JaCarta Management System v3.7

Руководство администратора. Часть 2

Функции управления

Версия продукта	3.7.1
Версия документа	1.00
Статус	Публичный
Дата	19 января 2024 г.
Листов	678

2024

Оглавление

1. О документе

1.1 Назначение документа

Настоящий документ является частью руководства администратора и представляет собой описание функций администрирования средств аутентификации и операций по управлению их жизненным циклом с помощью программного обеспечения JaCarta Management System (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. 8	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 CA Edition	Версия продукта, предназначенная для заказчиков, которые не используют компонент JMS Client
JMS Enterprise Edition	Полнофункциональная версия продукта, обеспечивающая автоматизацию администрирования электронных ключей на предприятии с использованием компонента JMS Client на рабочих станциях.
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
Messaging-токен	Аутентификатор, позволяющий проводить аутентификацию посредством 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
USB	Universal Serial Bus, универсальная последовательная шина
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
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. Устанавливается вместе с компонентом JMS Client
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
Резервная копия сертификата	В терминах JMS обозначает защищенный контейнер, содержащий в общем случае ключевую пару и сертификат, хранимый в защищенном хранилище JMS
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
Серверный агент JMS	Приложение с графическим пользовательским интерфейсом, предназначенное для конфигурирования сервера JMS. Устанавливается вместе с компонентом JMS Server
Унаследованный сертификат	Сертификат, хранящийся в памяти электронного ключа и зарегистрированный в JMS, но не находящийся под управлением JMS (т.е. данный сертификат не может быть перевыпущен в рамках JMS). Регистрация такого сертификата JMS происходит автоматически в процессе выпуска электронного ключа при использовании соответствующего профиля выпуска сертификата

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. Введение

2.1 Общие сведения

JaCarta Management System (JMS) - система, предназначенная для управления жизненным циклом электронных ключей (токенов и смарт-карт) в организации.

JMS обеспечивает:

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

⚠ В настоящем документе описание настроек JMS представлено на примере операционных систем Microsoft Windows Server 2012 и Microsoft Windows 7.

2.2 Состав JMS

В состав JMS входят следующие компоненты:

- JMS Server – серверный компонент JMS;
- JMS Admin – консоль управления JMS;
- JMS Client – пользовательский клиент JMS.

2.3 Поддержка соединения компонентов JMS с сервером JMS по SSL/TLS

Существует возможность защитить соединение сервера JMS с административным агентом из состава JMS Admin и клиентским агентом из состава JMS Client посредством протоколов SSL/TLS. Подробности настроек данных протоколов приведены в нескольких разделах руководства администратора, в частности см. «Руководство администратора. Часть 1» [2], раздел «Подготовка к использованию протоколов SSL/TLS».

2.4 Поддержка соединения сервера JMS с SQL-сервером по SSL/TLS

Существует возможность защитить соединение сервера JMS с сервером SQL посредством протоколов SSL/TLS. Подробное описание действий, необходимых для подготовки SQL-сервера к такому взаимодействию см. в документе «Руководство администратора. Часть 1» [2], раздел «Настройка SSL/TLS для работы cMicrosoft SQL Server».

2.5 Дополнительная документация

Рекомендуется дополнительно ознакомиться со следующими документами:

- «JC-Client. Руководство администратора» - содержит сведения по установке и настройке JC-Client;
- «eToken PKI Client. Руководство администратора» – содержит сведения по установке и настройке eToken PKI Client;
- «JC-PROClient для Windows. Справочное руководство» - содержит справочную информацию о JC-PROClient для Windows.
- «JaCarta Management System. Руководство пользователя» [1];
- «JaCarta Management System. Руководство администратора. Часть 1. Установка и настройка» [2];
- «JaCarta Management System. Руководство администратора. Часть 3. Установка и настройка сервера аутентификации (JAS)» [3].

3. Консоль управления JMS

Консоль управления JMS предоставляет графический интерфейс для администрирования JMS и доступна на тех компьютерах, на которых установлен компонент JMS Admin. Чтобы открыть окно консоли выполните следующие действия.

1. В меню **Пуск** выберите **JaCarta Management System** -> **Консоль управления JMS**.

