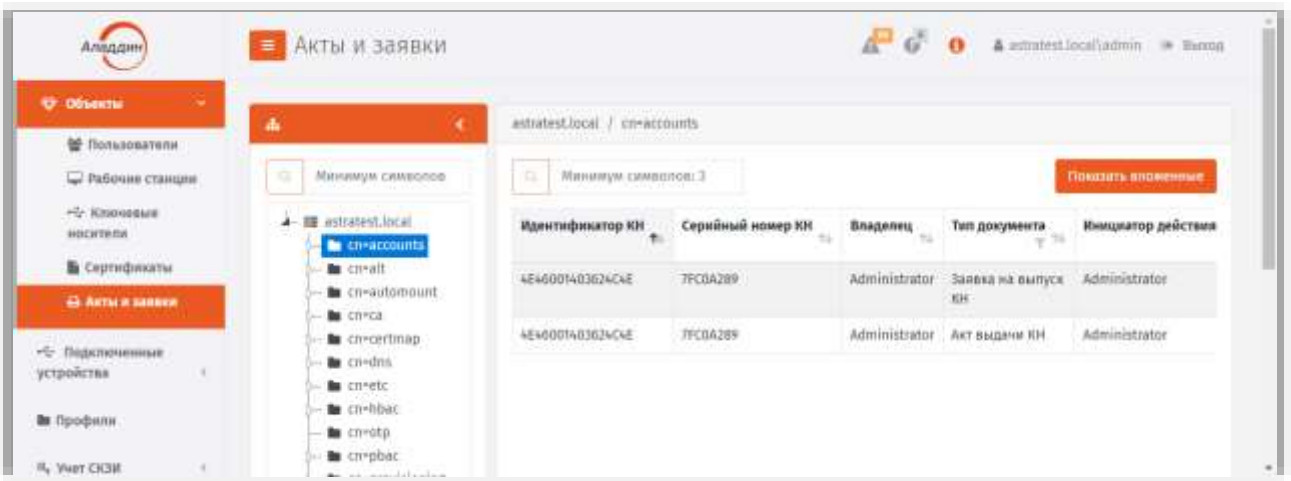


*Рис. 207 – Раздел **Объекты -> Акты и заявки***

2. Выберите документ в списке справа, нажмите на нем правой кнопкой мыши и выберите **Просмотр/Печать**.
   Отобразится страница следующего вида.

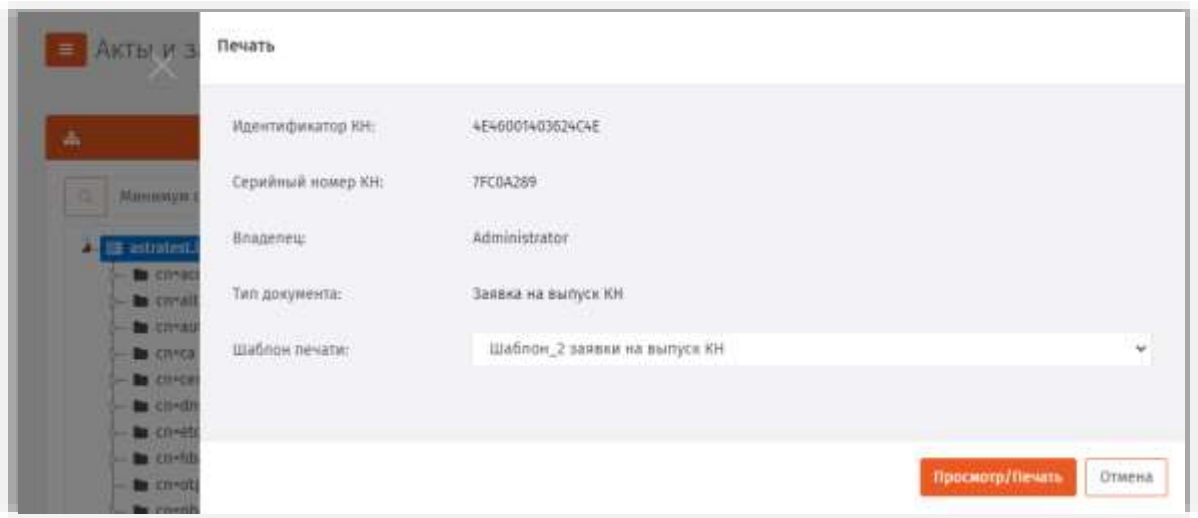


*Рис. 208 – Страница печати выбранного документа в разделе **Акты и заявки***

3. При необходимости в поле **Шаблон печати** выберите необходимый шаблон из раскрывающегося списка.
4. Нажмите **Просмотр/Печать**. Файл документа будет сохранен в папку загрузок браузера.

О создании и настройке **Шаблона печати** (шаблона печатной формы) подробнее см. раздел «Подсистема печати», с. 244.

3.8 Учет СКЗИ

JMS предоставляет возможность вести учет средств криптографической защиты информации (СКЗИ) как программных, так и аппаратных (включая ключевые носители).

Функция учета СКЗИ является лицензируемой, т.е. для того чтобы в консоли управления JMS стал доступен раздел **Учет СКЗИ** (Рис. 209) необходимо, чтобы в лицензию на продукт (JMS) была включена опция учета СКЗИ (оформляется частным договором при приобретении продукта).

Лицензионная опция учета СКЗИ содержит в себе ограничение на число поддерживаемых экземпляров СКЗИ; таким образом, при превышении числа зарегистрированных СКЗИ регистрация и администрирование новых СКЗИ становятся невозможными.

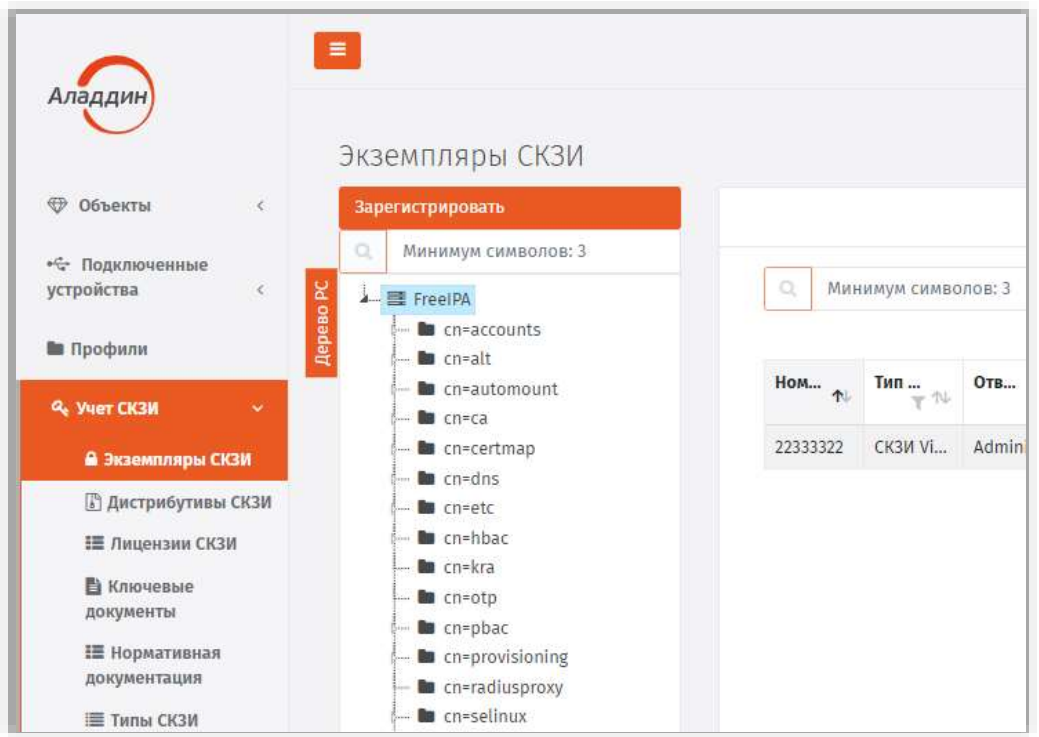


Рис. 209 – Раздел Учет СКЗИ консоли управления JMS

Поэкземплярный учет СКЗИ (в рамках лицензии на продукт JMS) осуществляется в следующем порядке:

- число свободных лицензий (на СКЗИ) уменьшается на единицу при регистрации одного экземпляра СКЗИ;
- число свободных лицензий (на СКЗИ) увеличивается на единицу при уничтожении одного экземпляра СКЗИ (см. разделы «Порядок управления программным СКЗИ», с. 310, «Порядок управления ключевым носителем как аппаратным СКЗИ», с. 307)

Учет СКЗИ, являющихся ключевыми носителями, ведется автоматически при их регистрации или выпуске (см. раздел «Порядок управления ключевым носителем как аппаратным СКЗИ», с. 307).

3.8.1 Описание элементов интерфейса в разделе учет СКЗИ

Раздел **учет СКЗИ** содержит следующие категории:

- **Экземпляры СКЗИ**
- **Дистрибутивы СКЗИ**
- **Лицензии СКЗИ**
- **Ключевые документы**
- **Нормативная документация**
- **Типы СКЗИ**
- **Типы нормативной документации**
- **Журнал событий**

Описание составляющих раздела **учет СКЗИ** приведено в таблице 59.

Табл. 59 Описание раздела Учет СКЗИ консоли управления JMS

Наименование	Назначение
Экземпляры СКЗИ	Для выполнения следующих действий с экземплярами СКЗИ: • просмотра списка и свойств зарегистрированных СКЗИ; • регистрации новых программных СКЗИ; • назначения/отмены назначения программному СКЗИ следующих категорий: – установившее экземпляр СКЗИ лицо; – рабочая станция; – лицензия; – дистрибутив; • назначения ответственного лица для экземпляра СКЗИ; • введения экземпляра СКЗИ в эксплуатацию; • выведения экземпляра СКЗИ из эксплуатации; • возвращения экземпляра СКЗИ в эксплуатацию; • уничтожения зарегистрированного программного СКЗИ; • управления учетом (прекратить учет/возобновить учет/ удалить учетную запись); • просмотра и печати нормативных документов, сформированных в течение жизненного цикла учета программных СКЗИ. **Примечание**. Экземпляры СКЗИ отображаются в окне консоли управления JMS с использованием дерева ресурсных систем. Кроме этого, имеются три опции: • **Показать вложенные** – отображаются все нижестоящие в дереве ресурсной системы экземпляры СКЗИ; • **Показывать неучитываемые** – отображаются экземпляры СКЗИ, для которых учет прекращен; • **Показывать уничтоженные** – отображаются экземпляры СКЗИ, которые были уничтожены.
Дистрибутивы СКЗИ	Для выполнения следующих действий с дистрибутивами СКЗИ: • просмотра списка и свойств зарегистрированных дистрибутивов СКЗИ; • регистрации новых дистрибутивов СКЗИ; • импорта дистрибутивов СКЗИ; • создания копии диска из эталонного дистрибутива СКЗИ (тиражирование); • редактирования свойств дистрибутива СКЗИ; • передачи (экспорта) дистрибутива СКЗИ и документации; • удаления дистрибутива СКЗИ или его копии; • просмотра и печати нормативных документов, сформированных в течение жизненного цикла учета дистрибутива СКЗИ.
Лицензии СКЗИ	Для выполнения следующих действий с лицензиями СКЗИ: • просмотра списка и свойств зарегистрированных лицензий; • регистрации лицензий (включая пакетную регистрацию); • назначения лицензии (назначение свободной лицензии экземпляру СКЗИ); • возврата лицензии (возврат лицензии в список свободных лицензий); • экспорта лицензий; • удаления лицензии (из списка зарегистрированных лицензий); • просмотра и печати нормативных документов, сформированных в течение жизненного цикла учета лицензии СКЗИ; • установка лицензий (физическая).

Наименование	Назначение
Ключевые документы	Для выполнения следующих действий с ключевыми документами: • просмотра списка и свойств ключевых документов; • просмотра и печати нормативных документов, сформированных в течение жизненного цикла ключевых документов. **Примечание 1**. Ключевой документ (КД) – это ключевая информация (КИ), записанная на электронный ключ (и хранящаяся на нем). Для JMS ключевой информацией является сертификат + закрытый ключ. **Примечание 2.** Ключевые документы отображаются в окне консоли управления JMS с использованием дерева ресурсных систем. Кроме этого, имеются две опции: • **Показать вложенные** – отображаются все нижестоящие в дереве ресурсной системы ключевые документы; • **Показывать неучитываемые** – отображаются ключевые документы, для которых учет прекращен. **Примечание 3.** Учет КИ и КД выполняется автоматически, независимо от учета экземпляров СКЗИ и поддерживается только для сертификатов, выпускаемых на КН, управляемые JMS.
Нормативная документация	Для выполнения следующих действий с нормативными документами: • просмотра списка и свойств нормативной документации; • печати нормативной документации. **Примечание 1.** Нормативная документация – это документация по учету СКЗИ и ключевых документов, формируемая в течение их жизненного цикла в результате возникновения различных событий (при создании, передаче, получении, выводе из эксплуатации и т.д.). **Примечание 2.** Нормативная документация отображается в окне консоли управления JMS с использованием дерева ресурсных систем. Кроме этого, имеется опция **Показать вложенные** при выборе которой отображаются все нижестоящие в дереве ресурсной системы нормативные документы.
Типы СКЗИ	Для выполнения следующих действий: • просмотра списка и свойств зарегистрированных типов СКЗИ; • редактирования свойств зарегистрированных типов СКЗИ; • регистрации программных и аппаратных типов СКЗИ; • удаления зарегистрированных типов СКЗИ. **Примечание.** Удаление встроенных типов СКЗИ невозможно. Редактирование свойств зарегистрированных типов СКЗИ возможно только для не основных атрибутов.
Типы нормативной документации	Для выполнения следующих действий с типами нормативной документации: • просмотра списка и свойств типов нормативной документации; • задания шаблона печати выбранному типу нормативной документации; • задания начального значения внутренней нумерации документов. **Примечание.** Для каждого типа нормативной документации ведется своя нумерация.

Наименование	Назначение
Журнал событий	Для выполнения следующих действий: • просмотра списка и свойств событий, происходящих с СКЗИ; • фильтрации событий, происходящих с СКЗИ по временным промежуткам; • поиск по столбцу **Пользователь**.

3.8.2 Типы СКЗИ

Действия, выполнение которых возможно в разделе **Учет СКЗИ** -> **Типы СКЗИ**, перечислены в Табл. 59.

В JMS существуют встроенные типы СКЗИ, которые устанавливаются с продуктом, и пользовательские, которые можно зарегистрировать самостоятельно.

Встроенные типы СКЗИ нельзя удалить или отредактировать. Новые регистрируемые в JMS типы СКЗИ можно редактировать и удалять.

СКЗИ по своим ключевым характеристикам подразделяются на **программные** и **аппаратные.**
В JMS заведены следующие встроенные типы СКЗИ:

Аппаратные СКЗИ:

- Криптотокен (все ключи Aladdin, содержащие приложение Криптотокен);
- Криптотокен 2 (все ключи Aladdin, содержащие приложение Криптотокен 2);
- ФКН (JaCarta CryptoPro);
- Рутокен ЭЦП.

Программные СКЗИ (с поддержкой лицензирования и распространения с помощью дистрибутивов):

- КриптоПро CSP 3.6;
- КриптоПро CSP 3.9;
- КриптоПро CSP 4.0;
- КриптоПро CSP 5.0;
- ViPNet CSP 3.2;
- ViPNet CSP 4.0;
- ViPNet CSP 4.2;
- ViPNet CSP 4.4.

При просмотре свойств зарегистрированных типов СКЗИ отображаются параметры, описание которых представлено в таблице 60.

Табл. 60 – Параметры типов СКЗИ

Параметр	Описание
Наименование	Наименование типа СКЗИ
Подтип	Допустимые значения: • **Пользовательский** – создается пользователем; • **Встроенный**

Параметр	Описание
Семейство	Допустимые значения: • **Программный** • **Аппаратный**
Лицензируемый (только для программных СКЗИ)	Допустимые значения: • **Да** – СКЗИ требует привязки к экземпляру лицензии его производителя для учета в JMS; • **Нет** – СКЗИ не требует привязки к экземпляру лицензии производителя для учета в JMS
Распространяемый на носителях (только для программных СКЗИ)	Допустимые значения: • **Да** – СКЗИ может быть привязан к дистрибутиву при учете в JMS; • **Нет** – СКЗИ не может быть привязан к дистрибутиву при учете в JMS
Переносимый	Допустимые значения: • **Да** – СКЗИ может быть привязан к конкретному месту установки; • **Нет** – СКЗИ не может быть привязан к конкретному месту установки;
Приложение (только для аппаратных СКЗИ)	Используемое приложение
Автосоздание экземпляров СКЗИ (только для программных СКЗИ)	Допустимые значения: • **Да** – учетная запись экземпляра программного СКЗИ будет автоматически создана в JMS при добавлении лицензии СКЗИ данного типа (при этом учетный номер программного СКЗИ будет совпадать с серийным номером лицензии); • **Нет**
Шаблон формирования идентификатора (только для программных СКЗИ)	Шаблон формирования идентификатора номера диска или дистрибутива
Сертификат ФСБ	Флаг наличия у СКЗИ сертификата ФСБ
Номер сертификата ФСБ	Номер сертификата ФСБ
Дата выдачи сертификата ФСБ	Дата выдачи сертификата ФСБ
Срок действия сертификата ФСБ	Срок действия сертификата ФСБ
Сертификат поддержки	Флаг наличия у СКЗИ сертификата технической поддержки
Номер сертификата технической поддержки	Номер сертификата технической поддержки
Дата выдачи сертификата технической поддержки	Дата выдачи сертификата технической поддержки
Срок действия сертификата технической поддержки	Срок действия сертификата технической поддержки

3.8.2.1 Регистрация программного типа СКЗИ

Для того чтобы зарегистрировать программный тип СКЗИ, выполните следующие действия:

1. Перейдите в раздел **Учет СКЗИ** –> **Тип СКЗИ** и нажмите **Зарегистрировать программный:**.

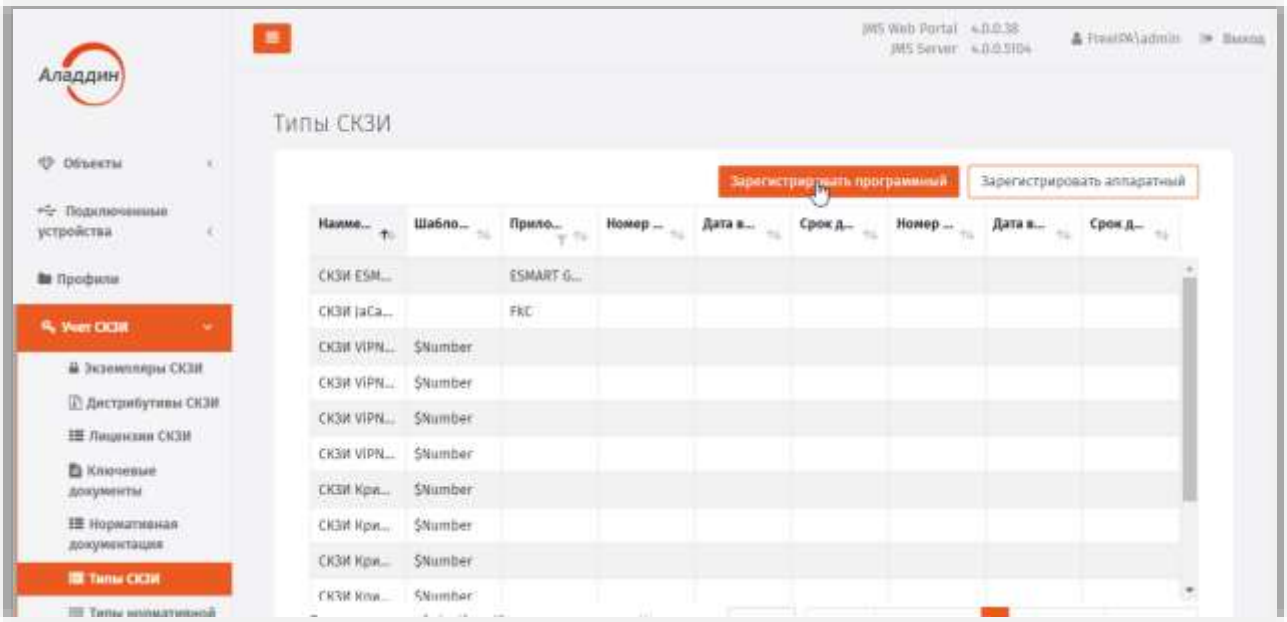


Рис. 210 – Вызов страницы регистрации программного типа СКЗИ

2. Отобразится страница создания программного типа СКЗИ:

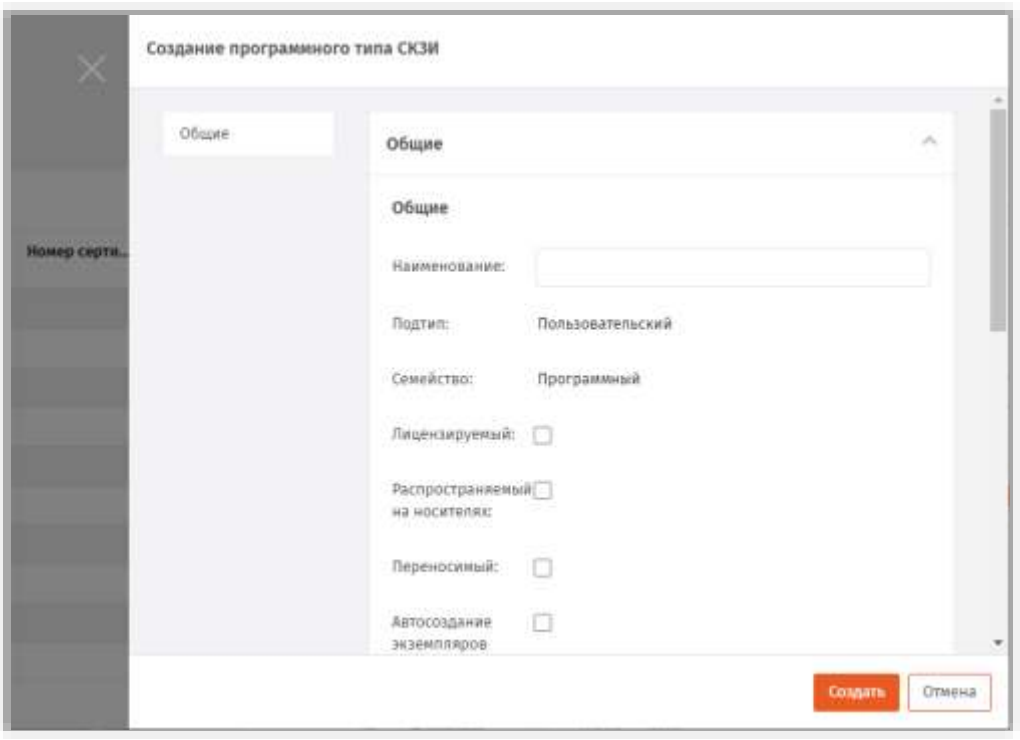


Рис. 211 – Вызов страницы регистрации программного типа СКЗИ

3. Введите **Наименование** типа СКЗИ и номер версии. Если необходимо выберите следующие опции:

- **Лицензируемый** (предусматривается использование Лицензии. Опция применима только для программных СКЗИ);
- **Распространяемый на носителях** (предусматривается распространение на дистрибутивах Опция применима только для программных СКЗИ);
- **Переносимый** (Может быть привязан к конкретному месту установки или нет);
- **Автосоздание экземпляров СКЗИ** (поддержка автоматического создания экземпляров СКЗИ (При регистрации лицензии СКЗИ, в свойствах типа которого установлена опция **Автосоздание экземпляров СКЗИ**, будет автоматически зарегистрирован экземпляр программного СКЗИ данного типа. При этом учетный номер программного СКЗИ будет совпадать с серийным номером лицензии);

4. Введите **шаблон формирования идентификатора** (Это шаблон, при использовании которого будет формироваться номер копии дистрибутива. Опция применима только для программных СКЗИ).
5. Если необходимо, выберите опцию **Сертификат ФСБ** и введите **Номер**, **Дату выдачи** и **Срок действия** сертификата ФСБ.
6. Если необходимо, выберите опцию **Сертификат поддержки** и введите **Номер**, **Дату выдачи** и **Срок действия** сертификата поддержки.
7. Нажмите **Создать**.

Зарегистрированный тип СКЗИ отобразится в окне консоли управления JMS в разделе **Учет СКЗИ** -> **Тип СКЗИ**.

3.8.2.2 Регистрация аппаратного типа СКЗИ

Для того чтобы зарегистрировать аппаратный тип СКЗИ, выполните следующие действия:

1. Перейдите в раздел **Учет СКЗИ** –> **Тип СКЗИ** и нажмите **Зарегистрировать аппаратный**.

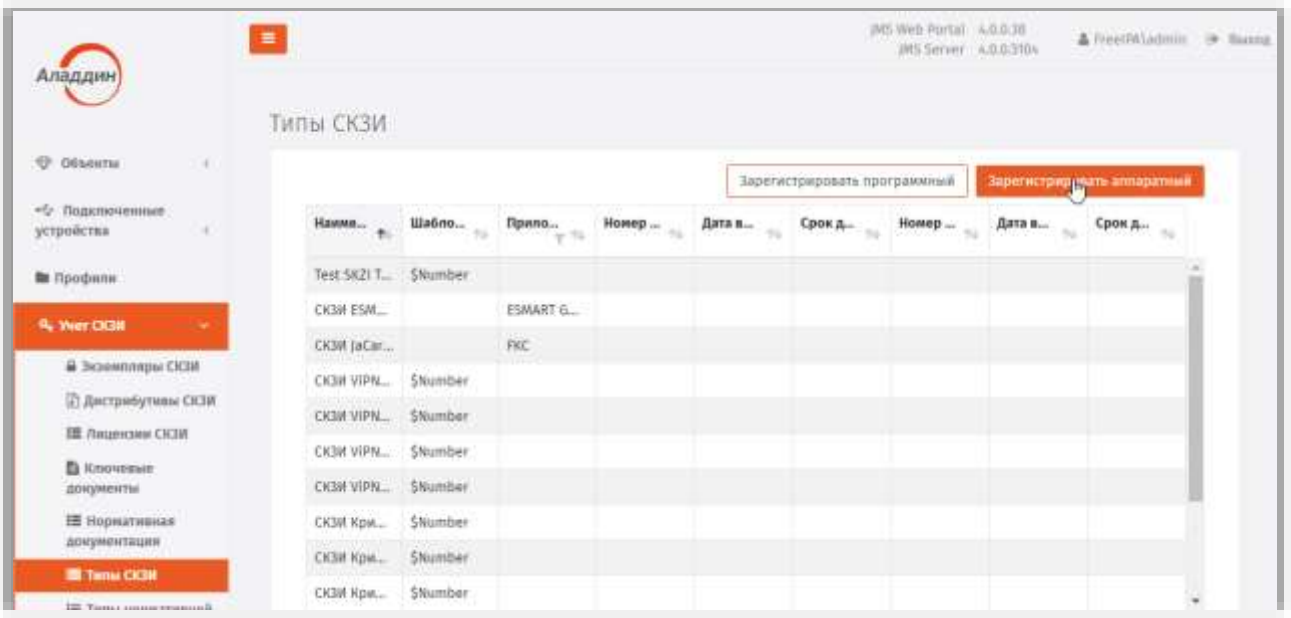


Рис. 212 – Вызов страницы регистрации программного типа СКЗИ

2. Отобразится страница создания аппаратного типа СКЗИ:

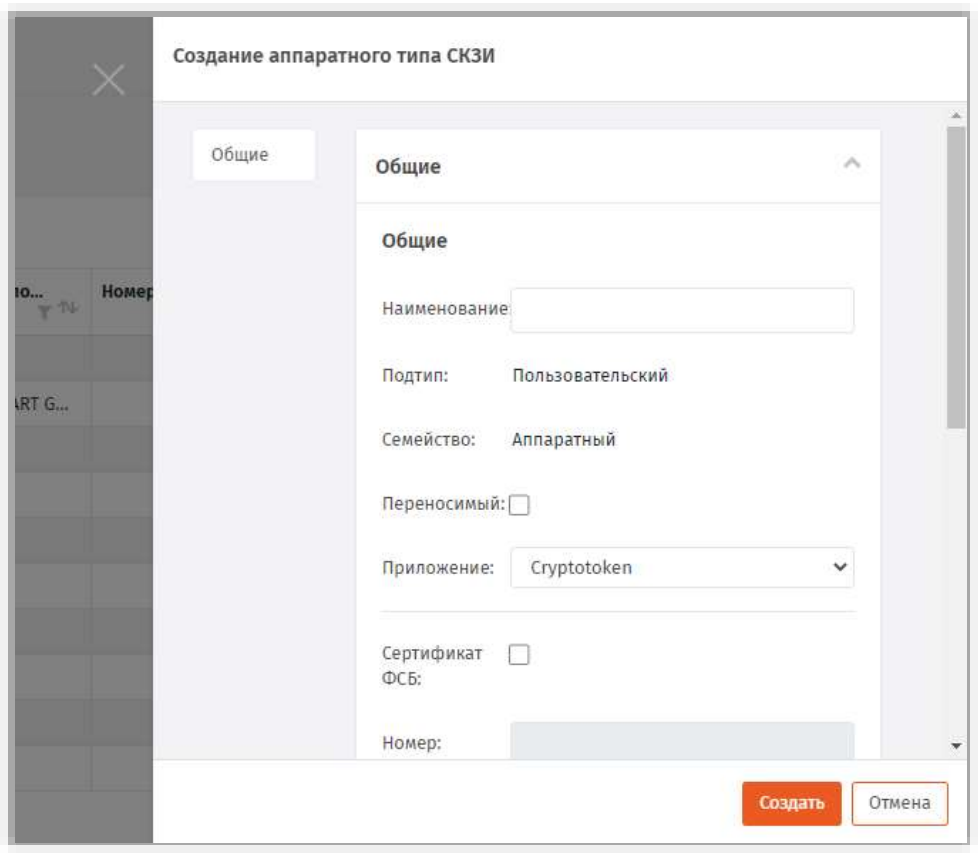


Рис. 213 – Вызов страницы регистрации аппаратного типа СКЗИ

3. В появившемся окне введите **Наименование** типа СКЗИ. Если необходимо выберите опцию **Переносимый**, из раскрывающегося списка в поле **Приложение** выберите приложение, используемое СКЗИ.
4. Если необходимо, выберите опцию **Сертификат ФСБ** и введите **Номер**, **Дату выдачи** и **Срок действия** сертификата ФСБ.
5. Если необходимо, выберите опцию **Сертификат поддержки** и введите **Номер**, **Дату выдачи** и **Срок действия** сертификата поддержки.
6. Нажмите **Создать**.

   Зарегистрированный тип СКЗИ отобразится в окне консоли управления JMS в разделе **Учет СКЗИ** -> **Тип СКЗИ**.

3.8.3 Типы нормативной документации

В JMS зарегистрирован ряд типов нормативных документов. Для каждого типа задается:

- шаблон для печати в виде документа в формате RTF;
- начальное значение внутренней нумерации документов.

Начальное значение внутренней нумерации документов можно изменять, но применяться оно будет только для новых документов.

При просмотре свойств типа нормативной документации отображаются параметры, описание которых представлено в таблице 61.

Табл. 61 – Параметры типа нормативных документов

Параметр	Описание
Наименование	Наименование нормативного документа
Тип сущности	Предмет, фигурирующий в нормативном документе: – экземпляр СКЗИ; – дистрибутив СКЗИ; – лицензия СКЗИ; – ключевая информация; – ключевой документ.
Шаблон номера документа	Шаблон номера документа. Свойство редактируемое.
Текущий номер	Текущий порядковый номер документа. Свойство редактируемое. Можно задавать начальный порядковый номер.
Шаблон печати	Шаблон печати. Свойство редактируемое. Шаблон печати задается с использованием подсистемы печати. Подробнее см. раздел «Подсистема печати», с. 244.

Для того чтобы просмотреть список нормативных документов, перейдите в раздел **Учет СКЗИ** -> **Типы нормативной документации:**

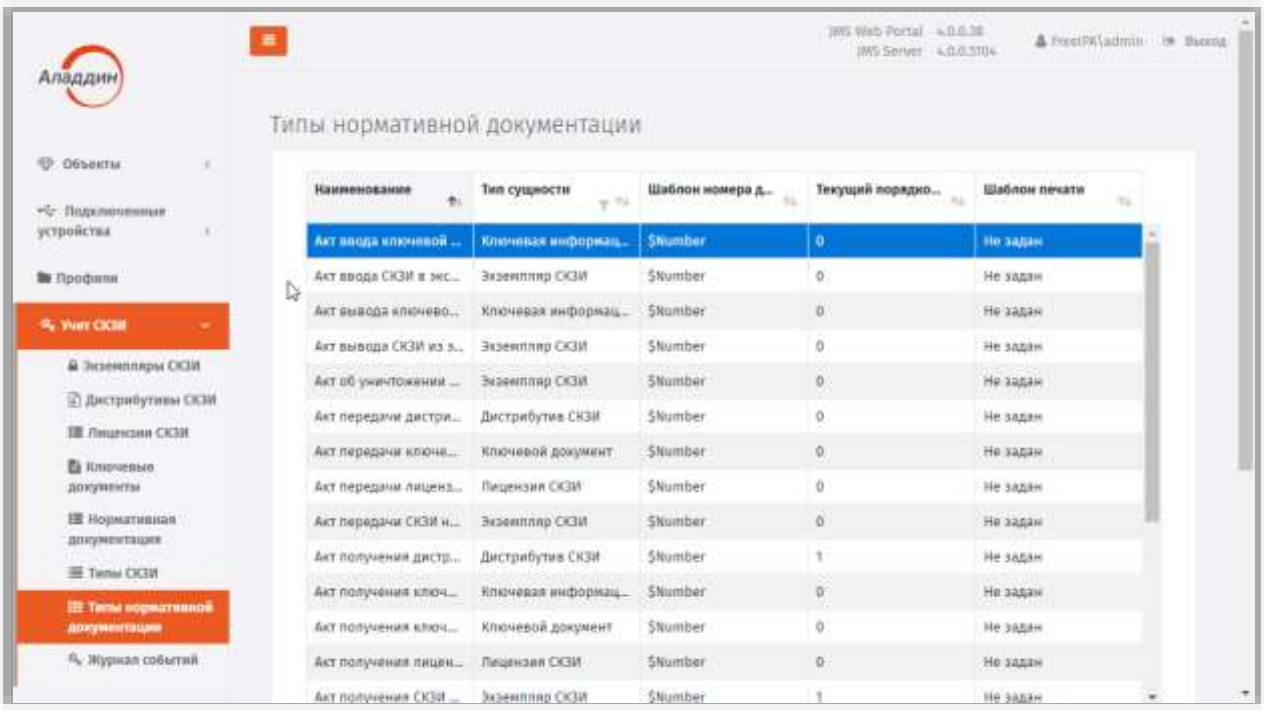


Рис. 214 – Страница типов нормативной документации

3.8.3.1 Задание шаблона печати

Для того чтобы задать шаблон печати для нормативного документа выполните следующие действия.

1. Выделите в списке типов нормативной документации тот тип нормативного документа, для которого вы хотите задать шаблон печати, нажмите правой кнопкой мыши и выберите **Свойства:**

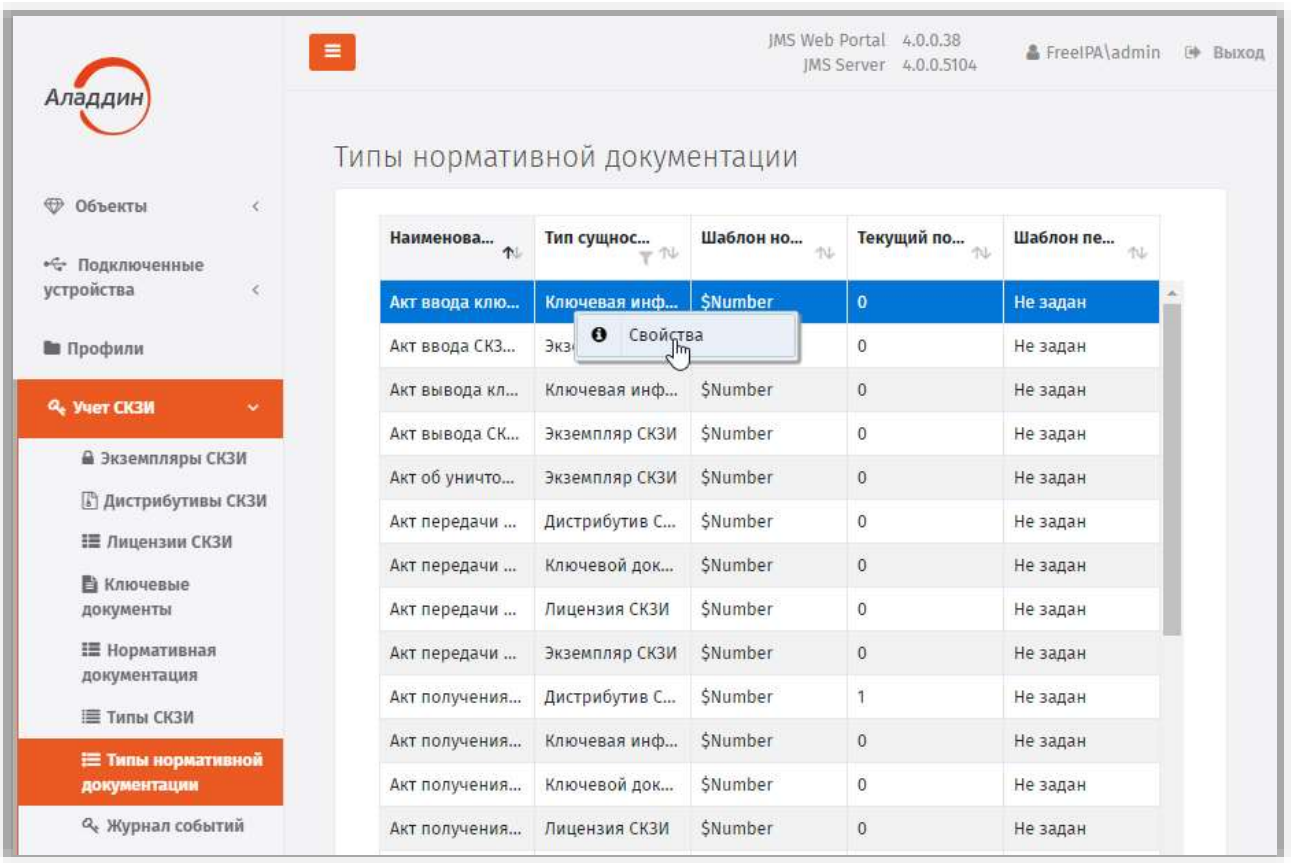


*Рис. 215 – Вызов страницы просмотра свойств **Типа нормативного документа***

2. Откроется страница свойств типа нормативного документа:

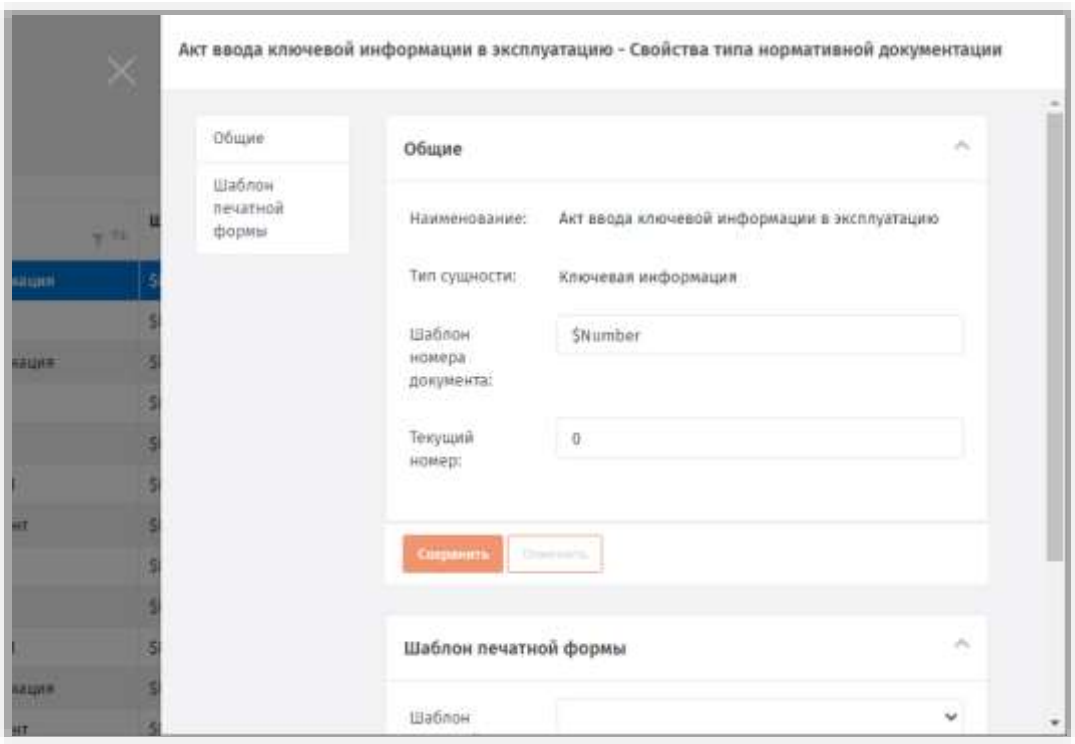


*Рис. 216 –Страница свойств **Типа нормативного документа***

3. Перейдите на вкладку **Шаблон печатной формы** и выберите в одноименном поле требуемый для задания тип шаблона.

Примечание. Если в раскрывающемся списке требуемого типа шаблона не оказалось, то его можно задать. Типы шаблонов печатной формы задаются в разделе **Настройки** –> **Шаблоны печати** (подробнее см. раздел «Подсистема печати», с. 244).

3.8.4 Экземпляры СКЗИ

Действия, выполнение которых возможно в разделе **Учет СКЗИ** -> **Экземпляры СКЗИ** перечислены в таблице 59.

При просмотре свойств зарегистрированных программных СКЗИ отображаются параметры, описание которых представлено в таблице 62.

Табл. 62 – Перечень свойств экземпляра СКЗИ

Параметр	Описание
Номер	Учетный номер экземпляра СКЗИ
Вид СКЗИ	Возможные значения: • **Аппаратный** • **Программный**
Тип СКЗИ	Тип СКЗИ (один из встроенных или пользовательских типов СКЗИ).
Описание	Текстовое описание

Параметр	Описание
Место установки	Текстовое описание места установки
От кого получено	Текстовое описанием лица, от которого СКЗИ получено
Ответственный за установку	Лицо, получившее СКЗИ в ответственное пользование
Рабочая станция	Рабочая станция, назначенная для экземпляра СКЗИ
Произвел установку	Имя пользователя, установившего данный экземпляр СКЗИ (см. «Установившее лицо», с. 222)
Дистрибутив	Дистрибутив, привязанный к данному экземпляру СКЗИ
Лицензия	Лицензия, привязанная к данному экземпляру СКЗИ
Путь	Полное имя контейнера, к которому привязан пользователь – владелец СКЗИ, в соответствующей ресурсной системе
Состояние	Текущее состояние экземпляра СКЗИ
Дата начала действия	Дата начала действия экземпляра СКЗИ
Дата прекращения действия	Дата прекращения действия экземпляра СКЗИ
Дата уничтожения	Дата уничтожения экземпляра СКЗИ
Ведение учета	Состояние программного СКЗИ. Возможны следующие значения: • **Да** – учет программного СКЗИ ведется (для работы с СКЗИ доступны операции изменения состояния жизненного цикла) • **Нет** – учет программного СКЗИ не ведется (для СКЗИ доступна только операция уничтожения учетной записи)

При просмотре списка экземпляров СКЗИ в верхней панели консоли управления JMS доступны дополнительные опции просмотра. Описание дополнительных опций просмотра представлено в таблице 63.

Табл. 63 – Описание дополнительных опций просмотра экземпляров СКЗИ

Наименование опции	Описание
Показывать вложенные	При выборе этой опции в списке будут дополнительно отображены СКЗИ, относящиеся к объектам ресурсной системы, которые являются вложенными по отношению к текущему выбранному объекту/контейнеру
Показывать неучитываемые	При выборе этой опции в списке отображаются СКЗИ, учет которых прекращен
Показывать уничтоженные	При выборе этой опции в списке отображаются СКЗИ, которые были уничтожены

3.8.4.1 Регистрация экземпляра СКЗИ

Для того чтобы зарегистрировать экземпляр СКЗИ выполните следующие действия.

1. Перейдите в раздел **Учет СКЗИ** -> **Экземпляры СКЗИ**, выберите нужный объект/контейнер ресурсной системы (например, cn) и в вверху нажмите **Зарегистрировать**.

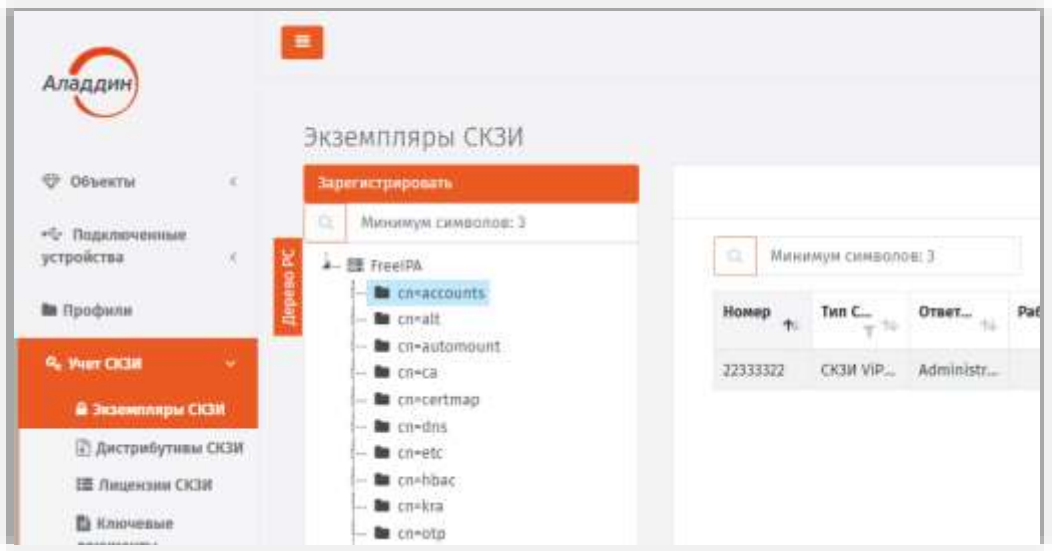


Рис. 217 – Вызов страницы регистрации программного СКЗИ

2. Откроется страница регистрации экземпляра СКЗИ:

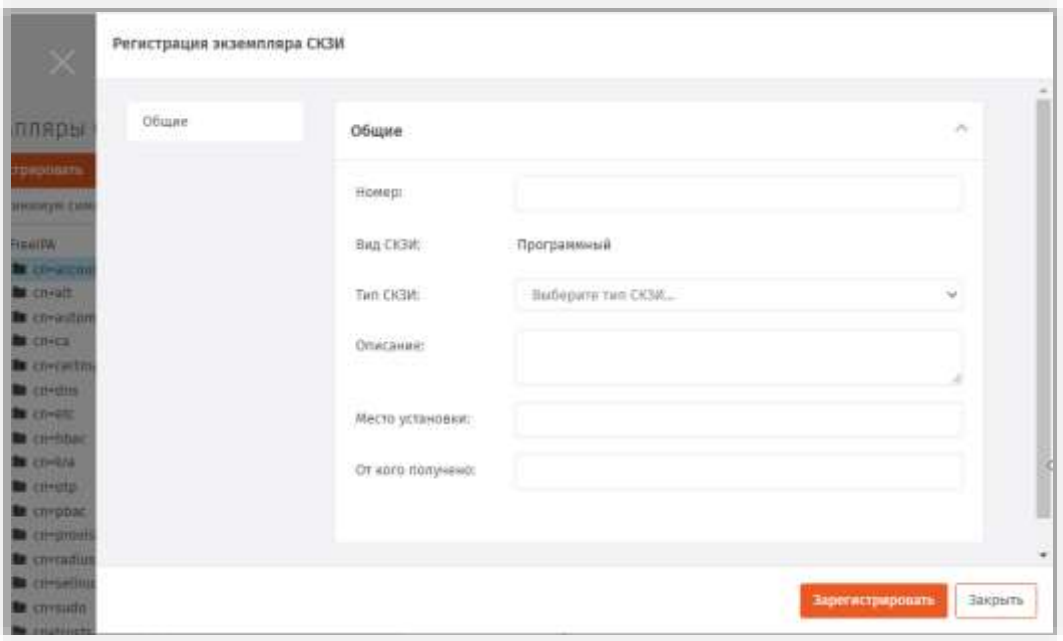


Рис. 218 – Страница регистрации экземпляра СКЗИ

3. Введите **Номер** экземпляра СКЗИ, из раскрывающегося списка выберите **Тип СКЗИ**, при необходимости заполните поле **Описание**, **Место установки** и поле **От кого получено**. Нажмите **Зарегистрировать**.

Примечания:

1. Регистрация СКЗИ типа КриптоПро CSP недоступна из раздела **Учет СКЗИ -> Экземпляры СКЗИ**. При попытке их ручной регистрации в пользовательском интерфейсе появляется соответствующее предупреждение. Экземпляры

данного типа СКЗИ будут автоматически зарегистрированы при добавлении их лицензии (см. толкование свойства **Автосоздание экземпляров СКЗИ** в разделе «Типы СКЗИ», с. 212).

2. Экземпляры программных СКЗИ типа КриптоПро CSP и ViPNet CSP создаются автоматически при обнаружении их инсталляций на рабочих станциях.
3. Экземпляры СКЗИ КриптоПро CSP, в которых активирована *демонстрационная лицензия* производителя, не могут быть зарегистрированы в JMS.

Зарегистрированное программное СКЗИ отобразится в окне консоли управления JMS в разделе **Учет СКЗИ** -> **Экземпляры СКЗИ**.

3.8.4.2 Управление назначением экземпляра СКЗИ

3.8.4.2.1 Установившее лицо

Для того чтобы назначить зарегистрированному экземпляру программного СКЗИ **Установившее лицо,** выполните следующие действия:

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр, нажмите на нём правой кнопкой мыши и выберите **Назначить установившее лицо**:

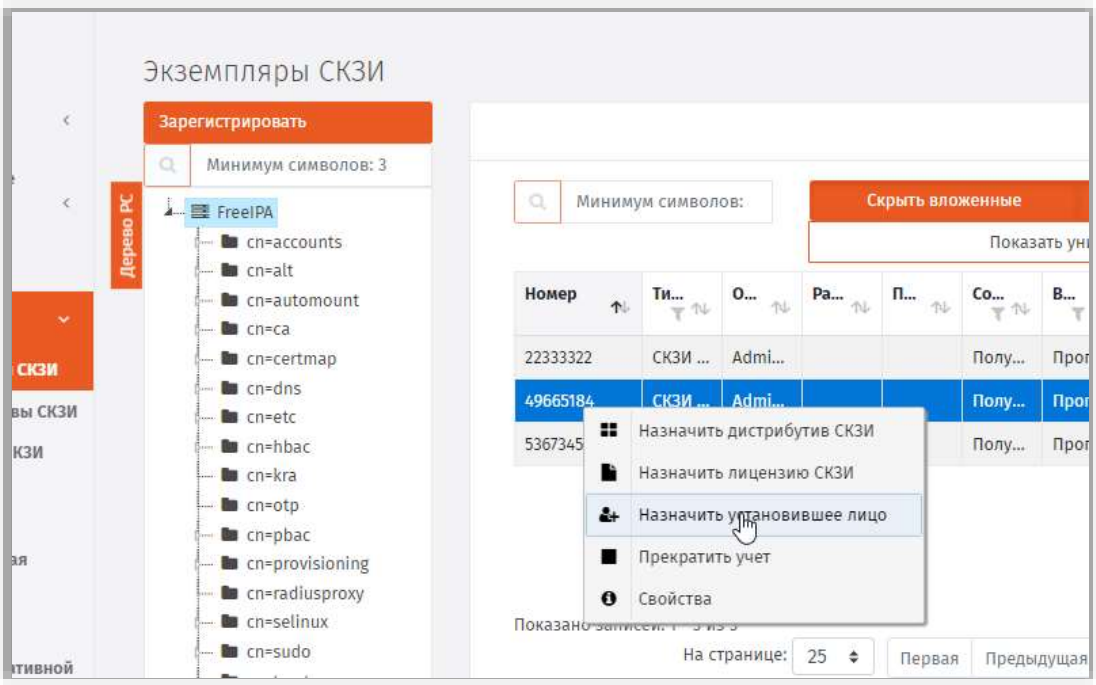


Рис. 219 –Назначение программному СКЗИ установившего лица

2. Откроется страница выбора пользователя в ресурсной системе:

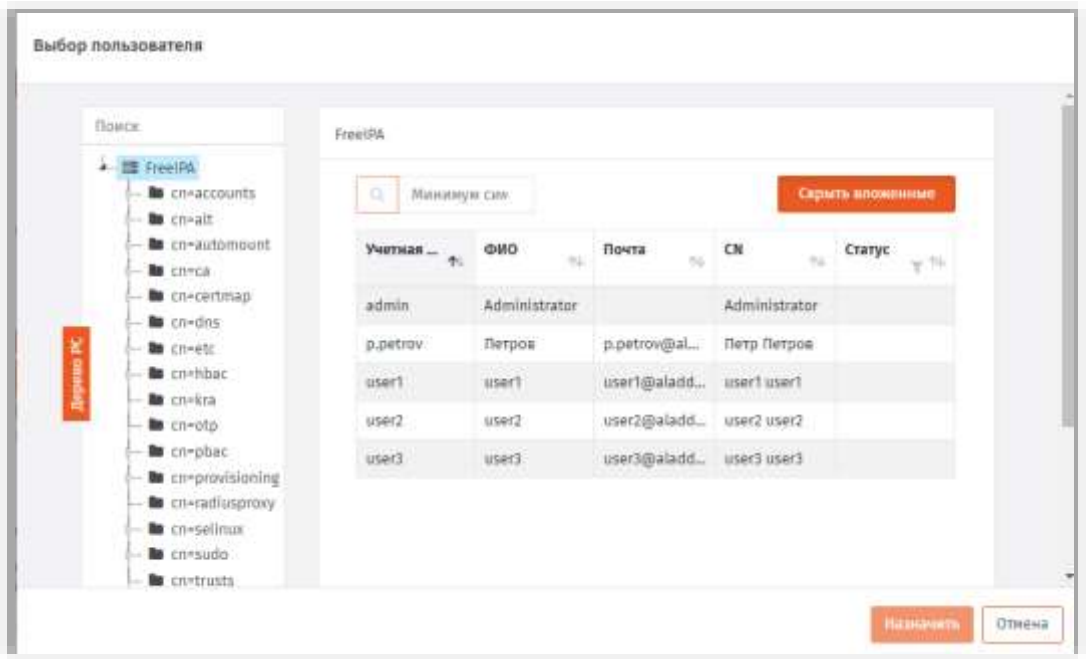


Рис. 220 –Страница выбора пользователя

3. Выберите пользователя и нажмите **Назначить**.

   Чтобы отменить назначение на странице экземпляров СКЗИ выберите данный экземпляр, нажмите на нем правой кнопкой мыши и выберите **Отменить назначение установившего лица**.

3.8.4.2.2 Дистрибутив

Для того чтобы назначить зарегистрированному экземпляру программного СКЗИ **Дистрибутив**, с которого производилась установка, выполните следующие действия:

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр, нажмите на нём правой кнопкой мыши и выберите **Назначить дистрибутиве СКЗИ.**

Примечание. Операция назначения дистрибутива необязательна.

2. В окне назначения дистрибутива в центре экрана выберите дистрибутив для назначения и нажмите **Назначить**.

   Чтобы отменить назначение на странице экземпляров СКЗИ выберите данный экземпляр, нажмите на нем правой кнопкой мыши и выберите **Отменить назначение дистрибутива СКЗИ**.

3.8.4.2.3 Лицензия

Для того чтобы назначить зарегистрированному экземпляру программного СКЗИ **Лицензию,** выполните следующие действия.

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр, нажмите на нём правой кнопкой мыши и выберите **Назначить лицензию СКЗИ.**
2. В окне назначения лицензии в центре экрана выберите лицензию для назначения и нажмите **Назначить**.

Чтобы отменить назначение на странице экземпляров СКЗИ выберите данный экземпляр, нажмите на нем правой кнопкой мыши и выберите **Отменить назначение лицензии СКЗИ**.

3.8.4.3 Управление эксплуатацией экземпляра СКЗИ

3.8.4.3.1 Назначить ответственное лицо

Для того чтобы назначить зарегистрированному экземпляру программного СКЗИ **Ответственное лицо,** выполните следующие действия.

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр, нажмите на нём правой кнопкой мыши и выберите **Назначить ответственное лицо.**
2. Откроется страница выбора пользователя в ресурсной системе.

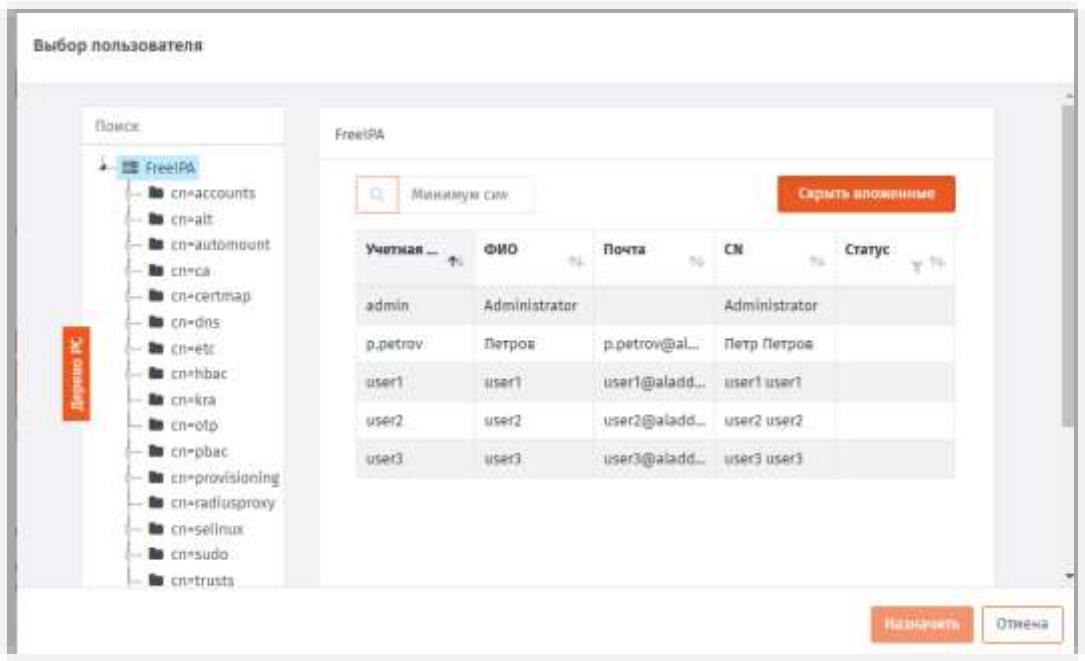


Рис. 221 –Страница выбора пользователя

3. Выберите пользователя и нажмите **Назначить**.

3.8.4.3.2 Ввести в эксплуатацию

Для того чтобы ввести в эксплуатацию зарегистрированный экземпляр программного СКЗИ, выполните следующие действия.

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр, нажмите на нем правой кнопкой мыши и выберите **Ввести в эксплуатацию.**

2. Откроется страница ввода в эксплуатацию:

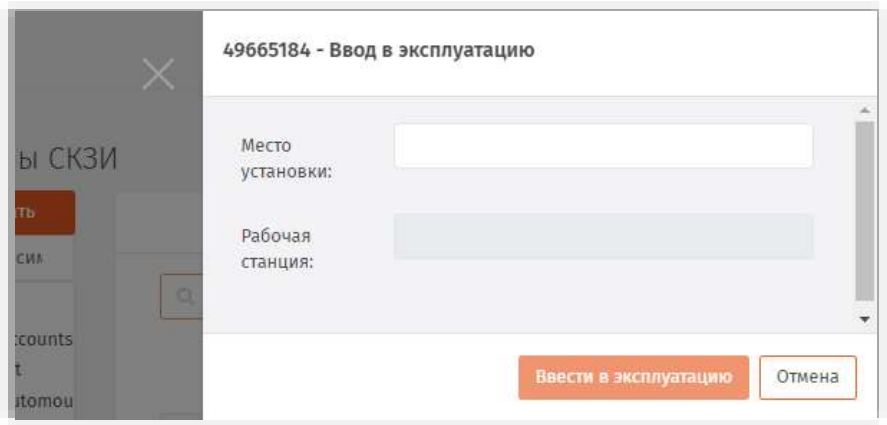


Рис. 222 –Страница ввода СКЗИ в эксплуатацию

3. Введите данные в поле **Место установки** и в поле **Рабочая станция** и нажмите **Ввести в эксплуатацию**.

Примечание. Поле **Место установки** – не обязательно для заполнения. Это поле заполняется, если требуется указать помещение или какое-то специфическое устройство (аппаратуру) и т.п.

3.8.4.3.3 Вывести из эксплуатации

Для того чтобы вывести из эксплуатации экземпляр программного СКЗИ, выполните следующие действия:

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр, нажмите на нем правой кнопкой мыши и выберите **Вывести из эксплуатации.**
2. Откроется окно подтверждения действия:

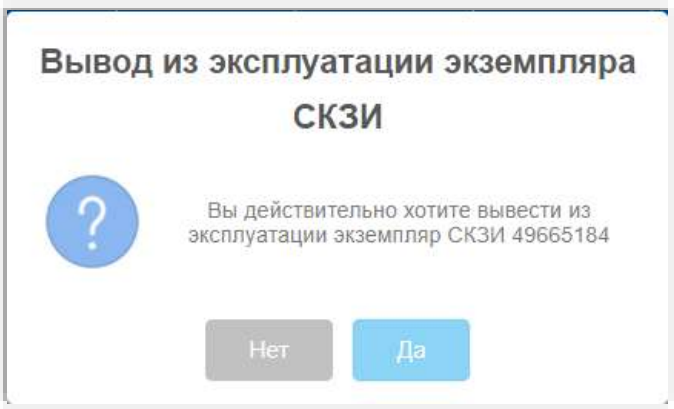


Рис. 223 –Окно подтверждения вывода экземпляра СКЗИ из эксплуатацию

3. Нажмите **Да**.

3.8.4.3.4 Вернуть в эксплуатацию

Для того чтобы вернуть в эксплуатацию экземпляр программного СКЗИ, выполните следующие действия:

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр, нажмите на нем правой кнопкой мыши и выберите **Вернуть в эксплуатацию.**
2. В окне подтверждения действия нажмите **Да**.

3.8.4.3.5 Уничтожить

Для того чтобы уничтожить зарегистрированный экземпляр программного СКЗИ, выполните следующие действия.

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр, нажмите на нем правой кнопкой мыши и выберите **Уничтожить.**
2. В окне подтверждения действия нажмите **Да**.

3.8.5 Дистрибутивы СКЗИ

Действия, выполнение которых возможно в разделе **Учет СКЗИ** -> **Дистрибутивы СКЗИ** перечислены в таблице 59.

В свойствах зарегистрированных дистрибутивов СКЗИ отображаются параметры, описание которых представлено в таблице 64.

Табл. 64 – Перечень свойств дистрибутива СКЗИ

Параметр	Описание
Учетный номер	Учетный номер экземпляра СКЗИ (номер компакт-диска или другой учетный номер другого носителя)
Тип СКЗИ	Тип СКЗИ (один из встроенных или пользовательских типов СКЗИ)
Название	Название Дистрибутива
Описание	Краткое текстовое описание Дистрибутива
Тип носителя	Текстовое описание типа носителя (Напр. CD-ROM)
От кого получено	Текстовое описание лица, от которого получен дистрибутив
Учетный номер документации	Учетный номер документации к СКЗИ, поставляемой с дистрибутивом. В качестве учетного номера документации следует указывать уникальный идентификатор, включающий в себя обозначение ведомости эксплуатационных документов СКЗИ согласно ГОСТ 19.101-77 и ГОСТ 19.103-77. Пример формирования учетного номера документации: <Обозначение *Ведомости эксплуатационных документов*>—<Номер СКЗИ>—<Учетный номер дистрибутива>
Место хранения	Место хранения Дистрибутива

Параметр	Описание
Ответственное лицо	Лицо, получившее Дистрибутив в ответственное пользование
Копия	Опция, отображающая факт – является ли Дистрибутив копией
Номер оригинала	Номер оригинала Дистрибутива
Дата создания	Дата создания Дистрибутива

3.8.5.1 Регистрация дистрибутива СКЗИ

Для того чтобы зарегистрировать дистрибутив СКЗИ, выполните следующие действия:

1. Перейдите в раздел **Учет СКЗИ** –> **Дистрибутивы СКЗИ** и вверху справа нажмите **Зарегистрировать**.
2. Откроется страница регистрации дистрибутива СКЗИ.
3. Введите **Учетный номер дистрибутива** СКЗИ, из раскрывающегося списка выберите **Тип СКЗИ**. При необходимости заполните поле **Описание**, **Тип носителя** и поле **От кого получено**, введите **Учетный номер документации**, **Место хранения** и **Ответственное лицо**. Если регистрируемый дистрибутив СКЗИ является копией – выберите опцию **Копия**, а в поле **Номер оригинала** введите номер оригинала дистрибутива. Нажмите **Зарегистрировать**.

Зарегистрированный дистрибутив СКЗИ отобразится в консоли управления JMS в разделе **Учет СКЗИ** -> **Дистрибутивы СКЗИ**.

3.8.5.2 Тиражирование копий дистрибутива

При копировании дистрибутива необходимо учитывать следующие особенности:

- копии диска присваивается свой учетный номер, который формируется из учетного номера оригинала, например, добавлением числа: учетный номер оригинала– ДСД01, учетный номер копии – ДСД01-1;
- эталонному диску может соответствовать документация;
- копия эталонного дистрибутива закрепляется за администратором;
- нумерация копий выполняется от оригинала с учетом счетчика копий, например, если сделаны копии 1,2,3, а затем копия 2 удалена, то следующая копия будет иметь номер 4;
- при создании копии есть возможность указать количество создаваемых копий;
- копии от копий создавать нельзя;
- есть возможность зарегистрировать существующую копию, при этом формируется нормативная документация (Акт создания дистрибутива СКЗИ и документации) с возможностью печати.

Для того чтобы копировать зарегистрированный Дистрибутив СКЗИ выполните следующие действия:

1. Выделите в списке зарегистрированных Дистрибутивов СКЗИ требуемый экземпляр, нажмите на нем правой кнопкой мыши и выберите **Копировать**.
2. На странице тиражирования дистрибутива укажите **Тип носителя** и **Количество копий оригинала**, затем нажмите **Копировать**.

3.8.5.3 Импорт дистрибутивов (пакетная регистрация)

Для того чтобы произвести пакетную регистрацию дистрибутивов с помощью мастера импорта дистрибутивов выполните следующие действия:

1. В консоли управления JMS откройте раздел **Учет СКЗИ -> Дистрибутивы СКЗИ.**
2. Вверху нажмите **Импорт (**Рис. 224**)**.

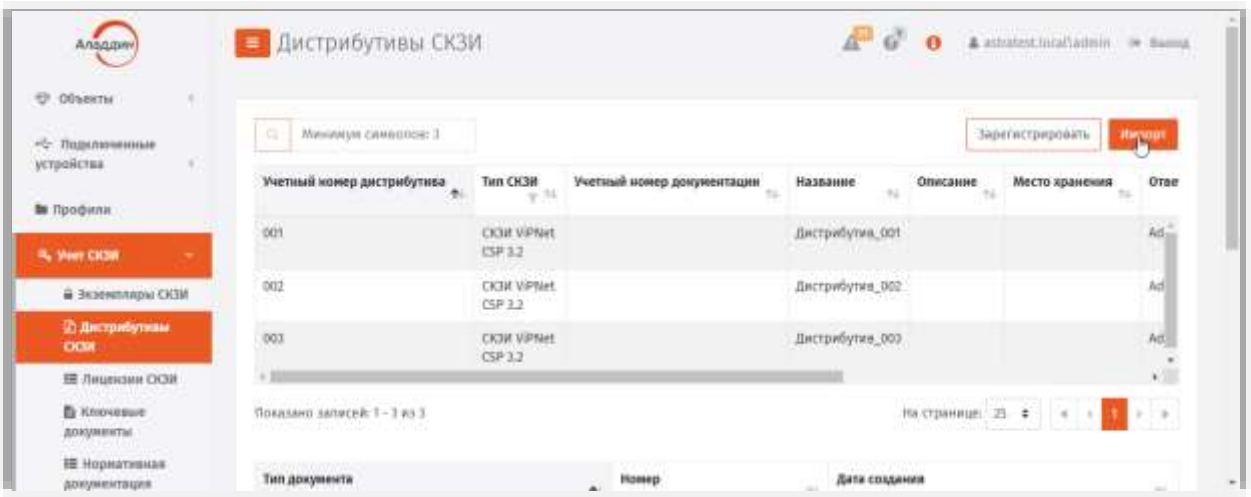


Рис. 224 – Вызов мастера импорта дистрибутивов СКЗИ

3. На странице мастера импорта дистрибутивов СКЗИ выберите значения в полях **Тип СКЗИ**, **Ответственное лицо** и укажите **Файл импорта** и нажмите **Далее**.

Примечание. Файл импорта представляет собой файл в формате *.CSV. Подробнее о структуре файла см. в разделе «Формат файлов импорта дистрибутива СКЗИ», ниже.

4. Следуйте указаниям мастера до завершения процедуры.

3.8.5.3.1 Формат файлов импорта дистрибутива СКЗИ

Файлы для импорта дистрибутивов СКЗИ имеют *.CSV формат. Первая строка файла содержит заголовок, перечисляющий имена полей через разделитель. Далее идут значения соответствующих полей дистрибутива СКЗИ также через разделитель. Разделитель соответствует знаку табуляции “\t”.

Заголовок файла описывает, каким образом значения из файла будут соотноситься со свойствами импортируемого дистрибутива СКЗИ. Он должен содержать определенный набор полей. Порядок перечисления полей произвольный. В случае наличия в файле произвольного дополнительного поля с неизвестным свойством, оно будет игнорироваться при импорте. Обязательные поля должны быть включены в заголовок файла импорта, в противном случае при импорте возникнет ошибка формата файла импорта «**В заголовке файла импорта не найдено обязательное поле {0}**».

Нижележащие файла содержат значения полей из заголовка для дистрибутива СКЗИ. Порядок следования значений должен соответствовать порядку объявленных поле в заголовке. Пустые значения полей могут быть представлены в виде пустой строки, ограниченной разделителями. Некоторые поля не могут иметь пустых значений. При создании такого дистрибутива произойдет ошибка, которая будет отображена в статистике Мастера импорта дистрибутивов СКЗИ. Значения нестроковых типов должны быть описаны в формате, позволяющем преобразование из строки файла импорта в значение указанного типа. Например, для булевого типа – “true”/”false”, для даты времени – dd.MM.yyyy.

Список полей файла импорта дистрибутива СКЗИ приведен в таблице 65.

Табл. 65 – Список полей файла импорта дистрибутивов СКЗИ

№	Наименование поля в файле	Наименование свойства	Тип свойства	Обязательное поле	Обязательное значение
1	Name	Name	Строковый	Да	Да
2	Description	Description	Строковый	Нет	Нет
3	PackageNumber	PackageNumber	Строковый	Да	Нет
4	DocumentNumber	DocumentNumber	Строковый	Нет	Нет
5	IsCopy	IsCopy	Булевый	Да	Да
6	OriginalNumber	OriginalNumber	Строковый	Нет	Нет
7	ReceivedFrom	ReceivedFrom	Строковый	Нет	Нет
8	MediaType	MediaType	Строковый	Нет	Нет

Пример файла импорта:

```
Name  Description PackageNumber    DocumentNumber    IsCopy      OriginalNumber
ReceivedFrom     MediaType
name1 description1     1          False       received_from1   media_type1
name2 description2     2          False       received_from2   media_type2
name3 description3     3     1    False       received_from3   media_type1
```

3.8.5.4 Экспорт списка дистрибутивов СКЗИ в файл

JMS позволяет экспортировать список дистрибутивов СКЗИ в файл с тем, чтобы данный список дистрибутивов можно было импортировать на другом экземпляре JMS.

Для того чтобы выполнить экспорт списка дистрибутивов в файл с помощью мастера экспорта дистрибутивов выполните следующие действия:

1. В консоли управления JMS откройте раздел **Учет СКЗИ -> Дистрибутивы СКЗИ.**
2. Выделите в списке зарегистрированных дистрибутивов СКЗИ требуемые экземпляры, нажмите правой кнопкой мыши и выберите **Экспорт** (Рис. 225).

Важно! Для экспорта допускается выбирать дистрибутивы только одного и того же типа СКЗИ. Для обеспечения этого требования можно воспользоваться механизмом фильтрации по полю **Тип СКЗИ** (установите фильтрацию только для одного типа дистрибутивов СКЗИ).

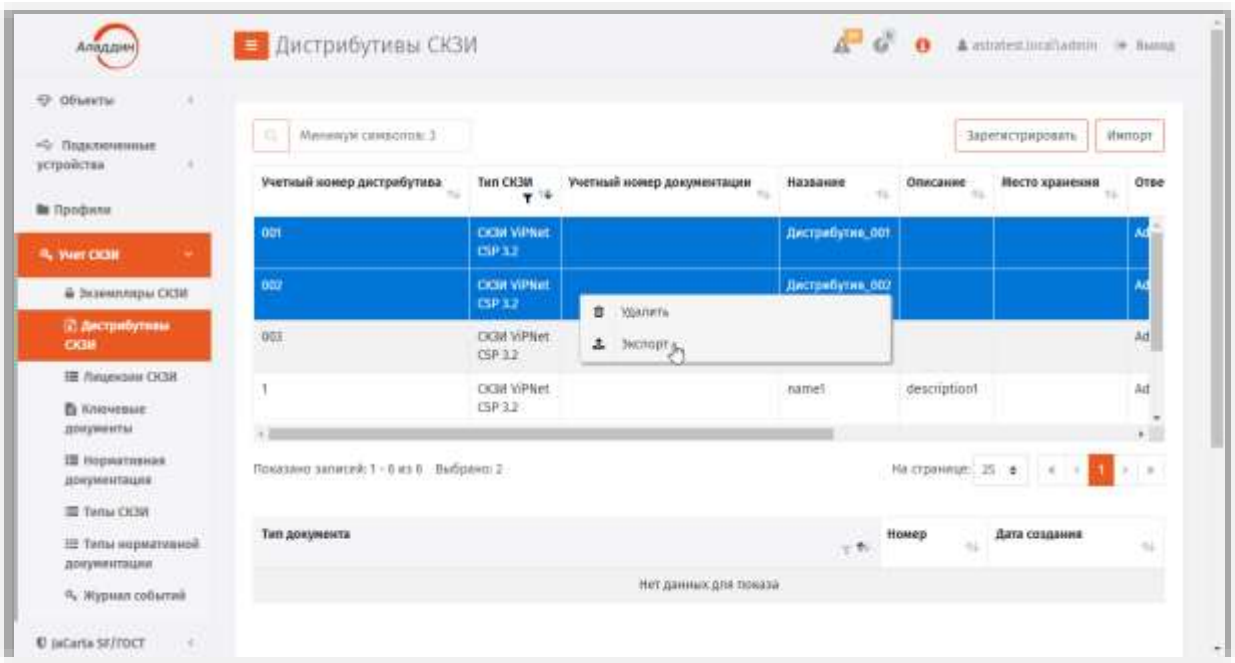


Рис. 225 – Вызов мастера экспорта дистрибутивов СКЗИ

3. Отобразится стартовая страница мастера экспорта дистрибутивов СКЗИ

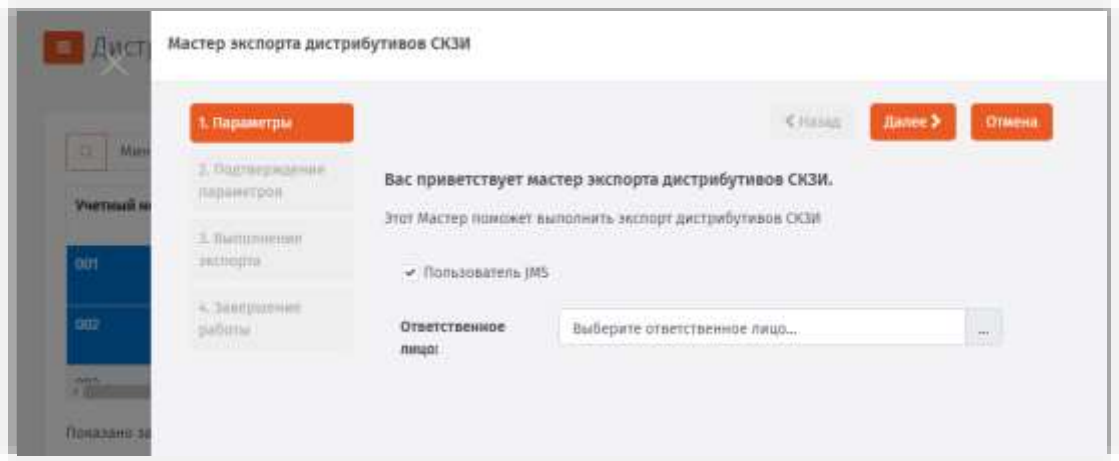


Рис. 226 – Стартовая страница мастера экспорта дистрибутивов СКЗИ

4. В случае если ответственное за СКЗИ лицо не является пользователем JMS, введите его имя вручную в поле **Ответственное лицо.** В противном случае выберите ответственное лицо из раскрывающегося списка.
5. Нажмите **Далее**.

Отобразится страница подтверждения параметров экспорта.

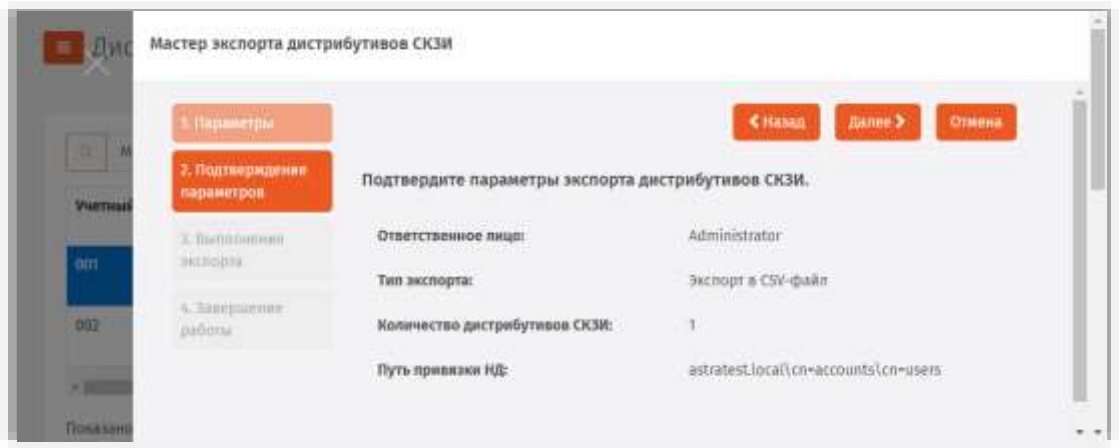


Рис. 227 –Страница подтверждения параметров экспорта дистрибутивов СКЗИ

6. Нажмите **Далее**.
7. В папку загрузок браузера сохранится файл экспорта с именем «ExportPackages.csv».

Примечание. Файл экспорта представляет собой файл в формате *.CSV. Формат файлов экспорта аналогичен формату файлов импорта. Подробнее о структуре файла см. в разделе «Формат файлов импорта дистрибутива СКЗИ», с. 228.

В файл экспорта записывается заголовок, согласно объявленным полям импорта дистрибутивов СКЗИ, ниже записываются значения этих полей в том же порядке. Одна строка соответствует одному дистрибутиву СКЗИ. При экспорте дистрибутивы удаляются из БД и могут быть повторно импортированы из файла экспорта.

Отобразится страница с отчетом о выполнении экспорта.

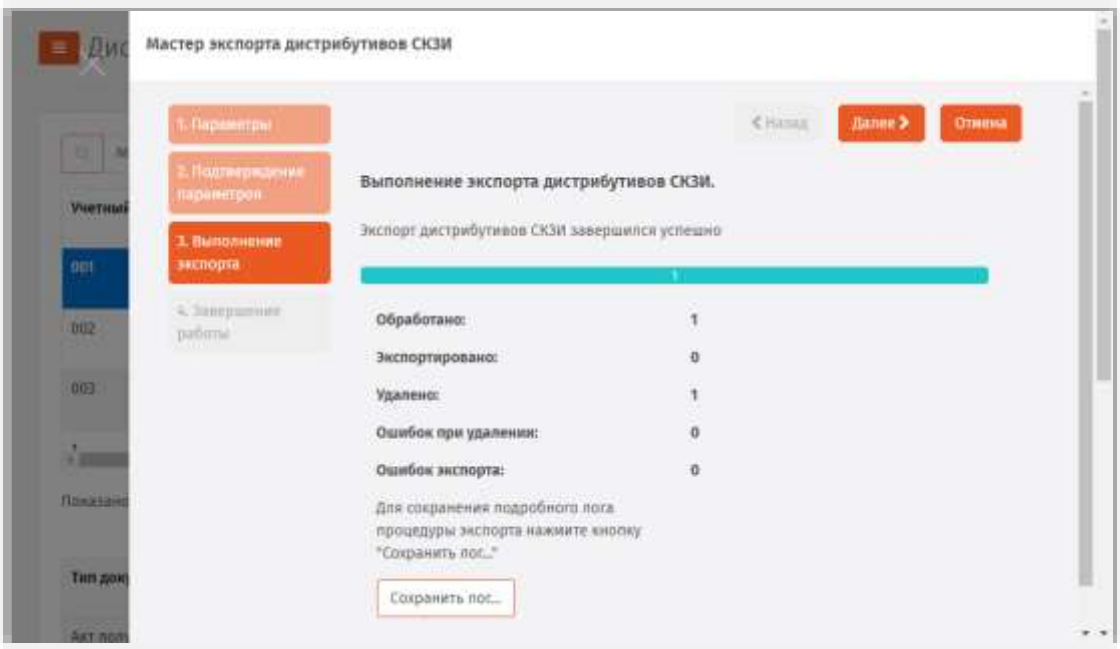


Рис. 228 –Страница с отчетом о выполнении экспорта дистрибутивов СКЗИ

8. При необходимости сохраните журнал процесса экспорта дистрибутивов СКЗИ (кнопка **Сохранить лог...**)
9. Нажмите **Далее**.
10. Нажмите **Завершить**, чтобы закончить работу мастера

По окончании экспорта информация об экспортированных дистрибутивах СКЗИ будет удалена с данного экземпляра сервера JMS. Полученный файл может быть использован для последующего импорта на другом экземпляре сервера JMS (см. раздел «Импорт дистрибутивов», с. 228).

3.8.5.5 Назначение (отмена назначения) дистрибутиву экземпляра СКЗИ

Для того чтобы назначить дистрибутиву экземпляр СКЗИ, выполните следующие действия:

1. В консоли управления JMS откройте раздел **Учет СКЗИ -> Дистрибутивы СКЗИ.**
2. Выберите в списке необходимый дистрибутив СКЗИ, нажмите на нем правой кнопкой мыши и выберите **Назначить экземпляр СКЗИ** (Рис. 229).

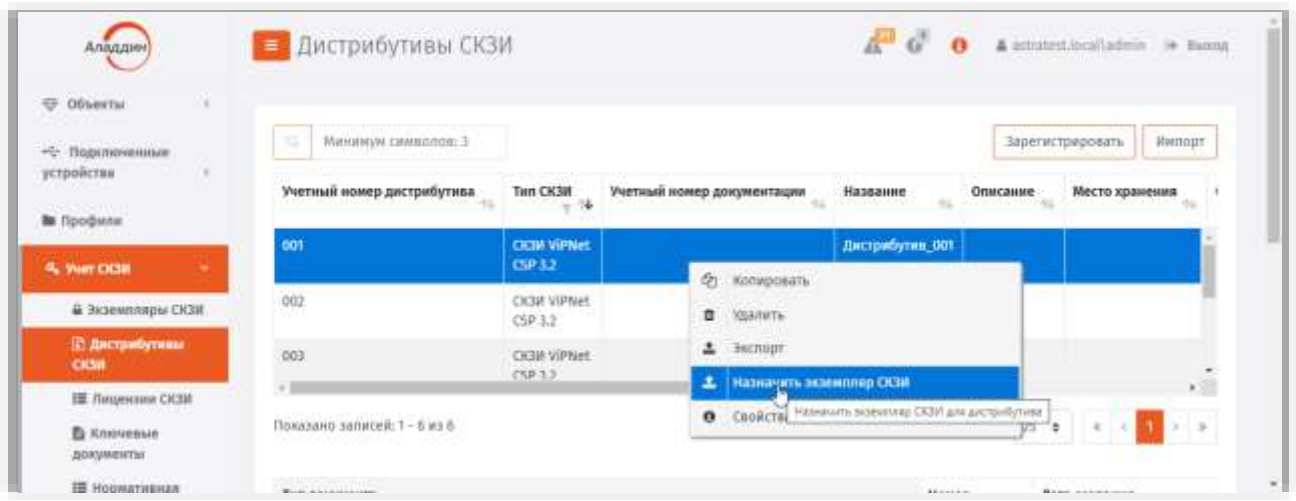


Рис. 229 – Выбор дистрибутива для назначению ему экземпляра СКЗИ

3. Откроется страница назначения экземпляра СКЗИ.

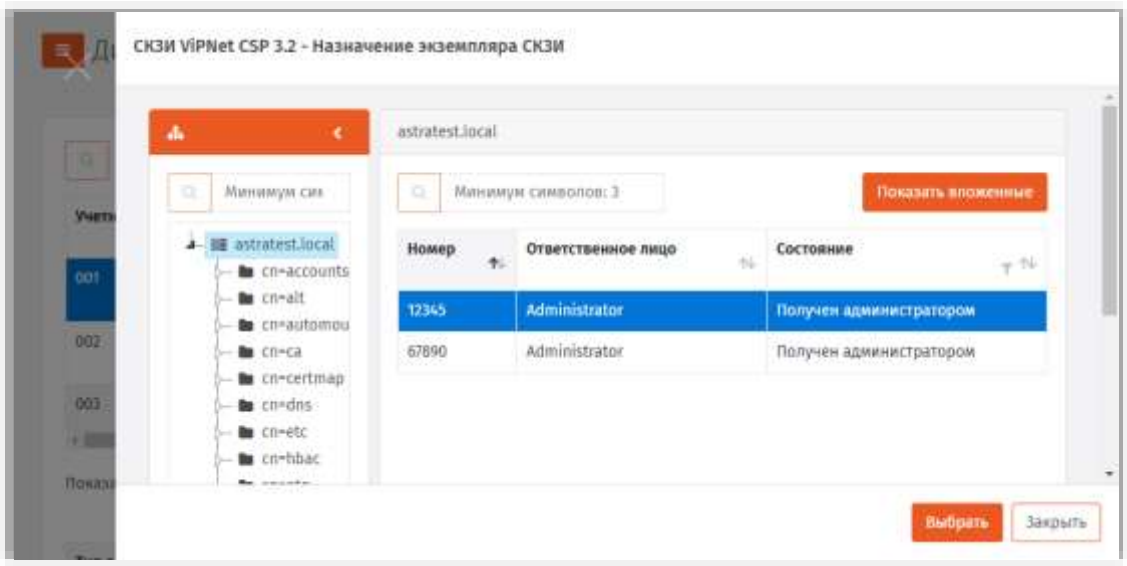


Рис. 230 – Выбор экземпляра СКЗИ

4. Выберите экземпляр СКЗИ и нажмите **Выбрать**.

После назначения дистрибутиву экземпляра СКЗИ в свойствах данного экземпляра в поле **Дистрибутив** будет отображаться назначенный дистрибутив.

Для того чтобы отменить назначение, выберите дистрибутив из списка и нажмите **Отменить назначение экземпляра СКЗИ**. После чего в появившемся окне подтвердите свой выбор, нажав **Да**.

3.8.6 Лицензии СКЗИ

Действия, выполнение которых возможно в разделе **Учет СКЗИ** -> **Лицензии СКЗИ** перечислены в таблице 59.

При просмотре списка зарегистрированных лицензий СКЗИ отображаются свойства, описание которых представлено в таблице 66.

Табл. 66 – Перечень свойств лицензии СКЗИ

Наименование свойства	Описание
Серийный номер	Серийный номер лицензии
Тип СКЗИ	Тип СКЗИ (один из встроенных или пользовательских типов СКЗИ)
Кем выдано	Название организации, кем выдана лицензия
Кому выдано	Название организации, кому выдана лицензия
Ответственное лицо	Лицо, получившее лицензию на ответственное применение
Физическое состояние	Физическое состояние лицензии (установлена, не установлена)
Логическое состояние	Логическое состояние лицензии (свободна, назначена)
Дата формирования	Дата формирования лицензии
Дата начала действия	Дата начала действия лицензии
Дата окончания действия	Дата окончания действия лицензии

3.8.6.1 Регистрация лицензии СКЗИ

Примечание. Если зарегистрировать лицензию на СКЗИ, относящегося к типу, у которого установлена опция **Автосоздание экземпляра СКЗИ**, то одновременно с регистрацией такой лицензии автоматически зарегистрируется и экземпляр СКЗИ данного типа.

Для того чтобы зарегистрировать лицензию СКЗИ, выполните следующие действия:

1. Перейдите в раздел **Учет СКЗИ –> Лицензии СКЗИ**.

Откроется страница следующего вида.

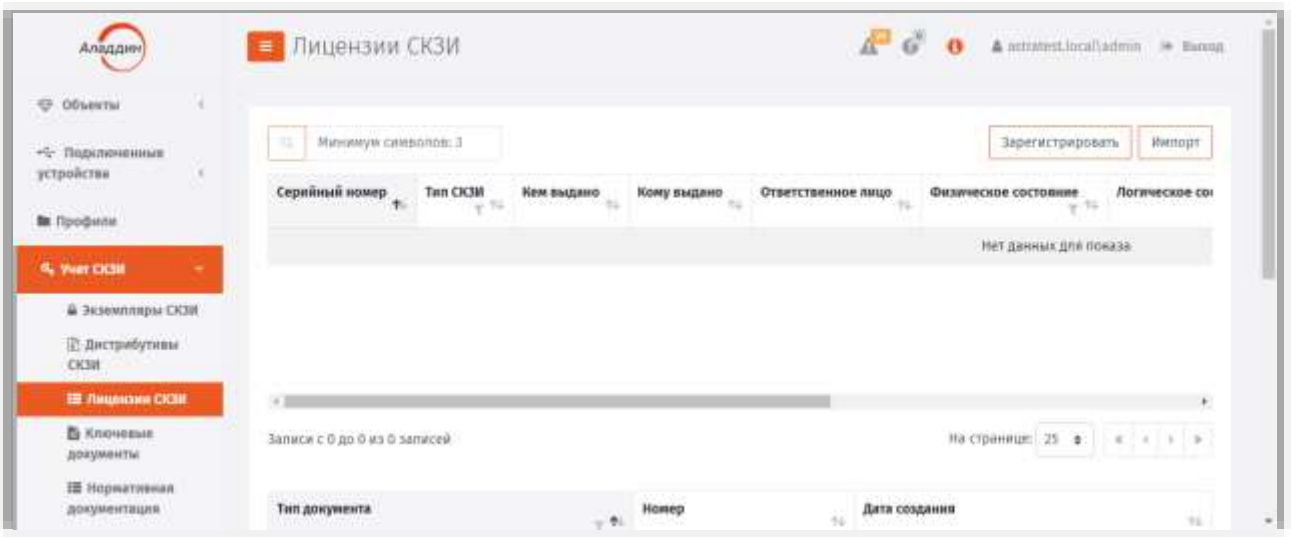


*Рис. 231 – Страница **Лицензии СКЗИ***

2. Нажмите вверху **Зарегистрировать**.
Откроется страница следующего вида.

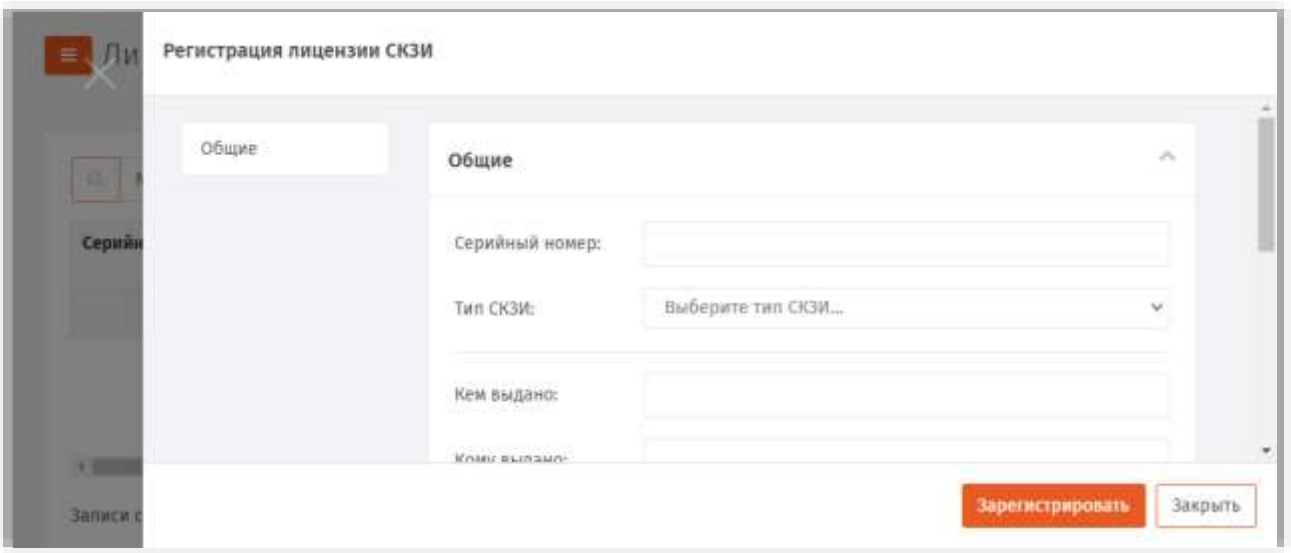


Рис. 232 – Страница регистрации Лицензии СКЗИ

3. Введите значения **Серийный номер*** лицензии СКЗИ, из раскрывающегося списка выберите **Тип СКЗИ**, заполните поля **Кем выдано** и **Кому выдано**, **Ответственное лицо***. При необходимости введите значения в полях **Дата формирования**, **Дата начала действия** и **Дата окончания действия**. Нажмите **Зарегистрировать**.

Примечание. Атрибуты, помеченные звёздочкой (*) обязательны для заполнения.

Зарегистрированная лицензия СКЗИ отобразится в окне консоли управления JMS в разделе **Учет СКЗИ** -> **Лицензии СКЗИ**.

3.8.6.2 Импорт лицензий (пакетная регистрация)

Для того чтобы произвести пакетную регистрацию лицензий с помощью мастера импорта лицензий выполните следующие действия.

1. В консоли управления JMS откройте раздел **Учет СКЗИ -> Лицензии СКЗИ.**
2. Вверху нажмите **Импорт (**Рис. 233**)**.

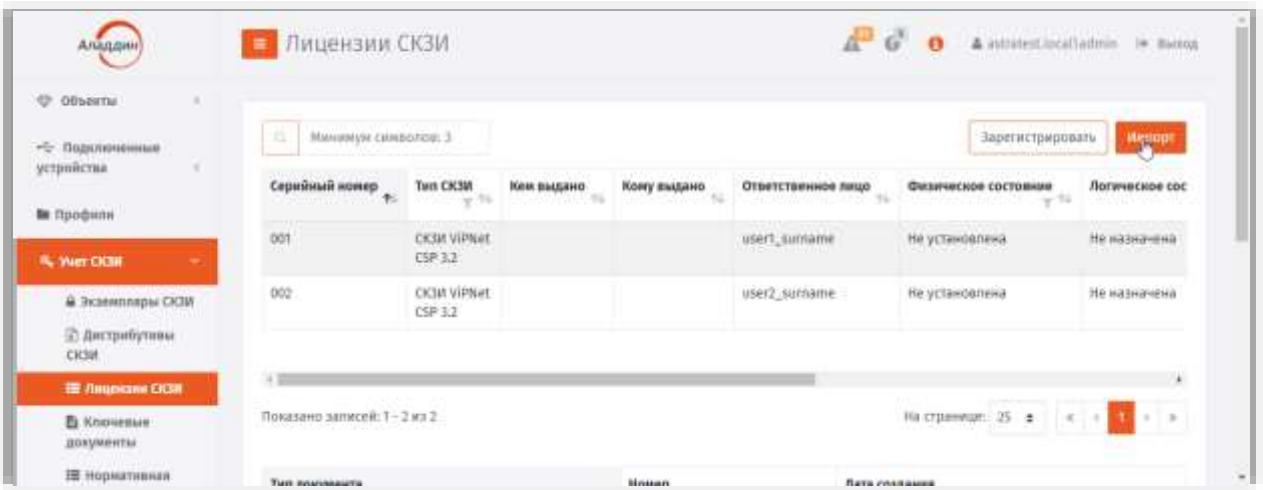


Рис. 233 – Вызов мастера импорта лицензий СКЗИ

3. На странице мастера импорта лицензий СКЗИ выберите значения в полях **Тип СКЗИ**, **Ответственное лицо** и укажите **Файл импорта** и нажмите **Далее**.

Примечание. Файл импорта представляет собой файл в формате *.CSV. Подробнее о структуре файла см. в разделе «Формат файлов импорта лицензий СКЗИ», ниже.

4. Следуйте указаниям мастера до завершения процедуры.

3.8.6.2.1 Формат файлов импорта лицензий СКЗИ

Файлы для импорта лицензий СКЗИ имеют *.CSV формат. Первая строка файла содержит заголовок, перечисляющий имена полей через разделитель (знак табуляции). Далее идут значения соответствующих полей лицензии СКЗИ, также через разделитель. Разделитель соответствует знаку табуляции “\t”.

Заголовок файла описывает, каким образом значения из файла будут соотноситься со свойствами импортируемой лицензии СКЗИ. Он должен содержать определенный набор полей. Порядок перечисления полей произвольный. В случае наличия в файле произвольного дополнительного поля с неизвестным свойством, оно будет игнорироваться при импорте. Обязательные поля должны быть включены в заголовок файла импорта, в противном случае при импорте возникнет ошибка формата файла импорта «**В заголовке файла импорта не найдено обязательное поле {0}**».

Нижележащие строки файла содержат значения полей из заголовка для лицензии СКЗИ. Порядок следования значений должен соответствовать порядку объявленных поле в заголовке. Пустые значения полей могут быть представлены в виде пустой строки, ограниченной разделителями. Некоторые поля не могут иметь пустых значений. При создании такой лицензии произойдет ошибка, которая будет отображена в статистике Мастера импорта лицензий СКЗИ. Значения нестроковых типов должны быть описаны в формате, позволяющем преобразование из строки файла импорта в значение указанного типа. Например, для булевого типа – “true”/”false”, для даты времени – dd.MM.yyyy.

Список полей файла импорта лицензий СКЗИ приведен в таблице 67.

Табл. 67 – Список полей файла импорта лицензий СКЗИ

№	Наименование поля в файле	Наименование свойства	Тип свойства	Обязательное поле	Обязательное значение
1	SerialNumber	SerialNumber	Строковый	Да	Да
2	IssuedName	IssuedName	Строковый	Нет	Нет
3	GrantedName	GrantedName	Строковый	Нет	Нет
4	IssuedDate	IssuedDate	Дата	Да	Нет
5	ValidFrom	ValidFrom	Дата	Да	Нет
6	ValidTo	ValidTo	Дата	Да	Нет

Пример файла импорта:

SerialNumber	IssuedName	GrantedName	IssuedDate	ValidFrom	ValidTo
1	issued_name1	granted_name1	16.12.2016	16.12.2016	16.01.2017
2	issued_name2	granted_name2	16.12.2016	16.12.2016	16.01.2017
3	issued_name3	granted_name3	16.12.2016	16.12.2016	16.01.2017

3.8.6.3 Экспорт списка лицензий СКЗИ в файл

JMS позволяет экспортировать список лицензий СКЗИ в файл с тем, чтобы данный список лицензий можно было импортировать на другом экземпляре JMS.

Для того чтобы выполнить экспорт списка лицензий в файл с помощью мастера экспорта лицензий выполните следующие действия.

1. В консоли управления JMS откройте раздел **Учет СКЗИ -> Лицензии СКЗИ.**
2. Выделите в списке зарегистрированных лицензий СКЗИ требуемые экземпляры, нажмите правой кнопкой мыши и выберите **Экспорт** (Рис. 225).

Важно! Для экспорта допускается выбирать лицензии только одного и того же типа СКЗИ. Для обеспечения этого требования можно воспользоваться механизмом фильтрации по полю **Тип СКЗИ** (установите фильтрацию только для одного типа лицензий СКЗИ).