Примечание. Первый запуск приложения Консоль управления JMS (т.е. если консоль управления запускается впервые после установки компонента JMS Server) может быть выполнен только от имени того пользователя, который осуществлял установку компонента JMS Server. Для запуска консоли управления от имени другого доменного пользователя Active Directory следует предварительно добавить этого пользователя в JMS и добавить ему одну из ролей JMS, имеющую право на запуск Консоли управления.

При первом запуске приложения Консоль управления JMS после того, как оно будет установлено на компьютере, пользователю будет предложено установить электронный ключ, с помощью которого будет выполняться его аутентификация в прилжоении. Для этого электронный ключ должен быть подсоединен к компьютеру.
При этом на экране отображается следущее приглашение.

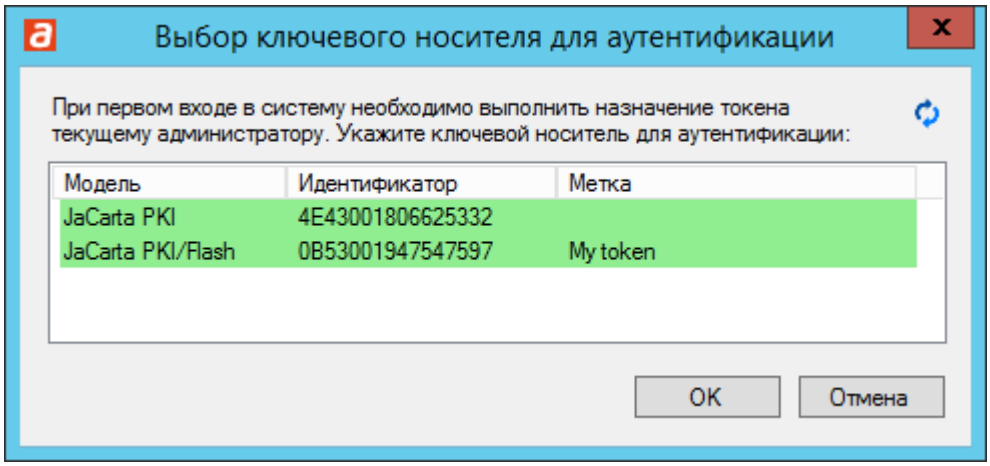


Рис. 1 – Окно выбора электронногоо ключа для аутентификации в консоли управления JMS

2. Выберите электронный ключ, с помощью которого вы будете выполнять аутентифкацию в консоли управления и нажмите OK.
Отобразится предупреждение следущего вида.

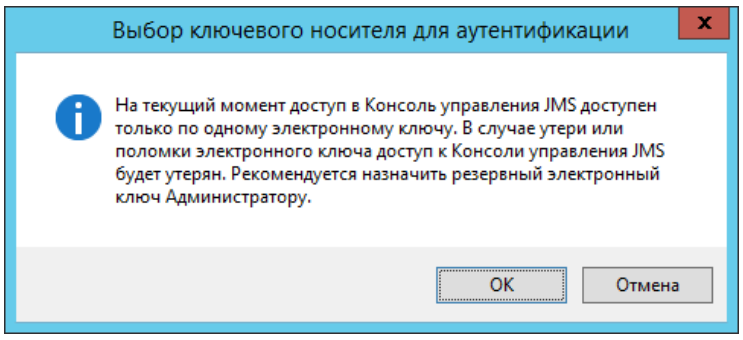


Рис. 2 – Предупреждении о возможности назначения резервного электронного ключа для аутентификации в консоли управления JMS

Примечание. Назначение электронного ключа пользователю может выполнить, например, Администратор ИБ из Консоли управления JMS после успешной аутентификации. Подробнее см. в разделе «Назначение электронного ключа пользователю», с. 71.

3. Нажмите **OK**.
   Отобразится окно ввода PIN-кода пользователя выбранного для аутентификации электронного ключа.

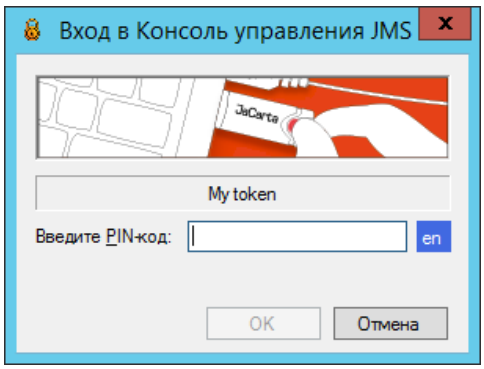


Рис. 3 – Окно ввода PIN-кода пользователя электронного ключа для аутентификации в консоли управления JMS

4. Введите PIN-код пользователя и нажимте **OK**.

После аутентификации консоль управления готова к использованию.

Интерфейс консоли управления JMS представлен на рис. 4.

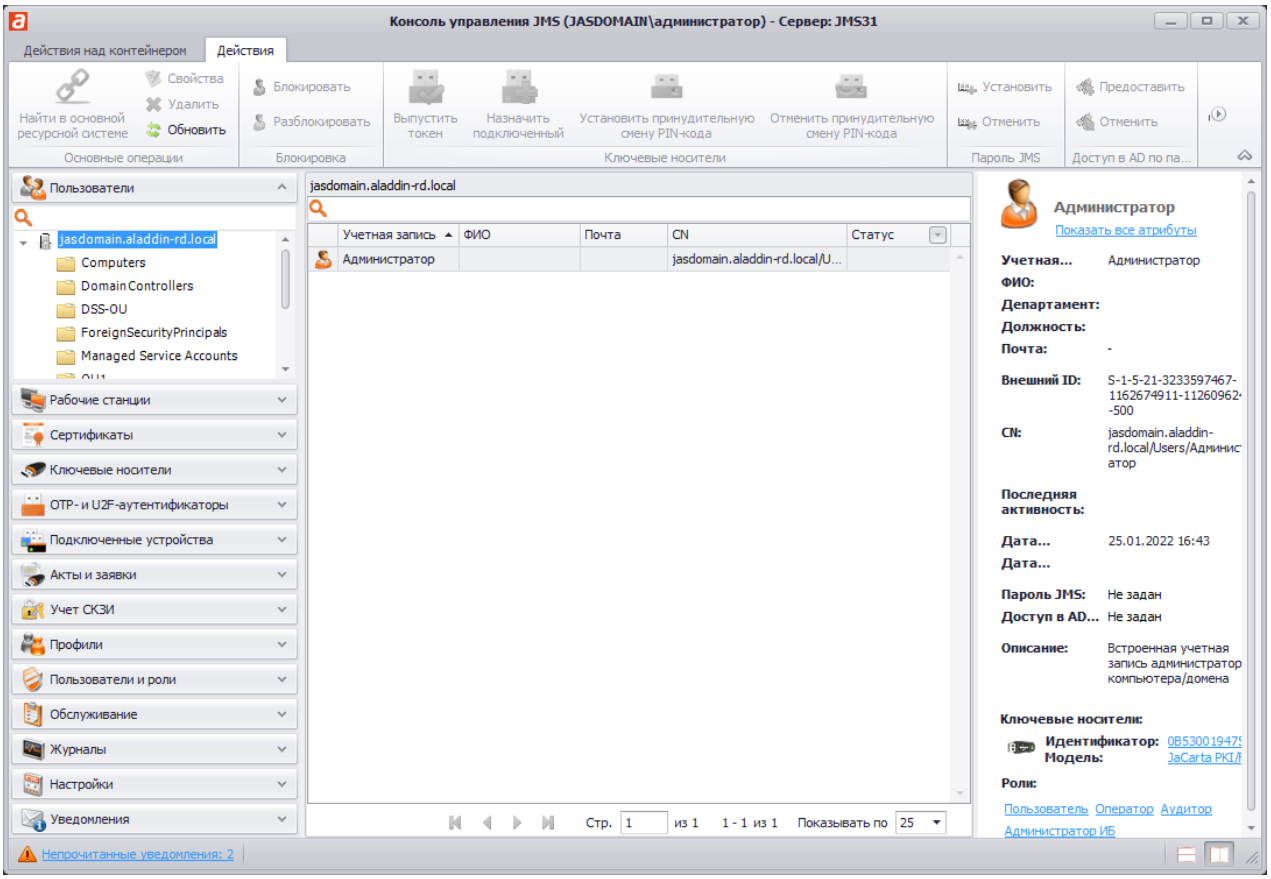


Рис. 4 – Интерфейс консоли управления JMS

В левой панели интерфейса расположен список разделов консоли управления JMS. В верхней панели располагаются вкладки ленты, соответствующие выбранному разделу. Лента на каждой

вкладке разделена на секции, содержащие группы действий, доступные в выбранном разделе JMS. Описание разделов JMS со ссылками на подробное описание доступных процедур представлено в табл. 3.