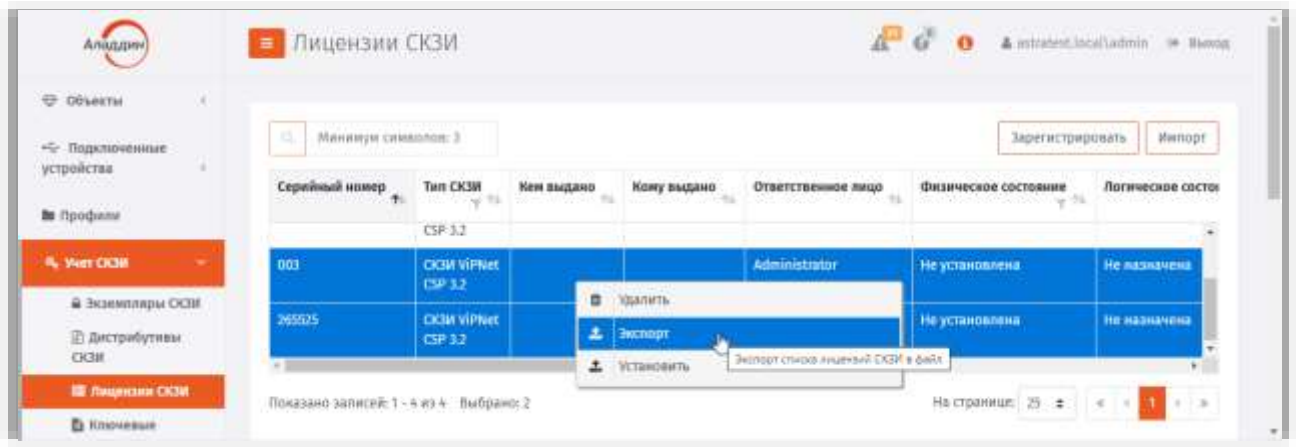


Рис. 234 – Вызов мастера экспорта лицензий СКЗИ

3. Отобразится стартовая страница мастера экспорта лицензий СКЗИ

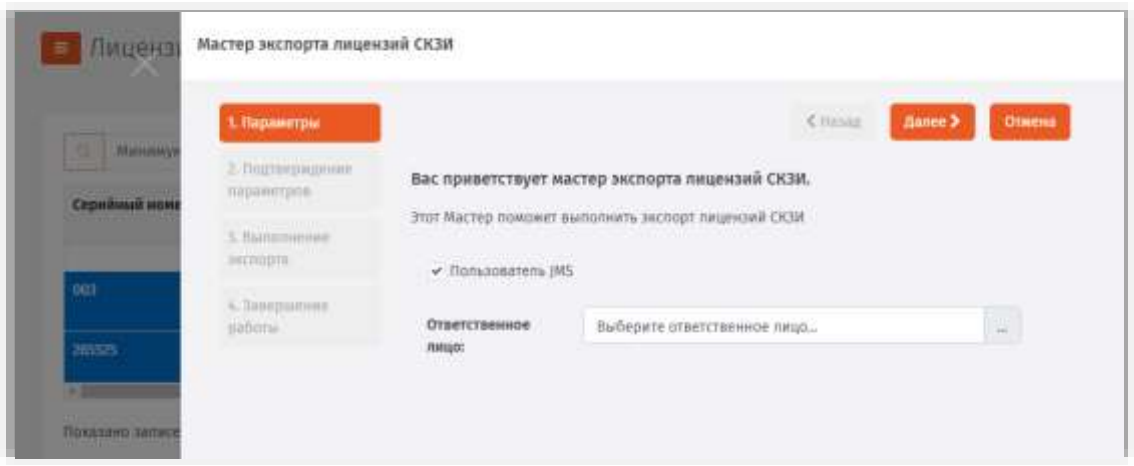


Рис. 235 – Стартовая страница мастера экспорта лицензий СКЗИ

4. Выберите **Ответственное лицо** и нажмите **Далее**.
Отобразится страница подтверждения параметров экспорта.

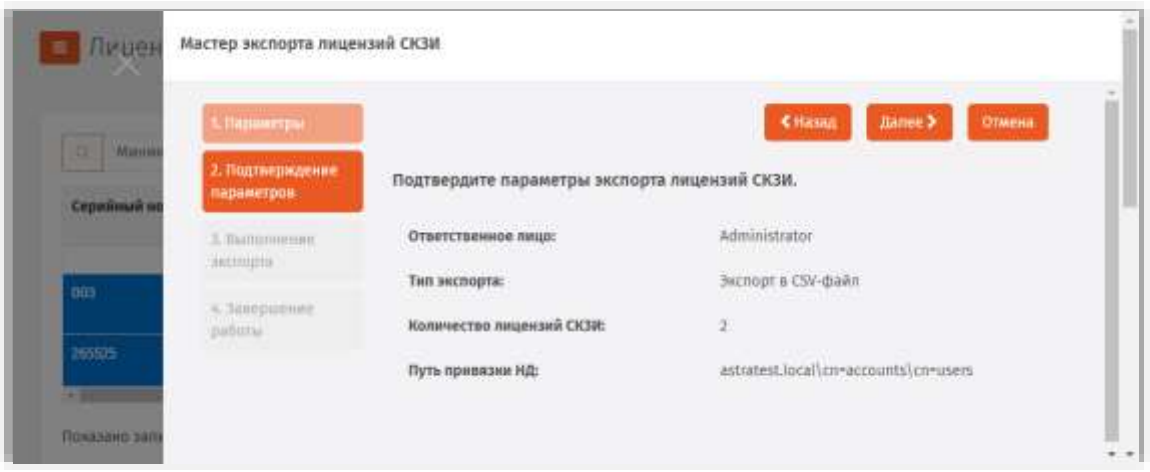


Рис. 236 –Страница подтверждения параметров экспорта лицензий СКЗИ

5. Нажмите **Далее**.

6. В папку загрузок браузера сохранится файл экспорта с именем «ExportLicences.csv».

Примечание. Файл экспорта представляет собой файл в формате *.CSV. Формат файлов экспорта аналогичен формату файлов импорта. Подробнее о структуре файла см. в разделе «Формат файлов импорта лицензий СКЗИ», с. 235.

В файл экспорта записывается заголовок, согласно объявленным полям импорта лицензий СКЗИ, ниже записываются значения этих полей в том же порядке. Одна строка соответствует одной лицензии СКЗИ. При экспорте лицензии удаляются из БД и могут быть повторно импортированы из файла экспорта.

Отобразится страница с отчетом о выполнении экспорта.

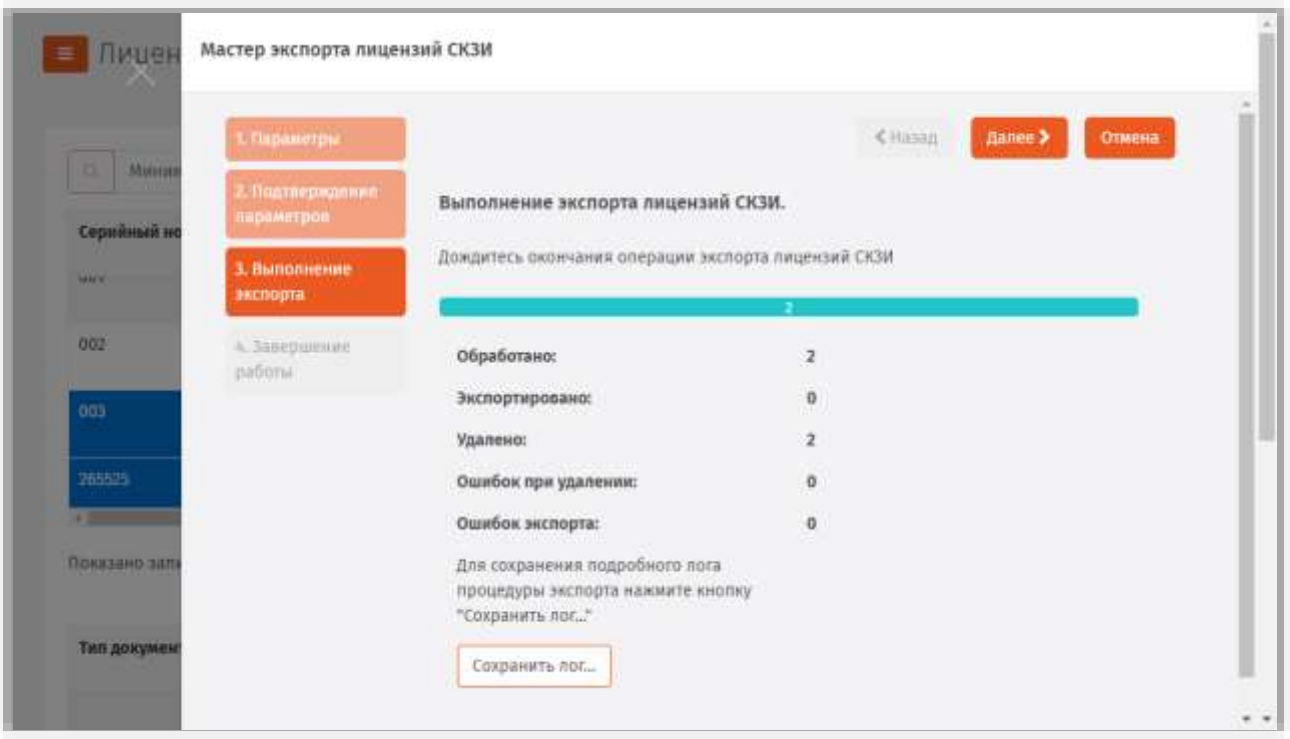


Рис. 237 –Страница с отчетом о выполнении экспорта лицензий СКЗИ

7. При необходимости сохраните журнал процесса экспорта лицензий СКЗИ (кнопка **Сохранить лог...**)
8. Нажмите **Далее**.
9. Нажмите **Завершить**, чтобы закончить работу мастера

По окончании экспорта информация об экспортированных лицензиях СКЗИ будет удалена с данного экземпляра сервера JMS. Полученный файл может быть использован для последующего импорта на другом экземпляре сервера JMS (см. раздел «235Импорт лицензий (пакетная регистрация)», с. 235).

3.8.6.4 Установка (отмена установки) лицензии

Для того чтобы установить лицензию, выполните следующие действия.

1. В консоли управления JMS откройте раздел **Учет СКЗИ -> Лицензии СКЗИ.**
2. Найдите в списке зарегистрированных лицензий СКЗИ требуемый экземпляр, нажмите на нём правой кнопкой мыши и выберите **Установить** (Рис. 238).

Примечание. Для установки лицензии необходимо, чтобы значение свойства **Физическое состояние** требуемого экземпляра лицензии было **Не установлена**, в противном случае – установка невозможна.

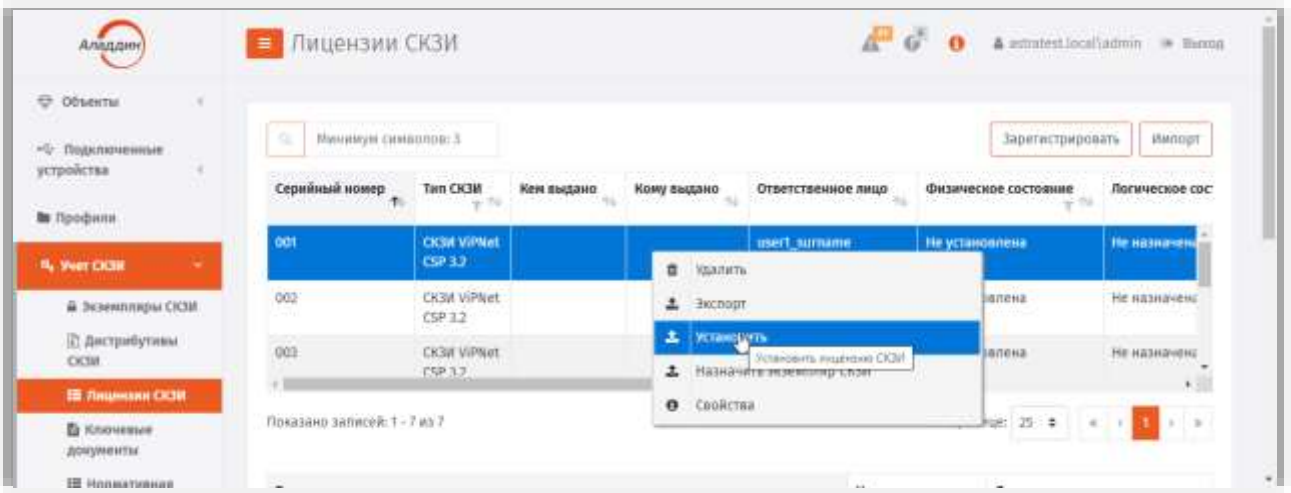


Рис. 238 – Установка лицензии

3. В окне подтверждения нажмите **Да**.

Для того чтобы отменить установку лицензии, выбрав соответствующую установленную лицензию нажмите **Отменить установку**.

3.8.6.5 Назначение (отмена назначения) лицензии экземпляра СКЗИ

Для того чтобы назначить лицензии экземпляр СКЗИ, выполните следующие действия.

1. В консоли управления JMS откройте раздел **Учет СКЗИ -> Лицензии СКЗИ.**
2. Найдите в списке зарегистрированных лицензий СКЗИ требуемый экземпляр, нажмите на нём правой кнопкой мыши и выберите **Назначить экземпляр СКЗИ** (Рис. 239).

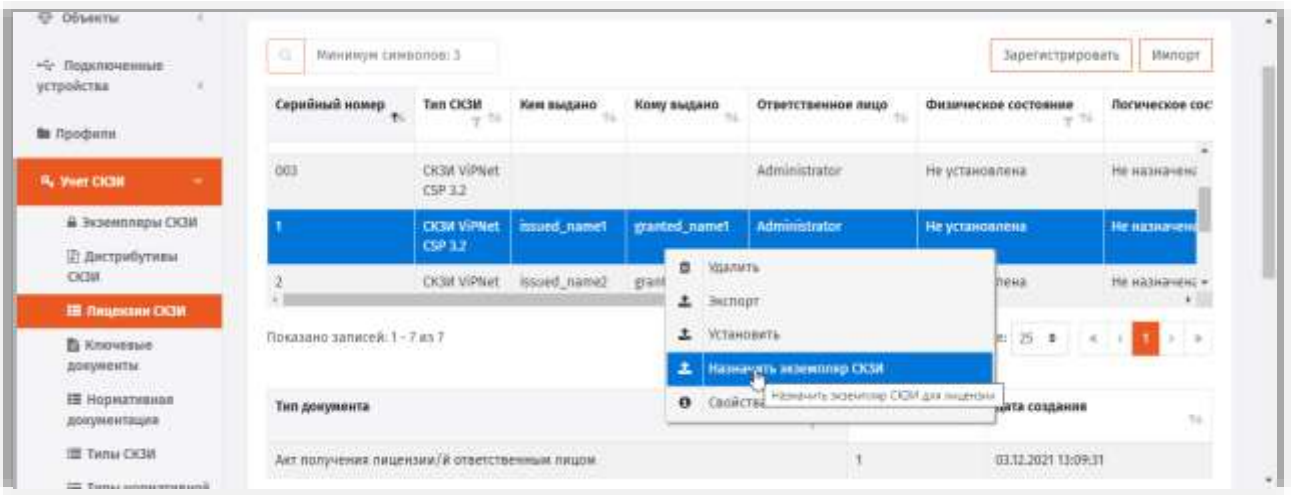


Рис. 239 – Запуск назначения лицензии экземпляра СКЗИ

3. Отобразится страница выбора СКЗИ.

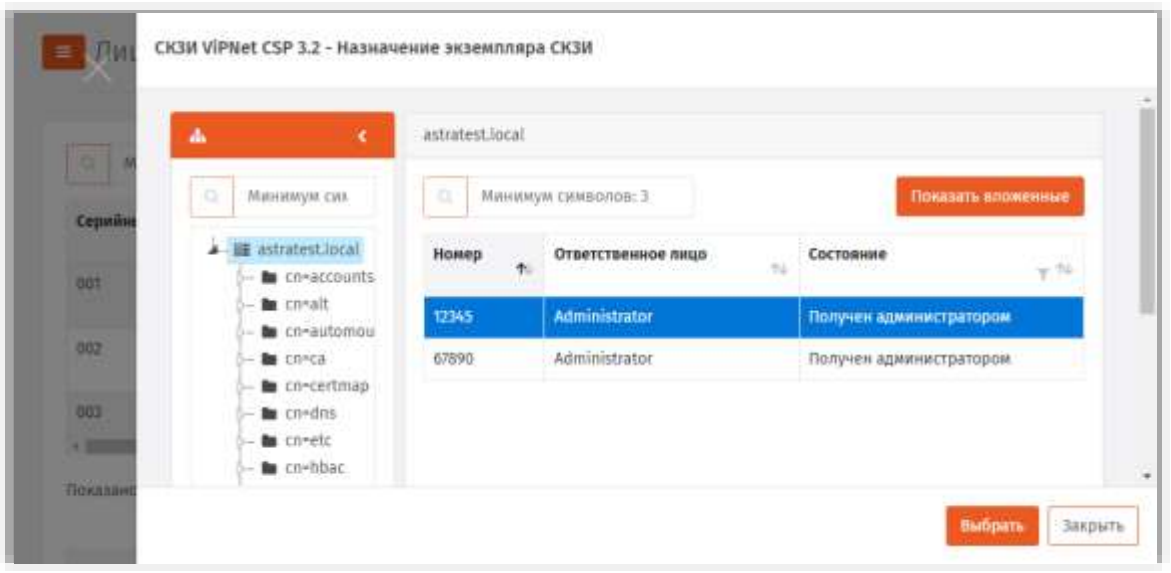


Рис. 240 – Страница выбора СКЗИ для его назначения лицензии

4. Выберите экземпляр СКЗИ и нажмите **Выбрать**.

Для того чтобы отменить назначение, выбрав соответствующую лицензию с назначенным СКЗИ нажмите **Отменить назначение экземпляра СКЗИ** после чего нажмите **Да** в окне запроса подтверждения.

3.8.6.6 Удаление лицензии

Для того чтобы удалить лицензию из списка зарегистрированных лицензий СКЗИ, выполните следующие действия.

1. В консоли управления JMS откройте раздел **Учет СКЗИ -> Лицензии СКЗИ.**
2. Найдите в списке зарегистрированных лицензий СКЗИ требуемый экземпляр, нажмите на нём правой кнопкой мыши и выберите **Удалить**.
3. В окне подтверждения действия нажмите **Да**.

3.8.7 Ключевые документы

Ключевой документ – это объект JMS, соответствующий сертификату, выпущенному в режиме offline (профиль **Выпуск сертификатов (режим офлайн)**, т.е. с использованием УЦ, подключенного к JMS с помощью компонента «Коннектор к Offline Certification Authority») и записываемый на выпущенный электронный ключ.

Действия, выполнение которых возможно в разделе **Учет СКЗИ** -> **Ключевые документы**, перечислены в таблице 59.

При просмотре списка ключевых документов отображаются свойства, описание которых представлено в таблице 68.

Табл. 68 – Перечень свойств ключевого документа

Наименование свойства	Описание
Номер КИ	Номер ключевой информации (сертификата)
Идентификатор КН	Идентификатор ключевого носителя
Номер корпуса КН	Номер корпуса ключевого носителя
Ответственное лицо	Лицо, получившее ключевой документ
От кого получено	Текстовое описание внешнего объекта (внешней организции; задается в профиле категории **Внешние объекты**), выпустившего настоящий ключевой документ (сертификат)
Состояние	Состояние КН, содержащего ключевой документ. (Возможны состояния: получен, введен в эксплуатацию, выведен из эксплуатации, учет прекращен и др.)
Дата создания	Дата создания ключевого документа
Дата передачи	Дата загрузки ключевого документа на ключевой носитель (в текущей версии JMS совпадает со значением **Дата получения**)
Дата уничтожения	Дата уничтожения ключевого документа

Для того чтобы просмотреть список ключевых документов, перейдите в раздел **Учет СКЗИ** -> **Ключевые документы (**Рис. 241**)**.

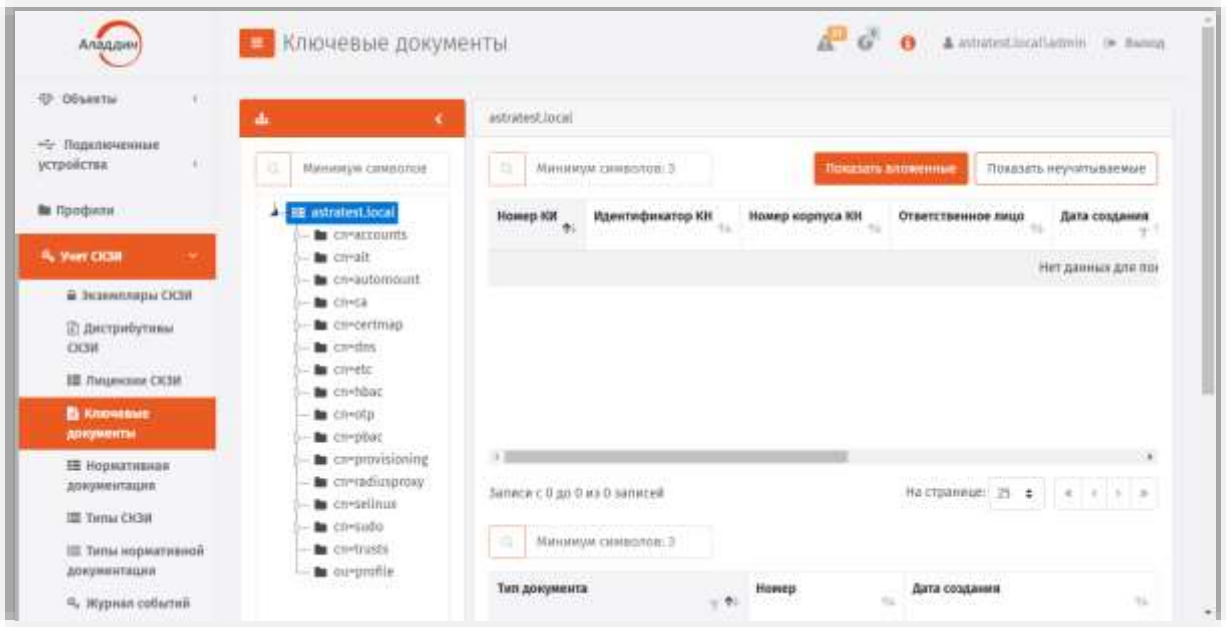


*Рис. 241 – Страница раздела **Учет СКЗИ –> Ключевые документы***

При просмотре списка ключевых документов вверху страницы доступны дополнительные опции просмотра. Описание дополнительных опций просмотра представлено в таблице 69.

Табл. 69

Наименование опции	Описание
Показывать вложенные	При выборе этой опции в списке будут дополнительно отображены ключевые документы, относящиеся к объектам ресурсной системы, которые являются вложенными по отношению к текущему выбранному объекту/контейнеру
Показывать неучитываемые	При выборе этой опции в списке ключевых документов отображаются те документы, учет которых был прекращен

3.8.8 Нормативная документация

Действия, выполнение которых возможно в разделе **Учет СКЗИ** -> **Нормативная документация** перечислены в таблице 59.

В JMS встроен набор заданных типов нормативных документов, требующихся для учета СКЗИ и всех формализованных действий с ними. Для каждого типа может быть задан:

- шаблон для визуализации и печати в формате RTF;
- начальное значение внутренней нумерации документов.

Начальное значение внутренней нумерации документов можно изменять. Измененное начальное значение будет применяться для вновь генерируемых нормативных документов. Настройка начального значения нумерации выполняется в разделе **Учет СКЗИ** –> **Типы нормативных документов**. Для изменения следует открыть свойства выбранного типа нормативной документации, нажать правой кнопкой мыши и выбрать Свойства. На открывшейся странице в поле **Текущий номер** следует вести номер, с которого начнется нумерация следующего сгенерированного документа данного типа). При этом внутренний номер документа может быть не уникален в рамках сервера JMS.

Формирование полного номера документа (т.е. номера, отражаемого в распечатанном нормативном документе) осуществляется в системе за счет подстановки внутреннего номера документа в так называемый *шаблон номера документа* (например *$Number*). Данный шаблон задается в свойствах выбранного типа нормативной документации в поле **Шаблон номера документа** (способ изменения см. по аналогии с полем **Текущий номер**, выше).

Нормативный документ хранится в системе в виде набора данных в формате XML. При необходимости его визуализировать или распечатать, данные документа форматируются по заданному шаблону RTF при помощи подсистемы печати. Для каждого типа документа ведется своя нумерация.

При просмотре списка нормативных документов отображаются свойства, описание которых представлено в таблице 70.

Табл. 70 – Перечень свойств нормативного документа

Наименование свойства	Описание
Номер	Учетный номер нормативного документа
Внутренний порядковый номер	Внутренний порядковый номер нормативного документа в рамках сервера, согласно начальному значению нумерации документов
Тип документа	Тип нормативного документа

Наименование свойства	Описание
Сущность учета	Тип объекта (экземпляр СКЗИ, дистрибутив, лицензия и др.) в рамках процедур учета СКЗИ, в отношении которого сформирован данный нормативный документ
Дата создания	Дата создания нормативного документа

Для того чтобы просмотреть список нормативных документов, перейдите в раздел **Учет СКЗИ** -> **Нормативная документация**.

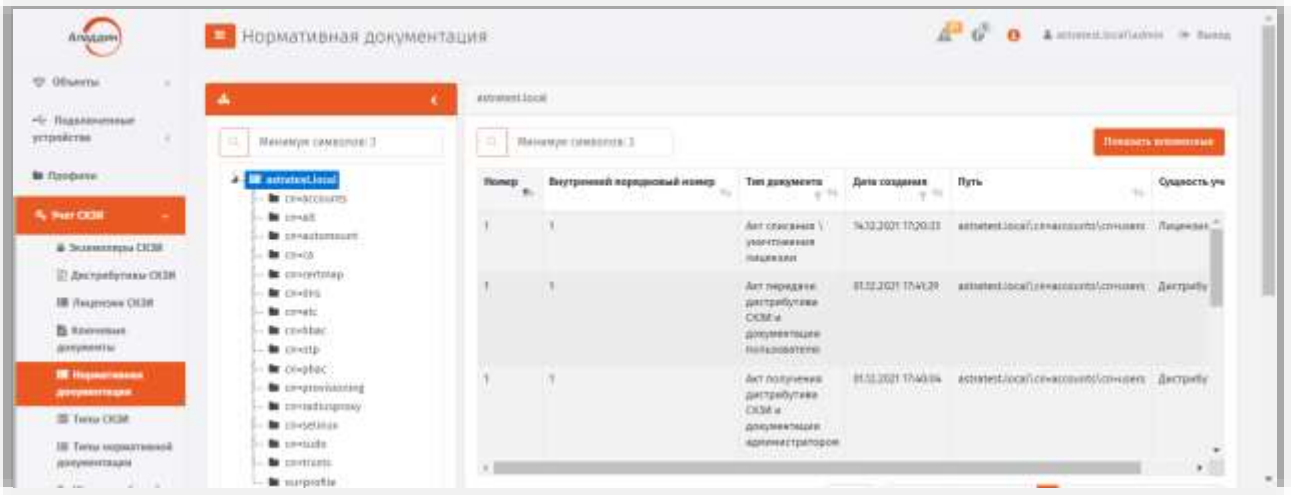


Рис. 242 – Вид страницы Учет СКЗИ –> Нормативная документация

Примечание. При просмотре списка нормативных документов справа вверху страницы доступна дополнительная опция просмотра **Показывать вложенные**. При выборе этой опции в списке будут дополнительно отображены документы, относящиеся к объектам ресурсной системы, которые являются вложенными по отношению к текущему выбранному объекту/контейнеру.

3.8.9 Журнал событий (учета СКЗИ)

JMS позволяет просматривать все события, произошедшие в процессе жизненного цикла СКЗИ.

При просмотре списка событий отображаются следующие параметры (Табл. 71).

Табл. 71 – Описание параметров событий учета СКЗИ

Наименование параметра	Описание
Дата	Дата и время возникновения события
Событие	Описание произошедшего события
Пользователь	Учетная запись пользователя, от имени которого совершалось действие, породившее данное событие

Для того чтобы просмотреть список событий, произошедших в процессе учета СКЗИ, перейдите в раздел **Учет СКЗИ** -> **Журнал событий**.

При просмотре событий существует возможность применения следующих временных фильтров для удобства просмотра событий за установленный промежуток времени:

- 1 час;
- 24 часа;
- 7 дней;
- 30 дней;
- Сегодня;
- Неделя;
- Месяц;
- Произвольный период;
- Все.

Кроме того предусмотрены:

- сортировка по дате;
- контекстная фильтрация (поиск) по столбцам **Событие**, **Пользователь**.

3.9 Подсистема печати

Подсистема печати консоли управления JMS предоставляет возможность формировать и печатать документы на основе создаваемых в ней шаблонов.

Основные функции подсистемы печати:

- централизованное хранение и управление шаблонами печати;
- формирование документов на основе RTF-шаблонов, методом подстановки необходимых данных в закладки, располагаемые внутри шаблона;
- вывод сформированных документов в диалог предварительного просмотра с возможностью последующей печати;
- отправка сформированных документов на печать.

3.9.1 Создание шаблона печати

Для создания шаблона печати выполните следующие действия:

1. Перейдите в раздел **Настройки** -> **Шаблоны печати** и нажмите **Создать** (см. рис. 243) .

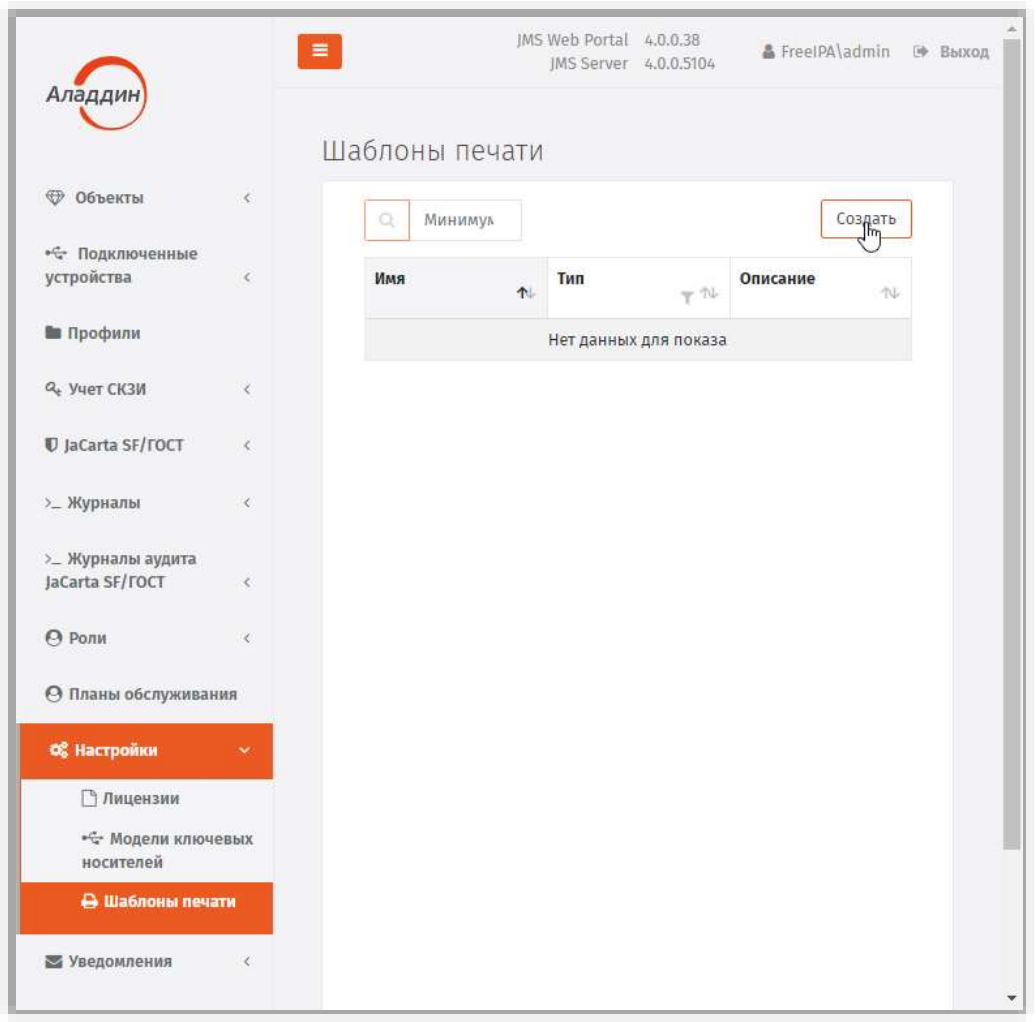


Рис. 243 – Создание шаблона печати

2. Откроется страница создания шаблона.

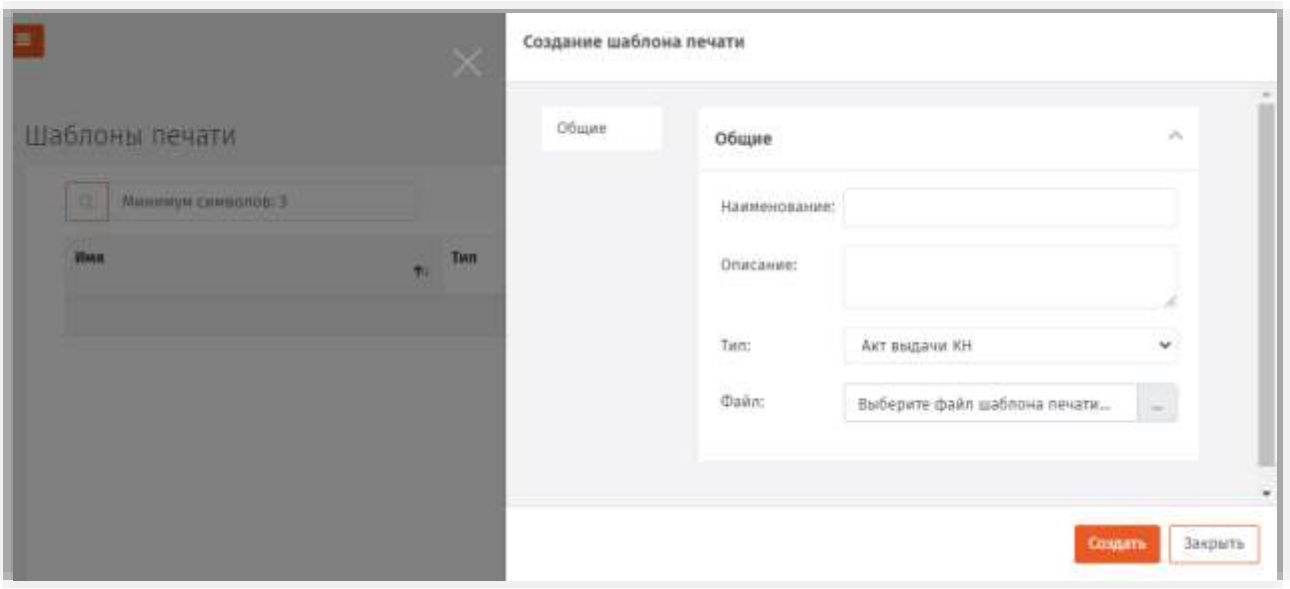


Рис. 244 – Страница создания шаблона печати

3. Введите имя шаблона в поле **Наименование,** при необходимости заполните поле **Описание**, выберите **Тип** шаблона (согласно Табл. 72), укажите место расположения файла шаблона (файла в формате .rtf) в поле **Файл** и нажмите **Создать**.

Примечание. Подробнее о создании файла шаблона в формате .rtf см. Создание файлов шаблонов в формате RTF.

Табл. 72 – Описание типов шаблонов

Тип шаблона	Описание
Акт выдачи КН	Содержит ФИО, логин, адрес электронной почты и др. персональные данные, а так же лицо, выдавшее и лицо, получившее КН.
Заявка на выпуск КН	Содержит текст заявления с просьбой о формировании и записи ключа электронной подписи на ключевой носитель, а так же указанием необходимых для этого персональных данных.
Заявка на сертификат	Содержит текст заявления с просьбой об изготовлении сертификата ключа проверки электронной подписи, а так же указанием необходимых для этого персональных данных.
Нормативный документ	Содержит сведения, отражающие различные события, возникающие в процессе учета СКЗИ. Данный тип шаблона используется только в рамках учета СКЗИ.
Сертификат	Содержит данные пользователя (ФИО, аккаунт, адрес электронной почты и др.) и данные сертификата (номер версии, серийный номер, даты срока действия и др.).

4. Созданный шаблон печати отобразится в списке шаблонов печати консоли управления JMS.

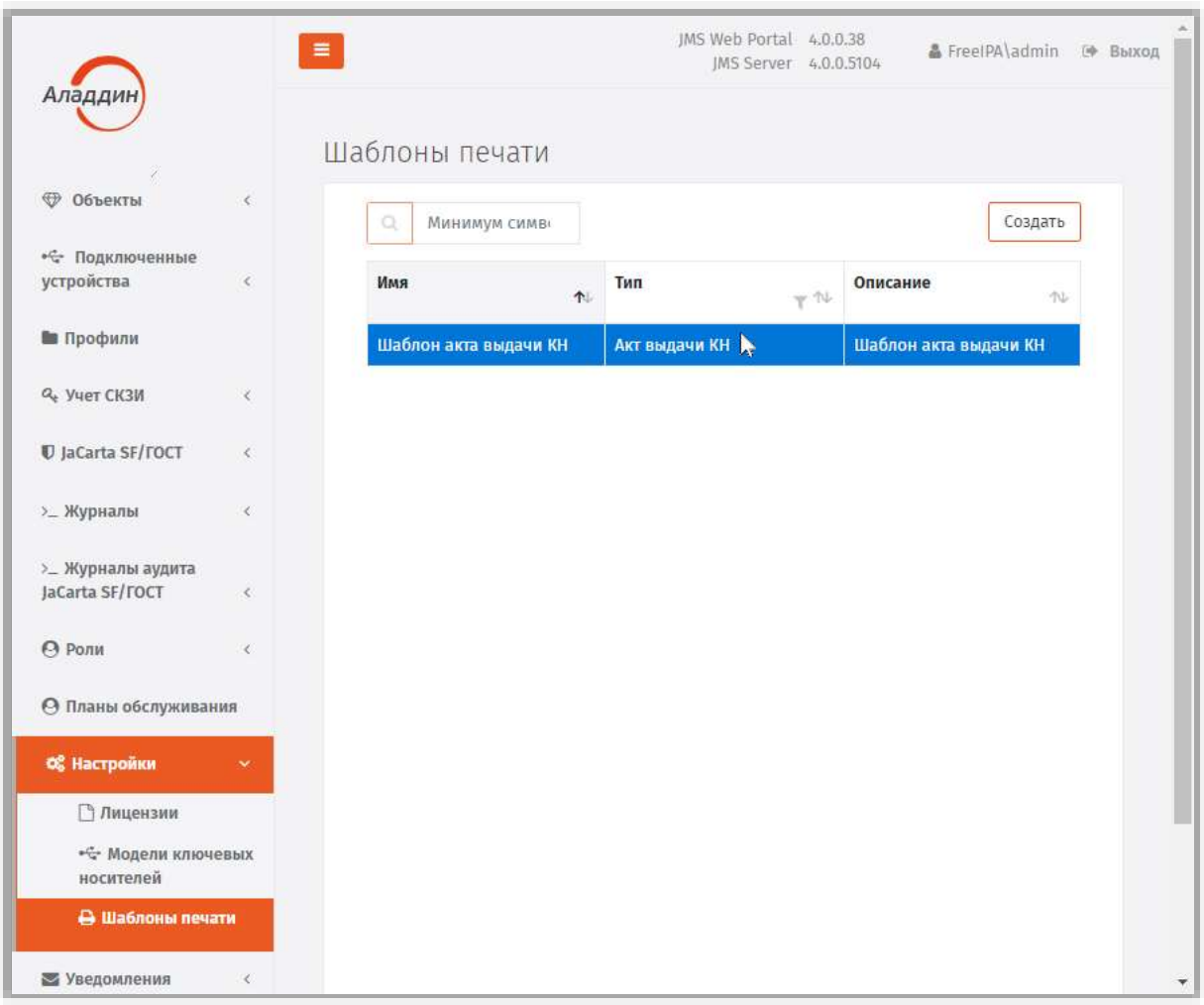


Рис. 245 – Отображение нового шаблона на странице шаблонов печати

3.9.2 Создание файлов шаблонов в формате RTF

Чтобы подготовить для JMS шаблон документа в формате RTF, выполните следующие действия:

1. Создайте документ Microsoft Word и заполните его необходимым содержимым.

Примечание. В настоящем документе для примера используется Microsoft Word 2016.

2. Добавьте в документ закладки, одноименные полям в базе данных JMS. Для этого выполните следующие действия:

2.1. переместите курсор в то место документа, в котором будет помещена закладка, соответствующая полю в базе данных JMS;
2.2. в ленточном меню Microsoft Word выберите **Вставка** -> **Закладка**;
2.3. отобразится следующее окно (см. рис. 246);

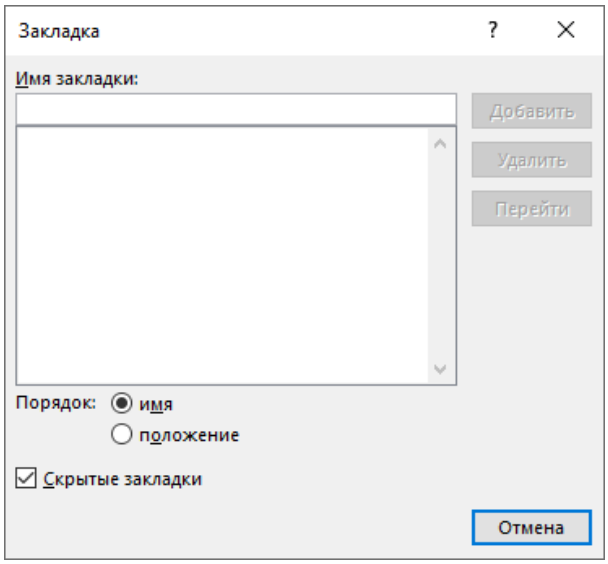


Рис. 246 – Добавление закладки в документ Microsoft Word

2.4. в поле **Имя закладки** введите имя, соответствующее названию поля в базе данных JMS (см. например, Табл. 73, ниже).

2.4.1. нажмите **Добавить** – окно добавления закладки закроется автоматически;
2.4.2. при необходимости повторите нужные действия для других закладок.

Примечание. Если одно и то же поле необходимо использовать в документе в качестве закладки два и более раз, следует воспользоваться соответствующим правилом работы с повторяющимися полями (см. раздел «Повторная печать полей в документе», ниже).

3. В зависимости от того, хотите ли вы отобразить закладки, чтобы проверить, как они размещены в документе, выполните следующие действия:

   - если вы не хотите отображать закладки в документе Microsoft Word, переходите к шагу 9 настоящей процедуры;
   - если вы хотите отобразить закладки в документе Microsoft Word, переходите к следующему шагу настоящей процедуры.

4. В ленточном меню Microsoft Word перейдите на вкладку **Файл** и выберите пункт **Параметры**.
5. В левой части окна выберите **Дополнительно**.
6. В секции **Показывать содержимое документа** слева установите флаг **Показывать закладки**.
7. Нажмите **ОК**, чтобы сохранить изменения.
8. Закладки будут отображены серым значком I..
9. Сохраните документ Microsoft Word в формате RTF.

Полный перечень полей БД JMS, используемых в шаблонах представлен в следующих разделах:

- «Создание шаблонов документов для выпуска КН и сертификата», ниже
- «Создание шаблонов документов по работе с СКЗИ», с. 253;
- «Создание шаблонов документов по работе с дистрибутивами СКЗИ», с. 255;
- «Создание шаблонов документов по работе с лицензиями на СКЗИ», с.257;
- «Создание шаблонов документов по работе с ключевыми документами», с. 258;
- «Создание шаблонов документов по работе с ключевой информацией», с. 260.

3.9.2.1 Повторная печать полей в документе

В случае если какое-либо из полей (закладок) необходимо повторить в документе (акте/заявке) в нескольких местах, то в шаблоне при повторном использовании поля (при добавлении закладки) в конце имени закладки (например KeyUsage), необходимо добавить числовой индекс (например, KeyUsage2). Количество таких индексов (и соответственно повторов поля) для одного поля ограничивается значением, которое задается в конфигурационном файле сервера JMS `/etc/aladdin/eap-engine/AppSettings.json`

с помощью параметра **`MaxBookmarkIndex`**. Значение данного параметра по умолчанию – 100. (при необходимости его можно изменить).

Пример блока конфигурации печати в конфигурационном файле сервера JMS приведен в разделе «Поддержка закладок с компонентами имен субъекта и издателя сертификата», с. 251

3.9.2.2 Создание шаблонов документов для выпуска КН и сертификата

Перечень доступных закладок, используемых в документах выпуска КН и сертификатов, представлен в табл. 73.

Табл. 73 – Закладки, соответствующие полям в базе данных

Закладка/поле	Описание	Типы шаблона:			
		Заявка на выпуск КН	**Акт выдачи КН**	**Заявка на сертификат**	**Сертификат**
FullName	Имя пользователя	+	+	+	+
AccountName	Имя учетной записи (логин)	+	+	+	+
Mail	Электронная почта	+	+	+	+
Department	Подразделение	+	+	+	+
Title	Должность	+	+	+	+
IssueDate	Дата выпуска (при печати подставляется текущая дата)	+	+	+	+
GlobalId	Идентификатор ключевого носителя	+	+	+	+
PublicKey	Значение открытого ключа в сертификате			+	
IssuerName	Сертификат: издатель				+
SerialNumber	Сертификат: серийный номер				+

Закладка/поле	Описание	Типы шаблона:			
		Заявка на выпуск КН	Акт выдачи КН	Заявка на сертификат	Сертификат
SubjectName	Сертификат: имя субъекта				+
IssuedOn	Сертификат: начало срока действия				+
ExpiredOn	Сертификат: окончание срока действия				+
Version	Сертификат: версия				+
SignatureAlgorithm	Сертификат: алгоритм ЭЦП				+
PublicKeySignatureAlgorithm	Сертификат: алгоритм открытого ключа				+
PublicKeyValue	Сертификат: значение открытого ключа				+
PublicKeyExchangeAlgorithm	Сертификат: описание открытого ключа				+
PublicKeySize	Сертификат: размер открытого ключа				+
InitiatorFullName	Имя инициатора действия, приведшего к созданию документа	+	+	+	+
PublicKeyAlgorithm	Алгоритм открытого ключа				+
PublicKeyParameters	Параметры открытого ключа				+
CertificateStartDate	Дата начала действия сертификата в формате ДД.ММ.ГГГГ				+
CertificateStartTime	Время начала действия сертификата в формате ЧЧ:ММ:СС				+
CertificateEndDate	Дата окончания действия сертификата в формате ДД.ММ.ГГГГ				+
CertificateEndTime	Время окончания действия сертификата в формате ЧЧ:ММ:СС				+
IssuerSignTool_SignTool	Сертификат: наименование средства электронной подписи				+

Закладка/поле	Описание	Типы шаблона:			
		Заявка на выпуск КН	Акт выдачи КН	Заявка на сертификат	Сертификат
IssuerSignTool_SignToolCert	Сертификат: реквизиты заключения о подтверждении соответствия средства электронной подписи				+
IssuerSignTool_CATool	Сертификат: наименование средства УЦ				+
IssuerSignTool_CAToolCert	Сертификат: реквизиты заключения о подтверждении соответствия средства УЦ				+
CertificatePolicies	Сертификат: класс средств УЦ				+
SubjectSignTool	Сертификат: используемое средство электронной подписи				+
KeyUsage	Сертификат: область использования ключа				+
EnhancedKeyUsage	Сертификат: расширенное использование ключа				+
SignatureValue	Сертификат: значение электронной подписи				+
SubjectKeyIdentifier	Сертификат: идентификатор ключа субъекта				+
AuthorityInfoAccess	Сертификат: доступ к информации о центрах сертификации				+
DistribPoints	Сертификат: точки распространения списка отзыва (CRL)				+
AuthorityKeyIdentifier	Сертификат: идентификатор ключа центра сертификатов				+
AKI_AuthorityCertSerialNumber	Сертификат: номер квалифицированного сертификата УЦ				+
BasicConstraints	Сертификат: основные ограничения				+

3.9.2.2.1 Поддержка закладок с компонентами имен субъекта и издателя сертификата

При формировании шаблонов документов для работы с сертификатами существует возможность создавать закладки не только с полными именами субъекта (SubjectName) и издателя (IssuerName), но и закладки с их отдельными компонентами.

Для компонентов имени субъекта закладки должны быть заданы в следующем формате:

- `SubjectName_<Обозначение компонента>` или
- `IssuerName_<Обозначение компонента>`

где <Обозначение компонента> — условное символьное обозначение компонента имени субъекта или издателя сертификата.

Например: SubjectName_CN, SubjectName_OGRN, SubjectName_E, IssuerName_INN

По сути, суффикс <Обозначение компонента> представляет собой условное обозначение OID-идентификатора соответствующего компонента DN-имени (Distinguished Name) субъекта или издателя.

Полный перечень соответствия OID-идентификаторов и обозначений компонентов имен можно самостоятельно сформировать и внести в файл конфигурации `/etc/aladdin/eap-engine/AppSettings.json` сервера JMS, добавив в него блок `PrintManager`.

Содержание данного блока по умолчанию приведено ниже:

```
{
      "Name": "PrintingManager",
      "Settings": {
        "MinBookmarkIndex": "1",
        "MaxBookmarkIndex": "100",
        "CustomAttributeCodes":
"OU,CN,C,S,L,O,T,OGRN,OGRNIP,SNILS,INN,E,givenName,name,sn,DisplayName",
        "CertificateDnMappings": "2.5.4.3=CN, 2.5.4.6=C, 2.5.4.8=S, 2.5.4.7=L,
2.5.4.10=O, 2.5.4.11=OU, 1.2.643.100.1=OGRN, 1.2.643.3.131.1.1=INN,
1.2.643.100.3=SNILS, 1.2.840.113549.1.9.1=E, 2.5.4.4=SN, 2.5.4.42=G, 2.5.4.9=STREET,
2.5.4.12=T"
      }
}
```

При этом в параметре **`CertificateDnMappings`** каждое дополнительное соответствие (OID – обозначение) можно добавить элементом перечисления "<OID компонента>=<Обозначение компонента>". Для корректного отображения компонентов имен важно проконтролировать, чтобы данные компоненты имени были установлены в соответствующей ресурсной системе.

При редактировании списка атрибутов из параметра **`CertificateDnMappings`** по окончании изменений следует выполнить логический перезапуск сервера JMS (последовательное выполнение команд *server stop* и *server start* консольного агента JMS, подробнее см. руководство по настройке и установке [2], «Приложение 2. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal»).

По умолчанию используются соответствия, указанные в Табл. 74.

Табл. 74 – Обозначения компонентов имен субъекта и издателя сертификата по умолчанию

OID-идентификатор	Обозначение компонента DN-имени	Описание
2.5.4.3	CN	Общее имя
2.5.4.6	C	Страна
2.5.4.8	S	Регион
2.5.4.7	L	Город
2.5.4.10	O	Организация
2.5.4.11	OU	Структурное подразделение
1.2.643.100.1	OGRN	Основной государственный регистрационный номер

OID-идентификатор	Обозначение компонента DN-имени	Описание
1.2.643.3.131.1.1	INN	Идентификационный номер налогоплательщика
1.2.643.100.3	SNILS	Страховой номер индивидуального лицевого счета
1.2.840.113549.1.9.1	E	Адрес электронной почты
2.5.4.4	SN	Фамилия
2.5.4.42	G	Имя и отчество
2.5.4.9	STREET	Адрес
2.5.4.12	T	Должность

Важно! В случае наличия в конфигурационном файле параметра **`CertificateDnMappings`** все планируемые к использованию OID-идентификаторы «по умолчанию» необходимо указать в нем явно (по примеру приведенного выше образца конфигурационного файла).

3.9.2.3 Создание шаблонов документов по работе с СКЗИ

Допустимые значения имен закладок, соответствующие названиям полей в БД JMS с их описанием и сведениями об использовании в нормативных документах жизненного цикла СКЗИ представлены в табл. 75.

Табл. 75 – Печатная форма СКЗИ

Закладка/поле	Описание	Типы нормативных документов:					
		Акт передачи СКЗИ администратору	Акт передачи СКЗИ ответственному пользователю	Акт ввода СКЗИ в эксплуатацию	Акт вывода СКЗИ из эксплуатации	Акт установки СКЗИ	Акт об уничтожении СКЗИ
		События, при возникновении которых создается нормативный документ:					
		Регистрация\Импорт\Возврат в эксплуатацию	Назначение экземпляра СКЗИ ответственному пользователю	Ввод СКЗИ в эксплуатацию	Вывод СКЗИ из эксплуатации	Установка СКЗИ	Уничтожение СКЗИ
DocumentNumber	**Номер нормативного документа**	+	+	+	+	+	+
DocumentCreatedDate	**Дата создания НД**	+	+	+	+	+	+

Закладка/поле	Описание	Типы нормативных документов:					
		Акт передачи СКЗИ администратору	Акт передачи СКЗИ ответственному пользователю	Акт ввода СКЗИ в эксплуатацию	Акт вывода СКЗИ из эксплуатации	Акт установки СКЗИ	Акт об уничтожении СКЗИ
		События, при возникновении которых создается нормативный документ:					
		Регистрация\Импорт\Возврат в эксплуатацию	Назначение экземпляра СКЗИ ответственному пользователю	Ввод СКЗИ в эксплуатацию	Вывод СКЗИ из эксплуатации	Установка СКЗИ	Уничтожение СКЗИ
ActionDate	Даты выполнения действия	+	+	+	+	+	+
ExecutorAccountName	Исполнитель (администратор JMS, выполнивший операцию)	+	+	+	+	+	+
ResponsibleUserName	Ответственное лицо	+	+	+	+	+	+
Number	Номер	+	+	+	+	+	+
WorkstationName	Рабочая станция		+	+	+	+	+
InstallLocation	Место установки		+	+	+	+	+
InstallUserName	Пользователь		+	+	+	+	+
InstallDate	Дата установки		+	+	+	+	+
StartDate	Дата ввода в эксплуатацию		+	+	+	+	+
EndDate	Дата вывода из эксплуатации		+	+	+	+	+
DestroyDate	Дата уничтожения						+
StateMask	Состояние	+	+	+	+	+	+
Description	Описание СКЗИ	+	+	+	+	+	+

Закладка/поле	Описание	Типы нормативных документов:					
		Акт передачи СКЗИ администратору	Акт передачи СКЗИ ответственному пользователю	Акт ввода СКЗИ в эксплуатацию	Акт вывода СКЗИ из эксплуатации	Акт установки СКЗИ	Акт об уничтожении СКЗИ
		События, при возникновении которых создается нормативный документ:					
		Регистрация\Импорт\Возврат в эксплуатацию	Назначение экземпляра СКЗИ ответственному пользователю	Ввод СКЗИ в эксплуатацию	Вывод СКЗИ из эксплуатации	Установка СКЗИ	Уничтожение СКЗИ
CryptoDeviceType	**Тип СКЗИ**	+	+	+	+	+	+
ReceivedFrom	**От кого получено**	+	+	+	+	+	+

3.9.2.4 Создание шаблонов документов по работе с дистрибутивами СКЗИ

Допустимые значения имен закладок, соответствующие названиям полей в БД JMS с их описанием и сведениями об использовании в нормативных документах жизненного цикла дистрибутива СКЗИ представлены в табл. 76.

Табл. 76 – Печатная форма дистрибутива СКЗИ

Закладка/поле	Описание	Типы нормативных документов:			
		Акт получения дистрибутива СКЗИ и документации	Акт создания дистрибутива СКЗИ и документации	Акт передачи дистрибутива СКЗИ и документации пользователю	Акт списания / уничтожения дистрибутива СКЗИ и документации
		События, при возникновении которых создается нормативный документ:			
		Регистрация\Импорт Дистрибутивов СКЗИ	Создание копий Дистрибутива	Экспорт Дистрибутива	Уничтожение Дистрибутива
DocumentNumber	**Номер нормативного документа**	+	+	+	+
DocumentCreatedDate	**Дата создания НД**	+	+	+	+
ActionDate	**Дата выполнения действия**	+	+	+	+
ExecutorAccountName	**Исполнитель (администратор JMS, выполнивший операцию)**	+	+	+	+
Name	**Наименование**	+	+	+	+
PackageNumber	**Номер**	+	+	+	+
PackageDocumentNumber	**Учетный номер документа**	+	+	+	+
Location	**Расположение**	+	+	+	+
IsCopy	**Копия?**	+	+	+	+
OriginalNumber	**Учетный номер оригинала**	+	+	+	+
OriginalName	**Наименование оригинала**		+		
OriginalDocumentNumber	**Учетный номер документа оригинала**		+		
ResponsibleUserName	**Ответственное лицо**	+	+	+	+
CryptoDeviceType	**Тип СКЗИ**	+	+	+	+

Закладка/поле	Описание	Типы нормативных документов:			
		Акт получения дистрибутива СКЗИ и документации	Акт создания дистрибутива СКЗИ и документации	Акт передачи дистрибутива СКЗИ и документации пользователю	Акт списания / уничтожения дистрибутива СКЗИ и документации
		События, при возникновении которых создается нормативный документ:			
		Регистрация\Импорт Дистрибутивов СКЗИ	Создание копий Дистрибутива	Экспорт Дистрибутива	Уничтожение Дистрибутива
Enabled	**Признак учета**	+	+	+	+
DestroyDate	**Когда уничтожил**				+
ReceivedFrom	**От кого получено**	+	+	+	+
MediaType	**Тип носителя**	+	+	+	+

3.9.2.5 Создание шаблонов документов по работе с лицензиями на СКЗИ

Допустимые значения имен закладок, соответствующие названиям полей в БД JMS с их описанием и сведениями об использовании в нормативных документах жизненного цикла лицензии на СКЗИ представлены в табл. 77.

Табл. 77 – Печатная форма лицензии на СКЗИ

Закладка/поле	Описание	Типы нормативных документов:		
		Акт получения лицензии/й ответственным лицом	Акт передачи лицензии ответственному лицу	Акт списания \ уничтожения лицензии
		События, при возникновении которых создается нормативный документ:		
		Регистрация\Импорт лицензий	Установка\Назначение лицензии\Отмена назначения\Экспорт лицензии	Уничтожение лицензии
DocumentNumber	Номер дистрибутива	+	+	+
DocumentCreatedDate	Дата создания НД	+	+	+
ActionDate	Дата выполнения действия	+	+	+
ExecutorAccountName	Исполнитель (администратор JMS, выполнивший операцию)	+	+	+
SerialNumber	Серийный номер	+	+	+
IsAttached	Назначена?	+	+	+
IsInstalled	Установлена?	+	+	+
ResponsibleUserName	Ответственное лицо	+	+	+
IssuedDate	Дата выдачи	+	+	+
IssuedName	Кем выдано	+	+	+
CryptoDeviceType	Тип СКЗИ	+	+	+
CryptoDeviceNumber	Номер СКЗИ	+	+	+
CryptoDeviceWorkstationName	Рабочая станция СКЗИ	+	+	+
CryptoDeviceInstallLocation	Место установки СКЗИ	+	+	+
ValidFrom	Действует с	+	+	+
ValidTo	Действует по	+	+	+
Enabled	Признак учета	+	+	+
DestroyDate	Когда уничтожил			+

3.9.2.6 Создание шаблонов документов по работе с ключевыми документами

Допустимые значения имен закладок, соответствующие названиям полей в БД JMS с их описанием и сведениями об использовании в нормативных документах жизненного цикла ключевого документа представлены в табл. 78.

Табл. 78 — Печатная форма ключевого документа

Закладка/поле	Описание	Типы нормативных документов:			
		Акт создания ключевых документов	Акт получения ключевых документов	Акт передачи ключевых документов	Акт уничтожения ключевых документов
		События, при возникновении которых создается нормативный документ:			
		Создание ключевых документов	Получение ключевых документов	Передача ключевых документов	Уничтожение ключевых документов
DocumentNumber	Номер нормативного документа	+	+	+	+
DocumentCreatedDate	Дата создания НД	+	+	+	+
ActionDate	Дата выполнения действия	+	+	+	+
Title	Наименование (сертификат ЭП)	+	+	+	+
CertificateSerialNumber	Серийный номер сертификата	+	+	+	+
TokenSerialNumber	Серийный номер КН	+	+	+	+
TokenModelName	Название модели КН	+	+	+	+
TokenCryptoNumber	ФСБ номер КН (если есть)	+	+	+	+
TokenBodyNumber	Номер корпуса КН	+	+	+	+
CreatorUserName	Кто создал\получил	+	+		
CreateDate	Когда создал\получил	+	+		
ResponsibleUserName	Кому передали (ответственное лицо)			+	
PublisherUserName	Кто передал			+	
PublishDate	Когда передали			+	
DestroyerUserName	Кто уничтожил				+
DestroyDate	Когда уничтожил				+

3.9.2.7 Создание шаблонов документов по работе с ключевой информацией

Допустимые значения имен закладок, соответствующие названиям полей в БД JMS с их описанием и сведениями об использовании в нормативных документах жизненного цикла СКЗИ представлены в табл. 79.

Табл. 79 – Печатная форма ключевой информации

Закладка/поле	Описание	Типы нормативных документов:				
		Акт создания ключевой информации	Акт получения ключевой информации	Акт ввода ключевой информации в эксплуатацию	Акт вывода ключевой информации из эксплуатации	Акт уничтожения ключевой информации
		События, при возникновении которых создается нормативный документ:				
		Создание ключевой информации	Получение ключевой информации	Ввод ключевой информации в эксплуатацию	Вывод ключевой информации из эксплуатации	Уничтожение ключевой информации
DocumentNumber	Номер нормативного документа	+	+	+	+	+
DocumentCreatedDate	Дата создания НД	+	+	+	+	+
ActionDate	Дата выполнения действия	+	+	+	+	+
Title	Наименование (сертификат ЭП)	+	+	+	+	+
CertificateSerialNumber	Серийный номер сертификата	+	+	+	+	+
CreatorUserName	Кто создал\получил	+	+			
CreateDate	Когда создал\получил	+	+			
PublisherUserName	Кто ввел в эксплуатацию			+		
PublishDate	Когда ввел в эксплуатацию			+		
RevokerUserName	Кто вывел из эксплуатации				+	
RevokeDate	Когда вывел из эксплуатации				+	
DestroyerUserName	Кто уничтожил					+
DestroyDate	Когда уничтожил					+

3.10 Глобальные группы JMS

Глобальные группы JMS используются, чтобы распространить действие привязок профилей JMS только на выбранных пользователей и рабочие станции. Например, если профиль JMS привязан к контейнеру пользователей **Users** (Пользователи), то по умолчанию (без применения глобальных групп JMS) этот профиль будет применяться ко всем пользователям этого контейнера и ко всем рабочим станциям, зарегистрированным в JMS. Если создать глобальную группу и включить в нее только определенных пользователей контейнера **Users** и определенные рабочие станции, после чего указать эту глобальную группу в настройках привязки профиля, можно ограничить область применения профиля двумя способами:

- профиль будет применяться только к тем пользователям и рабочим станциям, которые входят в указанную глобальную группу JMS;
- профиль будет применяться к пользователям и рабочим станциям, не входящим в указанную глобальную группу JMS.

Чтобы создать глобальную группу, выполните следующие действия.

1. В окне консоли управления перейдите в раздел **Объекты -> Пользователи,** в верхней панели нажмите **Действия** и выберите **Создать глобальную группу (**Рис. 247**)**.

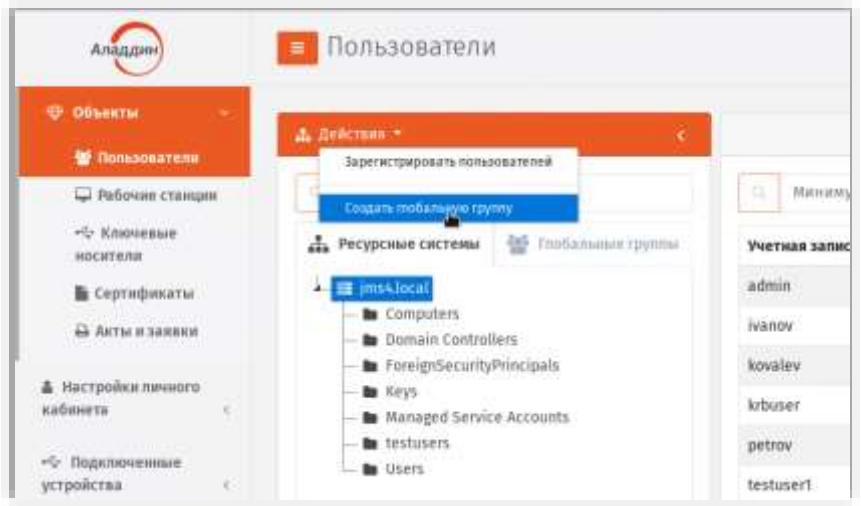


Рис. 247 – Начало процедуры создания новой глобальной группы

Отобразится следующее окно.

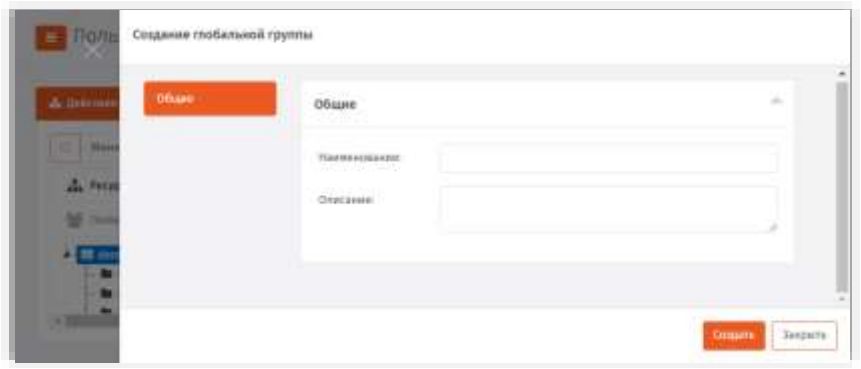


Рис. 248 – Создание новой глобальной группы

2. Введите наименование и описание глобальной группы в соответствующих полях, после чего нажмите **Создать**.

Новая глобальная группа на средней панели на вкладке **Глобальные группы**.

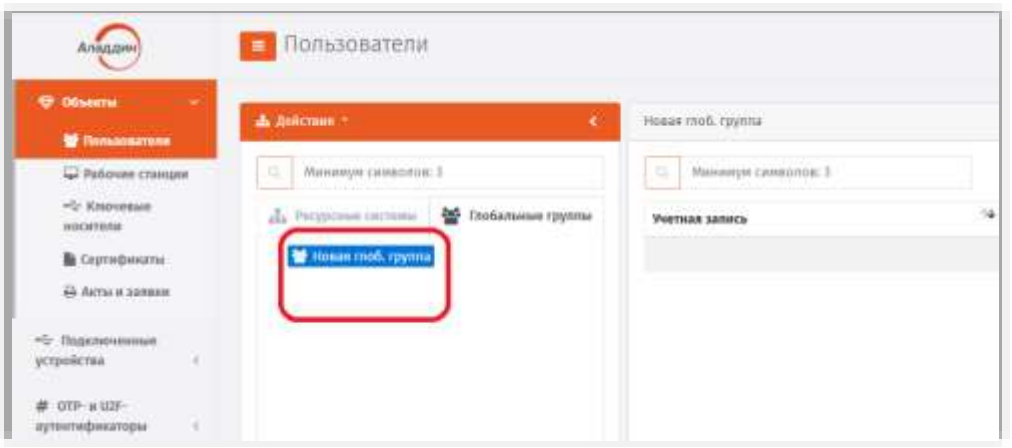


Рис. 249 – Созданная глобальная группа отображается в списке

3. Чтобы добавить в созданную глобальную группу пользователей, нажмите на ней правой кнопкой мыши и выберите **Добавить пользователей в группу**.
Отобразится следующее окно.

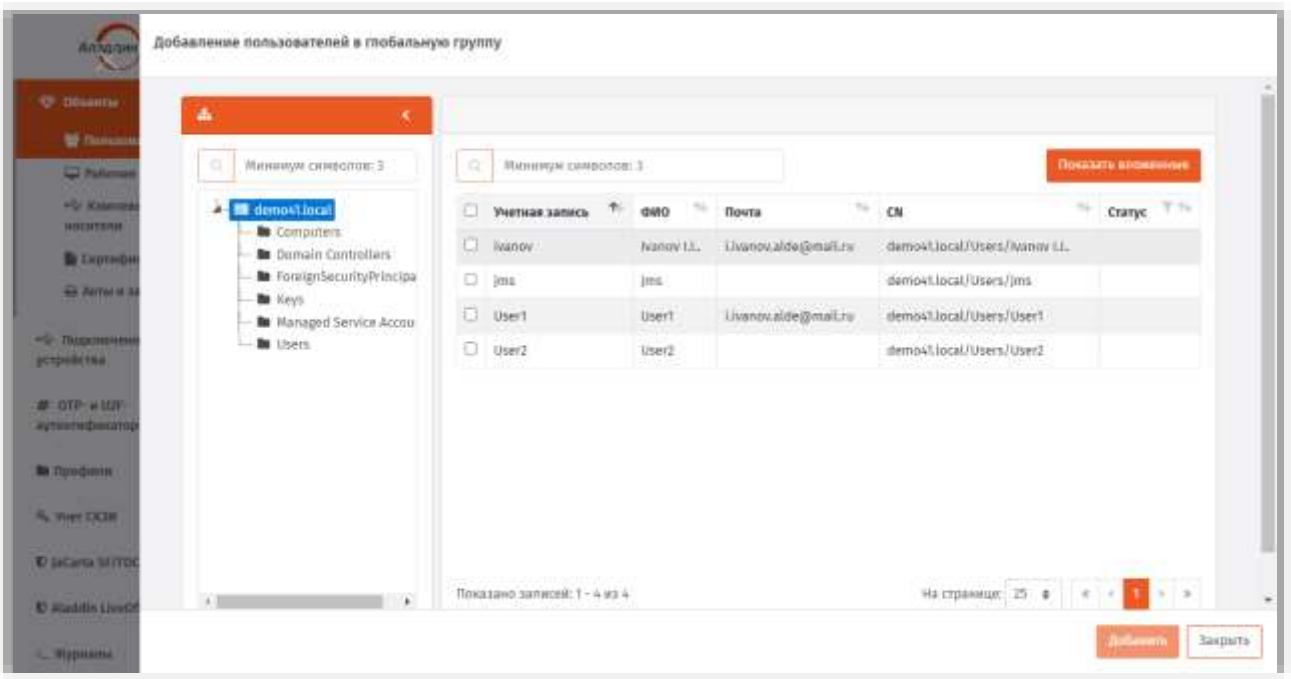


Рис. 250 – Добавление пользователей в глобальную группу

4. Отметьте пользователей, которых вы хотите добавить в глобальную группу, и нажмите **Добавить**.
5. Список добавленных пользователей будет отображаться в содержимом глобальной группы (Рис. 249, выше)
6. Чтобы добавить в глобальную группу рабочие станции, перейдите в раздел **Объекты -> Рабочие станции**, на средней панели вкладке Глобальные группы выберите нужную глобальную группу, нажмите на ней правой кнопкой мыши и выберите **Добавить рабочие станции в группу**.

Отобразится следующее окно.

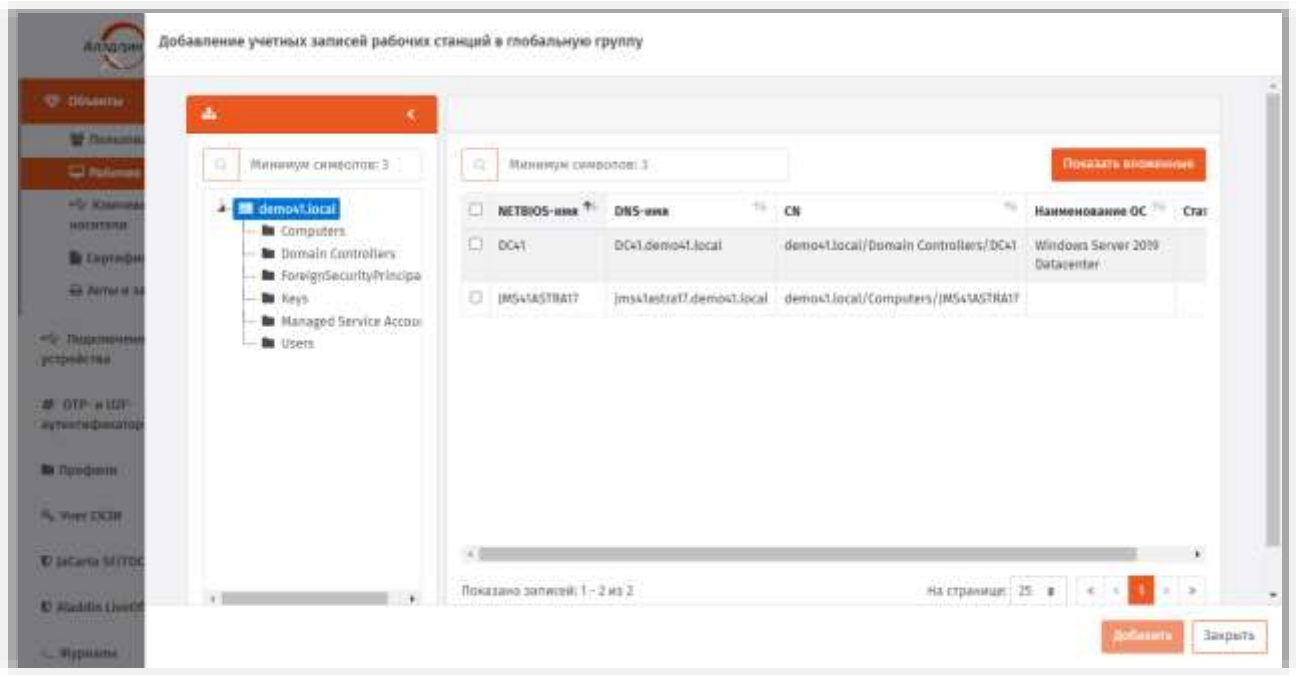


Рис. 251 – Добавление рабочих станций в глобальную группу

7. Отметьте рабочие станции, которые вы хотите добавить в глобальную группу, и нажмите **Добавить**.
8. Список добавленных рабочих станций будет отображаться на вкладке **Глобальные группы** раздела **Общие -> Рабочие станции**.

Созданную глобальную группу можно применять для ограничения действия привязки профилей JMS (см. «**Ограничение действия профилей через группы** домена/глобальные группы JMS», с. 197).

3.11 Ролевой метод разграничения доступа в JMS

В JMS реализован ролевой метод разграничения доступа к выполнению операций.

Предопределены следующие встроенные роли:

- **Пользователь;**
- **Оператор;**
- **Аудитор;**
- **Администратор ИБ;**
- **Запуск планов обслуживания** (выполняет запуск планов обслуживания с помощью внешней утилиты).

Правила ролевого разграничения доступа (полномочия субъектов доступа в отношении действий с объектами доступа в JMS) для встроенных ролей приведены Формуляре[4].

Кроме предопределенных встроенных ролей, изменение которых невозможно, JMS позволяет создавать новые (настраиваемые администратором) роли.

Порядок действий по созданию, редактированию и назначению ролей описан в соответствующем разделе (см. «Создание, редактирование и назначение ролей JMS», с. 264).

3.12 Создание, редактирование и назначение ролей JMS

В состав JMS входят стандартные роли, каждая из которых включает определенный набор операций. Список доступных ролей отображается в разделе **Роли -> Роли** консоли управления JMS:

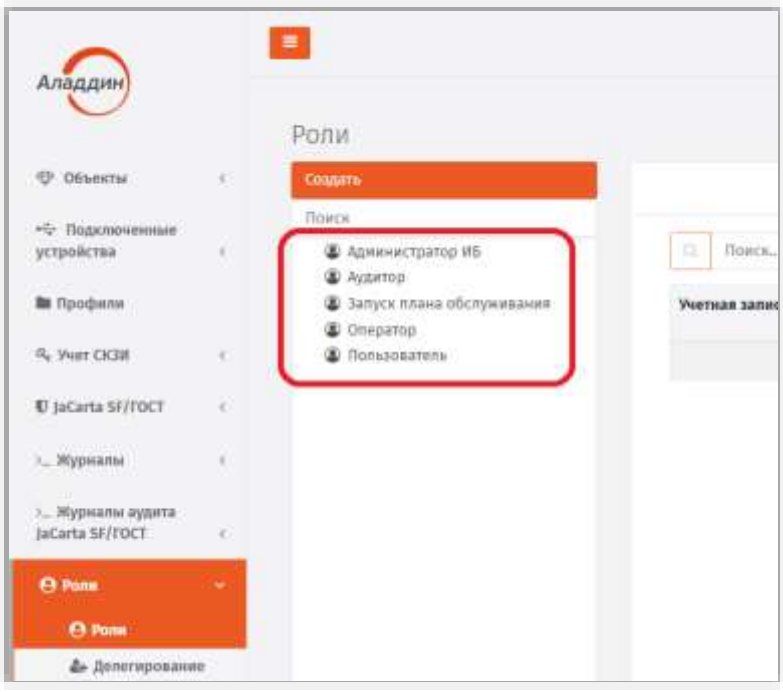


Рис. 252 – Состав стандартных ролей JMS, установленных по умолчанию

Классификация операций, права на выполнение которых составляют полномочия различных ролей, и описание этих операций приведены в приложении «Приложение 1. Права на выполнение операций», с. 336.

Чтобы посмотреть, какие операции включены в ту или иную роль, на выбранной роли нажмите правой кнопкой мыши и выберите **Свойства**, На открывшейся странице свойств роли доступ к операциям будут отображены в отдельной секции (Рис. 253).

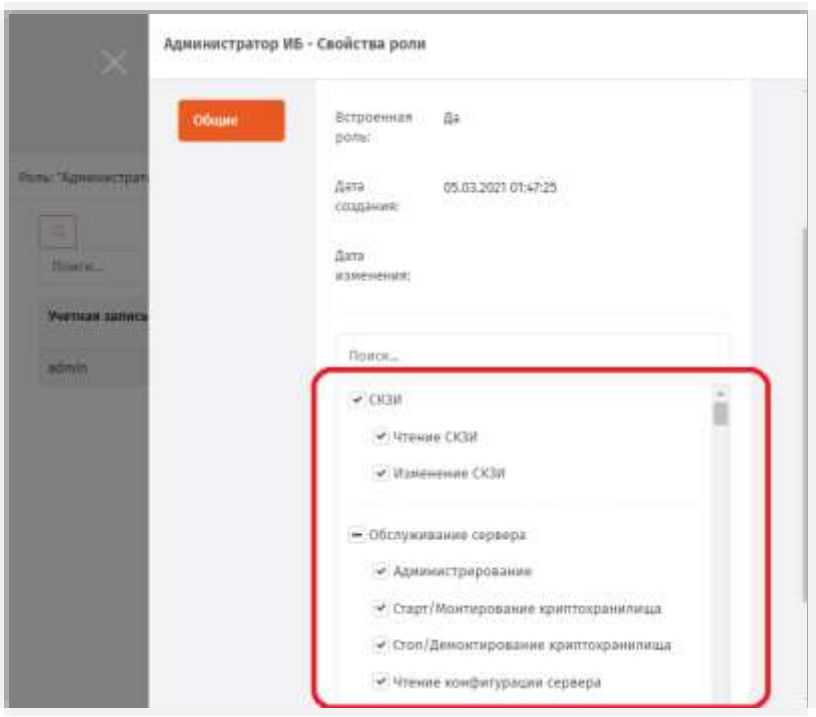


Рис. 253 – Секция настройки доступных операций на странице свойств роли

Для так называемых «встроенных ролей» JMS (**Пользователь**, **Оператор**, **Аудитор**, **Администратор ИБ**, **Запуск плана обслуживания**) список доступных операций изменить невозможно, тогда как при создании новой роли доступные операции можно включать/исключать из списка, устанавливая или снимая флаги напротив нужных операций. Чтобы создать новую роль, выполните процедуру «Создание новой роли JMS», с. 265.

Чтобы просмотреть список пользователей, которым назначена выбранная роль, выберите данную роль в средней панели. Список пользователей отобразится справа:

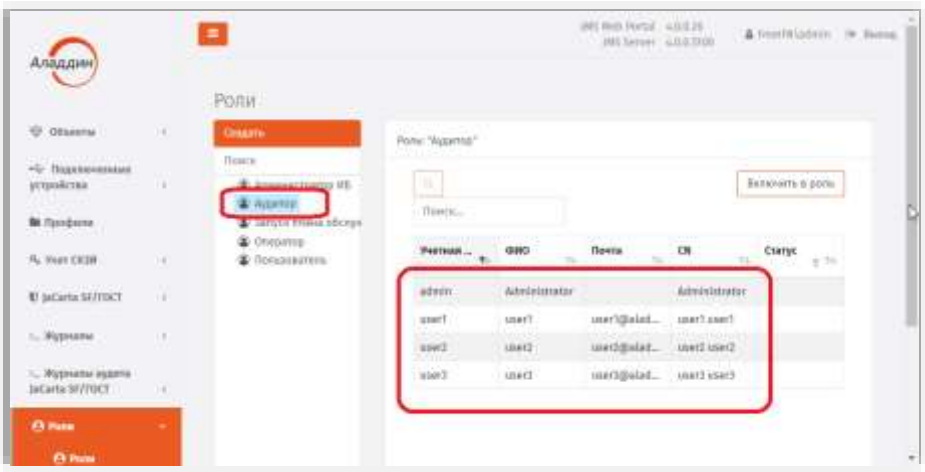


*Рис. 254 – Список пользователей, которым назначена роль **Аудитор***

3.12.1 Создание новой роли JMS

Чтобы создать новую роль JMS, выполните следующие действия.

9. В консоли управления JMS перейдите в раздел **Роли -> Роли** и в вверху нажмите **Создать**.

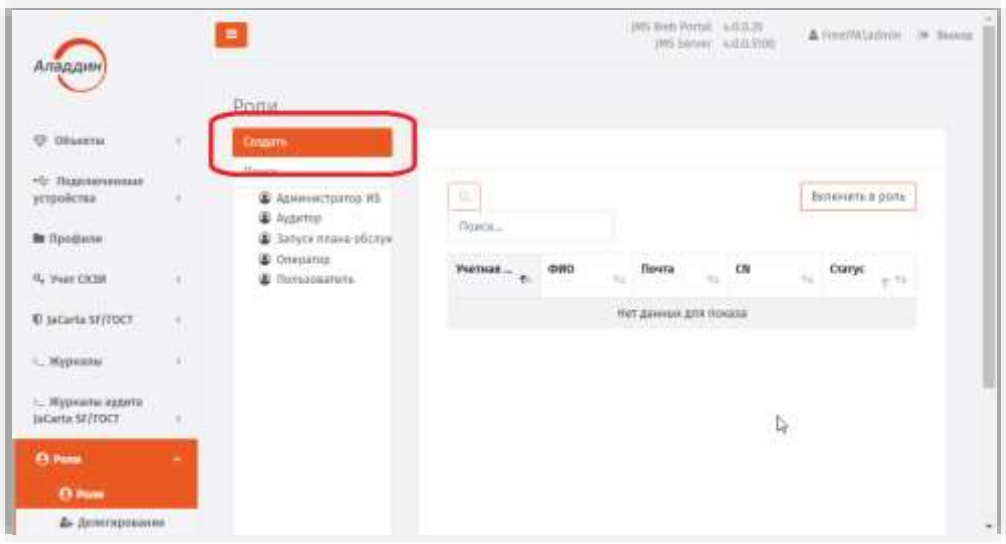


Рис. 255 – Управление созданием роли JMS

10. Отобразится страница создания роли.

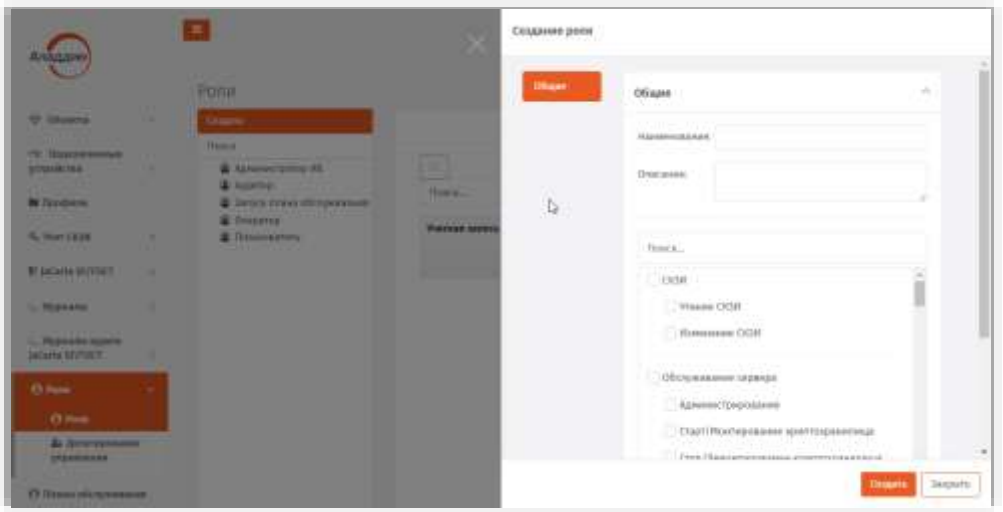


Рис. 256 – Страница создания роли JMS

11. Введите **Наименование** и **Описание** роли в соответствующих полях.
12. Выполните одно из следующих действий:

    – отметьте нужные категории (например **Обслуживание сервера**, Рис. 256) – в этом случае в роль будут включены все операции из отмеченных категорий;
    – отметьте отдельные операции, которые будут включены в роль.

13. Нажмите **Создать** и закройте страницу, нажав **Закрыть**.

Созданная роль отобразится на панели ролей:

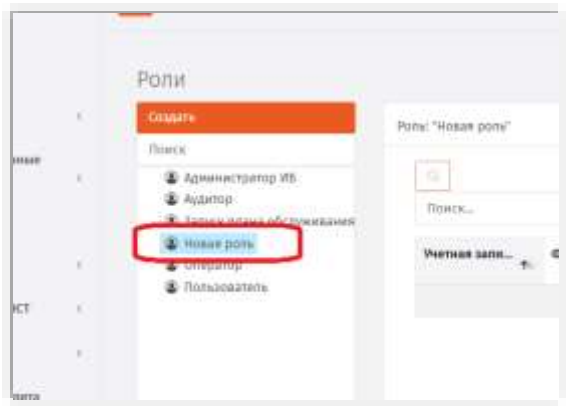


Рис. 257 – Отображение созданной роли

Теперь эту роль можно назначать пользователям JMS (см. «Назначение / отмена назначения ролей пользователям JMS», ниже).

3.12.2 Назначение / отмена назначения ролей пользователям JMS

Чтобы назначить роль пользователю/пользователем выполните следующие действия

1. Выберите данную роль в средней панели:

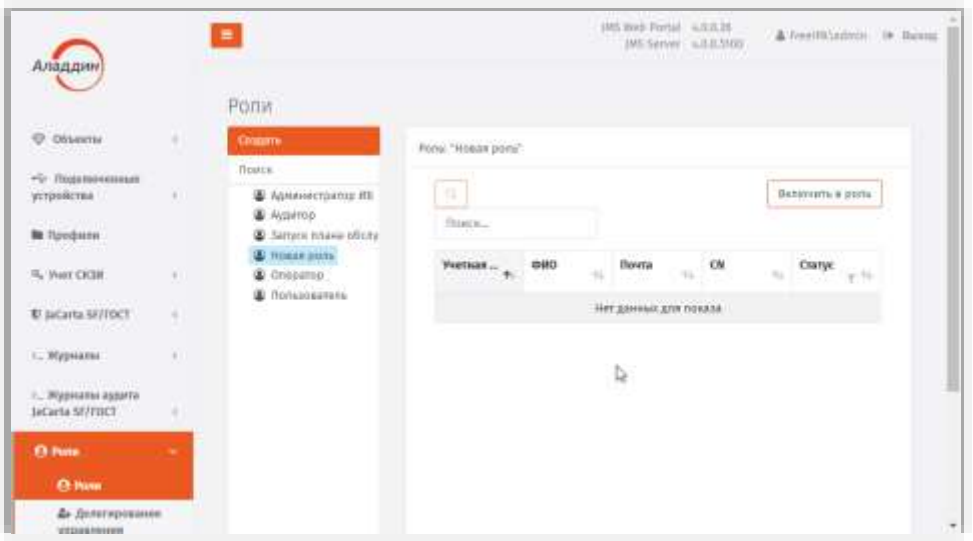


Рис. 258 – Выбор роли для назначения пользователю

2. Нажмите кнопку **Включить роль** (справа вверху) и на странице пользователей ресурсной системы выберите нужного пользователя и нажмите **Добавить**. Пользователи, которым назначена данная роль отобразятся в списке справа:

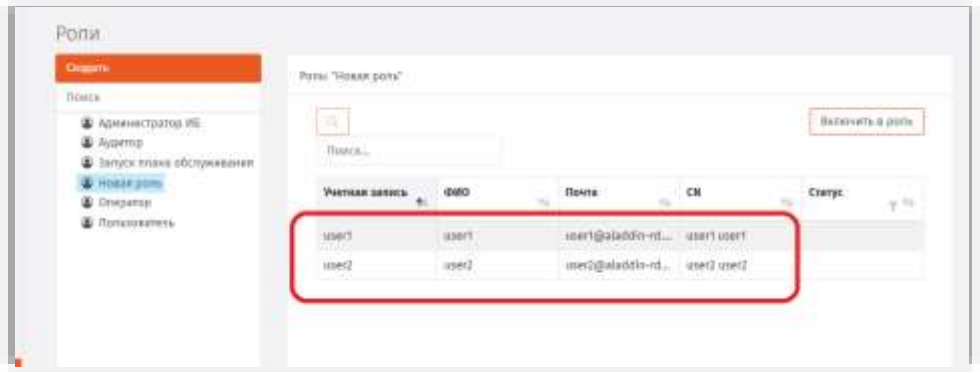


Рис. 259 – Отображение списка пользователей, которым назначена выбранная роль

3. Чтобы отменить назначение пользователю/пользователям роли выберите пользователя/пользователей на странице Роли (Рис. 259, выше), нажмите правой кнопкой мыши и в открывшемся меню выберите **Исключить из роли**.

3.12.3 Делегирование управления

JMS позволяет делегировать управление контейнером ресурсной системы определенным пользователям.

Пользователь JMS может делегировать другим пользователям только те полномочия, которыми он сам наделен (определяются полномочиями, или ролью, пользователя от имени которого запущена консоль управления JMS).

Перечень делегируемых полномочий (прав на выполнение тех или иных операций) можно найти в приложении «Приложение 1. Права на выполнение операций», с. 336.

Пользователь, которому делегировано управление, сможет выполнять набор разрешенных операций с этим контейнером. Чтобы делегировать управление контейнером пользователю JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Пользователи и роли -> Делегирование управления**.
2. В дереве ресурсной системы выберите контейнер, для которого вы хотите делегировать управление, нажмите на нем правой кнопкой мыши и выберите **Делегировать управление**:

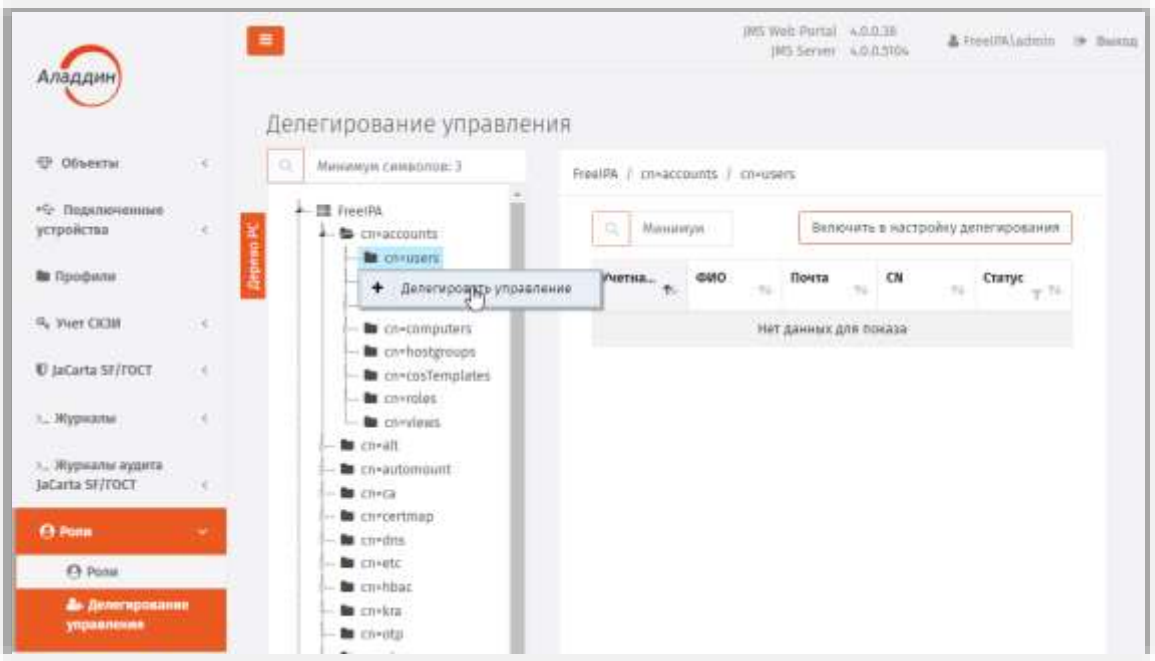


Рис. 260 – Выбор делегирования управления для выбранного контейнера ресурсной системы

3. Откроется страница создания настройки делегирования:

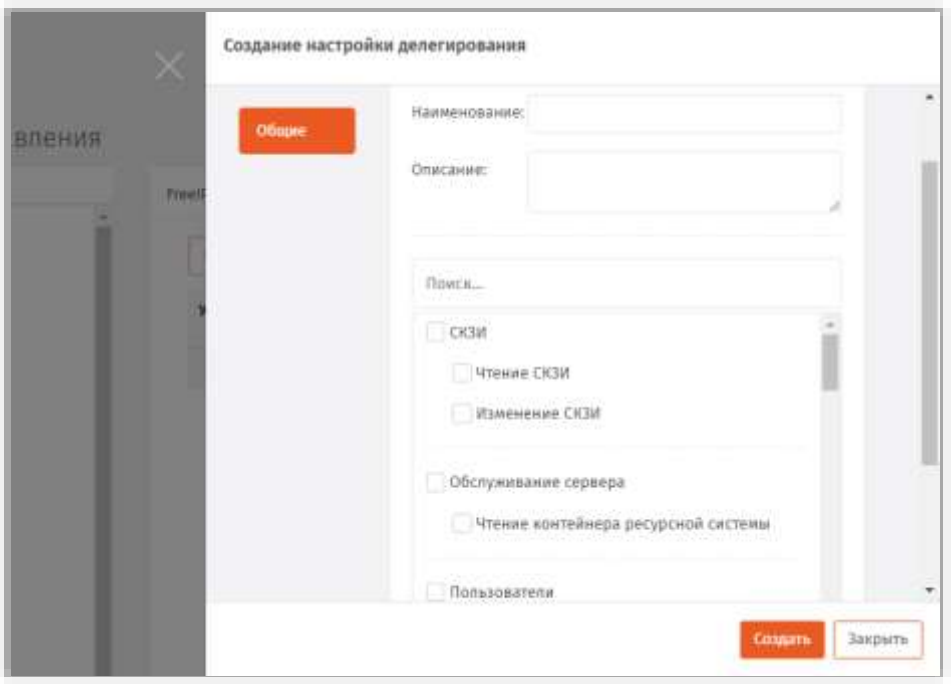


Рис. 261 – Страница создания настройки делегирования

4. В соответствующих полях введите наименование и описание настройки делегирования.
5. Отметьте операции, которые смогут совершать над контейнером пользователи, которым будет делегировано управление, и нажмите **Создать**.

Примечание. Некоторые операции, отсутствующие в полномочиях встроенных ролей JMS, не могут быть делегированы другим пользователям от имени пользователя со встроенной ролью. Подробнее о порядке

делегирования таких операций см. в разделе «Порядок делегирования полномочий, отсутствующих во встроенных ролях JMS», below.

6. Новая настройка делегирования появится в соответствующем контейнере ресурсной системы:

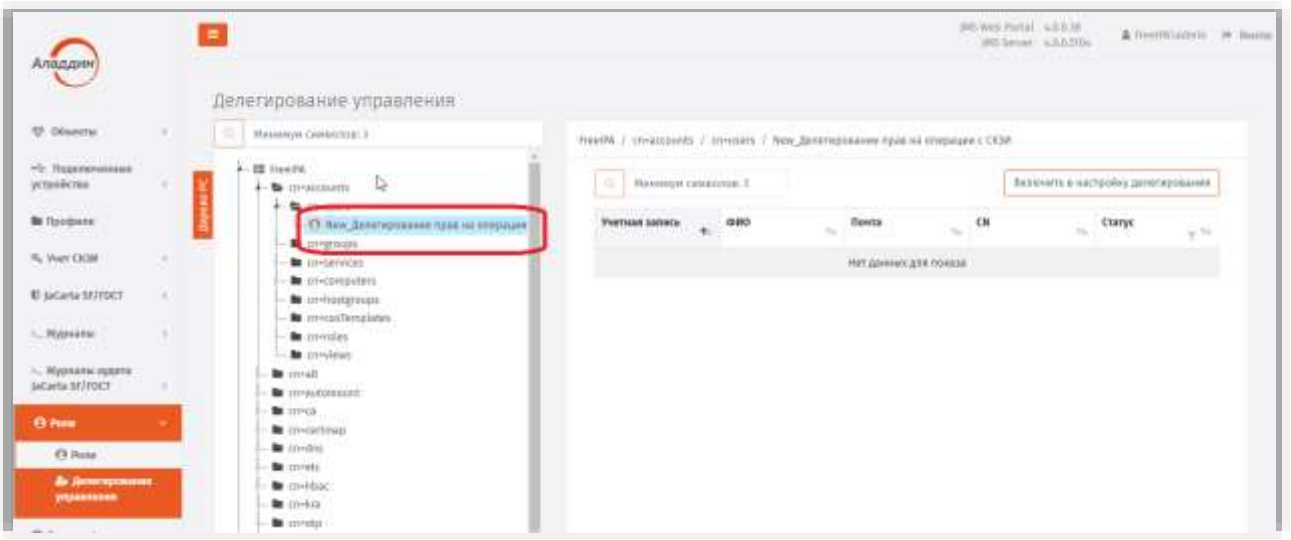


Рис. 262 – Отображение созданной настройки делегирования в дереве ресурсной системы

7. Выберите созданную настройку в дереве ресурсной системы и нажмите **Включить в настройку делегирования** в верхнем правом углу страницы.
8. Отобразится страница добавления пользователей в настройку делегирования:

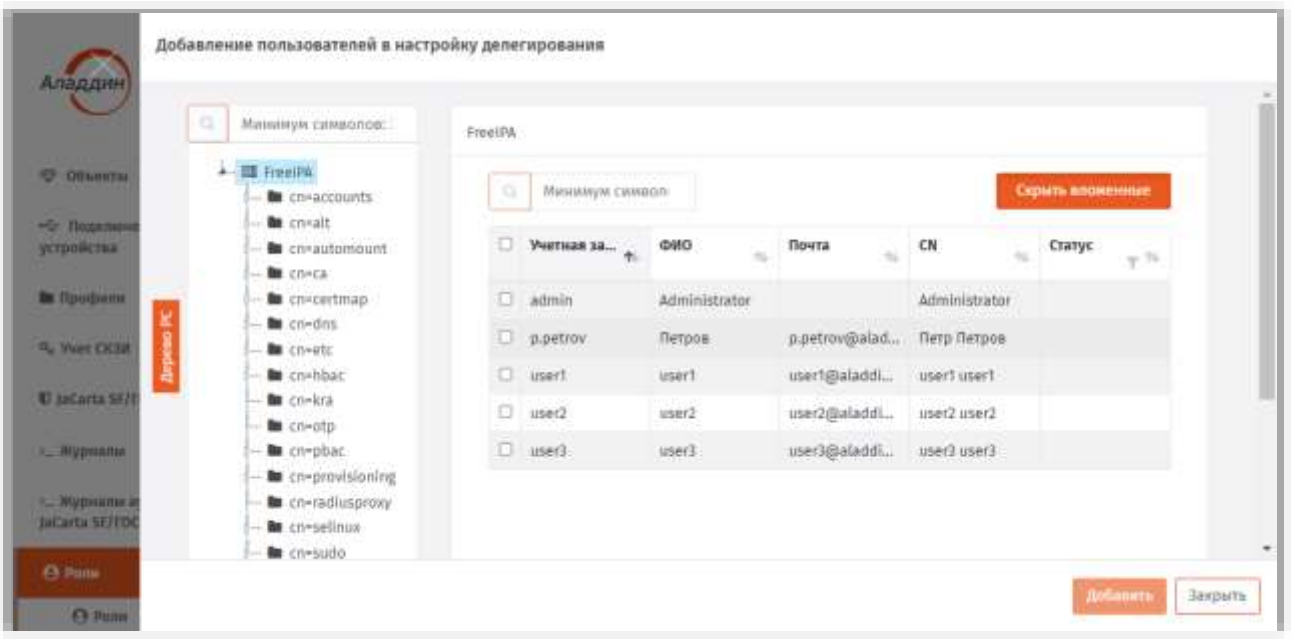


Рис. 263 – Страница добавления пользователей в настройку делегирования

9. Отметьте пользователей, которым будут делегировано управление, после чего нажмите **Добавить**.

Выбранные пользователи отобразятся в свойствах данной настройки:

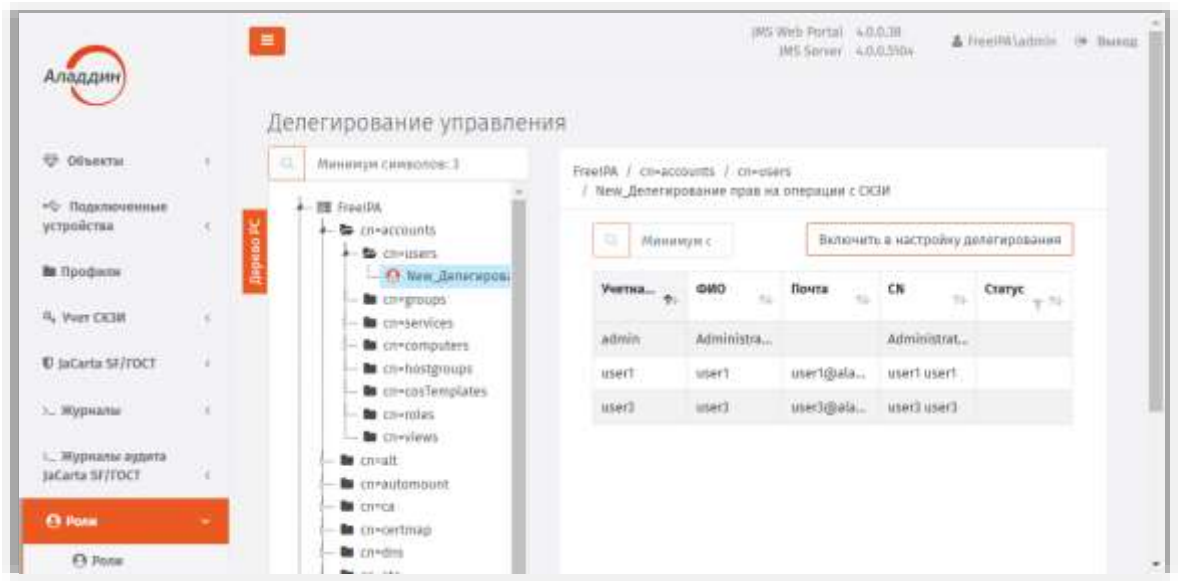


Рис. 264 – Настройка делегирования с перечнем включенных в нее пользователей

3.12.4 Порядок делегирования полномочий, отсутствующих во встроенных ролях JMS

В случае если правом на выполнение операции не наделена ни одна из встроенных ролей JMS (примером такой операции может быть **Разблокировка по PIN-коду администратора**), такие операции сопровождаются красным комментарием на странице создания настройки делегирования:

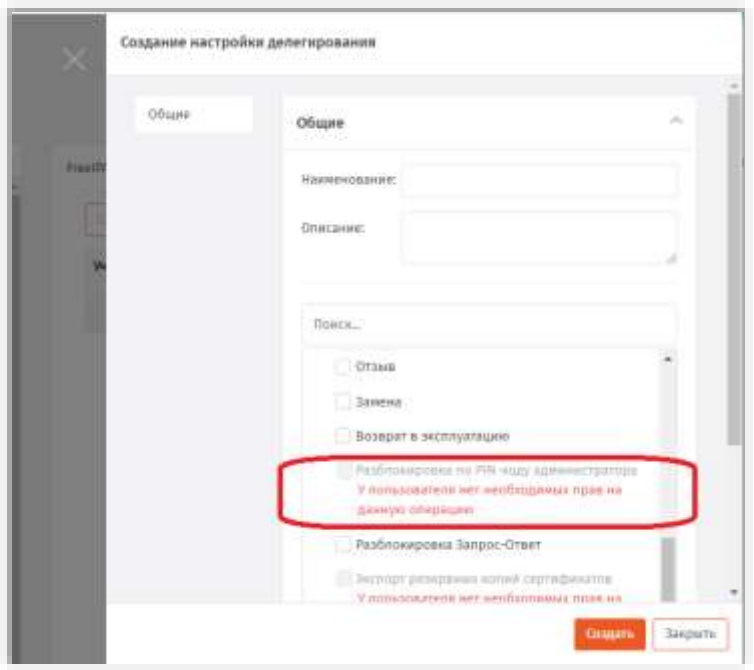


Рис. 265 – Пример операции, делегирование которой недоступно у встроенных ролей JMS

Делегирование такой операции может сделать доступным только у вновь созданной роли (т.е. у роли, не являющейся встроенной/предопределенной в JMS). Такая роль может быть создана от

имени пользователя с ролью Администратор ИБ и должна быть наделена правами делегирования полномочий.

Во вновь созданной роли следует включить полномочия на выполнение необходимой операции (например **Разблокировка по PIN-коду администратора**), и уже от имени пользователя с данной ролью выполнить делегирование данного полномочия какому-либо пользователю.

Порядок действий по добавлению полномочия в роль на примере операции **Разблокировка по PIN-коду администратора** приведен в разделе «Разблокировка подсоединенного электронного ключа», с. 59.

3.13 Планы обслуживания

План обслуживания - процедура, предназначенная для автоматизации массовых операций с объектами JMS, а также для выявления и устранения неполадок в работе JMS. В поставку JMS включены следующие планы обслуживания:

- «План обслуживания ключевых носителей», с. 285;
- «План обслуживания по умолчанию», с. 288;
- «План обслуживания рабочих станций», с. 290.
- «План обслуживания пользователей», с. 291;
- «План обслуживания сертификатов», с. 292;
- «План обслуживания СКЗИ», с. 295.

Каждый план включает одну или более задач, каждая из которых, в свою очередь, содержит набор параметров, в том числе флаг включения/отключения задачи (см. «Просмотр и редактирование задач планов обслуживания», с. 272).

План обслуживания по умолчанию следует запускать в первую очередь (см. «Запуск и просмотр результатов планов обслуживания», с. 274).

3.13.1 Просмотр и редактирование задач планов обслуживания

Чтобы просмотреть или отредактировать задачу, входящую в состав плана обслуживания, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Планы обслуживания**.

Страница консоли будет выглядеть следующим образом.

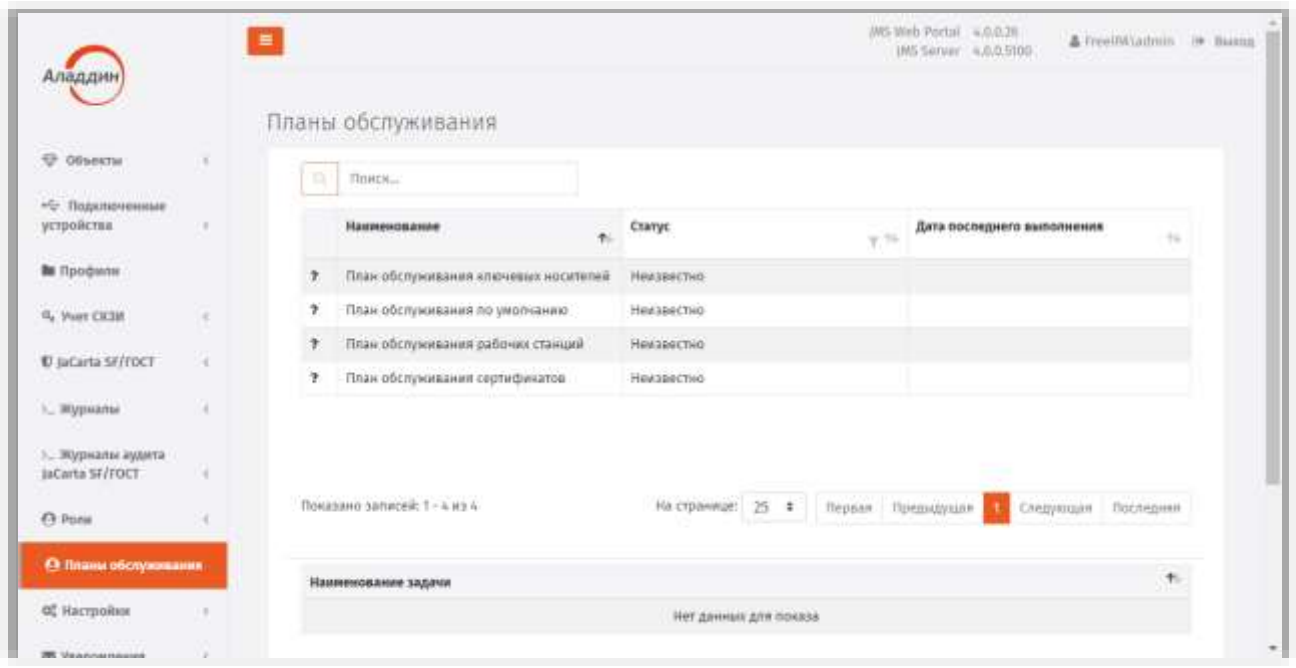


Рис. 266 – Планы обслуживания JMS

2. В центральной части страницы выберите нужный план обслуживания и нажмите на нём правой кнопкой мыши.

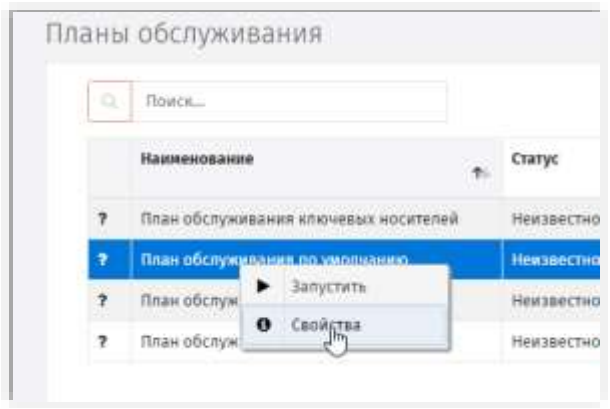


Рис. 267 – Переход к свойства плана обслуживания

3. В появившемся меню выберите пункт **Свойства**.
4. На странице свойств плана обслуживания выберите вкладку **Задачи:**

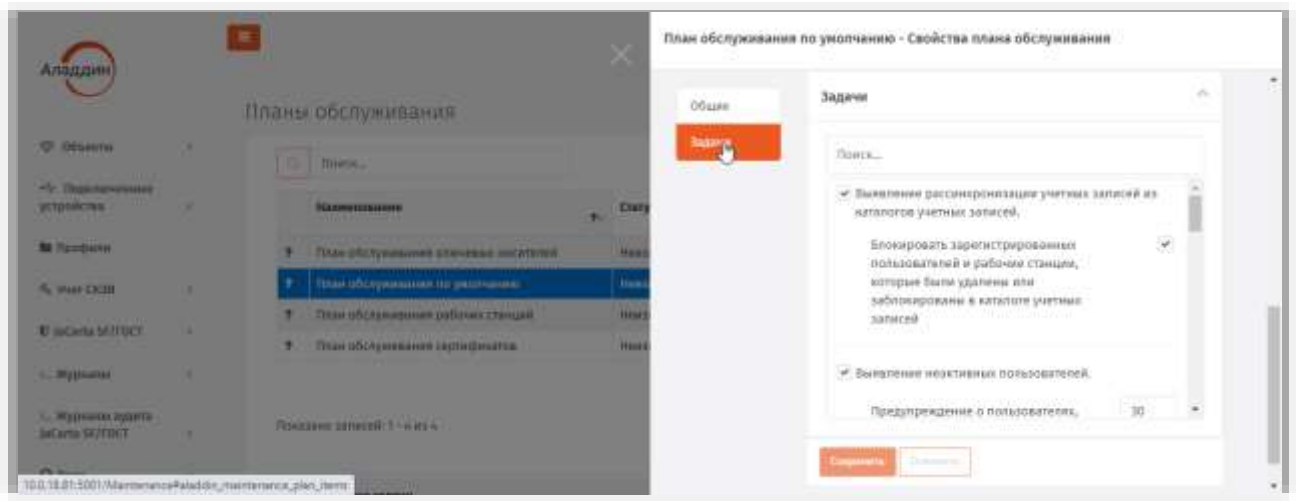


Рис. 268 – Вкладка Задачи в свойствах плана обслуживания

5. В зависимости от того, требуется ли выполнять каждую из задач, перечисленных в свойствах плана обслуживания (например, задачу **Выявление рассинхронизации учетных записей из каталогов учетных записей**), установите/сбросьте соответствующий ей флаг. В случае если задача должна запускаться, настройте остальные параметры, после чего нажмите **Сохранить**.

Примечание. Подробное описание задач каждого из планов обслуживания приведено в соответствующих разделах (3.13.5 – 3.13.11).

3.13.2 Запуск и просмотр результатов планов обслуживания

Важно! В настоящем разделе описан запуск плана обслуживания в так называемом «ручном режиме», т.е. из графического web-интерфейса административной консоли. Для автоматизации запуска планов обслуживания следует использовать команду *maintenance run* консольного агента JMS *Aladdin.EAP.Agent.Terminal*. Полная процедура автоматизации запуска планов обслуживания описана в руководство по настройке и установке JMS [2], в разделе «Настройка автоматического регулярного запуска планов обслуживания».

Чтобы запустить выполнение плана обслуживания, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Планы обслуживания**.

2. Выберите нужный план обслуживания, нажмите на нем правой кнопкой мыши и выберите **Запустить**.

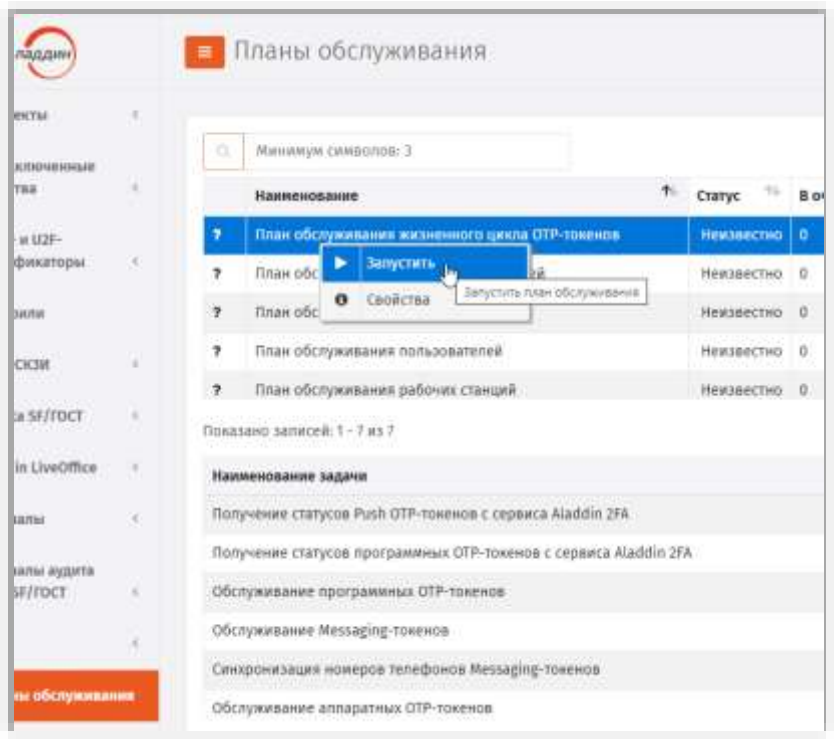


Рис. 269 – Запуск плана обслуживания на выполнение

3. Если вы запускаете **План обслуживания пользователей**, **План обслуживания рабочих станций** или **План обслуживания жизненного цикла OTP-токенов**, отобразится окно, как на Рис. 270, после чего следуйте дальнейшему описанию. В противном случае переходите к шагу 8.

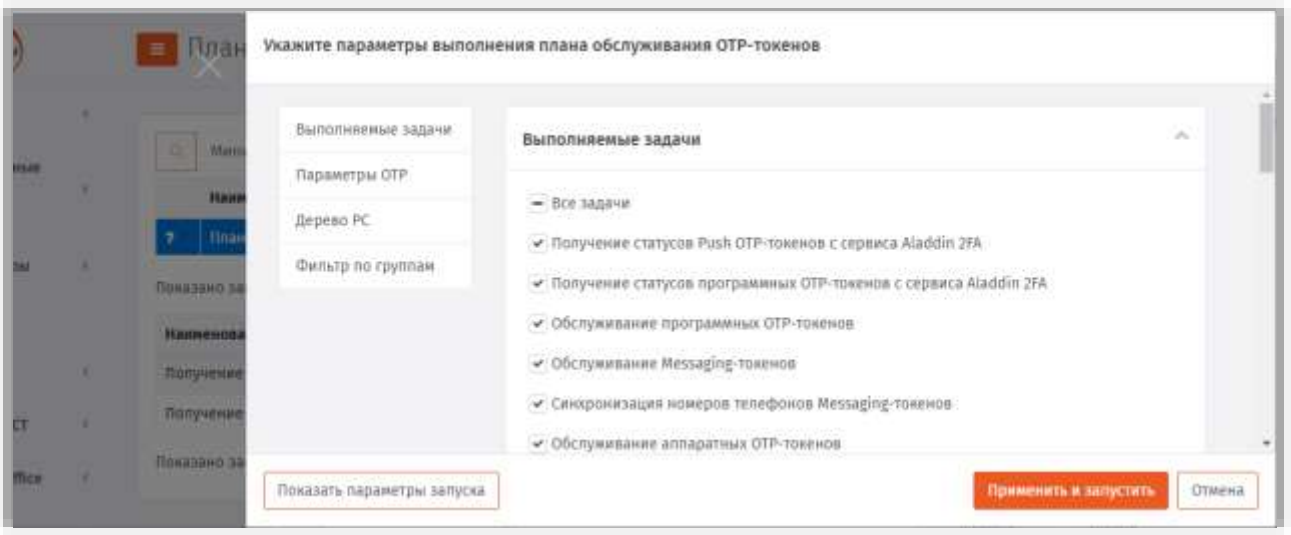


Рис. 270 – Окно настроек плана обслужинваия

4. При необходимости отредактируйте список задач, которые следует выполнить в ходе запуска данного плана обслуживания на вкладке **Выполняемые задачи** (параметры данных задач следует настроить заблаговременно, см. раздел «Просмотр и редактирование задач планов обслуживания», с. 272, подробное описание задач соответствующего плана обслуживания,

см. в соответствующих разделах, например «План обслуживания жизненного цикла OTP-токенов», с. 281).

5. В случае если вы настраиваете запуск *Плана обслуживания жизненного цикла OTP-токенов*, предоставляется возможность установить флаг **Обрабатывать пользователей, зарегистрированных за последние X часов**

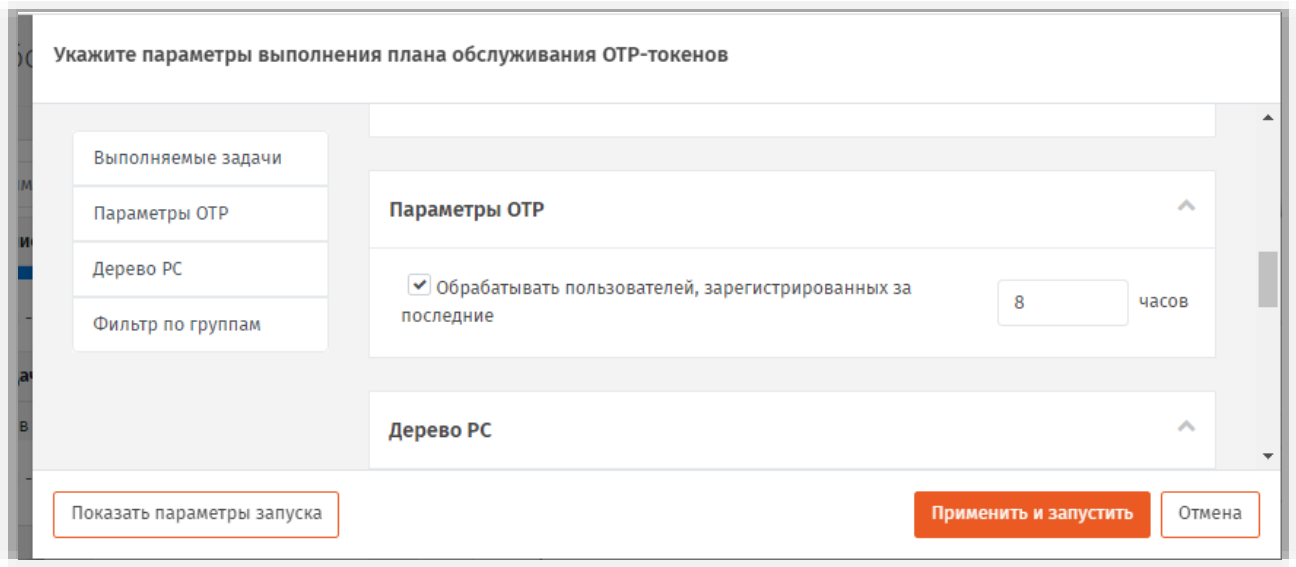


Рис. 271 – Ограничение запуска плана обслуживания для OTP-токенов, добавленных за последние X часов

Примечание. Данная настройка добавлена для снижения нагрузки на сервер при сканировании БД JMS в поиске недавно добавленных токенов. Опцией следует пользоваться с осторожностью, чтобы избежать игнорирование пользователей, добавленных до указанного срока. Опция удобна при регулярном запуске плана обслуживания с помощью команды *maintenance run* консольного агента JMS *Aladdin.EAP.Agent.Terminal*. (Подробнее см. в руководстве по настройке и установке JMS [2], раздел «Настройка автоматического регулярного запуска планов обслуживания»).

6. Чтобы настроить контейнер ресурсной системы, в котором содержатся объекты, подлежащие обслуживанию при текущем запуске данного плана, выберите вкладку **Дерево PC**. (При необходимости допускается выбор корневого объекта ресурсной системы, Рис. 272.

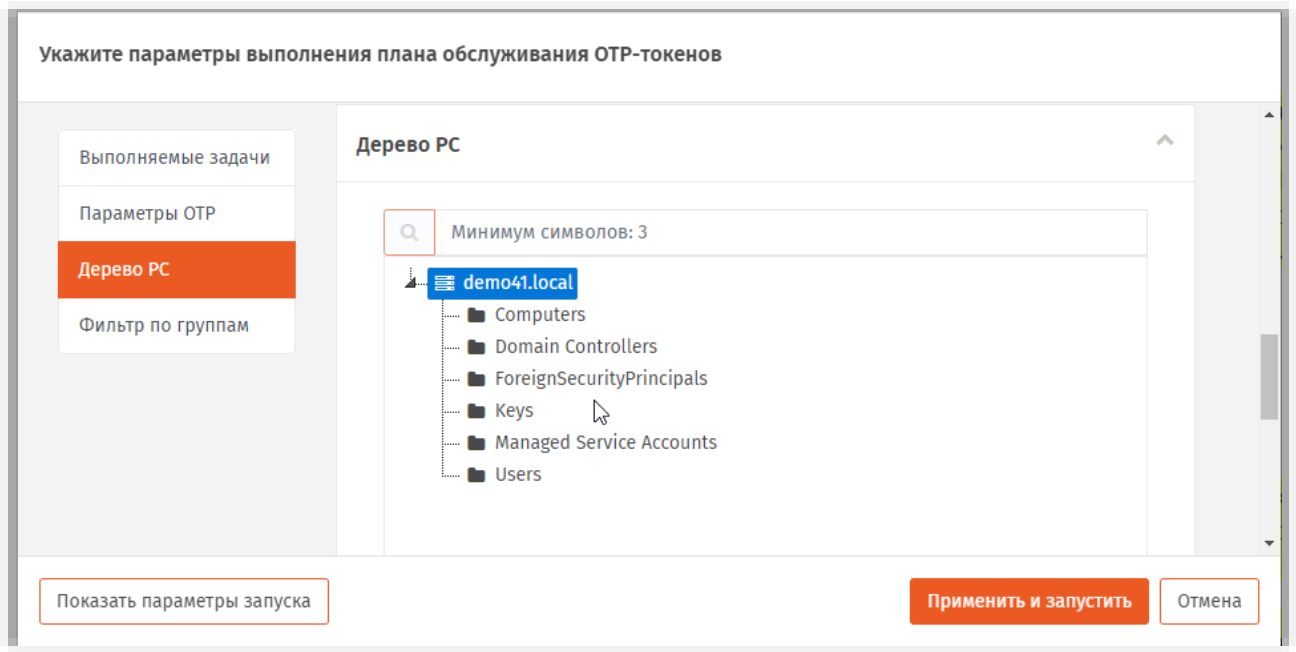


Рис. 272 – Вкладка выбора контейнера ресурсной системы

7. При необходимости выполните настройки **Фильтра по группам** (настройка реализована при запуске некоторых планов обслуживания, таких как *План обслуживания жизненного цикла OTP-токенов, План обслуживания пользователей, План обслуживание рабочих станций*), подробнее см. раздел «Настройка фильтра по глобальным и доменным группам для некоторых планов обслуживания», с. 278.
8. Нажмите **Применить и запустить**.
   При успешном выполнении плана обслуживания напротив его названия отобразится значок (см. рис. 273), а в столбце **Статус** будет отображен статус **Успешно завершен**.

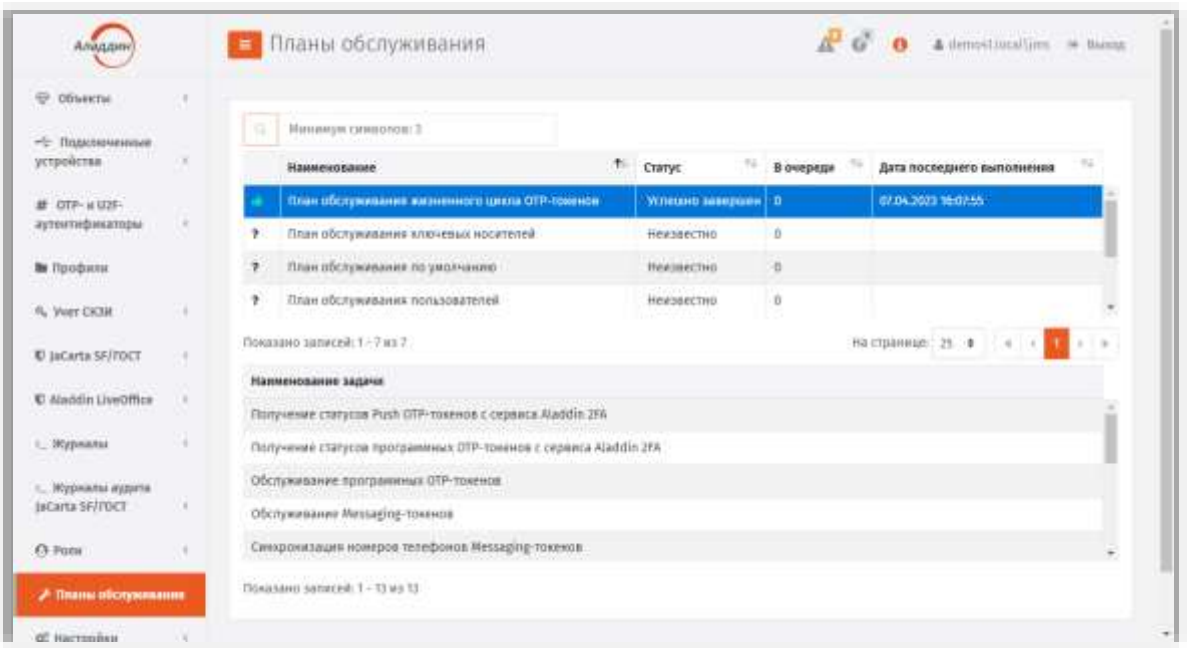


Рис. 273 – Результат выполнения плана обслуживания

9. Чтобы отобразить отчет о выполнении плана обслуживания, нажмите на нём правой кнопкой и выберите **Просмотреть отчет**.

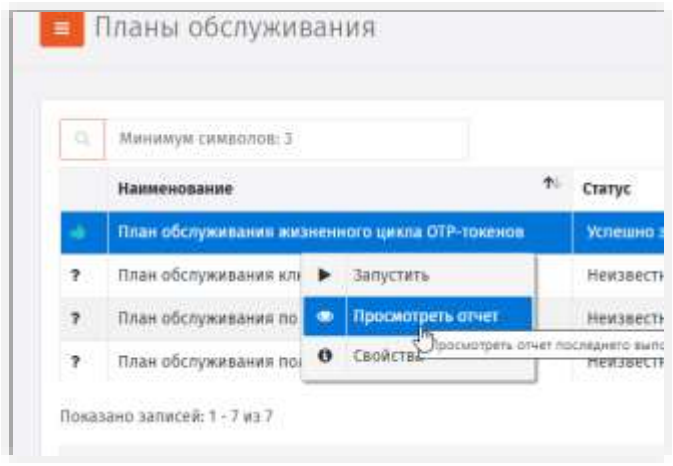


Рис. 274 – Запуск просмотра отчета о выполнении плана обслуживания

Отобразится страница отчета.

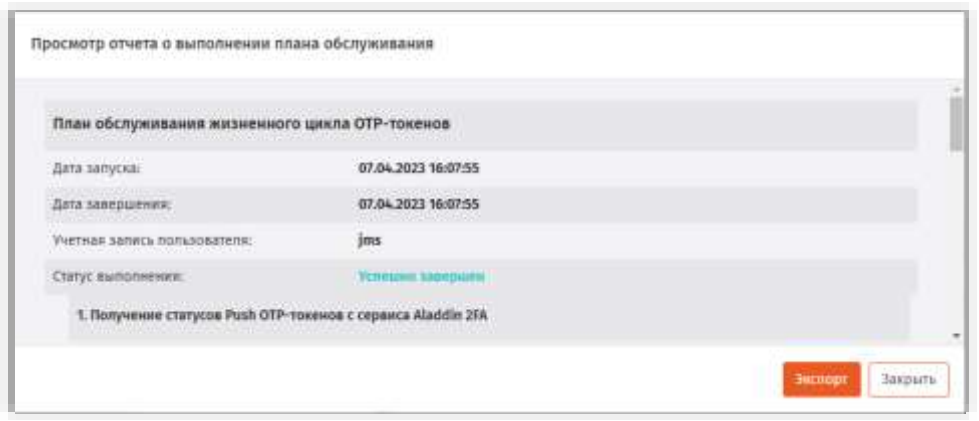


Рис. 275 – Отображение отчета о выполнении плана обслуживания

10. Чтобы экспортировать отчет в html-формате нажмите **Экспорт**. Файл отчёта будет сохранен в папку загрузок браузера.

3.13.3 Настройка фильтра по глобальным и доменным группам для некоторых планов обслуживания

При необходимости добавить для запуска плана обслуживания к объектам выбранного контейнера ресурсной системы объекты, относящиеся к доменным группам (группам домена ресурсной системы) или глобальным группам JMS (см. раздел «Глобальные группы JMS», с. 261), перейдите на вкладку **Фильтр по группам** свойств плана обслуживания(Рис. 276).

Примечание. В случае **Плана обслуживания жизненного цикла OTP-токенов** распространение плана на OTP-токены осуществляется по принципу их принадлежности пользователям (поскольку в данном случае действие доменных и глобальных групп распространяются на пользователей).

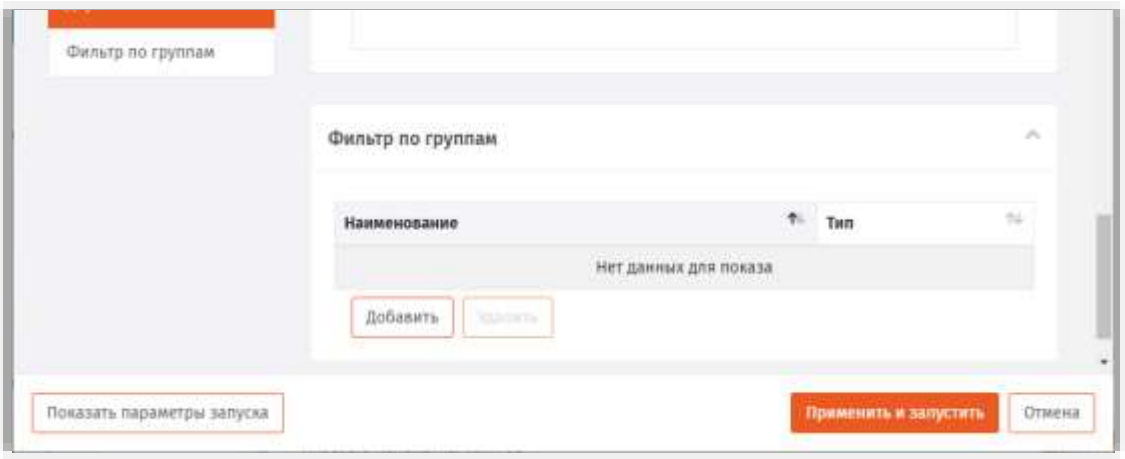


Рис. 276 – Вкладка выбора контейнера ресурсной системы

1. Нажмите **Добавить** (Рис. 276).
   Отобразится окно следующего вида.

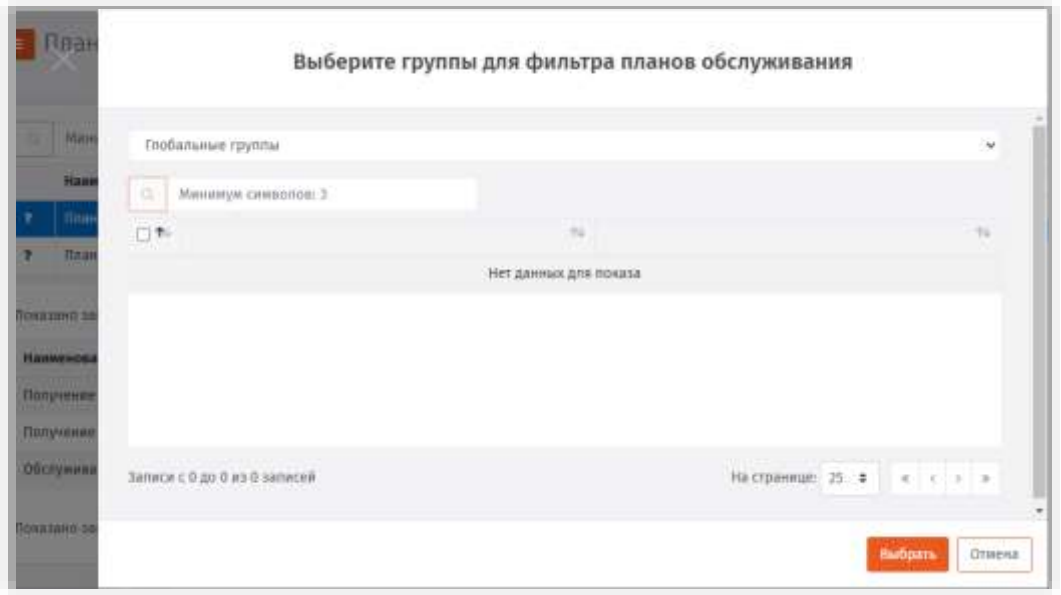


Рис. 277 – Окно добавления объектов, относящихся к доменным и/или глобальным группам

2. Для добавления объектов, относящихся к глобальны группам, выберите (отметьте) глобальные группы, объекты которых должны быть обработаны в ходе выполнения плана обслуживания.

   Примечание. Возможность добавления объектов (пользователей) за счет *глобальных групп JMS* реализована только для **Плана обслуживания жизненного цикла OTP-токенов**.

3. Для добавления объектов, относящихся к доменным группам, вверху окна нажмите раскрывающийся список.

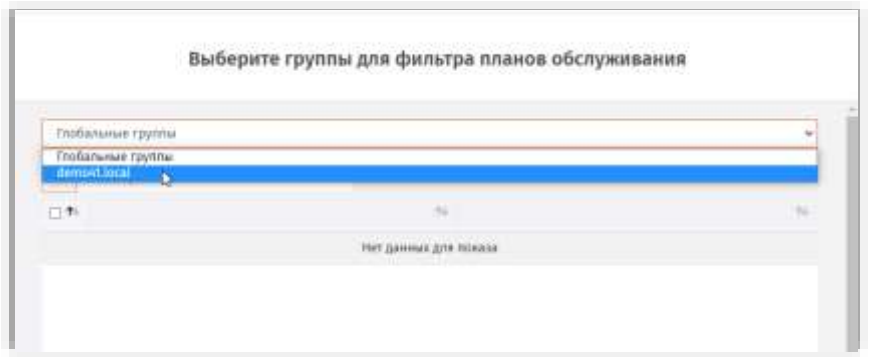


Рис. 278 – Выбор пункта доменных групп в окне фильтрации объектов

4. Выберите пункт с корневым контейнером соответствующей ресурсной системы. Отобразится окно следующего вида.

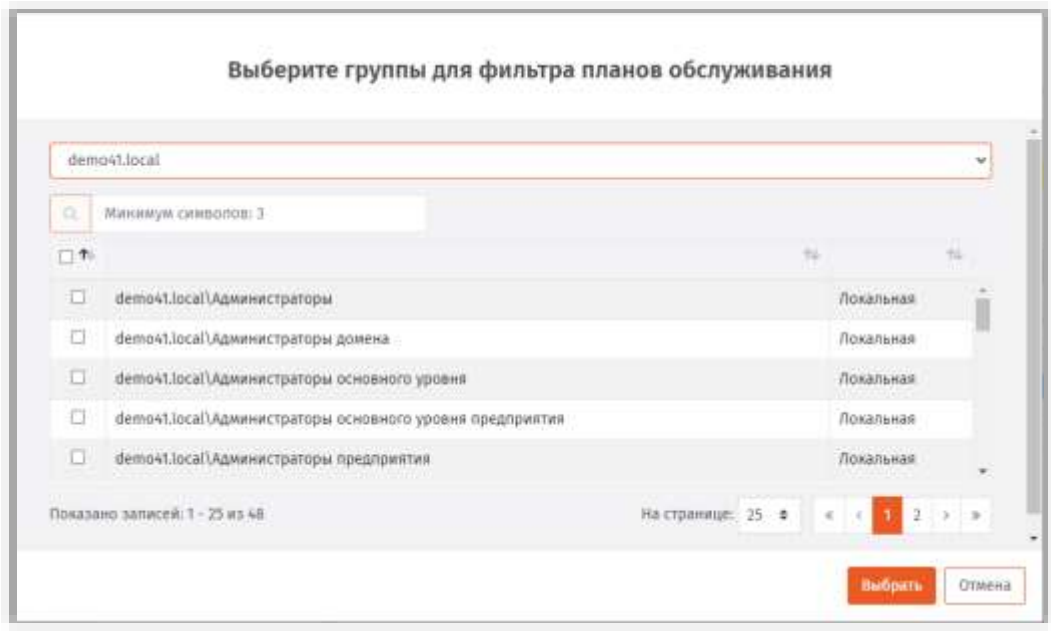


Рис. 279 – Выбор доменных групп в окне фильтрации объектов

5. Для добавления объектов, относящихся к доменным группам, выберите (отметьте) доменные группы, объекты которых должны быть обработаны в ходе выполнения плана обслуживания.
6. Нажмите **Выбрать**.

3.13.4 План обслуживания жизненного цикла OTP-токенов

План обслуживания жизненного цикла OTP-токенов содержит следующие задачи (см. Табл. 80).

План обслуживания применяется только к объектам в выбранном контейнере соответствующей ресурсной системы. Выбор ресурсной системы и ее контейнера выполняется в момент запуска плана обслуживания

Табл. 80 – План обслуживания жизненного цикла OTP-токенов

Название задачи	Описание и параметры задачи
Получение статусов Push OTP-токенов с сервиса Aladdin 2FA	Данная задача выполняет Получение статусов Push OTP-токенов с сервиса Aladdin 2FA. Возможные статусы: • **Ожидает активации** • **Активирован** • **Заблокирован по истечении времени активации** • **Не найден** Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Получение статусов программных OTP-токенов с сервиса Aladdin 2FA	Данная задача выполняет Получение статусов программных OTP-токенов с сервиса Aladdin 2FA. Возможные статусы: • **Ожидает активации** • **Активирован** • **Заблокирован по истечении времени активации** • **Не найден** Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Обслуживание программных OTP-токенов	Данная задача выполняет выпуск пользователям программных OTP-токенов в соответствии с привязанными к пользователям **Профилями выпуска программных OTP-токенов** (см. раздел «Настройка профиля выпуска программных OTP-токенов», с. 164). По окончании выполнения данной задачи выпущенные токены переходят в состояние **Используется**. Кроме этого, задача выполняет функции автоматизации действий над ранее выпущенными программными OTP-токенами в зависимости от их статуса. В частности, в случае если определен статус **Заблокирован по истечении времени активации** (см. задачу **Получение статусов программных OTP-токенов с сервиса Aladdin 2FA**, выше), то будет выполнено действие, установленное в параметре **Блокировка токена в Aladdin 2FA** профиля выпуска программного OTP-токена в секции **Параметры обновления профиля** (см. «Настройка профиля выпуска программных OTP-токенов», с. 164). Для отработки этой функциональности следует обеспечить предварительное выполнение задачи **Получение статусов программных OTP-токенов с сервиса Aladdin 2FA**, Параметры:

Название задачи	Описание и параметры задачи
	• Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Обслуживание Messaging-токенов	Данная задача выполняет выпуск пользователям messaging-токенов в соответствии с привязанными к пользователям **Профилями выпуска messaging-токенов** (см. раздел «Настройка профиля выпуска Messaging-токенов», с. 171). По окончании выполнения данной задачи выпущенные токены переходят в состояние **Используется**. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Синхронизация номеров телефонов Messaging-токенов	Данная задача выполняет обновление в БД JMS номера телефона, связанного с Messaging-токеном пользователя, в случае если в результате выполнения **Плана обслуживания по умолчанию** (задача *Выявление рассинхронизации учетных записей*) будет выявление изменение такого телефонного номера. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Обслуживание аппаратных OTP-токенов	Данная задача выполняет выпуск зарегистрированных и назначенных пользователям аппаратных OTP-токенов в соответствии с привязанными к пользователям **Профилями выпуска аппаратных OTP-токенов** (см. раздел «Настройка профиля выпуска аппаратных OTP-токенов», с. 158). По окончании выполнения данной задачи выпущенные токены переходят в состояние **Используется**. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Обслуживание Push OTP-токенов	Данная задача выполняет выпуск зарегистрированных и назначенных пользователям Push OTP-токенов в соответствии с привязанными к пользователям **Профилями выпуска Push OTP-токенов** (см. раздел «Настройка профиля выпуска Push OTP-токенов», с. 177). По окончании выполнения данной задачи выпущенные токены переходят в состояние **Используется**. Кроме этого, задача выполняет функции автоматизации действий над PUSH OTP-токенами в зависимости от полученных статусов ранее выпущенных токенов. В частности, в случае если определен статус **Заблокирован по истечении времени активации** (см. задачу **Получение статусов Push OTP-токенов с сервиса Aladdin 2FA**, выше), то будет выполнено действие, установленное в параметре **Блокировка токена в Aladdin 2FA** профиля выпуска PUSH OTP-токена в секции **Параметры обновления профиля** (см. «Настройка профиля выпуска Push OTP-токенов», с. 177). Для отработки этой функциональности следует обеспечить предварительное выполнение задачи **Получение статусов Push OTP-токенов с сервиса Aladdin 2FA**, Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Удаление Push OTP-токенов	Данная задача выполняет удаление Push OTP-токенов из связанной подсистемы A2FA.

Название задачи	Описание и параметры задачи
	Примечание. Удаление Push OTP-токенов в самой системе JMS/JAS производится на общих основаниях, т.е. автоматически, при выполнении условия, указанного в профиле выпуска, либо командой из консоли управления (как и для других типов OTP-аутентификаторов, таких как OTP- или Messaging-токены). Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания. • **Максимальное количество попыток удаления** – число попыток удаления Push OTP-токена из связанной подсистемы A2FA. Если связанная подсистема A2FA на команду удаления отвечает сообщением о сбое или невозможности выполнить в данный момент, попытка удаления будет произведена повторно при следующем выполнении плана обслуживания. Число таких попыток указывается в данном параметре. (Значение по умолчанию – **3**).
Удаление программных OTP-токенов	Назначение задачи и ее параметры аналогичны задаче **Удаление Push OTP-токенов (выше)**, но действия распространяются только на программные OTP-токены
Отслеживание активности OTP-аутентификаций	Данная задача выполняет отслеживание активности использования OTP-токенов пользователями и их автоматическую блокировку в случае прекращения их использования. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания. • **Отслеживать программные OTP-токены** • **Отслеживать аппаратные OTP-токены** • **Отслеживать Push OTP-токены** • **Отслеживать Messaging-токены** • **Заблокировать токен пользователя через ... дней неактивности** – устанавливает период в днях, через который указанные типы токенов будут заблокированы с момента последнего их использования; Значение по умолчанию: **60** • **Уведомлять пользователя по e-mail при наличии**—флаг устанавливает необходимость предупреждения (уведомления) пользователя о возможной блокировке OTP-токена в случае, если токен больше не используется: • **Отправлять уведомление после ... дней неактивности токена:** -- устанавливает период для предварительного уведомления пользователе (если установлен параметр **Уведомлять пользователя по e-mail при наличии**) Значение по умолчанию: **30** **Примечание.** данная задача будет выполнена для всех указанных типов OTP-токенов, зарегистрированных в JAS/JMS, независимо от ограничений контейнеров, указанных в области действия плана обслуживания.
Разблокировка OTP-токенов, заблокированных по перебору	Данная задача выполняет разблокировку OTP-токенов, заблокированных в результате атак «перебора OTP-кодов» для предотвращения эффекта (атаки) отказа в обслуживании пользователей. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания. • **Отслеживать программные OTP-токены** • **Отслеживать аппаратные OTP-токены** • **Отслеживать Push OTP-токены**

Название задачи	Описание и параметры задачи
	• **Отслеживать Messaging-токены** • **Разблокировать токены пользователя через ... минут** – следует указать интервал в минутах, через который после блокировки токенов по причине атаки перебора значений OTP их следует разблокировать; Значение по умолчанию: **60** **Примечание.** данная задача будет выполнена для всех указанных типов OTP-токенов, зарегистрированных в JAS/JMS, независимо от ограничений контейнеров, указанных в области действия плана обслуживания. (Действие распространяется только на токены, заблокированные по причине атаки перебора значений OTP-кода)
Экспорт журнала аутентификаций	Данная задача выполняет экспорт журнала аутентификаций сервера JAS в машиночитаемом формате для его последующей загрузки в другие системы отчётности. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания. • **Экспортировать журнал начиная с даты** – следует указать дату, с которой будет выполнена выгрузка данных. По умолчанию выгрузка производится за всё время ведения журнала; • **Последующий экспорт начиная с последнего успешного экспорта** – установленный флаг обеспечивает продолжение выгрузки информации с момента последней успешной выгрузки данных; • **Экспортировать в формате XML** – для обеспечания корректной выгрузки данных следует выбрать хотя бы один из двух предлагаемых форматов (XML или CSV); • **Экспортировать в формате CSV** – то же; • **Путь сохранения файлов экспорта:** Значение по умолчанию: **C:\Users\Public\AuthLogs** • **Шаблон имени файла:** Значение по умолчанию: **%Year%-%Month%-%Day%_%Hour%-%Minute%_authlog** • **Перезаписывать файл экспорта**
Построение отчета по OTP-, Push- и Messaging-токенам	Данная задача выполняет построение отчета по действующим OTP-, Push- и Messaging-токенам и его выгрузку в виде Excel-файла или отправку данного файла на адрес электронной почты. Задача позволяет настроить параметры отчета (см. параметры ниже). Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания. • **Включать в отчет программные OTP-токены** • **Включать в отчет аппаратные OTP-токены** • **Включать в отчет Push OTP-токены** • **Включать в отчет Messaging-токены** • **Начальная дата выгрузки** – укажите дату выпуска / регистрации / последнего изменения статуса, начиная с которой следует помещать информацию о действующих токенах в отчёт; **Примечание.** Здесь и далее под «датой» как критерием отбора токена подразумевается значение одного из его свойств: • **Дата регистрации** – в случае если последнее событие было связано с выпуском/перевыпуском токена;

Название задачи	Описание и параметры задачи
	• **Дата изменения** – в случае если последнее событие было связано с изменением статуса (или других свойств) токена. • **Конечная дата выгрузки** – укажите дату выпуска / регистрации / последнего изменения статуса, которой следует завершить помещение в отчёт информации о действующих токенах; • **Включать в отчет только вновь созданные или измененные аутентификаторы** – установите флаг, если следует установить период для построения отчета, от сегодняшней даты на N дней назад (задается параметром **Количество дней выборки по изменениям аутентификаторов**, ниже); • **Количество дней выборки по изменениям аутентификаторов:** Значение по умолчанию: **30**; • **Отправлять отчет по e-mail** • **Email для отправки отчета (множественный ввод адресов через «;»):** -- укажите адреса, если установлен флаг **Отправлять отчет по e-mail** • **Сохранять отчет в файл** – установите флаг, если отчёт следует сохранять фал (путь к файлу устанавливается следующим параметром **Путь сохранения файлов отчета**; Имя файла определяется параметром **Шаблон имени файла**); • **Путь сохранения файлов отчета** Значение по умолчанию: **C:\Users\Public\OtpAuthenticators** • **Шаблон имени файла** Значение по умолчанию: **%Year%-%Month%-%Day%_%Hour%-%Minute%_OtpAuthenticators** • **Перезаписывать файл отчета** – установите флаг, если файл отчёта с тем же именем следует перезаписать, в противном случае имени файла будет присвоен индекс и он сохранится в отдельный файл;

3.13.5 План обслуживания ключевых носителей

План обслуживания ключевых носителей содержит следующие задачи (табл. 81).

Табл. 81 – План обслуживания ключевых носителей

Название задачи	Описание и параметры задачи
Отзыв/отключение ключевого носителя в случае удаления или блокировки пользователя	Данная задача выполняет операцию отключения электронных ключей, принадлежащих пользователям, которые были заблокированы в результате выполнения **Плана обслуживания по умолчанию** (см. «План обслуживания по умолчанию», с. 288,задача **Выявление рассинхронизации учетных записей из каталогов учетных записей**). По окончании выполнения данной задачи электронные ключи заблокированных пользователей переходят в состояние **Отключен**. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Проверка привязки назначенных ключевых носителей к контейнеру	В рамках задачи анализируются все зарегистрированные электронные ключи, назначенные пользователям: • если пользователь был перемещен в новый контейнер ресурсной системы, туда же будут перемещены его электронные ключи; • если пользователь был удален вместе с контейнером, электронный ключ будет перемещен в корневой контейнер ресурсной системы.

Название задачи	Описание и параметры задачи
	Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Проверка привязки неназначенных ключевых носителей к контейнеру	В данной задаче анализируются все зарегистрированные электронные ключи, которые не были выпущены. Если контейнер ресурсной системы, к которой привязан электронный ключ, удален из ресурсной системы, ключевой носитель перемещается в корневой контейнер ресурсной системы. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Проверка на наличие свободных ключевых носителей меньше порогового значения	В рамках задачи в JMS подсчитывается число электронных ключей со статусом «Зарегистрирован». Если число таких ключей меньше порогового значения, которое задается в параметрах задачи, то будет сгенерировано соответствующее уведомление в журнале предупреждений. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Порог минимального количества свободных ключевых носителей** – пороговое значение, при снижении ниже которого генерируется уведомление
Проверка значений счетчика количества подключений USB-носителей	В рамках данной задачи будут проанализированы все зарегистрированные в JMS ЭН (электронных носителей) JaCarta SF/ГОСТ. Если общее количество подключений ЭН превышает указанный в задаче процент от гарантийного числа подключений, то будет создано соответствующее предупреждение для администратора (журнал **Предупреждения**). В зависимости от величины значения, данное предупреждение может иметь уровень warning (для ЭН с количеством подключений более указанного процента, но ниже 100% от гарантии) и error (для ЭН с количеством подключений более 100% от гарантии). Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания. • **Процент от гарантии, после которого будут предупреждения (%)** • **Гарантийное количество подключений USB-носителей**
Проверка общего времени работы устройства USB-носителей	В рамках данной задачи будут проанализированы все зарегистрированные в JMS ЭН (электронных носителей) JaCarta SF/ГОСТ. Если общее время работы ЭН превышает указанный в задаче процент от гарантийного общего времени работы, то будет создано соответствующее предупреждение для администратора (журнал **Предупреждения**). В зависимости от величины значения, данное предупреждение может иметь уровень warning (для ЭН с временем работы более указанного процента, но ниже 100% от гарантии) и error (для ЭН с временем работы более 100% от гарантии). Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания. • **Процент от гарантии, после которого будут предупреждения (%)** • **Гарантийное общее время работы USB-носителей (часов)**

Название задачи	Описание и параметры задачи
Проверка количества неправильных извлечений USB-носителей	В рамках данной задачи будут проанализированы все зарегистрированные в JMS ЭН (электронных носителей) JaCarta SF/ГОСТ. Если количество неправильных извлечений ЭН превышает указанное в задаче значение, то будет создано соответствующее предупреждение для администратора (журнал **Предупреждения**). Предупреждение будет иметь уровень error (для ЭН превышающих указанное в задаче значение). Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания. • **Количество неправильных извлечений USB-носителей**
Включение ключевого носителя разблокированного пользователя	Выполняет разблокировку электронные ключи, принадлежащих незаблокированным пользователям, даже в том случае, если электронный ключ был заблокирован вручную администратором. По умолчанию данная задача отключена. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.

3.13.6 План обслуживания настроек личного кабинета

План обслуживания настроек личного кабинета предназначен для переноса настроек, указанных в профиле **Доступ в личный кабинет** (см. раздел «Настройка профиля доступа в личный кабинет JWM», с. 193) в свойства объектов *Пользователь*, к которым привязан данный профиль.

План обслуживания настроек личного кабинета содержит следующие задачи (см. Табл. 82)

Табл. 82 – План обслуживания настроек личного кабинета

Название задачи	Описание и параметры задачи
Синхронизация прав доступа	Позволяет синхронизировать права доступа в личный кабинет пользователя на JWM, настроенные в профиле **Доступ в личный кабинет** (см. раздел «Настройка профиля доступа в личный кабинет JWM», с. 193) со свойствами объектов *Пользователь*, к которым привязан данный профиль. Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.

3.13.7 План обслуживания по умолчанию

План обслуживания по умолчанию содержит следующие задачи (табл. 83).

Табл. 83 – План обслуживания по умолчанию

Название задачи	Описание и параметры задачи
Выявление рассинхронизации учетных записей из каталогов учетных записей	Позволяет синхронизировать состояние базы данных JMS и по отношению к используемой ресурсной системе. Данная задача отвечает также за отслеживание необходимости перевыпуска сертификата пользователя при изменении атрибутов пользователя, указанных администратором JMS на вкладке **Ключевые атрибуты** профиля выпуска сертификата. Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Блокировать зарегистрированных пользователей и рабочие станции, которые были удалены или заблокированы в каталоге учетных записей** – если пользователи или рабочие станции были удалены из используемой ресурсной системы или заблокированы, то они будут заблокированы в JMS. (Чтобы приостановить действие электронных ключей заблокированных пользователей, необходимо выполнить план обслуживания ключевых носителей.) • **Разблокировать пользователей, на момент выполнения плана обслуживания не заблокированных в ресурсной системе** – установите флаг, если разблокировку пользователей в ресурсной системе нужно синхронизировать с JMS • **Разблокировать рабочие станции, на момент выполнения плана обслуживания не заблокированные в ресурсной системе** – установите флаг, если разблокировку рабочих станций в ресурсной системе нужно синхронизировать с JMS
Проверка лицензионного состояния сервера	Задача имеет следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Предупреждение об окончании срока действия лицензии за … (дней)** – позволяет указать, за сколько дней до истечения срока действия лицензии в отчете о выполнении плана обслуживания будет отображаться соответствующее предупреждение. • **Предупреждение об исчерпании лимита рабочих станций** – параметр не используется
Выявление рассинхронизации профилей	Профили JMS привязаны к контейнерам (каталогам) используемой ресурсной системы. Эта задача позволяет синхронизировать профили JMS с ресурсной системой в случае рассинхронизации. Задача имеет следующий параметр: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания**.**
Проверка настроек делегирования	Задание проверяет все настройки делегирования JMS. Если настройка делегирования связана с несуществующим контейнером (например, контейнер удален во FreeIPA), выполняется отмена этого делегирования. В журнал плана обслуживания (журнал **Отчеты планов обслуживания**) заносится соответствующее событие. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Проверка истекшего доступа в Active Directory по паролю	**Задача не используется в текущей версии JMS.** Отменяет временный доступ в Active Directory по паролю, если срок такого доступа истек.

Название задачи	Описание и параметры задачи
	Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Выявление назащищенных параметров профилей	Выявляет и помещает в защищенную область БД JMS все параметры профилей, требующие защиты (перемещение выполняется, например, при обновлении ПО JMS, если в прежней версии ПО JMS данные параметры еще не были перемещены в защищенную область БД, или при создании новой базы данных). • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Проверка рассинхронизации контейнеров СКЗИ, ключевой информации, нормативных и ключевых документов	В рамках задачи выполняется анализ всех зарегистрированные в JMS экземпляров СКЗИ, экземпляров ключевой информации и ключевых документов. Если ответственный пользователь, к которому привязана сущность, был перемещен в новый контейнер – все связанные с ним СКЗИ-сущности будут перемещены в новый контейнер. Если пользователь был удален вместе с контейнером, СКЗИ-сущности будут перемещены в корневой контейнер ресурсной системы. Также выполняется анализ всех существующих нормативных документов, созданных в целях учета СКЗИ. Если контейнер, к которому привязан документ, удален в ресурсной системе, то документ будет перемещен в корневой контейнер ресурсной системы. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Проверка рассинхронизации контейнеров актов и заявок	В рамках данной задачи выполняется анализ всех существующих актов и заявок, созданных для электронных ключей. Если контейнер, к которому привязан документ (акт / заявка) удален в ресурсной системе, то документ будет перемещен в корневой контейнер ресурсной системы. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.
Выполнение ротации логов	Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Удалять записи в логах старше ... (месяцев)** (имеются в виду журнал **Отчеты планов обслуживания**)– позволяет задать число месяцев, за которое будут сохраняться записи журнала. Более старые записи о событиях будут удаляться. • **Автоматически выполнять переразбиение на секции при изменении настроек политики ротации записей журнала событий (только для SQL Server Enterprise Edition).**
Удаление истёкших токенов обновления токенов аутентификации.	В рамках задачи из БД JMS будут удалены токены обновления токенов аутентификации (JWT Refresh Token), у которых истёк срок действия, либо был удалён/заблокирован пользователь, к которому был привязан токен обновления. Переполнение БД устаревшими токенами обновления (в зависимости от различных факторов, таких как срок действия Refresh Token, число активных пользователей, частота аутентификации пользователей) может привести с деградации производительности СУБД, поэтому требуется регулярная очистка

Название задачи	Описание и параметры задачи
	БД. Производителем рекомендуется запускать задачу (в рамках плана обслуживания) раз в день. Параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания**.**

3.13.8 План обслуживания рабочих станций

План обслуживания рабочих станций содержит перечисленные ниже задачи (Табл. 84).

План обслуживания применяется только к объектам в выбранном контейнере соответствующей ресурсной системы. Выбор ресурсной системы и ее контейнера выполняется в момент запуска плана обслуживания.

Табл. 84 – План обслуживания рабочих станций

Название задачи	Описание и параметры задачи
Выявление рабочих станций, которые не аутентифицировались в течение указанного периода времени	Задача выполняет поиск рабочих станций, которые неактивны (не аутентифицировались) в течение указанного периода времени. • Если от последней аутентификации рабочей станции до момента выполнения плана обслуживания прошло время меньшее значения «короткое время» (см. параметры, ниже), то ей присваивается статус **Активна**. • Если от последней аутентификации рабочей станции до момента выполнения плана обслуживания прошло время большее значения «короткое время» (см. параметры, ниже), но меньшее значения «длительное время», то ей присваивается статус **Неактивна в течение краткого периода времени**. В отчете о выполнении плана в связи с этим событием отображается предупреждение. • Если от последней аутентификации рабочей станции до момента выполнения плана обслуживания прошло время большее значения «длительное время», то ей присваивается статус **Неактивна в течение длительного периода времени**. В отчете о выполнении плана в связи с этим событием отображается ошибка. Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Выявлять рабочие станции, не выходящие на связь короткое время … (дней)**; • **Выявлять рабочие станции, не выходящие на связь длительное время … (дней)**. **Примечание.** Значение, задаваемое для длительного периода должно быть больше значения, задаваемого для короткого периода.
Выявление рабочих станций с устаревшей версией клиента	Задача выполняет поиск рабочих станций, на которых установлена версия клиента более ранняя, чем указано в параметрах данной задачи (см. ниже). Если на рабочей станции установлена версия клиента более ранняя, чем указано в параметре **Проверять актуальность версии клиента**, то в поле **Статус версии клиента** ей присваивается значение **Устаревшая**. В отчете о выполнении плана в связи с этим событием отображается предупреждение. Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Проверять актуальность версии клиента** – в данном поле следует указать актуальную версию клиента в формате: `[1-3 цифры].[1-3 цифры].[1-3 цифры].[1-4 цифры]`

Название задачи	Описание и параметры задачи
Автоматическая регистрация рабочих станций из ресурсных систем	Позволяет автоматически зарегистрировать в JMS рабочие станции из выбранного контейнера ресурсной системы по указанным критериям фильтрации. Является альтернативой «массовой регистрации» рабочих станций в ручном режиме из консоли управления JMS. Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Регистрировать заблокированные рабочие станции** – при установке флага рабочие станции, заблокированные в связанной ресурсной системе, будут зарегистрированы также в JMS. При этом у данных рабочих станций в JMS также будет установлен статус блокировки; • **Фильтровать рабочие станции по дате создания** – при установке флага выполняется регистрация рабочих станций, зарегистрированных в ресурсной системе только за период (относительно текущего момента), указанный в поле **Регистрировать только рабочие станции, созданные за последние ... (дней)** Опция позволяет оптимизировать выборку данных из ресурсной системы и ускорить отработку плана облуживания. Параметр используется только ресурсными системами Active Directory и Remote Active Directory, для других типов ресурсных систем – параметр игнорируется. (Механизм действия: фильтрация рабочих станций из ресурсной системы выполняется по полю whenChanged). • **Фильтровать рабочие станции по глобальному счетчику изменений (USN)** – фильтр применим только к ресурсным системам Active Directory. Фильтр позволяет ускорить выполнение плана обслуживания и исключить постоянный перебор одних и тех же учетных записей, что негативно влияет на производительность ресурсной системы (AD). (Задействованный механизм – дополнительная фильтрация по глобальному счетчику изменений объектов контроллера домена). Фильтр работает независимо от фильтра **Фильтровать рабочие станции по дате создания.** Фильтр эффективен только в случае регулярного автоматического запуска плана обслуживания средствами команды *maintenance run* консольного агента JMS *Aladdin.EAP.Agent.Terminal* (подробнее см. в руководстве по настройке и установке JMS [2], раздел «Настройка автоматического регулярного запуска планов обслуживания») в применении к одному и тому же контейнеру ресурсной системы (в общем случае, к корню ресурсной системы) в доменах с большим числом рабочих станций. В случае если план обслуживания запускается вручную для разных контейнеров, целесообразнее использовать только фильтр **Фильтровать рабочие станции по дате создания**.

3.13.9 План обслуживания пользователей

План обслуживания рабочих станций содержит перечисленные ниже задачи (Табл. 85).

План обслуживания применяется только к объектам в выбранном контейнере соответствующей ресурсной системы. Выбор ресурсной системы и ее контейнера выполняется в момент запуска плана обслуживания.

Табл. 85 – План обслуживания пользователей

Название задачи	Описание и параметры задачи
Автоматическая регистрация пользователей из ресурсных систем	Позволяет автоматически зарегистрировать в JMS пользователей из выбранного контейнера ресурсной системы по указанным критериям фильтрации. Является альтернативой «массовой регистрации» пользователей в ручном режиме из консоли управления JMS.

Название задачи	Описание и параметры задачи
	Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Регистрировать заблокированных пользователей** – при установке флага пользователи, заблокированные в связанной ресурсной системе, будут зарегистрированы также в JMS; • **Фильтровать пользователей по дате создания** – при установке флага выполняется регистрация пользователей, зарегистрированных в ресурсной системе только за период (относительно текущего момента), указанный в поле **Регистрировать только пользователей, созданных за последние … (дней)** Опция позволяет оптимизировать выборку данных из ресурсной системы и ускорить отработку плана облуживания. Параметр используется только с ресурсными системами Active Directory и Samba AD, для других типов ресурсных систем – параметр игнорируется. (Механизм действия: фильтрация пользователей из ресурсной системы выполняется по полю whenChanged). • **Фильтровать пользователей по глобальному счетчику изменений (USN)** – фильтр применим только к ресурсным системам Active Directory и Samba AD. Фильтр позволяет ускорить выполнение плана обслуживания и исключить постоянный перебор одних и тех же учетных записей, что негативно влияет на производительность ресурсной системы. (Задействованный механизм – дополнительная фильтрация по глобальному счетчику изменений объектов контроллера домена). Фильтр работает независимо от фильтра **Фильтровать пользователей по дате создания.** Фильтр эффективен только в случае регулярного автоматического запуска плана обслуживания средствами команды *maintenance run* консольного агента JMS *Aladdin.EAP.Agent.Terminal* (подробнее см. в руководстве по настройке и установке JMS [2], раздел «Настройка автоматического регулярного запуска планов обслуживания») в применении к одному и тому же контейнеру ресурсной системы (в общем случае, к корню ресурсной системы) в доменах с большим числом пользователей. В случае если план обслуживания запускается вручную для разных контейнеров целесообразнее использовать только фильтр **Фильтровать пользователей по дате создания**.

3.13.10 План обслуживания сертификатов

План обслуживания сертификатов содержит следующие задачи (Табл. 86).

Табл. 86 – План обслуживания сертификатов

Название задачи	Описание и параметры задачи
Выявляет сертификаты JMS с истекшим или истекающим сроком действия	В рамках задачи анализируются сертификаты в БД, выпущенные JMS, в состояниях «Выпущен на КН», «Заблокирован во внешней системе» и «Сохранен на КН» на предмет истечения их сроков действия. Если срок действия сертификата истек, или истекает в течение заданного в настройках задачи количества дней, то будет создано соответствующее предупреждение для администратора (журнал **Предупреждения**). Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Предупреждение об окончании срока действия сертификата за … (дней)** – позволяет указать, за сколько дней до истечения срока действия сертификата в отчете о выполнении плана обслуживания будет отображаться соответствующее предупреждение.

Название задачи	Описание и параметры задачи
Выявляет внешние сертификаты с истекшим или истекающим сроком действия	В рамках задачи анализируются внешние сертификаты в БД, в состоянии «Внешний объект», на предмет истечения их сроков действия. Если срок действия сертификата истек, или истекает в течение заданного в настройках задачи количества дней, то будет создано соответствующее предупреждение для администратора (журнал **Предупреждения**). Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Предупреждение об окончании срока действия сертификата за ... (дней)** – позволяет указать, за сколько дней до истечения срока действия сертификата в отчете о выполнении плана обслуживания будет отображаться соответствующее предупреждение.
Выявляет унаследованные сертификаты с истекшим или истекающим сроком действия	В рамках задачи анализируются сертификаты в БД со статусом **Унаследован** на предмет истечения их сроков действия. Если срок действия сертификата истек, или истекает в течение заданного в настройках задачи количества дней, то будет создано соответствующее предупреждение для администратора (журнал **Предупреждения**). Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Предупреждение об окончании срока действия сертификата за ... (дней)** – позволяет указать, за сколько дней до истечения срока действия сертификата в отчете о выполнении плана обслуживания будет отображаться соответствующее предупреждение.
Выявляет сертификаты операторов с истекшим или истекающим сроком действия	В рамках данной задачи анализируются сертификаты операторов JMS, хранящиеся в БД, на предмет истечения их сроков действия. Если срок действия сертификата истек, или истекает в течение заданного в настройках задачи количества дней, то будет создано соответствующее предупреждение для администратора (журнал **Предупреждения**). Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Предупреждение об окончании срока действия сертификата за ... (дней)** – позволяет указать, за сколько дней до истечения срока действия сертификата оператора JMS в журнале **Предупреждения** будет появляться соответствующее сообщение**.**
Выявляет сертификаты в хранилище пользователя с истекшим или истекающим сроком действия	В рамках данной задачи будут проанализированы сертификаты в БД со статусом **Унаследован**, тип носителя **Реестр хранилище пользователя**, на предмет истечения их сроков действия. Если срок действия сертификата истек, или истекает в течение заданного в настройках задачи количества дней, то будет создано соответствующее предупреждение для администратора (журнал **Предупреждения**). Если в атрибутах сертификата указан e-mail (Subject или SubjectAlternativeName тип RFC822) и он совпадает с e-mail зарегистрированного в JMS пользователя, то при соответствующей настройке (см. «Уведомления о событиях, связанных с использованием JMS», с. 295) данному пользователю будет отправлено уведомление по электронной почте. Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Предупреждение об окончании срока действия сертификата за ... (дней)** – за сколько дней до истечения срока действия сертификата JMS в журнале **Предупреждения** будет появляться соответствующее сообщение, а если указан e-mail (см. выше), то и высылаться уведомление по электронной почте**.**

Название задачи	Описание и параметры задачи
Выявляет сертификаты в хранилище ПК с истекшим или истекающим сроком действия	В рамках данной задачи будут проанализированы сертификаты в БД со статусом **Унаследован**, тип носителя **Реестр хранилище ПК**, на предмет истечения их сроков действия. Если срок действия сертификата истек или истекает в течение заданного в настройках задачи количества дней, то будет создано соответствующее предупреждение для администратора (журнал **Предупреждения**). Если в атрибутах сертификата указан e-mail (Subject или SubjectAlternativeName тип RFC822) и он совпадает с e-mail зарегистрированного в JMS пользователя, то при соответствующей настройке (см. «Уведомления о событиях, связанных с использованием JMS», с. 295) данному пользователю будет отправлено уведомление по электронной почте. Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Предупреждение об окончании срока действия сертификата за ... (дней)** – за сколько дней до истечения срока действия сертификата JMS в журнале **Предупреждения** будет появляться соответствующее сообщение, а если указан e-mail (см. выше), то и высылаться уведомление по электронной почте**.**
Выявляет сертификаты на файловой системе ПК с истекшим или истекающим сроком действия	В рамках данной задачи будут проанализированы сертификаты в БД со статусом **Унаследован**, тип носителя **Файл**, на предмет истечения их сроков действия. Если срок действия сертификата истек, или истекает в течение заданного в настройках задачи количества дней, то будет создано соответствующее предупреждение для администратора (журнал **Предупреждения**). Если в атрибутах сертификата указан e-mail (Subject или SubjectAlternativeName тип RFC822) и он совпадает с e-mail зарегистрированного в JMS пользователя, то при соответствующей настройке (см. «Уведомления о событиях, связанных с использованием JMS», с. 295) данному пользователю будет отправлено уведомление по электронной почте. Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания; • **Предупреждение об окончании срока действия сертификата за ... (дней)** – за сколько дней до истечения срока действия сертификата JMS в журнале **Предупреждения** будет появляться соответствующее сообщение, а если указан e-mail (см. выше), то и высылаться уведомление по электронной почте**.**
Выявляет внешние сертификаты, не опубликованные в ресурсной системе	Выполняет анализ всех внешних сертификатов, взятых под управление, у которых в профиле *Внешние объекты* установлена опция **Опубликовать сертификат во внешнюю систему**, но которые по каким-то причинам не были опубликованы. Все выявленные сертификаты будут повторно опубликованы в ресурсную систему. Данная задача может быть задействована, например, при обновлении устаревших версий JMS, в которых публикация сертификата во внешней ресурсной системе еще не поддерживалось. **Примечание.** Под «внешней системой» подразумевается внешняя ресурсная система. В текущей версии JMS в качестве такой внешней ресурсной системы поддерживается только Active Directory. Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.

Название задачи	Описание и параметры задачи
Выявляет сертификаты с зависшим статусом, по причинам удаления ключевого носителя в системе или его перевыпуска	В рамках данной задачи будут выявлены сертификаты с «зависшим статусом», у которых связанные ключевые носители были ранее удалены. Выявленные проблемные сертификаты будут принудительно удалены путем простановки статуса Deleted и записи DeletedDate. Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания.

3.13.11 План обслуживания СКЗИ

План обслуживания СКЗИ содержит следующие задачи (Табл. 87).

Табл. 87 – План обслуживания СКЗИ

Название задачи	Описание и параметры задачи
Автоматический ввод в эксплуатацию программных СКЗИ	Позволяет автоматически вводить в эксплуатацию (см. «Рис. 291 – Жизненный цикл программного СКЗИ», с. 310) экземпляры программных СКЗИ, которые привязаны к лицензии и назначены пользователям. Задача содержит следующие параметры: • Флаг запуска задачи. Установите флаг в случае, если задача должна быть выполнена во время выполнения плана обслуживания

3.14 Уведомления о событиях, связанных с использованием JMS

Существует возможность настроить автоматическую рассылку по электронной почте уведомлений о событиях, связанных с использованием JMS. Получателями таких уведомлений могут быть пользователи и администраторы

3.14.1 Шаблоны уведомлений

Для оформления уведомлений о событиях JMS используются шаблоны - в состав JMS входит один стандартный шаблон (**Общий шаблон email-уведомлений**). Список доступных шаблонов доступен в разделе **Уведомления -> Шаблоны** консоли управления JMS (см. рис. 280).

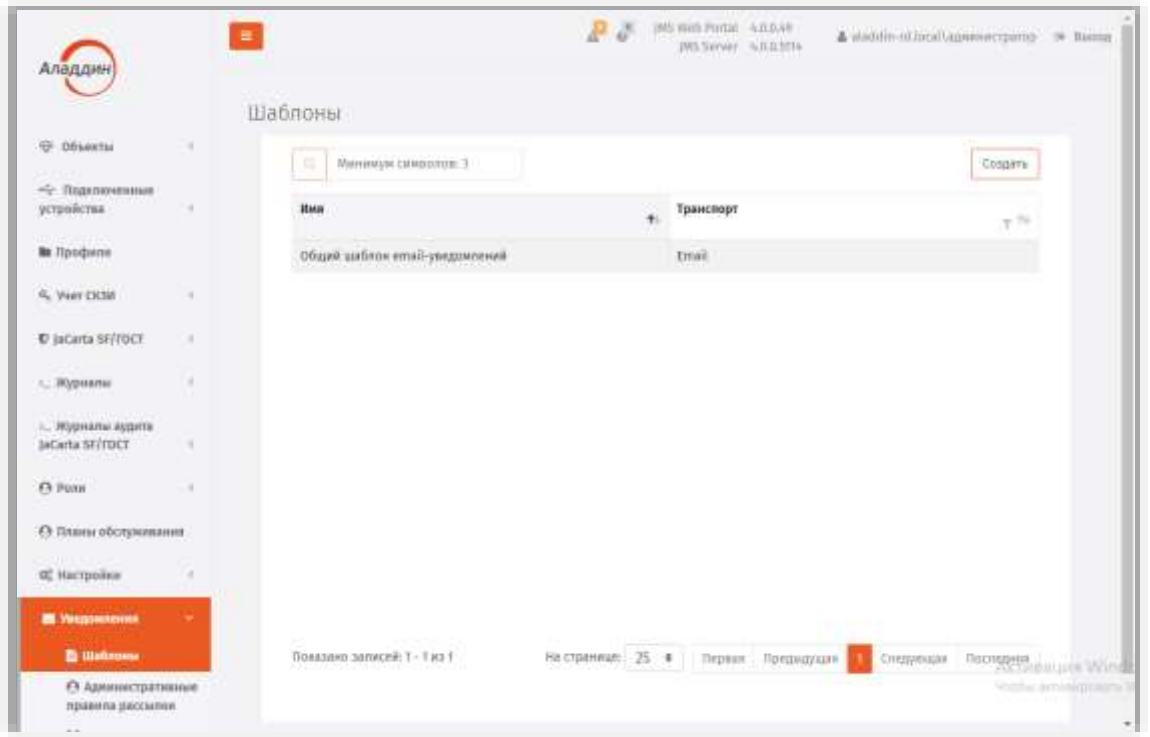


Рис. 280 – Список доступных шаблонов уведомлений

Шаблон уведомлений представляет собой HTML-файл, содержащий переменные, которые заменяются соответствующими значениями события JMS. На рис. 281 приведен стандартный шаблон из состава JMS (**Общий шаблон email-уведомлений**), отображенный в браузере.

$Message	
Класс события:	$EventMessageType
Дата события:	$EventDate
Тип события:	$EventType
Администратор:	$AdminUserName
Сообщение:	$Message
Исключение:	$Exception

Рис. 281 – Шаблон уведомлений по умолчанию

В шаблонах уведомлений о событиях JMS можно использовать шесть переменных (см. Табл. 88) – все они включены в стандартный шаблон из состава JMS (**Общий шаблон email-уведомлений**).

Табл. 88 – Переменные шаблона уведомлений

Переменная	Описание
$EventMessageType	Категория события (Журнал аудита, Предупреждения или Клиентские события).
$EventDate	Дата наступления события.
$EventType	Тип события. Возможны следующие типы событий: • **Информация**; • **Ошибка**; • **Предупреждение**; • **Критическая ошибка**.
$AdminUserName	Имя пользователя администратора, который выполнял действие, приведшие к событию.
$Message	Текст, сопровождающий событие.
$Exception	Текст исключения для событий с типом «ошибка» или «критическая ошибка».

Таким образом, для оформления уведомлений о событиях JMS вы можете:

- использовать стандартный шаблон уведомлений (**Общий шаблон email-уведомлений**), входящий в состав JMS (см. Табл. 88, с. 297);
- отредактировать стандартный шаблон уведомлений (**Общий шаблон email-уведомлений**) – для этого вам следует экспортировать стандартный шаблон (см. «Экспорт шаблона уведомлений из JMS», с. 297), внести изменения, после чего импортировать отредактированный шаблон в JMS (см. «Загрузка/замена шаблонов уведомлений в JMS», с. 298);
- создать шаблон уведомлений вручную, после чего импортировать его в JMS (см. «Загрузка/замена шаблонов уведомлений в JMS», с. 298).

По завершении подготовки шаблона уведомлений переходите к настройке параметров рассылки административных и пользовательских уведомлений – см. «Административные и пользовательские уведомления», с. 299.

3.14.1.1 Экспорт шаблона уведомлений из JMS

Чтобы экспортировать шаблон уведомлений о событиях JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Уведомления -> Шаблоны**.
2. В центральной части окна выберите шаблон, который вы хотите экспортировать, и в верхней панели нажмите **Свойства**.
3. В отобразившемся окне перейдите на вкладку **Настройки**.
4. На вкладке **Настройки** щелкните на кнопке **Экспорт** и укажите путь экспортируемого шаблона.

Теперь вы можете отредактировать экспортированный шаблон и/или загрузить его в JMS (см. «Загрузка/замена шаблонов уведомлений в JMS»).

3.14.1.2 Загрузка/замена шаблонов уведомлений в JMS

Чтобы загрузить подготовленный шаблон уведомлений в JMS или заменить уже загруженный шаблон уведомлений, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Уведомления -> Шаблоны**.
2. В зависимости от условий выберите один из следующих вариантов:

   – если вы хотите загрузить свой шаблон уведомлений в JMS, в верхнем правом углу нажмите **Создать**.
   – если вы хотите отредактировать шаблон уведомлений, уже загруженный в JMS (например, **Общий шаблон email-уведомлений**), выберите этот шаблон в таблице, нажмите правой кнопкой мыши и выберите **Свойства**.

   Отобразится страница следующего вида.

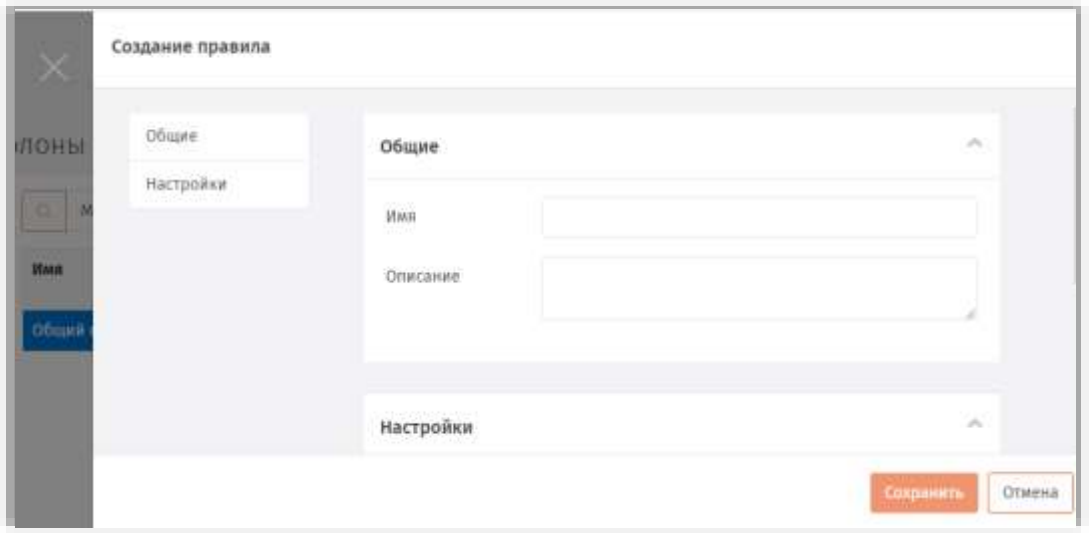


*Рис. 282 – Вкладка **Общие** окна свойств создаваемого/заменяемого шаблона уведомлений*

3. Введите/отредактируйте в соответствующих полях имя и описание создаваемого/заменяемого шаблона, после чего перейдите на вкладку **Настройки**. Страница примет следующий вид.

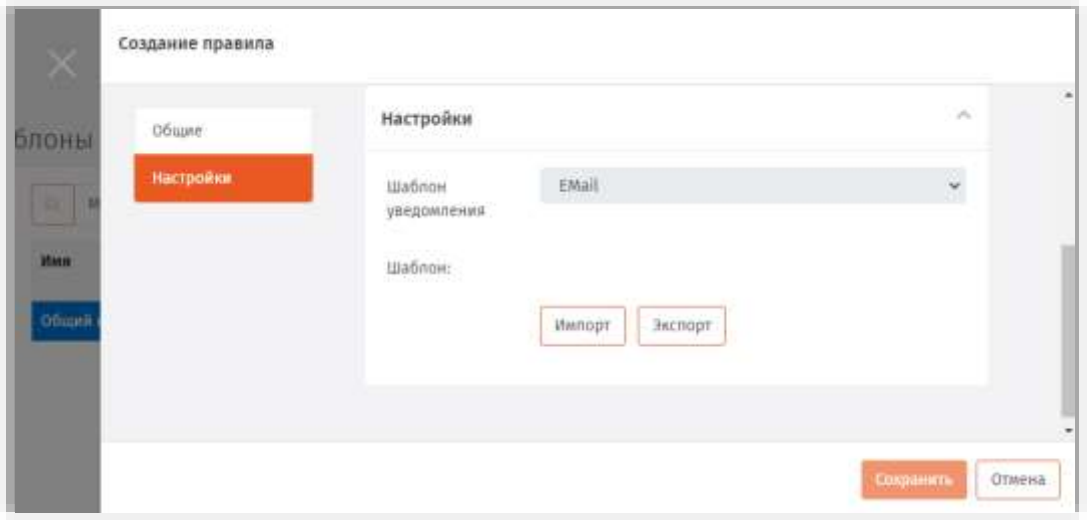


*Рис. 283 – Вкладка **Настройки** страницы свойств создаваемого/заменяемого шаблона уведомлений*

4. Чтобы загрузить новый шаблон, нажмите **Импорт**, после чего укажите путь к ранее созданному шаблону уведомлений.

Если вы заменяете уже существующий шаблон, он будет отображен в секции **Шаблон**.

Новый шаблон отобразится на странице.

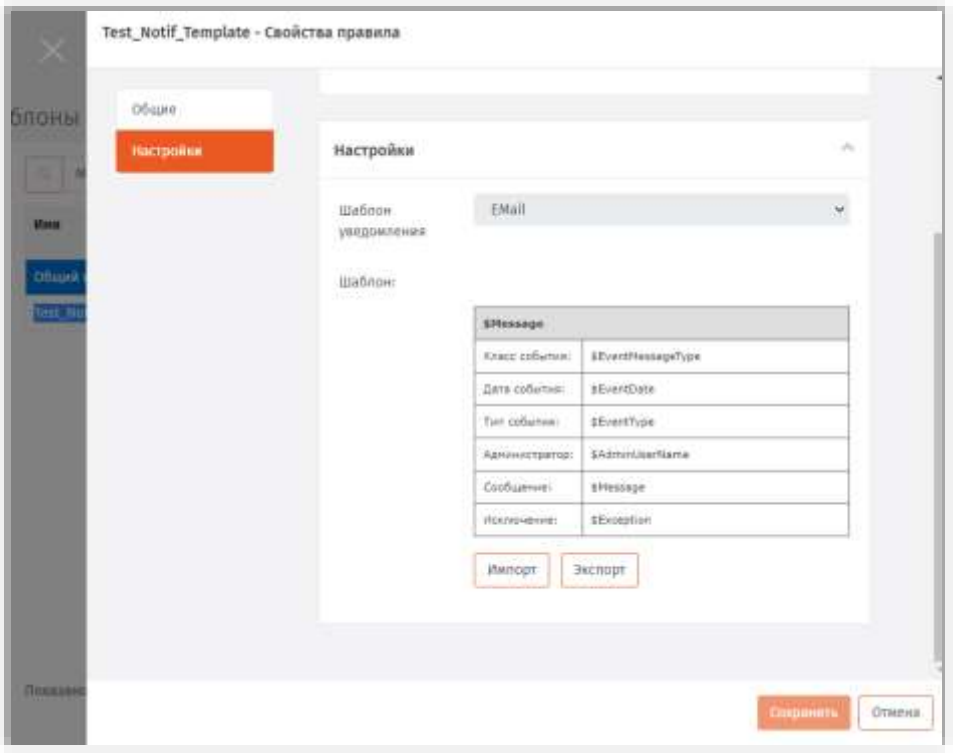


*Рис. 284 – Шаблон уведомлений отображается на вкладке **Настройки***

5. Нажмите **ОК** для завершения процедуры.

3.14.2 Административные и пользовательские уведомления

В JMS поддерживаются уведомления для следующих категорий событий:

- журнал аудита (раздел **Журналы**);
- предупреждения (раздел **Журналы**);
- клиентские события (раздел **Журналы**);
- журнал событий безопасности (раздел **Журналы аудита JaCarta SF/ГОСТ**);
- журнал попыток НСД **Журналы аудита JaCarta SF/ГОСТ**.

Так же уведомления делятся на две группы – пользовательские и административные. Пользовательские – это те уведомления, которые получает пользователь, административные – те уведомления, которые получает администратор.

Администраторы могут получать уведомления обо всех событиях, связанных с использованием JMS, тогда как список событий, о которых могут получать сообщения пользователи, ограничен.

Пользовательские уведомления относятся напрямую к конкретному пользователю – например, событие «Пользователь удален из ролей и добавлен в роли». В то же время похожее событие «В роль добавлены пользователи» относится непосредственно к роли, поэтому оно не может быть пользовательским.

Для категории событий **Журнал аудита** любое пользовательское уведомление может быть также административным (см. табл. 89).

Для событий из журнала **Клиентские события** поддерживаются только административные уведомления.

Табл. 89 – Группы уведомлений

Пользовательские уведомления	Административные уведомления
• Журнал аудита (часть событий журнала) • Предупреждения (часть событий)	• Журнал аудита (все события журнала) • Предупреждения (все события) • Клиентские события

Одно или несколько уведомлений могут быть отражены в правилах рассылки.

⚠ В правилах рассылки уведомлений, установленных в системе по умолчанию (**Административные уведомления** и **Пользовательские уведомления**), отсутствуют события, по наступлении которых отправляются уведомления. Таким образом, если вы собираетесь использовать данные правил рассылки, необходимо их отредактировать, отметив те события, по наступлении которых будут рассылаться уведомления.

Уведомления о событиях могут как рассылаться на адреса электронной почты администратора и каждого из пользователей JMS, так и одновременно передаваться для фиксации на внешний сервер журналирования событий по протоколу syslog.

3.14.2.1 Настройка административных уведомлений

Чтобы создать или отредактировать правило рассылки административных уведомлений о событиях JMS, выполните следующие действия:

1. В консоли управления JMS перейдите в раздел. **Уведомления -> Административные правила рассылки**.

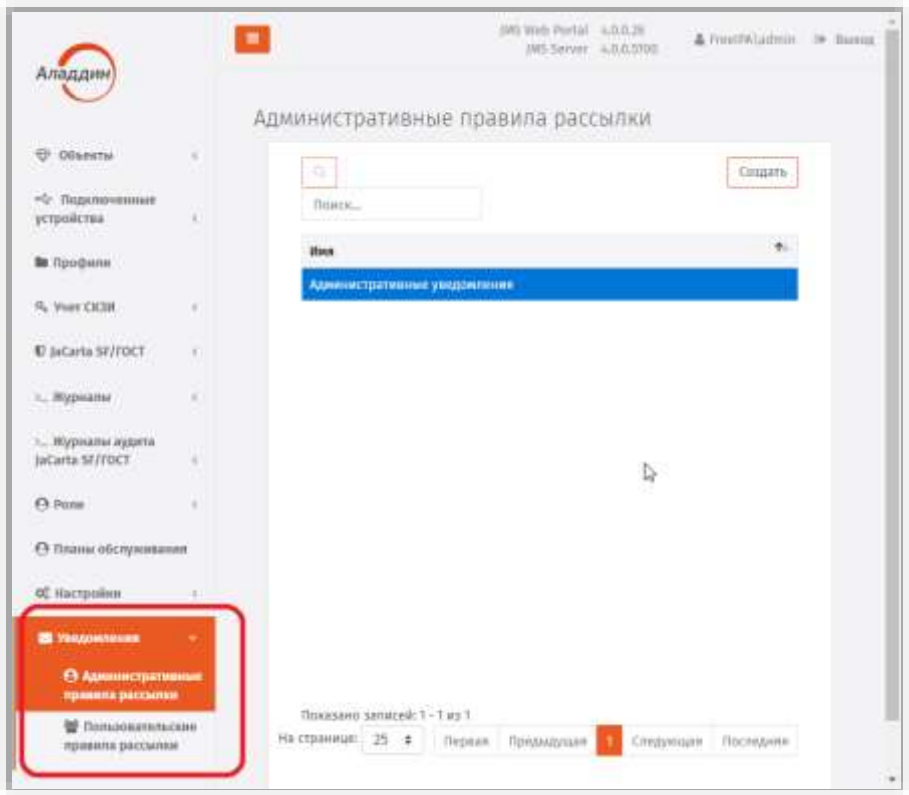


*Рис. 285 – **Уведомления** консоли управления JMS*

2. Выполните одно из следующих действий:

   – если вы хотите отредактировать существующее правило, выберите его в центральной части окна, нажмите правой кнопкой мыши и выберите **Свойства**.
   – если вы хотите создать новое правило, вверху **Создать**.

   Отобразится страница следующего вида.

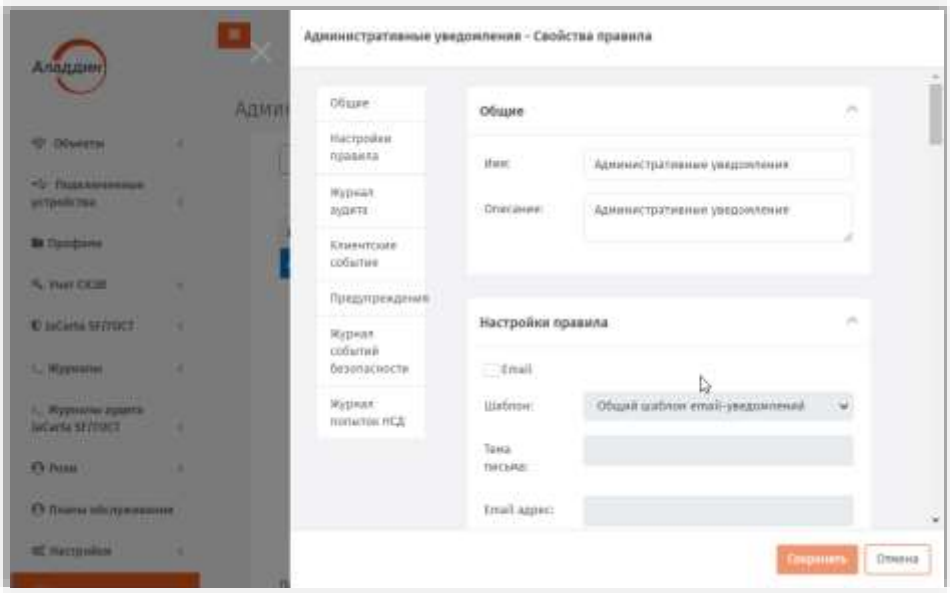


Рис. 286 –

3. На вкладке **Общие** отредактируйте имя и описание правила рассылки уведомлений в соответствующих полях, после чего перейдите на вкладку **Настройки правила**.

Страница примет следующий вид.

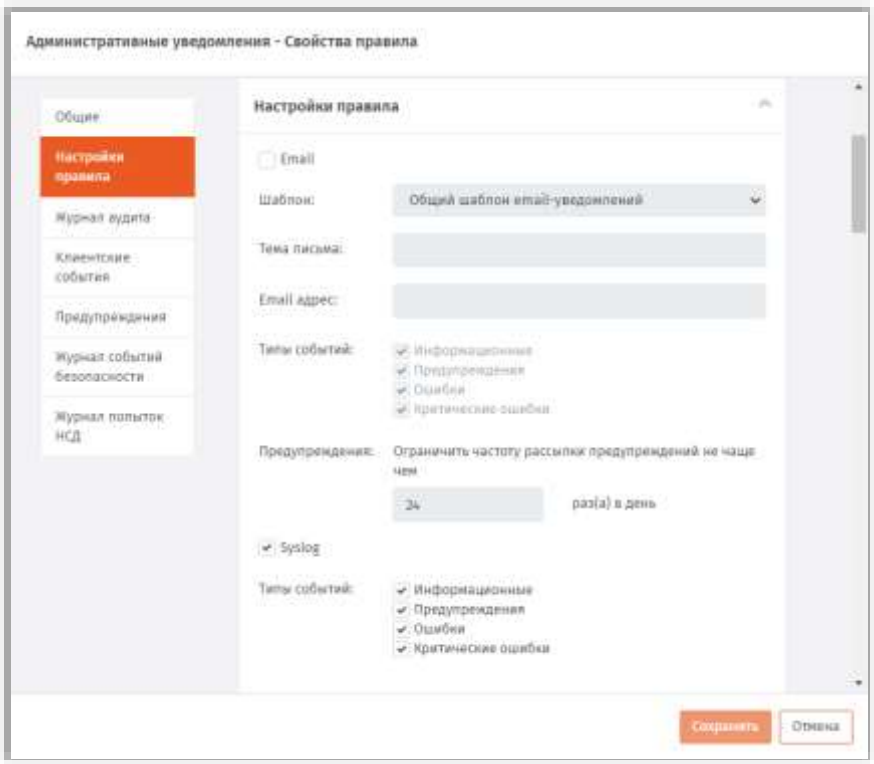


*Рис. 287 – Вкладка **Настройки правила***

4. Выполните настройку, руководствуясь табл. 90.

Табл. 90 – Настройка правила уведомлений о событиях JMS

Настройка	Описание
Секция **Email**	
Email	Установите флаг, если в качестве одного из транспортов уведомлений следует использовать электронную почту. **Примечание.** Для обеспечения работы уведомлений по электронной почте в консольном агенте JMS должен быть настроен соответствующий транспорт (см. описание команды **smtp** консольного агента Aladdin.EAP.Agent.Terminal в руководстве по установке и настройке JMS [2], раздел «Приложение 3. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal»)
Шаблон	Подготовленный шаблон уведомлений. **Примечание.** В текущей версии JMS доступен единственный предопределенный шаблон – **Общий шаблон email-уведомлений.**
Тема письма	Текст, который будет отображаться в поле **Тема** сообщения электронной почты.
Email адрес	Адрес электронной почты администратора, на который будут отправляться административные уведомления. Это поле отсутствует при настройке правил рассылки пользовательских уведомлений – адреса электронной почты пользователей берутся из ресурсной системы.

Настройка	Описание
Типы событий	Позволяет отметить, при наступлении каких типов событий будет отправляться уведомление: • **Информационные**; • **Ошибки**; • **Предупреждения**; • **Критические ошибки**.
Предупреждения	Для предупреждений можно ограничить частоту рассылки – «не чаще, чем N раз(а) в сутки». Это правило относится к однотипным событиям, при возникновении которых создается не новое предупреждение, а увеличивается счетчик количества возникновений существующего. Это может быть актуально для предупреждений, которые возникают регулярно, например, предупреждение об обращении к серверу незарегистрированной рабочей станции.
Секция **Syslog**	
Syslog	Установите флаг, если в качестве одного из транспортов уведомлений следует использовать сервер Syslog. (Флаг установлен по умолчанию) **Примечание.** Для передачи сообщений на сервер Syslog в консольном агенте JMS должен быть настроен соответствующий транспорт (см. описание команды **syslog** консольного агента Aladdin.EAP.Agent.Terminal в руководстве по установке и настройке JMS [2], раздел «Приложение 3. Справочник команд консольного агента Aladdin.EAP.Agent.Terminal»).

5. Перейдите на вкладку **Журнал аудита**.
Страница примет следующий вид.

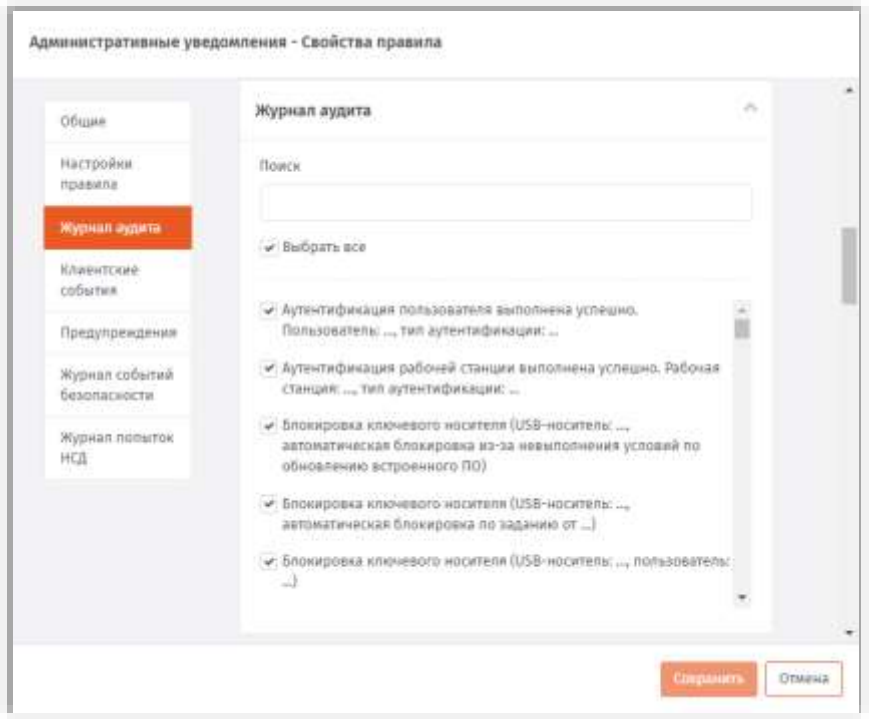


*Рис. 288 – Вкладка **Настройки правила***

6. Установите флаги напротив событий, о которых следует выполнять уведомление администратора JMS (фиксировать в журнале syslog). Чтобы отметить все события,

установите флаг напротив пункта **Выбрать все**). Для удобства можно воспользоваться фильтрацией событий по названиям с помощью поля **Поиск**.

Чтобы уведомление было отправлено, тип отмеченного события должен совпадать с одним из типов, отмеченным на вкладке **Настройки правила** (см. табл. 90, с. 302). Например, если на вкладке **Настройки правила** в поле **Типы событий** отмечено **Ошибки** и **Критическая ошибки**, а на вкладке **Журнал аудита** отмечено событие **Выпуск ключевого носителя**, то при успешном выпуске ключевого носителя уведомление о выпуске ключевого носителя отправлено не будет, т.к. тип событий **Информационные** не был отмечен. В данном случае уведомление о выпуске ключевого носителя будет отправлено, только если во время выпуска произошла ошибка или критическая ошибка.

7. Последовательно выполните настройки на вкладках

   - **Клиентские события**;
   - **Предупреждения**;
   - **Журнал событий безопасности**;
   - **Журнал попыток НСД**;

   по аналогии с тем, как была выполнена настройка на вкладке **Журнал аудита** (на шаге 6).

8. Нажмите **Сохранить**, чтобы сохранить изменения.

3.14.2.2 Настройка пользовательских уведомлений

1. В консоли управления JMS перейдите в раздел. **Уведомления -> Пользовательские правила рассылки**.

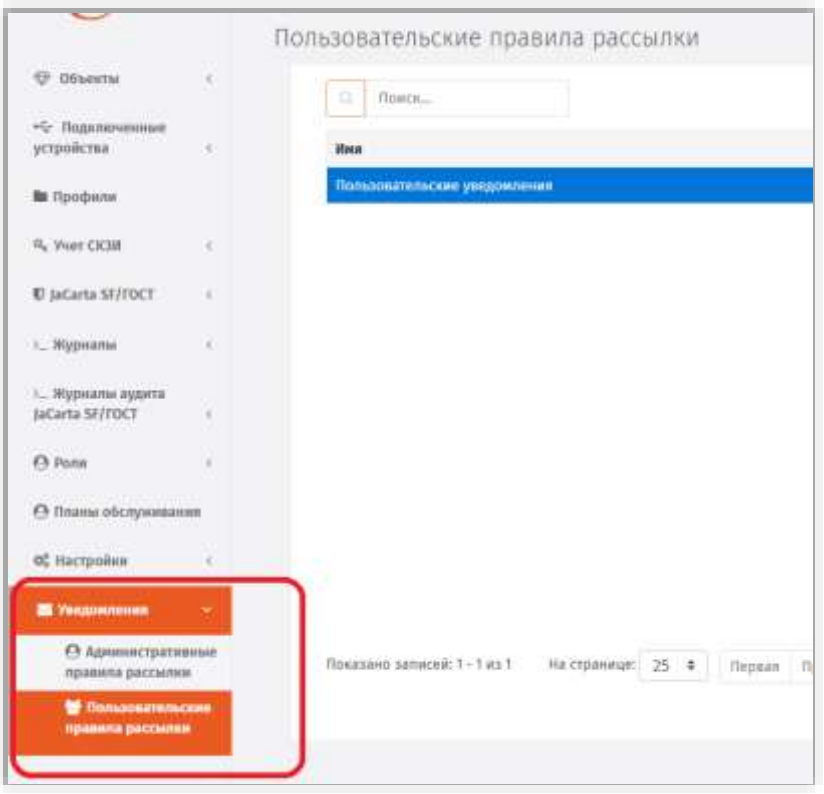


*Рис. 289 – **Уведомления –> Пользовательские правила рассылки** консоли управления JMS*

2. Выполните настройки по аналогии с тем, как они делаются для административных уведомлений (раздел «Настройка административных уведомлений», с. 300) со следующими отличиями:

   - для пользовательской рассылки доступен только e-mail-транспорт (отсутствует транспорт syslog);
   - отсутствует настройка адреса электронной почты (в качестве адреса для рассылки используется e-mail-адрес, определенный для каждого пользователя JMS в ресурсной системе, например во FreeIPA)
   - для рассылки доступны уведомления для событий только из двух типов:
     - **Журнал аудита**;
     - **Предупреждения**.

3. По окончании настройки для сохранения введенных данных нажмите **Сохранить**.

4. Взятие под управление JMS электронных ключей

JMS предоставляет возможность взять под управление электронные ключи (и объекты, содержащиеся в их памяти), выпущенные до установки и настройки JMS. Например, в организации до установки JMS имеются ключи, в память которых записаны сертификаты, выпущенные на имя пользователей с помощью удостоверяющего центра (УЦ) DogTag. Вы можете настроить параметры выпуска этих электронных ключей в JMS таким образом, чтобы они были взяты под управление без повторного выпуска сертификатов, уже содержащихся в памяти этих электронных ключей.

Примечание. Взятие под управление электронных ключей с сертификатами возможно только при условии, что JMS имеет подключение к УЦ, выпустившим данные сертификаты.

Взятие под управление может относиться к следующим типам объектов, содержащимся в памяти электронного ключа:

- сертификаты, выпущенные центром сертификации Microsoft CA;
- сертификаты, выпущенные УЦ DogTag
- сертификаты, выпущенные в режиме offline (профиль **Выпуск сертификатов (режим офлайн)**).

Чтобы взятие под контроль электронного ключа произошло без повторного выпуска объектов, необходимо соблюсти следующие условия:

1. В настройках профиля выпуска электронных ключей (см. «Настройка профиля выпуска электронных ключей», с. 97) необходимо выбрать вариант **Без инициализации** для следующих способов выпуска:

   - **Способ выпуска для консоли администратора** – если выпуск будет производиться администратором в консоли управления JMS;
   - **Способ выпуска для клиентского агента** – если выпуск будет производиться пользователем.

   ВАЖНО! ПРИ НЕСОБЛЮДЕНИИ ДАННЫХ УСЛОВИЙ ПРИ ВЫПУСКЕ ЭЛЕКТРОННОГО КЛЮЧА ВСЕ ИМЕЮЩИЕСЯ НА НЕМ ДАННЫЕ (ВКЛЮЧАЯ СЕРТИФИКАТЫ) БУДУТ УДАЛЕНЫ.

2. Также необходимо, чтобы совпадали следующие параметры (см. табл. 91 ниже), в противном случае – в память электронного ключа будет записан новый объект.

Табл. 91 – Условие взятия под управление без повторного выпуска объектов

Тип объекта	Шаблон сертификата пользователя	Атрибуты пользователя
Сертификаты, выпущенные центром сертификации Microsoft.	Шаблон сертификата пользователя, используемый при выпуске электронного ключа с помощью JMS, должен совпадать с шаблоном сертификата пользователя, использованным ранее.	Атрибуты пользователя (такие как имя пользователя, адрес электронной почты и т.п.) должны совпадать с атрибутами пользователя, на имя которого производится выпуск.
Сертификаты, выпущенные в режиме offline (профиль **Выпуск сертификатов (режим офлайн)**)	Вместо условия совпадения параметров шаблона, должно соблюдаться условие выпуска сертификата пользователя удостоверяющим центром, сертификат которого явно указан на вкладке **Взятие под управление** окна настройки профиля **Выпуск сертификатов (режим офлайн)** (при этом в хранилище сертификатов сервера JMS, в разделе доверенных корневых сертификатов, должна быть загружена цепочка сертификатов, необходимая для проверки сертификата УЦ)	

3. При выпуске электронного ключа необходимо предъявить PIN-код пользователя электронного ключа.

5. Регистрация в JMS сертификатов сторонних УЦ (внешних объектов)

JMS позволяет регистрировать и вести учет электронных ключей с записанными в их память внешними объектами (сертификатами, выпущенными сторонними УЦ). После такой регистрации JMS отслеживает срок действия данных сертификатов и уведомляет об их истечении.

Для регистрации в JMS электронного ключа с находящимся на нем сертификатом, выпущенным сторонним УЦ, необходимо выполнить следующие действия:

1. Сохранить корневой сертификат УЦ и все промежуточные сертификаты УЦ цепочки сертификатов (включая сертификат издающего УЦ) в доверенные корневые центры (Trusted Root) на сервер JMS (или на все узлы кластера серверов JMS, если развернут кластер).

Данные сертификаты УЦ (корневой и цепочка сертификатов) используется только для получения дополнительного критерия отбора внешних объектов (проверки выпуска внешнего объекта конкретным УЦ). Если такой критерий отбора не требуется, данный шаг (сохранение сертификатов УЦ) можно не выполнять.

2. Зарегистрировать в JMS пользователя, для которого будет выпущен электронный ключ.
3. Создать, настроить и привязать профиль **Внешние объекты** к пользователю JMS. Подробнее см. раздел «Создание и настройка профиля Внешние объекты», с. 151.
4. Создать новый или настроить имеющийся профиль **Выпуск ключевых носителей** для выпускаемого электронного ключа и привязать его к пользователям. Подробнее см. разделы «Настройка профиля выпуска электронных ключей», с. 97; «Привязка профилей», с. 195.

Важно! В настройках профиля выпуска электронных ключей для обоих способов выпуска (**Способ выпуска для консоли администратора** и **Способ выпуска для клиентского агента**) следует выбрать вариант **Без инициализации**, В ПРОТИВНОМ СЛУЧАЕ ПРИ ВЫПУСКЕ ЭЛЕКТРОННОГО КЛЮЧА ВСЕ ИМЕЮЩИЕСЯ НА НЕМ ДАННЫЕ (ВКЛЮЧАЯ СЕРТИФИКАТЫ) БУДУТ УДАЛЕНЫ.

5. Подключить электронный ключ к компьютеру.
6. Зарегистрировать и выпустить электронный ключ. Подробнее см. «Выпуск ЭК/ЗНИ администратором», с. 39.

Если электронный ключ выпускается из клиента JMS, то при выпуске и синхронизации электронного ключа внешний объект также будет зарегистрирован в JMS. Таким образом, возможно регистрировать в JMS внешние объекты, как из консоли управления JMS, так и из интерфейса клиента JMS.

6. Примеры управления СКЗИ

6.1 Порядок управления ключевым носителем как аппаратным СКЗИ

Ключевой носитель (КН) может интерпретироваться в JMS как аппаратное СКЗИ только в случае, если в нем установлено сертифицированное криптографическое приложение.

В текущей реализации JMS в качестве аппаратных СКЗИ поддерживаются электронные ключи компании Аладдин (обозначения приложения в JMS – **ГОСТ**, **ГОСТ 2**).

Все операции над ключевыми носителями как аппаратными СКЗИ осуществляются в разделах **Объекты -> Ключевые носители** или **Подключенные устройства -> Ключевые носители** консоли управления JMS. При этом статус такого СКЗИ можно отслеживать в разделе **Учет СКЗИ** -> **Экземпляры СКЗИ**.

Управление *КН как СКЗИ* осуществляется в соответствии с жизненным циклом, изображенным на Рис. 290.

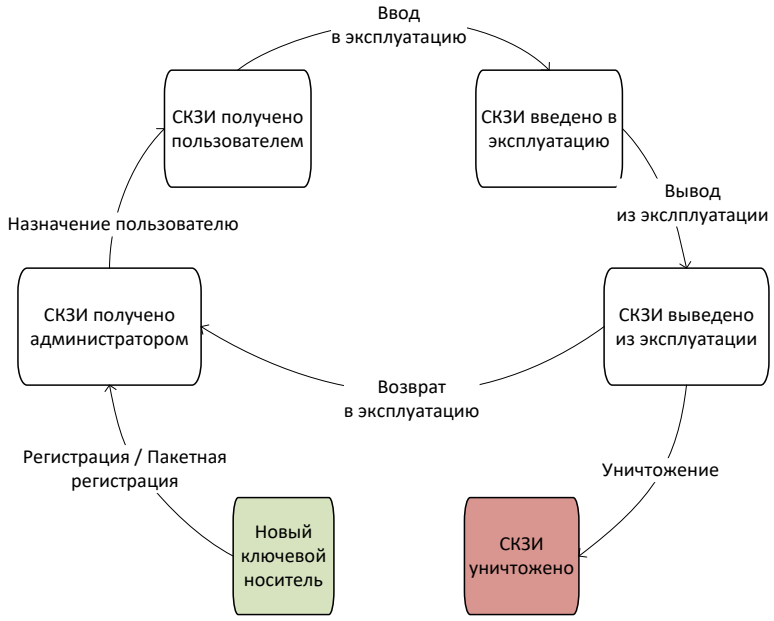


Рис. 290 – Жизненный цикл ключевого носителя как аппаратного СКЗИ

В настоящем примере все операции управления жизненным циклом *КН как СКЗИ* выполняются из консоли управления JMS с непосредственным подключением ключевого носителя к компьютеру консоли.

Часть операций управления жизненным циклом *КН как СКЗИ* (в частности, *назначение пользователю, ввод в эксплуатацию* и *вывод из эксплуатации*) можно также выполнить из клиентского агента.

6.1.1 Порядок регистрации КН-СКЗИ

Чтобы зарегистрировать *КН как СКЗИ* выполните следующие действия:

1. Подключите КН к компьютеру, на котором запущена консоль управления JMS.
2. В консоли управления JMS в разделе **Подключенные устройства -> Ключевые носители** выберите КН в списке подключенных устройств и выполните действия по его регистрации (подробнее см. в «Регистрация подсоединенных ЭК/ЗНИ в JMS», с. 30). В процессе выполнения мастера регистрации в поле **Номер СКЗИ** следует ввести регистрационный номер СКЗИ в соответствии с паспортом данного СКЗИ.

В результате регистрации:

- экземпляру СКЗИ будет присвоен статус **Получен администратором** (статус СКЗИ можно проверить в разделе **Учет СКЗИ** -> **Экземпляры СКЗИ**);
- в JMS будет автоматически сгенерирован нормативный документ «Акт получения СКЗИ администратором» (см. раздел «Нормативная документация», с. 242)

Регистрация КН некоторых типов (в частности, всех электронных ключей производства компании Аладдин с установленным приложением ГОСТ) в JMS в качестве СКЗИ может быть выполнена также в пакетном режиме (см. раздел «Импорт (пакетная регистрация) ЭК/ЗНИ в JMS», с. 32). Для этого следует использовать файл пакетной регистрации в формате XML, поставляемый производителем. Такой файл уже содержит регистрационные номера СКЗИ для всех импортируемых КН.

6.1.2 Порядок назначения КН-СКЗИ пользователю

Для назначения *КН как СКЗИ* пользователю в разделе **Подключенные устройства -> Ключевые носители** выберите необходимый КН (уже зарегистрированный как СКЗИ) и в верхней панели нажмите **Назначить пользователю** (подробнее см. «Назначение / отмена назначения ЭК/ЗНИ пользователю», с . 35).

В результате назначения:

- экземпляру СКЗИ будет присвоен статус **Получен пользователем**;
- в JMS будет автоматически сгенерирован нормативный документ «Акт передачи СКЗИ новому ответственному пользователю».

6.1.3 Порядок ввода КН-СКЗИ в эксплуатацию

Для ввода *КН как СКЗИ* в эксплуатацию в разделе **Подключенные устройства -> Ключевые носители** выберите подключенный к компьютеру КН и вверху страницы нажмите **Выпустить** (или **Зарегистрировать и выпустить**, если КН еще не зарегистрирован, подробнее см. «Выпуск ЭК/ЗНИ администратором», с. 39).

В результате ввода СКЗИ в эксплуатацию:

- экземпляру СКЗИ будет присвоен статус **Введен в эксплуатацию**;
- в JMS будет автоматически сгенерирован нормативный документ «Акт ввода СКЗИ в эксплуатацию».

Примечания:

1. В случае если электронный ключ еще не зарегистрирован в JMS (или зарегистрирован, но не назначен пользователю), он также может быть введен в эксплуатацию как СКЗИ из консоли управления JMS путем выпуска, см. «Выпуск ЭК/ЗНИ администратором», с. 39 (регистрацию КН как СКЗИ и его назначение пользователю следует произвести в процессе выпуска).
2. КН, зарегистрированный в JMS как СКЗИ, может быть введен в эксплуатацию также путем его выпуска из клиента JMS аутентифицировавшимся пользователем (т.е. открывшим сеанс работы с JMS). Для этого клиенту JMS (клиентскому агенту) должен быть разрешен выпуск электронного ключа (см. разделы «Настройка профиля клиентского агента», с. 101 и «Привязка профилей», с. 195)

6.1.4 Порядок вывода КН-СКЗИ из эксплуатации

Для вывода *КН как СКЗИ* из эксплуатации в разделе **Подключенные устройства -> Ключевые носители** выберите необходимый КН, вверху страницы нажмите **Вывод из эксплуатации** и выберите **Отозвать** (подробнее см. «Отзыв ЭК/ЗНИ », с . 50).

В результате вывода СКЗИ из эксплуатации:

- экземпляру СКЗИ будет присвоен статус **Выведен из эксплуатации**;
- в JMS будет автоматически сгенерирован нормативный документ «Акт вывода СКЗИ из эксплуатации».

КН как СКЗИ после вывода из эксплуатации может быть уничтожен (см. «Порядок уничтожения КН-СКЗИ», ниже) или возвращен в эксплуатацию (см. «Порядок возврата КН-СКЗИ в эксплуатацию», ниже).

6.1.5 Порядок возврата КН-СКЗИ в эксплуатацию

Для возврата *КН как СКЗИ* в эксплуатацию в разделе **Объекты -> Ключевые носители** выберите выведенный из эксплуатации КН (в данном разделе статус отображается как **Отозван**), нажмите на нем правой кнопкой мыши и выберите **Вернуть в эксплуатацию** (подробнее см. «Возврат в эксплуатацию ЭК/ЗНИ », с. 57).

В результате возврата СКЗИ в эксплуатацию:

- экземпляру СКЗИ будет присвоен статус **Получен администратором** (т.е. СКЗИ возвращается на этап жизненного цикла «СКЗИ получено администратором» согласно Рис. 290, с. 308);
- в JMS будет автоматически сгенерирован нормативный документ «Акт получения СКЗИ администратором».

6.1.6 Порядок уничтожения КН-СКЗИ

В случае уничтожения *КН как СКЗИ* (т.е. его физического разрушения согласно правилам пользования соответствующего СКЗИ) в JMS следует произвести *настоящую* операцию.

Важно! Перед тем как уничтожить *КН как СКЗИ,* его следует вывести из эксплуатации (см. «Порядок вывода КН-СКЗИ из эксплуатации», выше).

Чтобы уничтожить *КН как СКЗИ,* в разделе или **Объекты -> Ключевые носители** выберите КН, предварительно выведенный из эксплуатации, нажмите на нем правой кнопкой мыши и выберите **Удалить** (подробнее см. «Удаление ЭК/ЗНИ», с. 62).

В результате уничтожения СКЗИ:

- экземпляру СКЗИ будет присвоен статус **Уничтожен**;
- в JMS будет автоматически сгенерирован нормативный документ «Акт об уничтожении СКЗИ».

Учетная запись уничтоженного СКЗИ остается в JMS (данную запись невозможно удалить).

Для отображения всех уничтоженных СКЗИ в разделе **Учет СКЗИ** -> **Экземпляры СКЗИ** вверху страницы следует нажать **Показывать уничтоженные**.

Учетный номер уничтоженного СКЗИ (поле **Номер**) не может быть использован в дальнейшем при регистрации новых СКЗИ.

6.2 Порядок управления программным СКЗИ

Управление программным СКЗИ осуществляется в соответствии с жизненным циклом, изображенным на Рис. 291.

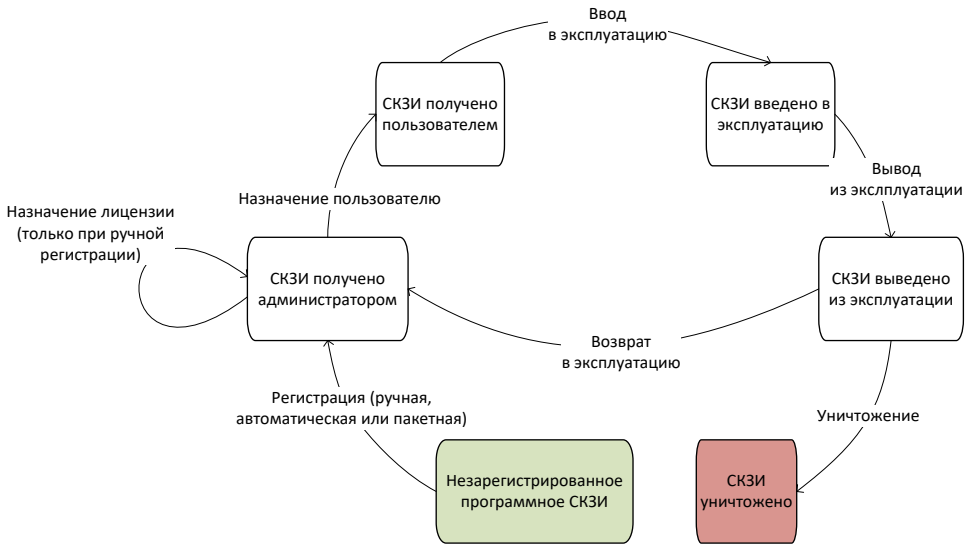


Рис. 291 – Жизненный цикл программного СКЗИ

Все операции над программным СКЗИ и отслеживание его статуса осуществляются в разделе **Учет СКЗИ -> Экземпляры СКЗИ** консоли управления JMS.

6.2.1 Порядок регистрации программного СКЗИ

Для регистрации программного СКЗИ можно воспользоваться одним из перечисленных ниже способов.

Ручная регистрация программных СКЗИ

Чтобы зарегистрировать программное СКЗИ вручную в консоли управления JMS в разделе **Учет СКЗИ -> Экземпляры СКЗИ** необходимо выполнить следующие действия**:**

1. Вверху страницы нажмите **Зарегистрировать** и выполните необходимые действия по регистрации (подробнее см. в «Регистрация экземпляра СКЗИ», с. 221).
2. В списке экземпляров СКЗИ выберите только что зарегистрированное СКЗИ, нажмите на нем правой кнопкой мыши и выберите **Назначить лицензию СКЗИ** (подробнее см. в разделе «Лицензия», с. 223).

Примечание. Ручная регистрация из раздела **Учет СКЗИ** -> **Экземпляры СКЗИ** недоступна для программных СКЗИ типа КриптоПРО CSP. Их регистрация осуществляется только в автоматическом или пакетном режиме, см. ниже.

Автоматическая регистрация программных СКЗИ с опцией Автосоздание

В случае если у типа программного СКЗИ установлена опция **Автосоздание экземпляров СКЗИ** (см. раздел «Типы СКЗИ», с. 212), при регистрации его лицензии в консоли администрирования JMS (см. в раздел «Регистрация лицензии СКЗИ», с. 233), будет автоматически зарегистрирован экземпляр СКЗИ с учетным номером, идентичным номеру зарегистрированной лицензии.

Пакетная регистрация программных СКЗИ с опцией Автосоздание

В случае если у типа программного СКЗИ установлена опция **Автосоздание экземпляров СКЗИ** (см. раздел «Типы СКЗИ», с. 212), при пакетной регистрации лицензий СКЗИ такого типа (см. раздел «Импорт лицензий (пакетная регистрация)», с. 235), будут автоматически зарегистрированы экземпляры СКЗИ с учетными номерами, идентичными номерам зарегистрированных лицензий. Формат CSV-файла для пакетной регистрации приведен в разделе «Формат файлов импорта лицензий СКЗИ», с. 235.

В результате регистрации (любыми из перечисленных выше способов) программного СКЗИ:

- экземпляру СКЗИ будет присвоен статус **Получен администратором** (статус СКЗИ можно проверить в разделе **Учет СКЗИ** -> **Экземпляры СКЗИ**);
- в JMS будет автоматически сгенерирован нормативный документ «Акт получения СКЗИ администратором» (см. раздел «Нормативная документация», с. 242). В случае пакетной регистрации в одном документе будут перечислены все зарегистрированные СКЗИ.

6.2.2 Порядок назначения программного СКЗИ пользователю

Для назначения программного СКЗИ пользователю в разделе **Учет СКЗИ -> Экземпляры СКЗИ** выберите необходимый экземпляр СКЗИ со статусом *Получен администратором*, нажмите на нем правой кнопкой мыши и в контентном меню выберите **Назначить ответственное лицо** (подробнее см. «Назначить ответственное лицо», с . 224).

В случае если инсталлированное на рабочей станции программное СКЗИ было зарегистрировано в JMS автоматически (см. «Порядок регистрации программного СКЗИ», выше), его назначение пользователю, первому открывшему пользовательский сеанс работы клиента JMS на данной рабочей станции (после такой автоматической регистрации СКЗИ), также будет выполнено автоматически.

В результате назначения:

- экземпляру СКЗИ будет присвоен статус *Получен пользователем*;
- в JMS будет автоматически сгенерирован нормативный документ «Акт передачи СКЗИ новому ответственному пользователю».

6.2.3 Порядок ввода программного СКЗИ в эксплуатацию

Для ввода программного СКЗИ в эксплуатацию в разделе **Учет СКЗИ -> Экземпляры СКЗИ** выберите необходимый экземпляр СКЗИ со статусом *Получен пользователем* , нажмите на нем правой кнопкой мыши и в контекстном меню выберите **Ввести в эксплуатацию** (подробнее см. «Ввести в эксплуатацию», с . 224).

В результате ввода СКЗИ в эксплуатацию:

- экземпляру СКЗИ будет присвоен статус **Введен в эксплуатацию**;
- в JMS будет автоматически сгенерированы следующие нормативные документы:
  - «Акт установки СКЗИ»;
  - «Акт ввода СКЗИ в эксплуатацию»;
  - «Акт передачи лицензии ответственному лицу».

6.2.4 Порядок вывода программного СКЗИ из эксплуатации

Для вывода программного СКЗИ из эксплуатации в разделе **Учет СКЗИ -> Экземпляры СКЗИ** выберите необходимый экземпляр СКЗИ со статусом *Введен в эксплуатацию*, нажмите на нем правой кнопкой мыши и в контекстном меню выберите **Вывести из эксплуатации** (подробнее см. «Вывести из эксплуатации», с . 225).

В результате вывода из эксплуатации:

- экземпляру СКЗИ будет присвоен статус **Выведен из эксплуатации**;
- в JMS будет автоматически сгенерированы следующие нормативные документы:
  - «Акт передачи лицензии ответственному лицу»;
  - «Акт получения СКЗИ администратором»;
  - «Акт вывода СКЗИ из эксплуатации».

Программное СКЗИ после вывода из эксплуатации может быть уничтожено (см. «Порядок уничтожения программного СКЗИ», ниже) или возвращено в эксплуатацию (см. «Порядок возврата программного СКЗИ в эксплуатацию», ниже).

6.2.5 Порядок возврата программного СКЗИ в эксплуатацию

Для возврата программного СКЗИ в эксплуатацию в разделе **Учет СКЗИ -> Экземпляры СКЗИ** выберите необходимый экземпляр СКЗИ со статусом *Выведен из эксплуатации,* нажмите на нем правой кнопкой мыши и в контекстном меню выберите **Вернуть в эксплуатацию** (подробнее см. «Вернуть в эксплуатацию», с . 226).

В результате возврата СКЗИ в эксплуатацию:

- экземпляру СКЗИ будет присвоен статус **Получен администратором** (т.е. СКЗИ возвращается на этап жизненного цикла «СКЗИ получено администратором» согласно рис. Рис. 291, с. 310);
- в JMS будет автоматически сгенерирован нормативный документ «Акт получения СКЗИ администратором».

6.2.6 Порядок уничтожения программного СКЗИ

В случае уничтожения программного СКЗИ (т.е. его физического разрушения согласно правилам пользования соответствующего СКЗИ) в JMS следует произвести *настоящую* операцию.

Важно! Перед тем как уничтожить программное СКЗИ, его следует вывести из эксплуатации (см. «Порядок вывода программного СКЗИ из эксплуатации», выше).

Чтобы уничтожить программное СКЗИ, в разделе **Учет СКЗИ -> Экземпляры СКЗИ** выберите экземпляр программного СКЗИ со статусом *Выведен из эксплуатации,* нажмите на нем правой

кнопкой мыши и в контекстном меню выберите **Уничтожить** (подробнее см. в разделе «Уничтожить», с. 226).

В результате уничтожения СКЗИ:

- экземпляру СКЗИ будет присвоен статус **Уничтожен**;
- в JMS будет автоматически сгенерирован нормативный документ «Акт об уничтожении СКЗИ».

Учетная запись уничтоженного СКЗИ остается в JMS (данную запись невозможно удалить).

Для отображения всех уничтоженных СКЗИ в разделе **Учет СКЗИ** -> **Экземпляры СКЗИ** в верхней панели следует нажать **Показывать уничтоженные**.

Учетный номер уничтоженного СКЗИ (поле **Номер**) не может быть использован в дальнейшем при регистрации новых СКЗИ.

6.3 Управление учетом СКЗИ

JMS позволяет выполнять операции над учетной записью экземпляра СКЗИ (прекращение/возобновление учета и удаление самой записи) после его регистрации в системе на всех этапах жизненного цикла до уничтожения СКЗИ (см. Рис. 290, с. 308 и Рис. 291, с. 310). Функция управления учетом (включая удаление учетной записи) может быть использована, например, в случае ошибочной регистрации СКЗИ.

Прекращение учета экземпляра СКЗИ. Чтобы прекратить учет СКЗИ, в разделе **Учет СКЗИ** -> **Экземпляры СКЗИ** выберите в списке необходимый экземпляр СКЗИ, нажмите на нем правой кнопкой мыши и выберите **Прекратить учет** в контекстном меню. В окне подтверждения действия нажмите **Да**. Выбранный экземпляр СКЗИ приобретет статус *Учет прекращен* (отражается в столбце **Состояние**).

Возобновление учета экземпляра СКЗИ. Чтобы возобновить учет СКЗИ, в разделе **Учет СКЗИ** -> **Экземпляры СКЗИ** выполните следующие действия.

1. Выберите в списке экземпляр СКЗИ со статусом *Учет прекращен* (для этого нужно включить фильтр **Показать неучитываемые** над таблицей).
2. Нажмите на нем правой кнопкой мыши и выберите **Возобновить учет** в контекстном меню.
3. В окне подтверждения действия нажмите **Да**.

Выбранный экземпляр СКЗИ приобретет статус, который он имел до прекращения учета (например, *Получен администратором*).

Удаление учетной записи экземпляра СКЗИ. Для удаления учетной записи экземпляра СКЗИ в разделе **Учет СКЗИ** -> **Экземпляры СКЗИ** выберите в списке необходимый экземпляр СКЗИ со статусом *Учет прекращен*, нажмите не нем правой кнопкой мыши, в контекстном меню выберите **Удалить учетную запись,** В окне подтверждения действия нажмите **Да**. Учетная запись данного экземпляра СКЗИ будет удалена из базы данных JMS.

Примечание. Удаление из JMS учетной записи экземпляра СКЗИ со статусом *Уничтожен* невозможно.

7. Журналы

Раздел **Журналы** консоли управления содержит журналы событий, происходящих с объектами учета системы JMS, а также отчеты планов обслуживания самой системы JMS.

Примечание. Помимо журналов событий, отображаемых в интерфейсе JMS и описанных в настоящем разделе, ведутся также файловые журналы диагностики работы самой системы JMS. Состав данных журналов описан в руководстве по установке и настройке JMS [2], в разделе «Журналы диагностики JMS»

Консоль управления JMS предоставляет администратору следующие типы журналов событий в JMS

- **Журнал аудита**;

- **Клиентские события**;
- **Предупреждения**;
- **Отчеты планов обслуживания**.

Во всех типах журналов доступны следующие инструменты управления.

1. Фильтрация по полю **Описание**.
   Во всех журналах доступна фильтрация по полю **Описание**. Для фильтрации записей введите строку, которую должно содержать поле **Описание**, начиная с первого символа.

2. Фильтрация по временным периодам.
   При просмотре событий существует возможность применения следующих временных фильтров для удобства просмотра событий за установленный промежуток времени:

   - **1 час**;
   - **24 часа**;
   - **7 дней**;
   - **30 дней**;
   - **Сегодня**;
   - **Неделя**;
   - **Месяц**;
   - **Произвольный период** (позволяет задать период отображения вручную);
   - **Все**.

3. Фильтрация по отдельным полям.

   Некоторые поля в таблицах содержат значок фильтрации ( ), при нажатии на который можно выбрать категорию значения в данном поле для фильтрации записей (), по которой можно фильтровать (Рис. 292).

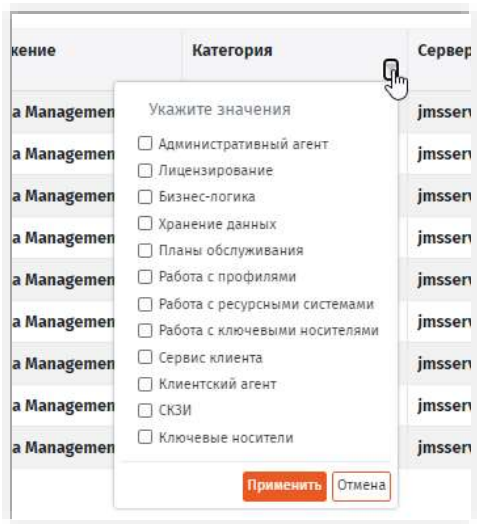


Рис. 292 – Фильтрация записей журнала по значениям выбранного поля

4. Чтобы настроить состав столбцов таблицы событий нажмите в заголовочной части таблицы правой кнопкой мыши и выберите пункт **Выбрать столбцы**:

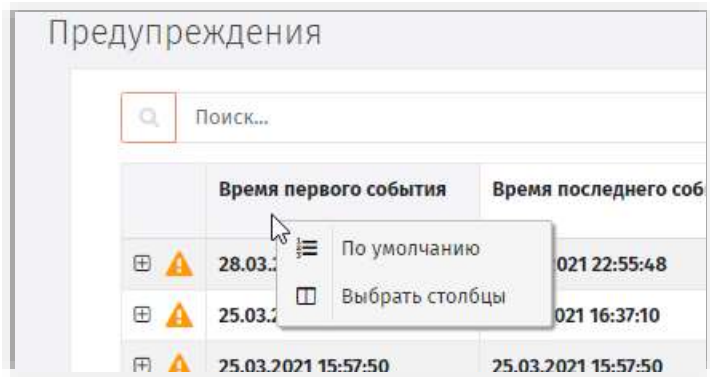


Рис. 293 – Вызов настройки состава столбцов таблицы событий

В появившемся интерфейсе настройте состав столбцов для отображения с помощью флажков слева:

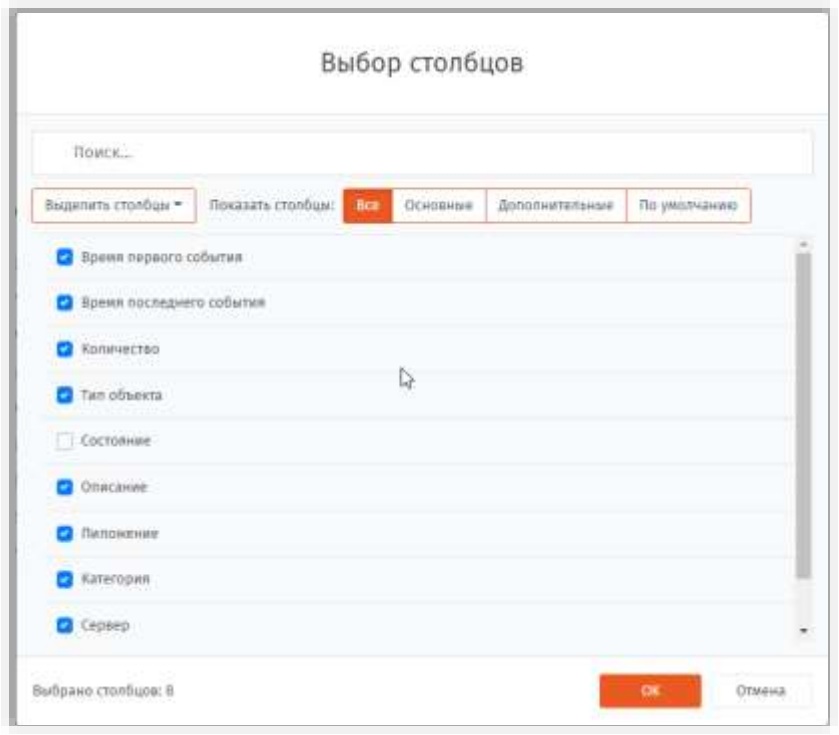


Рис. 294 – Выбор столбцов для отображения

Чтобы вернуть состав столбцов к исходному состоянию нажмите кнопку вверху **По умолчанию**.

5. Чтобы получить подробную информацию о событии, в первом столбце нажмите на значок ⊞. При этом откроется полный состав информации о выбранном событии.

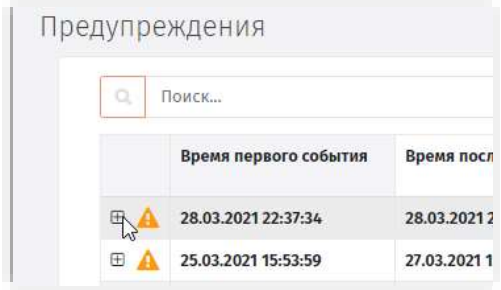


Рис. 295 – Выбор записи для раскрытия ее детализации

7.1 Журнал аудита: специальные средства управления

В Журнале аудита предоставляется возможность фильтрования событий по типу:

- **Все события**
- **Успешные**
- **Предупреждения**
- **Ошибки**
- **Фатальные**

Кроме того, предоставляются возможности:

- сортировка по полю **Время события**;
- фильтрация событий по полю **Категория**.

7.2 Клиентские события: специальные средства управления

Записи в журнале клиентских событий можно сортировать по столбцу **Время события**.

7.3 Предупреждения: специальные средства управления

Записи в журнале **Предупреждения** можно:

- сортировать по полю **Время последнего события**;
- фильтровать по полям **Типа объекта** и **Категория**.

7.4 Отчеты планов обслуживания: специальные средства управления

Записи в журнале **Отчеты планов обслуживания** можно сортировать по полям:

- **Дата запуска**
- **Дата завершения**
- **Кол-во ошибок**
- **Кол-во критических ошибок**
- **Сервер**

8. Журналы аудита JaCarta SF/ГОСТ

Для хранения и просмотра событий, регистрируемых в электронных ключах (электронных носителях – ЭН) JaCarta SF/ГОСТ, в консоли управления JMS предусмотрен специальный раздел – **Журналы аудита JaCarta SF/ГОСТ**.

События, отображаемые в разделе **Журналы аудита JaCarta SF/ГОСТ**, соответствуют событиям, фиксируемым во внутренней памяти ЭН JaCarta SF/ГОСТ. Описание системы журналирования в ЭН JaCarta SF/ГОСТ см. в документации из комплекта их поставки.

Записи о событиях загружаются из памяти ЭН JaCarta SF/ГОСТ в JMS автоматически при каждой синхронизации данных ЭН (как из консоли администрирования, так и из клиента JMS). При каждой такой загрузке журналы, хранимые в памяти ЭН, очищаются.

8.1 Просмотр журналов и фильтрация записей по полям

При просмотре журналов событий в разделе **Журналы аудита JaCarta SF/ГОСТ** пользователю предоставляется возможность выполнять выборочный анализ информации, в частности:

- сортировка записей по полю **Дата события** (путем нажатия на ячейку с названием поля);
- отбор непрочитанных сообщений (кнопка **Показывать только непрочитанные** над таблицей);
- фильтрация по типу события (доступны опции **Все**, **Критическая информация**, **Предупреждения**, **Информация**);
- фильтрация по периоду (кнопки **Все**, **1 Час**, **Произвольный период** и др.);
- поиск-фильтрация по текстовым полям, таким как **Владелец USB-носителя** или **Организация**, с использование панели поиска (значок );
- фильтрация по полю **Цвет USB-носителя** (подробнее см. ниже).

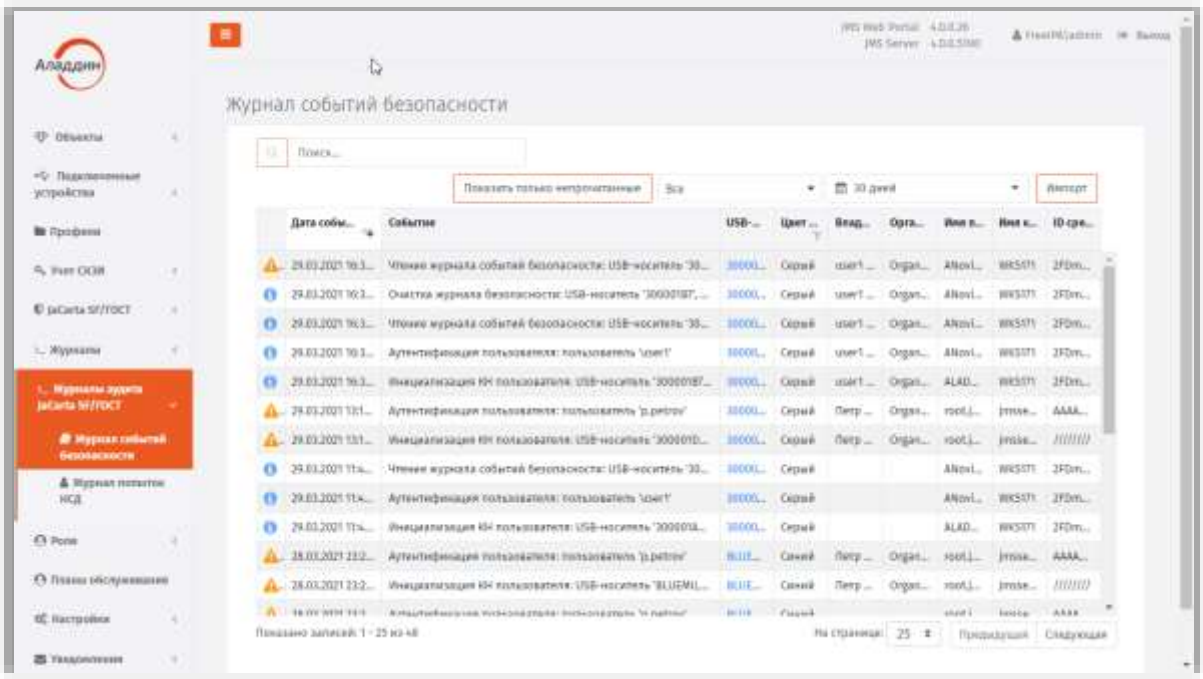


*Рис. 296 – Содержимое раздела **Журнал аудита JaCarta SF/ГОСТ -> Журнал событий** безопасности в консоли управления JMS*

Для фильтрации событий по полю **Цвет USB-носителя** следует нажать на значок фильтра в заголовке поля, выбрать необходимые пункты в раскрывающемся списке и нажать **Применить**:

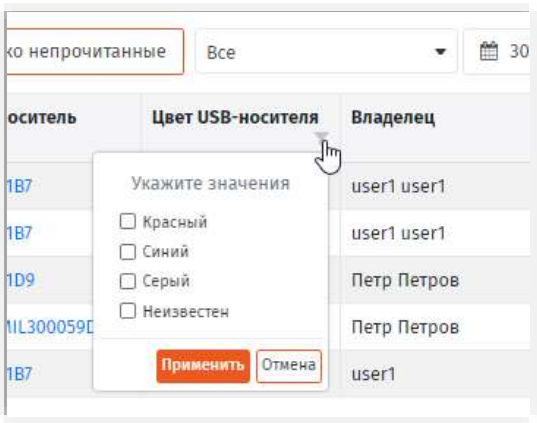


Рис. 297 – Установка фильтра на поле таблицы

8.2 Импорт журналов аудита JaCarta SF/ГОСТ

ЗНИ (ЭН) JaCarta SF/ГОСТ предполагают возможность выгрузки хранящихся в них журналов событий в виде файлов (подробнее см. документацию из комплекта поставки JaCarta SF/ГОСТ) посредством стороннего (по отношению к JMS) ПО. JMS позволяет импортировать эти файлы журналов событий безопасности и попыток несанкционированного доступа (НСД) к защищенным разделам памяти ЭН.

Для импорта в JMS журналов, которые были выгружены из электронных ключей JaCarta SF/ГОСТ с помощью ПО, входящего в комплект поставки данных ключей, необходимо скопировать данные журналы в папку, доступную из Консоли управления JMS. При этом следует сохранить имена файлов и структуру папок такими же, какими они были созданы с помощью ПО из комплекта поставки JaCarta SF/ГОСТ, в частности:

- журнал аудита событий НСД должен иметь имя nsd.log;
- журнал аудита событий безопасности должен иметь имя secure.log;
- дерево папок и их именование должны соответствовать следующему шаблону <Путь к папке с журналами в файловой системе>\<Серийный номер носителя>\<Дата>, например: `c:\journals\BLUEMIL20007A57\2018_4_4_18-30-15\nsd.log`

Для того чтобы импортировать подготовленные файлы журналов выполните следующие действия.

1. В разделе **Журналы аудита JaCarta SF/ГОСТ** консоли управления JMS откройте любой из подразделов (например **Журнал события безопасности**)

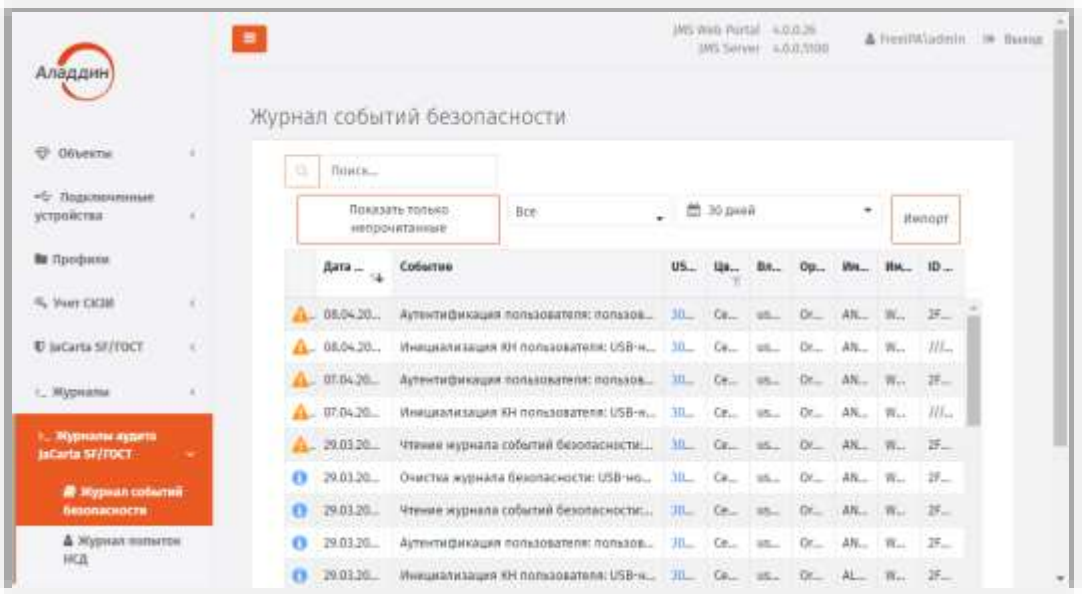


Рис. 298 – Журнал событий безопасности перед импортом файлов журналов

2. Справа вверху нажмите **Импорт**. Откроется страница импорта журналов SF/ГОСТ

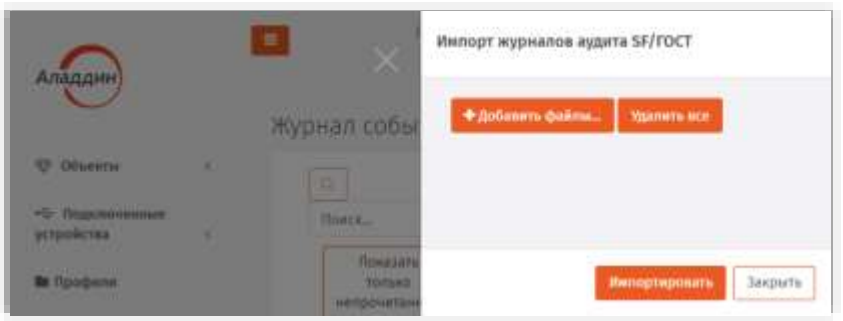


Рис. 299 – Страница импорта журналов аудита SF/ГОСТ

3. Нажмите **+Добавить файлы** и выберите папку с файлами. Обнаруженные файлы отобразятся в интерфейсе.

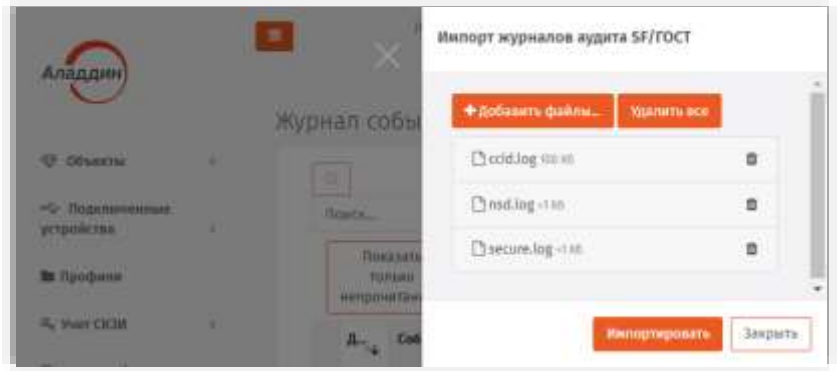


Рис. 300 – Отображение обнаруженных файлов журналов

4. Нажмите **Импортировать**. Отобразится результат импорта.

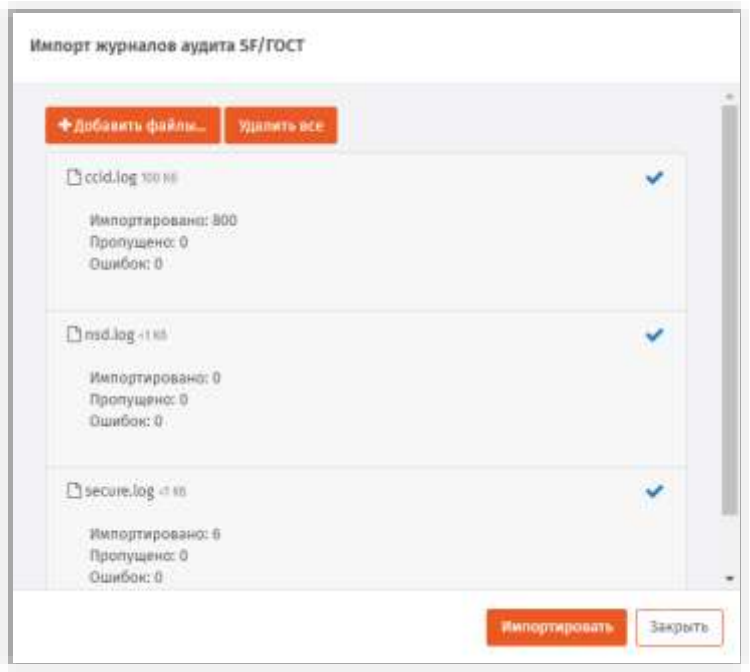


Рис. 301 – Отображение результата импорта журналов JaCarta SF/ГОСТ

5. Нажмите **Закрыть** для завершения процедуры импорта журналов.

По окончании работы мастера в JMS должны быть загружены все события, содержащиеся в импортируемых файлах журналов безопасности и НСД. Алгоритм импорта предотвращает повторную загрузку в JMS уже зарегистрированных ранее событий.

9. JMS Web Manager (JWM)

JMS Web Manager (JWM), или Личный кабинет (ЛК) – компонент JMS, который позволяет пользователям управлять своими электронными ключами и OTP-аутентификаторами как внутри корпоративной сети, так и из внешней сети с помощью web-браузера по протоколам http и https.

становка и настройка JWM и его специального коннектора для JMS описана в первой части руководства администратора [2].

JWM включает в себя следующие основные компоненты:

- Расширение консоли администратора **Настройки личного кабинета**, подробнее см. в разделе «Настройки личного кабинета», ниже.
- **внутренний web-портал самообслуживания пользователей**, предназначенный для использования внутри корпоративной сети (подробнее см. в руководстве пользователя [1], раздел «Web-портал самообслуживания пользователей (личный кабинет)»);
- **внешний web-портал самообслуживания пользователей** – то же, но для подключения из внешней сети (подробнее см. в руководстве пользователя [1], раздел «Аутентификация и работа на внешнем портале самообслуживания»).

9.1 Настройки личного кабинета

Важно! Раздел **Настройки личного кабинета** (Рис. 302) консоли управления JMS становится доступен после установки расширения **JWM-коннектор для JMS** (подробнее см. руководство по установке и настройке [2], раздел «JWM-коннектор для JMS») на компьютере, где развернуто приложение *Консоль управления JMS*.

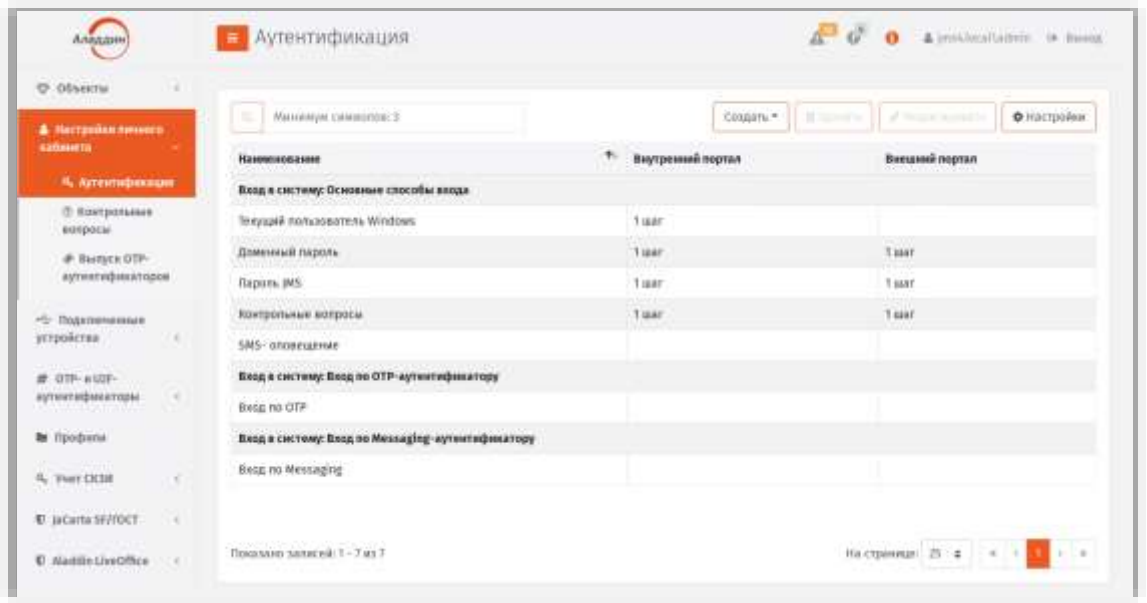


*Рис. 302 – Раздел **Настройки личного кабинета** консоли управления*

Раздел содержит следующие пункты:

- **Аутентификация** (см. «Раздел Аутентификация», ниже);
- **Контрольные вопросы**;
- **Выпуск OTP-аутентификаторов**.

9.1.1 Раздел Аутентификация

В разделе **Настройки личного кабинета ->Аутентификация** осуществляется настройка способов аутентификации пользователя в личном кабинете JWM, которые отображаются в виде вкладок на web-странице аутентификации пользователя (Рис. 303, подробнее см. руководство пользователя [1]).

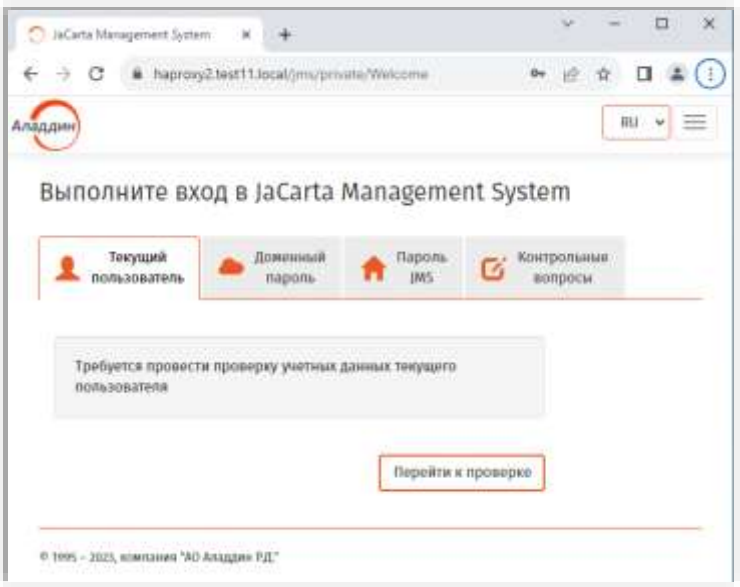


Рис. 303 – Страница аутентификации пользователя на Web-портале JWM

Для того чтобы настроить способы аутентификации пользователя на Web-портале JWM выполните следующие действия.

1. Откройте раздел **Настройки личного кабинета** -> **Аутентификация** в консоли управления Отобразится следующее окно.

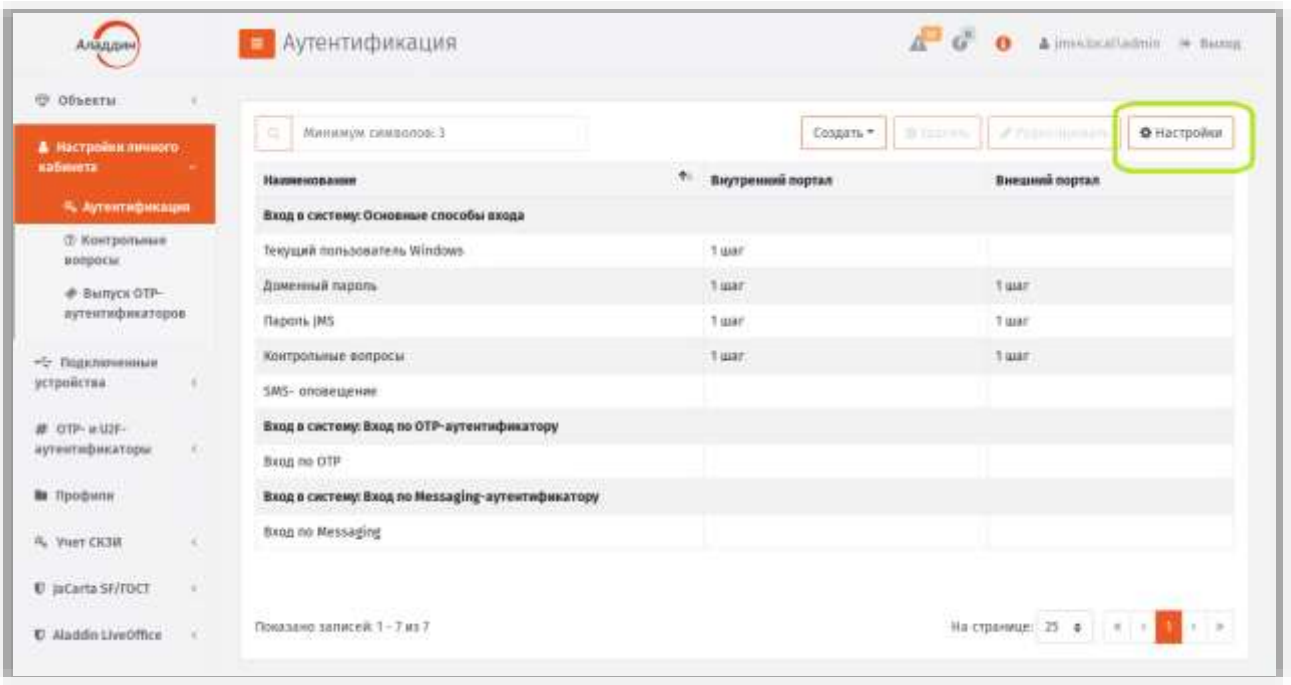


*Рис. 304 – Настройка раздела **Авторизация** личного кабинета (JWM)*

2. Для выполнения общих настроек аутентификации нажмите **Настройки** на верхней панели.

Отобразится страница следующего вида.

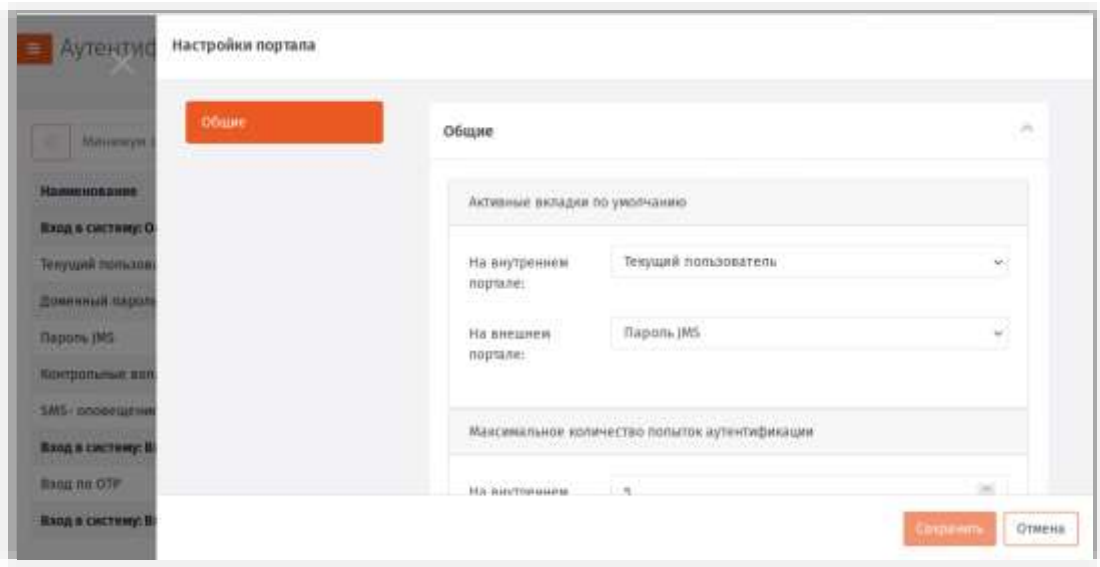


Рис. 305 –Окно настроек аутентификации в ЛК на портале JWM

3. Выполните общие настойки аутентификации в ЛК руководствуясь Табл. 92.

Табл. 92 – Общие настройки аутентификации в ЛК на портале JWM

Настройка	Описание
<Секция> **Максимальное количество попыток аутентификации**	
На внутреннем портале	Максимальное число последовательных неудачных попыток аутентификации пользователя, по достижении которого происходит блокировка пользователя на внутреннем портале. **Примечание.** При аутентификации по контрольным вопросам одной попыткой аутентификации считается заполнение и отправка ответов на контрольные вопросы, число которых определяется настройкой **Количество случайно выбираемых вопросов** Значение по умолчанию: **5**
На внешнем портале	Та же настройка для внешнего портала Значение по умолчанию: **5**
<Секция> **Время жизни сессии от последнего действия**	
На внутреннем портале, минут	Предельное время бездействия на странице личного кабинета внутреннего портала после успешной аутентификации пользователя. По истечении данного времени страница будет переведена в стартовое состояние запроса аутентификации. Значение по умолчанию: **15** минут
На внешнем портале, минут	Та же настройка для внешнего портала.

Настройка	Описание
	Значение по умолчанию: **5** минут
<Секция> **Карточка пользователя**	
Отображать для внутреннего портала	Флаг отображения вкладки «Карточка» на веб-странице личного кабинета пользователя на внутреннем портале (подробнее о вкладке см. руководство пользователя [1], раздел «Функции, доступные пользователю в личном кабинете портала самообслуживания»). При сбросе флага в личном кабинете данная вкладка, содержащая персональную и конфиденциальную информацию пользователя, будет скрыта. По умолчанию вкладка отображается.
Отображать для внешнего портала	Та же настройка для внешнего портала
<Секция> **Управление контрольными вопросами**	
Отображать список вопросов для внутреннего портала	Флаг отображения вкладки «Вопросы» на веб-странице личного кабинета пользователя на внутреннем портале (подробнее о вкладке см. руководство пользователя [1], раздел «Функции, доступные пользователю в личном кабинете портала самообслуживания»). При сбросе флага в личном кабинете данная вкладка будет скрыта. По умолчанию вкладка отображается.
Отображать список вопросов для внешнего портала	Та же настройка для внешнего портала. По умолчанию вкладка скрыта.

4. Для настройки вкладок страницы аутентификации пользователя в ЛК JWM выберите соответствующую строку с названием типа входа (аутентификации) в ЛК в центральной части страницы (Рис. 304, с.322) и нажмите **Редактировать** на верхней панели. Выполните настройку, руководствуясь Табл. 93.

Табл. 93 – Пункты настроек вкладок на web-странице аутентификации пользователя в ЛК JWM

Название пункта	Описание
<Секция> **Вход в систему: основные способы входа**	
Текущий пользователь	Данный пункт предназначен для настройки вкладки **Текущий пользователь** Вкладка используется для авторизации пользователя, уже прошедшего процедуру аутентификации в ОС, где запущен web-браузер. Если пользователь зарегистрирован в JMS, не заблокирован и имеет право подключения к соответствующему порталу, то открытие личного кабинета произойдет без запроса аутентификационных данных. Порядок настройки описан в разделе «Настройка вкладки Текущий пользователь», с. 325.
Доменный пароль	Данный пункт предназначен для настройки вкладки **Доменный пароль**

Название пункта	Описание
	Вкладка используется для аутентификации пользователя в ЛК путем ввода своего имени и пароля, установленного в соответствующей ресурсной системе (AD, FreeIPA и др.). Порядок настройки описан в разделе «Настройка вкладки Доменный пароль», с. 327
Пароль JMS	Данный пункт предназначен для настройки вкладки **Пароль JMS** Вкладка используется для аутентификации пользователя в ЛК путем ввода временного пароля, назначенного ему для работы в JMS (см. «Установка и отмена назначения временного пароля для работы с JMS», с. 17). Порядок настройки описан в разделе «Настройка вкладки Пароль JMS», с. 328
Контрольные вопросы	Данный пункт предназначен для настройки вкладки **Контрольные вопросы** Вкладка используется для аутентификации пользователя в ЛК путем ввода ответа на контрольные вопросы. Порядок настройки описан в разделе «Настройка вкладки Контрольные вопросы», с. 330
SMS-оповещение	Данный пункт предназначен для настройки вкладки **SMS-оповещение** Вкладка используется для проверки личности пользователя в ЛК путем аутентификации по SMS. Порядок настройки описан в разделе «Настройка вкладки SMS-оповещение», с. 332 **Примечание.** Подробнее о настройке аутентификации с помощью SMS-оповещения см. в разделе «Настройка аутентификации пользователя в JWM по SMS-оповещению» с. 334).
<Секция> **Вход в систему: Вход по OTP-аутентификатору**	
Вход по OTP	Данный пункт предназначен для настройки вкладки **Вход по OTP** Вкладка используется для аутентификации пользователя в ЛК с помощью одноразового пароля (OTP), получаемого с помощью одного из типов OTP-аутентификаторов.
<Секция> **Вход в систему: Вход по Messaging-аутентификатору**	
Вход по Messaging	

9.1.1.1 Настройка вкладки Текущий пользователь

Для настройки вкладки выполните следующие действия.

1. Окно параметров вкладки **Текущий пользователь** выглядит следующим образом.

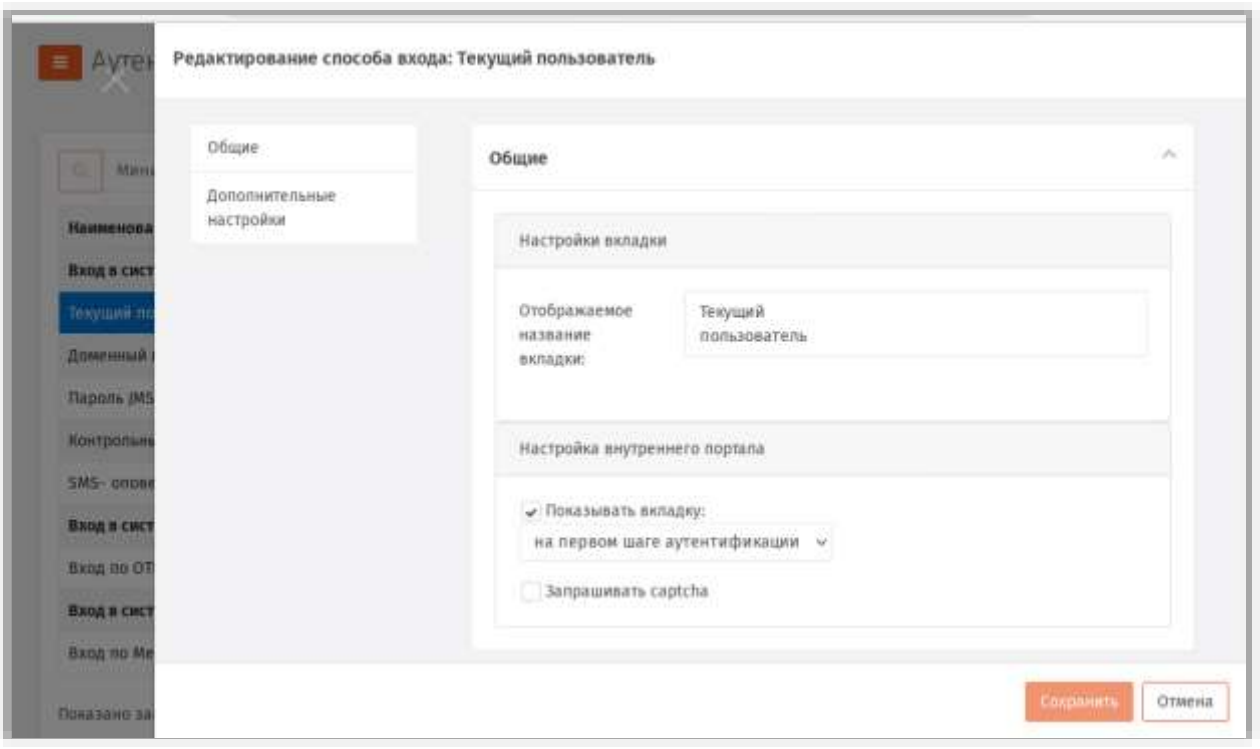


Рис. 306 – Настройка вкладки Текущий пользователь

2. Выполните настройку, руководствуясь Табл. 94.

Табл. 94 – Параметры настройки вкладки Текущий пользователь

Параметр	Описание
<Секция> **Настройки вкладки**	
Отображаемое название вкладки	При необходимости отредактируйте отображаемое в web-интерфейсе название вкладки. Значение по умолчанию: **Текущей пользователь**
<Секция> **Настройка внутреннего портала**	
Показывать вкладку	Установите флаг, если вкладка должна отображаться при аутентификации пользователя на внутреннем портале JWM. **Примечание.** Вкладка может отображаться только на первом шаге аутентификации. Значение шага аутентификации не меняется (всегда отображается значение «на первом шаге аутентификации») Значение по умолчанию: установлен
Запрашивать captcha на внутреннем портале	Флаг необходимости заполнения «капча»-поля пользователями при аутентификации (для предотвращения DDoS-атак на портал). Имеет смысл только при отображении данной вкладки.

Параметр	Описание
	По умолчанию не установлен.

3. По окончании настройки нажмите **Сохранить** (Рис. 306) для сохранения изменений.

9.1.1.2 Настройка вкладки Доменный пароль

1. Окно параметров вкладки **Доменный пароль** выглядит следующим образом.

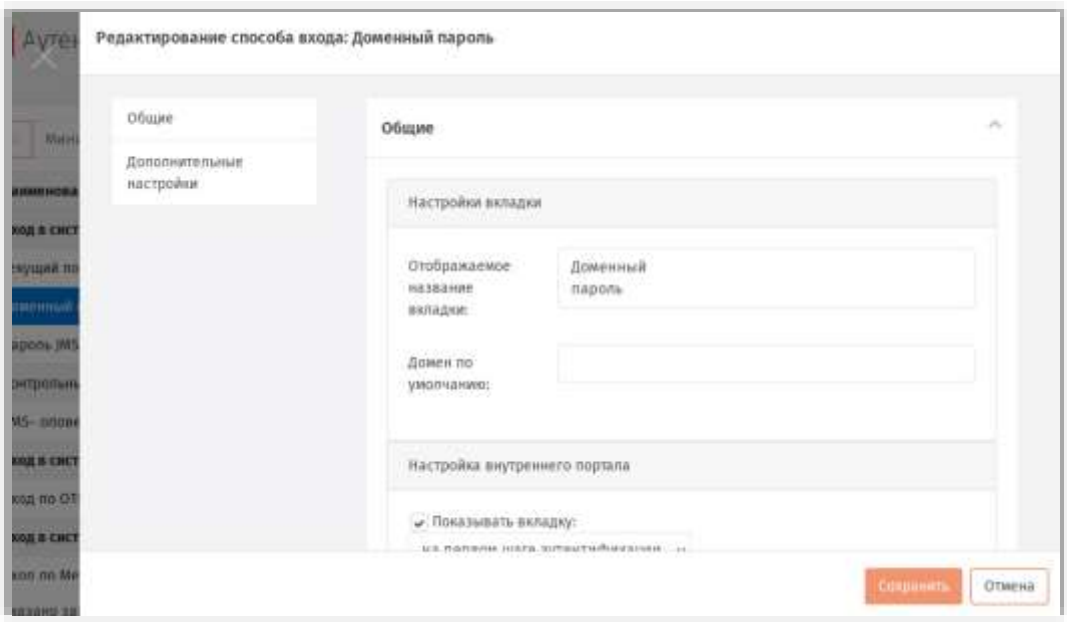


*Рис. 307 – Настройка вкладки **Доменный пароль***

2. Выполните настройку, руководствуясь Табл. 95.

Табл. 95 –Настройки вкладки Доменный пароль

Параметр	Описание
<Секция> **Настройки вкладки**	
Отображаемое название вкладки	При необходимости отредактируйте отображаемое в web-интерфейсе название вкладки. Значение по умолчанию: **Доменный пароль**
Домен по умолчанию	Значение по умолчанию имени домена пользователя. Данное значение добавляется к имени пользователя при его аутентификации на портале, если в форме ввода имя пользователя было указано без домена. Значение по умолчанию: пустая строка
<Секция> **Настройка внутреннего портала**	

Параметр	Описание
Показывать вкладку	Установите флаг, если вкладка должна отображаться при аутентификации пользователя на внутреннем портале JWM. Значение по умолчанию: установлен При выборе флага активируется выпадающий список из двух значений: • **на первом шаге аутентификации** – выберите параметр, если проверка пароля осуществляется в качестве **первого** шага двухфакторной аутентификации; • **на втором шаге аутентификации** – выберите параметр, если проверка пароля осуществляется в качестве **второго** шага двухфакторной аутентификации;
Проверять второй фактор первым	Флаг инверсии порядка проверки факторов аутентификации (при его установке логически первым будет проверен второй фактор с прекращением дальнейших проверок, например чтобы предотвратить атаку перебора значений логина/пароля). Флаг становится доступным при выборе значения **на первом шаге аутентификации** предыдущей настройки.
Запрашивать captcha	Флаг необходимости заполнения «капча»-поля пользователями при аутентификации (для предотвращения DDoS-атак на портал). Имеет смысл только при отображении данной вкладки. Значение по умолчанию: не установлен
<Секция> **Настройка внешнего портала**	
Показывать вкладку **Проверять второй фактор первым** **Запрашивать captcha**	Параметры имеют то же назначение, что и для случая внутреннего портала (выше). Для внешнего портала параметр **Запрашивать captcha** установлен по умолчанию

3. По окончании настройки нажмите **Сохранить** для сохранения изменений.

9.1.1.3 Настройка вкладки Пароль JMS

Под «Паролем JMS» в качестве способа аутентификации подразумевается временный пароль, действующий только в рамках JMS, который предоставляется пользователю, если тот временно утратил возможность аутентификации по доменному паролю и электронному ключу (подробнее см. «Установка и отмена назначения временного пароля для работы с JMS», с. 17).

1. Окно параметров вкладки **Пароль JMS** выглядит следующим образом.

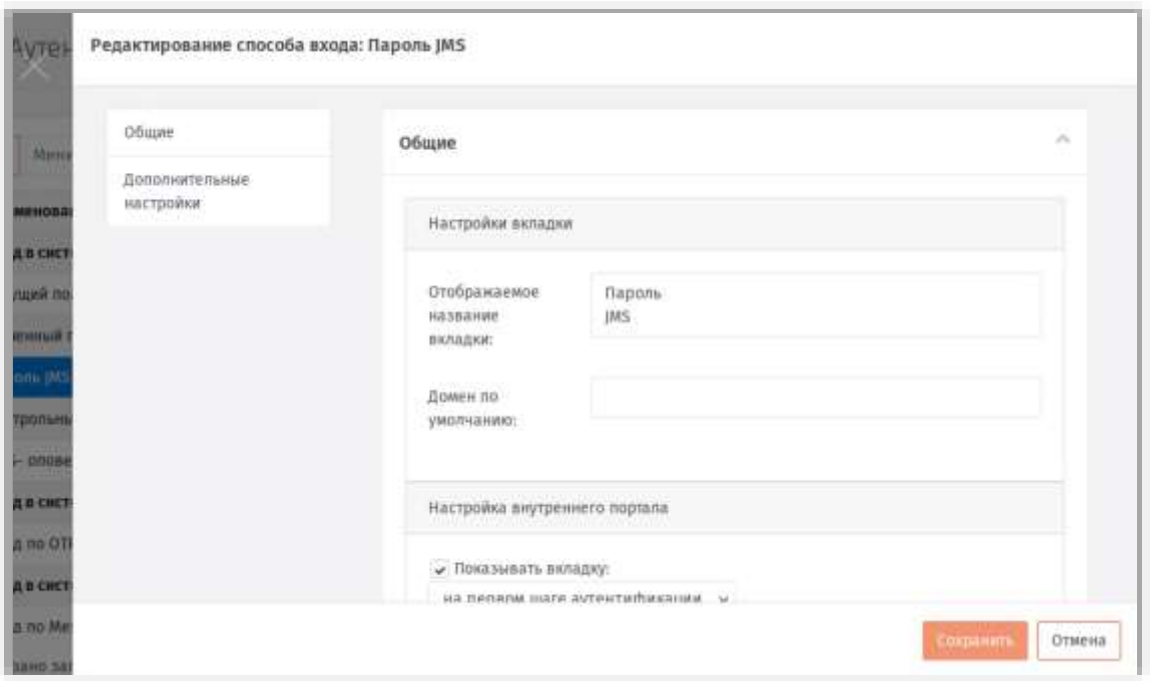


*Рис. 308 – Настройка вкладки **Пароль JMS***

2. Выполните настройку, руководствуясь Табл. 96.

Табл. 96 –Настройки вкладки Пароль JMS

Параметр	Описание
<Секция> **Настройки вкладки**	
Отображаемое название вкладки	При необходимости отредактируйте отображаемое в web-интерфейсе название вкладки. Значение по умолчанию: **Пароль JMS**
Домен по умолчанию	Значение по умолчанию имени домена пользователя. Данное значение добавляется к имени пользователя при его аутентификации на портале, если в форме ввода имя пользователя было указано без домена. Значение по умолчанию: пустая строка
<Секция> **Настройка внутреннего портала**	
Показывать вкладку	Установите флаг, если вкладка должна отображаться при аутентификации пользователя на внутреннем портале JWM. Значение по умолчанию: установлен При выборе флага активируется выпадающий список из двух значений: • **на первом шаге аутентификации** – выберите параметр, если проверка пароля осуществляется в качестве **первого** шага двухфакторной аутентификации; • **на втором шаге аутентификации** – выберите параметр, если проверка пароля осуществляется в качестве **второго** шага двухфакторной аутентификации

Параметр	Описание
Проверять второй фактор первым	Флаг инверсии порядка проверки факторов аутентификации (при его установке логически первым будет проверен второй фактор с прекращением дальнейших проверок, например чтобы предотвратить атаку перебора значений логина/пароля). Флаг становится доступным при выборе значения **на первом шаге аутентификации** предыдущей настройки.
Запрашивать captcha	Флаг необходимости заполнения «капча»-поля пользователями при аутентификации (для предотвращения DDoS-атак на портал). Имеет смысл только при отображении данной вкладки. Значение по умолчанию: не установлен
<Секция> **Настройка внешнего портала**	
Показывать вкладку **Проверять второй фактор первым** **Запрашивать captcha**	Параметры имеют то же назначение, что и для случая внутреннего портала (выше). Для внешнего портала параметр **Запрашивать captcha** установлен по умолчанию

3. По окончании настройки нажмите **Сохранить** для сохранения изменений.

9.1.1.4 Настройка вкладки Контрольные вопросы

1. Окно настройки параметров **Контрольные вопросы** выглядит следующим образом.

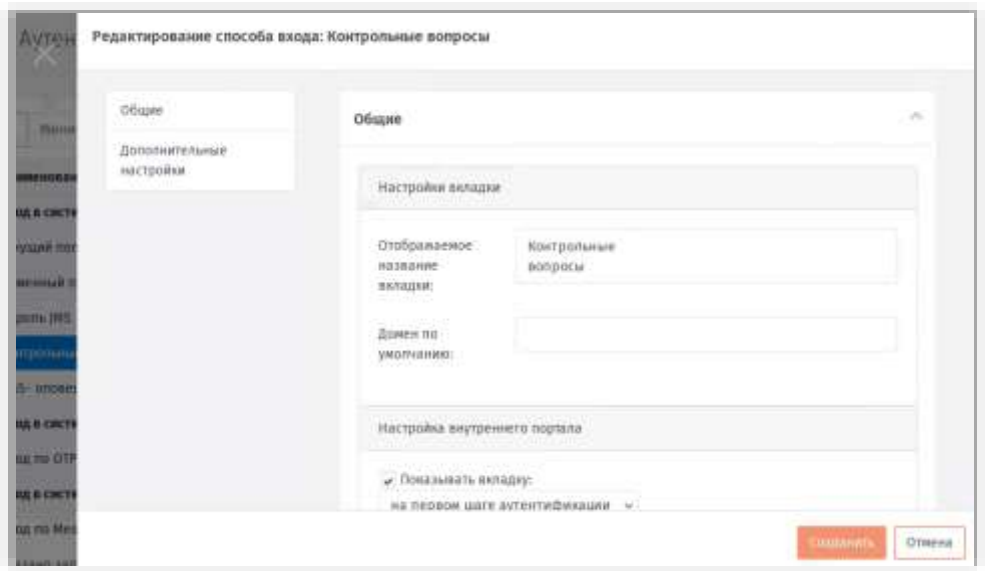


*Рис. 309 –Раздел **Общие** настроек вкладки Контрольные вопросы*

2. Выполните настройки, руководствуясь Табл. 97.

Табл. 97 –Настройки вкладки Контрольные вопросы

Параметр	Описание
<Секция> **Настройки вкладки**	
Отображаемое название вкладки	При необходимости отредактируйте отображаемое в web-интерфейсе название вкладки. Значение по умолчанию: **Контрольные вопросы**
<Секция> **Настройка внутреннего портала**	
Показывать вкладку	Установите флаг, если вкладка должна отображаться при аутентификации пользователя на внутреннем портале JWM. Значение по умолчанию: установлен При выборе флага активируется выпадающий список из двух значений: • **на первом шаге аутентификации** – выберите параметр, если проверка по данному фактору осуществляется в качестве **первого** шага двухфакторной аутентификации; • **на втором шаге аутентификации** – выберите параметр, если проверка по данному фактору осуществляется в качестве **второго** шага двухфакторной аутентификации
Запрашивать captcha	Флаг необходимости заполнения «капча»-поля пользователями при аутентификации (для предотвращения DDoS-атак на портал). Имеет смысл только при отображении данной вкладки. Значение по умолчанию: не установлен
<Секция> **Настройка внешнего портала**	
Показывать вкладку **Запрашивать captcha**	Параметры имеют то же назначение, что и для случая внутреннего портала (выше). Для внешнего портала параметр **Запрашивать captcha** установлен по умолчанию
(раздел **Дополнительные настройки**) <Секция> **Параметры аутентификации**	
Пропускать второй шаг, если не заданы ответы	Флаг отмены второго шага двухфакторной аутентификации, если Контрольные вопросы не были определены пользователем. **Примечание.** По факту полная отмена второго шага (с превращением в однофакторную аутентификацию) произойдет лишь если для второго шага определён единственный способ (Контрольные вопросы). В общем же случае пользователю будут предложены альтернативные способы аутентификации для второго шага, если они были определены. Значение по умолчанию: не установлен
Не использовать, если есть активный аутентификатор JAS	Флаг отмены проверки по *Контрольным вопросам*, если в настройках аутентификации пользователя (на том же шаге аутентификации) определен дополнительный фактор аутентификации посредством JAS, такой как OTP- или Messaging-токен **Примечание.** Отмена проверки по *Контрольным вопросам* проявляется в отсутствии соответствующей вкладки на web-странице аутентификации пользователя.

Параметр	Описание
	Значение по умолчанию: не установлен

3. По окончании настройки нажмите **Сохранить** для сохранения изменений.

9.1.1.5 Настройка вкладки SMS-оповещение

1. Окно настройки параметров **SMS-оповещение** выглядит следующим образом.

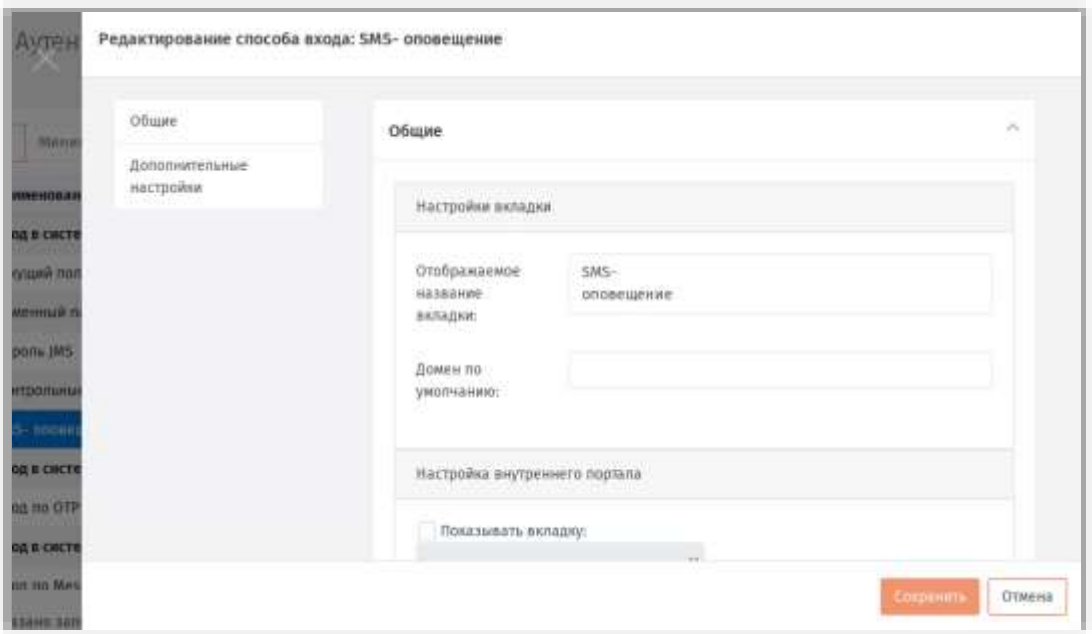


*Рис. 310 –Раздел **Общие** настроек вкладки SMS-оповещение*

2. Выполните настройки, руководствуясь Табл. 98.

Табл. 98 –Настройки вкладки SMS-оповещение

Параметр	Описание
<Секция> **Настройки вкладки**	
Отображаемое название вкладки	При необходимости отредактируйте отображаемое в web-интерфейсе название вкладки. Значение по умолчанию: **SMS-оповещение**
Домен по умолчанию	Значение по умолчанию имени домена пользователя. Данное значение добавляется к имени пользователя при его аутентификации на портале, если в форме ввода имя пользователя было указано без домена. Значение по умолчанию: пустая строка

Параметр	Описание
<Секция> **Настройка внутреннего портала**	
Показывать вкладку	Установите флаг, если вкладка должна отображаться при аутентификации пользователя на внутреннем портале JWM. Значение по умолчанию: не установлен При выборе флага активируется выпадающий список из двух значений: • **на первом шаге аутентификации** – выберите параметр, если проверка по данному фактору осуществляется в качестве **первого** шага двухфакторной аутентификации; • **на втором шаге аутентификации** – выберите параметр, если проверка по данному фактору осуществляется в качестве **второго** шага двухфакторной аутентификации
Запрашивать captcha	Флаг необходимости заполнения «капча»-поля пользователями при аутентификации (для предотвращения DDoS-атак на портал). Имеет смысл только при отображении данной вкладки. Значение по умолчанию: не установлен
<Секция> **Настройка внешнего портала**	
Показывать вкладку **Запрашивать captcha**	Параметры имеют то же назначение, что и для случая внутреннего портала (выше). Для внешнего портала параметр **Запрашивать captcha** установлен по умолчанию
(раздел **Дополнительные настройки**) <Секция> **Настройки SMS**	
Использовать телефон из атрибута	Укажите имя атрибута ресурсной системы, из которого JMS необходимо получать телефонный номер абонента рассылки. Значение по умолчанию: telephoneNumber **Примечание.** Подробнее о настройке аутентификации с помощью SMS-оповещения см. в разделе «Настройка аутентификации пользователя в JWM по SMS-оповещению» с. 334)
Длина кода подтверждения в SMS	Параметр устанавливает длину кода для аутентификации пользователя на портале. Допустимый диапазон значений настройки: 3—15 Значение по умолчанию: 6 **Примечание.** Подробнее о настройке аутентификации с помощью SMS-оповещения см. в разделе «Настройка аутентификации пользователя в JWM по SMS-оповещению» с. 334)
Период действия SMS, сек	Параметр устанавливает время действия кода из SMS для аутентификации пользователя на портале (в секундах) Значение по умолчанию: 120
<Секция> **Параметры аутентификации**	
Пропускать второй шаг, если не задан телефон	Флаг отмены второго шага двухфакторной аутентификации, если в ресурсной системе (см. параметр **Использовать телефон из атрибута**, выше) не определено значение номера телефона.

Параметр	Описание
	Примечание. По факту полная отмена второго шага (с превращением в однофакторную аутентификацию) произойдет лишь если для второго шага определён единственный способ (SMS-оповещение). В общем же случае пользователю будут предложены альтернативные способы аутентификации для второго шага, если они были определены. Значение по умолчанию: не установлен
Не использовать, если есть активный аутентификатор JAS	Флаг отмены проверки по SMS-оповещению, если в настройках аутентификации пользователя (на том же шаге аутентификации) определен дополнительный фактор аутентификации посредством JAS, такой как OTP- или Messaging. **Примечание.** Отмена проверки по *SMS-оповещению* проявляется в отсутствии соответствующей вкладки на web-странице аутентификации пользователя. Значение по умолчанию: не установлен

3. По окончании настройки нажмите **Сохранить** для сохранения изменений.

9.1.1.6 Настройка аутентификации пользователя в JWM по SMS-оповещению

Важно! Аутентификация посредством SMS-оповещения доступна только в случае приобретения лицензии на сервер JAS и установки данного продукта.

В JWM предусмотрена возможность аутентификации пользователя в личном кабинете с помощью одноразового пароля, генерируемого самими JWM и передаваемого через канал SMS. Данный способ не требует настройки каких-либо профилей для создания OTP-аутентификаторов и их привязки к пользователям. Настройка касается всех пользователей JMS. Механизм генерации одноразовых паролей реализован в рамках самого модуля JWM.

Для обеспечения работы аутентификации пользователя в личном кабинете JWM по SMS-оповещению выполните следующие действия.

1. Убедитесь, что у пользователя в ресурсной системе в поле для телефонного номера установлен его персональный телефонный номер.
   Имя атрибута ресурсной системы, в котором следует указывать персональный телефонный номер пользователя, отображается в поле **Использовать телефон из атрибута** в настройках вкладки SMS-оповещения (см. раздел «Настройка вкладки SMS-оповещение», с. 332).

   Примечание. Например для ресурсной системы AD имя такого атрибута по умолчанию – *telephoneNumber* – соответствует значению свойств пользователя AD, отображаемому в поле **Номер телефона** на вкладке **Общие** свойств пользователя из mmc-оснастки *Active Directory – пользователи и компьютеры*. Внеся соответствующий номер в ресурсную систему, не забудьте выполнить синхронизацию учетных данных пользователей в ресурсной системе с JMS посредством выполнения плана обслуживания по умолчанию (см. раздел «План обслуживания по умолчанию», с. 288).

2. Выполните настройки Messaging-транспорта в серверном агенте JAS согласно руководству по установке и настройке JAS [3] (раздел «Порядок настройки транспорта для работы с Messaging-токенами»).

   Примечание. Сервис аутентификации пользователей в JWM по SMS-оповещению использует тот же транспорт, что и Messaging-токены.

10. Учет пользовательских лицензий в продукте JMS

Согласно схеме лицензирования продукта, ограничение на его использование накладывается по числу пользовательских лицензий, при этом задействование (учет) одной пользовательской лицензии происходит только по факту привязки электронного ключа (или сертификата, выпущенного в хранилище пользователя) к пользователю. В случае прекращения привязки к пользователю всех электронных ключей (сертификатов, выпущенных в хранилище пользователя) пользовательская лицензия высвобождается и может быть задействована вновь.

По факту исчерпания всех приобретенных заказчиком пользовательских лицензий в приложениях JMS отображается соответствующее предупреждение. Дальнейшая привязка в JMS электронных ключей (или сертификатов) к пользователю становится невозможной до освобождения уже имеющихся или покупки дополнительных лицензий.

Примечание. Помимо пользовательских лицензий в продукте также предусмотрено лицензирование других ресурсов: подключений к внешним ресурсным системам, выпуска сертификатов во внешних УЦ, учета СКЗИ и др.

10.1 Процедура учета (блокировки) пользовательской лицензии

При выполнении с электронным ключом операции **Назначить пользователю**, см. раздел «Жизненный цикл ЭК/ЗНИ», с. 28 (операция может быть выполнена автоматически в процессе выпуска электронного ключа) происходит «блокирование» одной пользовательской лицензии (при условии, что пользователю *еще не были назначены* электронные ключи/сертификаты).

«Блокировка» одной пользовательской лицензии выполняется также в случае разблокирования пользователя, на которого был выпущен хотя бы один электронный ключ/сертификат (см. раздел «Блокировка/разблокировка пользователей», с. 19).

10.2 Процедура освобождения пользовательской лицензии

При выполнении с электронным ключом операций **Вернуть в эксплуатацию** или **Удалить** (см. раздел «Жизненный цикл ЭК/ЗНИ», с. 28) происходит «освобождение» одной пользовательской лицензии (при условии, что пользователю не назначены в JMS другие электронные ключи/сертификаты).

«Разблокировка» одной пользовательской лицензии выполняется также в случае блокировки пользователя, на которого был выпущен хотя бы один электронный ключ/сертификат (см. раздел «Блокировка/разблокировка пользователей», с. 19).

Приложения

Приложение 1. Права на выполнение операций в JMS

Табл. 99 – Права на выполнение операций в JMS и их делегирование

Операция (право на выполнение операции)	Описание	Делегируемая операция
СКЗИ		
Чтение СКЗИ	Позволяет читать все разделы учета СКЗИ	+
Изменение СКЗИ	Позволяет регистрировать/редактировать экземпляры, дистрибутивы, лицензии, типы СКЗИ и типы НД, а также заполнять номера СКЗИ для КН с апплетом ГОСТ	+
Обслуживание сервера		
Администрирование	Необходимо для запуска административной консоли	
Старт/Монтирование хранилища	Позволяет запускать сервер бизнес-логики и монтировать криптохранилище	
Стоп/Демонтирование хранилища	Позволяет останавливать сервер бизнес-логики и демонтировать криптохранилище	
Чтение конфигурации сервера	Необходимо для запуска административной консоли, а также чтения настроек в серверном агенте (вкладки **Настройка** и **Каталоги учетных записей**)	
Изменение конфигурации сервера	Дает право изменения настроек в серверном агенте (вкладки **Настройка** и **Каталоги учетных записей**)	
Чтение планов обслуживания	Необходимо для чтения списка планов обслуживания и чтения всего раздела **Журналы**	
Выполнение планов обслуживания	Позволяет запускать планы обслуживания	
Изменение настроек плана обслуживания	Позволяет изменять настройки планов обслуживания	
Чтение лицензий	Позволяет читать информацию о загруженных лицензиях	
Управление лицензиями	Позволяет добавлять/удалять лицензии	
Чтение журнала событий	Позволяет читать события в журналах	
Запись в журналы событий	Разрешает помечать записи в журнале **Предупреждения** как прочитанные, а также публиковать в **Журнале аудита** ошибки при выпуске/синхронизации ключевых носителей	
Чтение из каталога учетных записей	Базовое право на чтение объектов ресурсной системы	
Чтение контейнера ресурсной системы	Расширение базового права чтения каталога учетных записей на все или отдельные контейнеры ресурсной системы (используется при делегировании данного права в отношении отдельных контейнеров)	+
Управление поставщиками криптографии	Позволяет добавлять новые поставщики криптографии с помощью серверного агента	
Управление перечнем поддерживаемых ключевых носителей	В текущей версии JMS операция не используется	

Операция (право на выполнение операции)	Описание	Делегируемая операция
Пользователи		
Чтение	Позволяет отображать зарегистрированных пользователей в контейнерах	+
Регистрация	Позволяет зарегистрировать пользователей	+
Удаление	Позволяет удалять ранее зарегистрированных пользователей	+
Изменение	Позволяет производить блокировку/разблокировку пользователей (операции **Блокировать**/**Разблокировать**)	+
Открытие сеанса пользователя	В текущей версии JMS операция не используется	
Управление паролем пользователя	Позволяет назначать/отменять назначение временного пароля JMS пользователю для открытия пользовательского сеанса работы с JMS	+
Управление доступом в Active Directory по паролю	Позволяет предоставлять временный пароль AD пользователю для входа в операционную систему по паролю	+
Рабочие станции		
Чтение	Позволяет отображать зарегистрированные рабочие станции в контейнерах ресурсной системы	+
Регистрация	Позволяет регистрировать рабочие станции	+
Удаление	Позволяет удалять ранее зарегистрированные рабочие станции	+
Изменение	Позволяет производить блокировку/разблокировку рабочих станций	+
Удаление сертификата рабочей станции	Позволяет выполнять удаление объектов (сертификатов) на рабочих станциях	+
Ключевые носители		
Чтение	Позволяет отображать список ключевых носителей в разделе **Ключевые носители** и в свойствах пользователей. Действие данного права распространяется также на ридеры смарт-карт.	+
Изменение	Позволяет Устанавливать/Отменять принудительную смену PIN-кода, изменять текущий административный PIN-код в БД, обновлять атрибуты ключевых носителей (номера корпуса, СКЗИ, СЗИ)	+
Регистрация ключевого носителя	Позволяет зарегистрировать электронные ключи из разделов **Подключенные устройства -> Ключевые носители** (для подключенных КН) и **Ключевые носители** (через файл пакетного импорта; но в этом случае необходимо добавить право **Импорт**, см. ниже). Действие данного права распространяется также на ридеры смарт-карт.	+
Назначение пользователю	Позволяет назначать ключевые носители пользователям. Действие данного права распространяется также на ридеры смарт-карт.	+
Выпуск	Позволяет производить выпуск ключевых носителей	+
Удаление	Позволяет удалять ранее зарегистрированные ключевые носители. Действие данного права распространяется также на ридеры смарт-карт.	+
Включение/Отключение	Позволяет производить включение/отключение ключевых носителей	+
Отзыв	Позволяет производить отзыв ключевых носителей	+

Операция (право на выполнение операции)	Описание	Делегируемая операция
Замена	Позволяет производить замену ключевых носителей	+
Возврат в эксплуатацию	Позволяет выполнять возврат в эксплуатацию отозванных ключевых носителей	+
Разблокировка по PIN-коду администратора	Позволяет выполнять из консоли администратора разблокировку подсоединенных электронных ключах и заменять отпечатки пальцев в электронных ключах с приложением PKI/BIO	+
Разблокировка Запрос-Ответ	Позволяет выполнять удаленную разблокировку ключевых носителей с использованием механизма Запрос-Ответ	+
Чтение из УЦ	Позволяет создавать новые профили выпуска сертификатов, в частности, дает возможность отображать список УЦ (только для ЦС Microsoft) и шаблонов на вкладках **Подключение** / **Подключение к УЦ**	
Чтение объекта на КН	Позволяет отображать свойства и содержимое электронного ключа, также позволяет отображать объекты (сертификаты) в свойствах рабочей станции, электронного ключа и в разделе **Сертификаты**	
Чтение коннекторов	Позволяет отображать объекты, созданные дополнительными коннекторами (Indeed и др.) в свойствах пользователя, электронного ключа и в разделе **Сертификаты**	
Экспорт резервных копий сертификатов	Позволяет экспортировать сертификат и соответствующий закрытый ключ, которые имеют резервные копии в БД, в контейнер pfx или на другой ключевой носитель	+
Импорт резервных копий сертификатов	Позволяет производить импорт сертификатов вместе с закрытым ключом из контейнеров pfx или из ЦС (с настроенным Key Recovery Agent в MSCA)	+
Синхронизация	Позволяет выполнять синхронизацию ключевых носителей, а также блокировку/разблокировку, отзыв и удаление объектов (сертификатов) на ключевых носителях	+
Миграция	Позволяет производить операцию перемещения ключевых носителей между подразделениями (контейнерами ресурсных систем). Действие данного права распространяется также на ридеры смарт-карт.	+
Удаление резервных копий сертификатов	Позволяет удалять резервную копию объектов, выпущенных на КН (экран «Сертификаты»)	+
Импорт	Позволяет выполнять импорт ключевых носителей из файла. Действие данного права распространяется также на ридеры смарт-карт.	+
Экспорт	Позволяет выполнять экспорт зарегистрированных ключевых носителей в файл. Действие данного права распространяется также на ридеры смарт-карт.	+
Очистка	Позволяет выполнять удаление всех объектов из приложений на электронном ключе, путем инициализации данных приложений	+
Выпуск с восстановлением объектов	Позволяет выполнять выпуск ключевых носителей с возможностью восстановления объектов из резервной копии	+
Роли		
Чтение	Позволяет отображать информацию о созданных ролях	
Создание	Позволяет создавать новые роли	
Удаление	Позволяет удалять ранее созданные роли	

Операция (право на выполнение операции)	Описание	Делегируемая операция
Изменение	Позволяет изменять ранее созданные роли	
Управление членством роли	Позволяет назначать/отменять назначение роли пользователям	
Делегирование		
Чтение настроек делегирования	Доступ на чтение привязок настроек и свойств делегирования	
Управление настройками делегирования	Позволяет выполнять делегирование полномочий и редактировать настройки делегирования	+
Глобальные группы		
Чтение	Доступ на чтение списка глобальных групп	
Создание	Позволяет создавать глобальные группы	
Удаление	Позволяет удалять глобальные группы	
Изменение	Позволяет изменять наименование и описание глобальной группы	
Управление членством глобальной группы	Позволяет добавлять /удалять пользователей в/из глобальных групп	
Профили		
Чтение типов профилей	Позволяет отображать зарегистрированные типы профилей	
Чтение экземпляров профилей	Позволяет отображать созданные экземпляры профилей	
Добавление нового типа профиля	Позволяет добавлять новые типы профилей	
Добавление нового экземпляра профиля	Позволяет создавать новые экземпляры профилей	
Изменение экземпляра профиля	Позволяет редактировать созданные экземпляры профилей	
Удаление экземпляра профиля	Позволяет удалять экземпляры профилей	
Управление привязкой и наследованием профиля	Позволяет выполнять привязку/отвязку экземпляров профилей и включать/отключать наследование действия экземпляров профилей во вложенных контейнерах ресурсной системы	+
Приложения		
Чтение	В текущей версии JMS операция не используется	
Регистрация	В текущей версии JMS операция не используется	
Категории событий		
Чтение	Требуется для просмотра журнала событий – необходима для сортировки и группировки событий по Категории событий	
Регистрация	В текущей версии JMS операция не используется	
Печать		
Чтение шаблонов / Печать документов	Позволяет выполнять чтение загруженных в JMS шаблонов печати	
Изменение шаблонов печати	Позволяет создавать, изменять настройки и удалять шаблоны печати	
JaCarta SF/ГОСТ – Контейнеры		
Чтение	Позволяет прочитать список учетных записей контейнеров JaCarta SF/ГОСТ, импортированных в JMS	
Удаление	Позволяет удалить учетную запись контейнера JaCarta SF/ГОСТ из JMS	

Операция (право на выполнение операции)	Описание	Делегируемая операция
Изменение	Позволяет изменить данные учетной записи контейнера JaCarta SF/ГОСТ в JMS	
Импорт	Позволяет импортировать контейнеры JaCarta SF/ГОСТ в JMS	
Экспорт	Позволяет экспортировать контейнеры JaCarta SF/ГОСТ из JMS	
JaCarta SF/ГОСТ – Журналы аудита		
Чтение	Позволяет читать события журналов аудита JaCarta SF/ГОСТ	
Импорт	Позволяет импортировать события журналов аудита в JMS	
Экспорт	В текущей версии JMS операция не используется (функционал не реализован)	
JaCarta SF/ГОСТ – Встроенное ПО		
Чтение	Позволяет читать список зарегистрированных учетных записей файлов обновлений встроенного ПО для JaCarta SF/ГОСТ	
Регистрация	Позволяет создавать учетную запись файла обновления встроенного ПО для JaCarta SF/ГОСТ	
Удаление	Позволяет удалить учетную запись файла обновления встроенного ПО	
Изменение	Позволяет изменить данные учетной записи файла обновления встроенного ПО	
JaCarta SF/ГОСТ – Ключевые носители		
Создание контейнера автономного монтирования	Позволяет создавать контейнер автономного монтирования (kko) защищенных CD- и RW-дисков на электронном носителе	+
Отзыв контейнера автономного монтирования	Позволяет отзывать ранее созданный контейнер автономного монтирования защищенных CD- и RW-дисков на электронном носителе	+
Создание контейнера для сервера авторизации	Позволяет создавать контейнеры монтирования скрытых разделов (kkl) защищенных CD- и RW-дисков на электронном носителе	+

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

Список литературы

1 RU.АЛДЕ.03.16.001-05 34 01. Руководство пользователя [Текст]. — «Аладдин Р.Д.» — Файл «JMS-4LX Руководство Пользователь.docx»

2 RU.АЛДЕ.03.16.001-05 32 01-1. Руководство администратора. Часть 1. Установка и настройка [Текст]. — «Аладдин Р.Д.» — Файл «JMS-4LX Руководство Администратор 1.docx»

3 RU.АЛДЕ.03.16.001-05 32 01-3. Руководство администратора. Часть 3. Установка и настройка сервера аутентификации (JAS) [Текст]. — «Аладдин Р.Д.». — Файл «JMS-4LX Руководство Администратор 3.docx»

4 RU.АЛДЕ.03.16.001-05 30 01-1. Формуляр [Текст]. — «Аладдин Р.Д.»

5 Комплект документации программных средств для USB-носителя «JACARTA SF/ГОСТ»

- USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа главного администратора. Руководство оператора. [Текст]. — АО «Аладдин Р.Д.»
- USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Программа администратора. Руководство оператора. [Текст]. — АО «Аладдин Р.Д.»
- USB-носитель «JaCarta SF/ГОСТ». Комплект программных средств. Программный комплекс интеграции и администрирования. Локальный сервер авторизации. Руководство оператора. [Текст]. — АО «Аладдин Р.Д.»

Полезные web-ресуры

1 Microsoft. Developer Network. Documentation. X509VerificationFlags Enumeration: https://msdn.microsoft.com/en-us/library/system.security.cryptography.x509certificates.x509verificationflags(v=vs.110).aspx

2 FIDO Alliance. Download Specifications. https://fidoalliance.org/download/

3 Как создать центральное хранилище для административных шаблонов групповой политики в Windows и управлять им. https://support.microsoft.com/ru-ru/help/3087759/how-to-create-and-manage-the-central-store-for-group-policy-administra

Регистрация изменений

Версия	Изменения
1.02	Добавлено описание функциональности версии JMS 4.1.
1.01	Доработки по промежуточному релизу
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