 В каждом разделе содержится секция **Помощь** со значком **О программе** – нажатие на этот значок отображает сведения о JMS. Т.к. значок во всех разделах выполняет одну и ту же функцию, его описание не включено в таблицу

Табл. 3 – Описание разделов консоли управления JMS

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
Пользователи		**Действия над контейнером**	**Регистрация**	• **Зарегистрировать** – позволяет зарегистрировать в JMS выбранных пользователей; • **Зарегистрировать всех** – позволяет зарегистрировать в JMS всех пользователей выбранного контейнера Active Directory. Сведения о регистрации пользователей представлены в подразделе «Регистрация пользователей в JMS», с. 36.
			Принудительная смена PIN-кода	• **Установить принудительную смену PIN-кода** – если эта настройка включена, все пользователи в выбранном контейнере должны будут сменить PIN-код электронного ключа для работы с JMS (см. «Установка и отмена принудительной смены PIN-кода», с. 40); • **Отменить принудительную смену PIN-кода** – отключает предыдущую настройку.
			Резервное копирование	**Экспорт** - позволяет экспортировать резервные копии объектов, выпущенных на электронные ключи пользователей (см. «Экспорт резервных копий объектов, выпущенных на электронный ключ», с. 112).
			Содержимое	**Отображать вложенные** - отображает все учетные записи из вложенных контейнеров ресурсной системы.
		Действия	**Основные операции**	• **Найти в основной ресурсной системе** – позволяет найти основную учетную запись пользователя, по которой проверяется аутентификация и привязка профилей; • **Свойства** – открывает окно свойств выбранного пользователя; • **Удалить** – позволяет удалить пользователя из JMS (см. «Удаление пользователей из JMS», с. 47); • **Обновить** – обновляет сведения, отображаемые в центральной части интерфейса.
			Блокировка	• **Блокировать** – позволяет заблокировать пользователя (см. «Блокировка/разблокировка пользователей», с. 46); • **Разблокировать** – позволяет разблокировать заблокированного пользователя.
			Ключевые носители	• **Выпустить токен** – позволяет выпустить электронный ключ для выбранного пользователя (см. «Выпуск электронного ключа администратором», с. 75); • **Назначить подключенный** – позволяет назначить подключенный электронный ключ пользователю (см. «Назначение электронного ключа пользователю», с. 71);

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
				• **Установить принудительную смену PIN-кода** – если эта настройка включена, выбранный пользователь или пользователи должны будут сменить PIN-код электронного ключа для работы с JMS (см. «Установка и отмена принудительной смены PIN-кода», с. 40); • **Отменить принудительную смену PIN-кода** – отменяет предыдущую настройку для выбранного пользователя или пользователей (см. «Установка и отмена принудительной смены PIN-кода», с. 40).
			Временный пароль	• **Установить** – установка временного пароля для работы с JMS; • **Отменить** – отмена временного пароля для работы с JMS. См. «Установка и отмена назначения временного пароля для работы с JMS», с. 41.
			Доступ AD по паролю	• **Предоставить** - предоставление пользователю временного доступа в Active Directory с помощью пароля; • **Отменить** – отмена доступа к Active Directory по временному паролю. См. «Предоставление и отмена временного доступа в Active Directory по паролю», с. 42
Рабочие станции (Раздел отсутствует в версии продукта *JMS CA Edition*)		**Действия**	**Основные операции**	• **Зарегистрировать** – позволяет зарегистрировать отдельные рабочие станции в JMS; • **Зарегистрировать все** – позволяет зарегистрировать все рабочие станции выбранного контейнера в JMS; • **Свойства** – отображает окно свойств рабочей станции; • **Удалить** – позволяет удалить рабочую станцию из JMS; • **Обновить** – обновляет сведения, отображаемые в центральной части интерфейса.
			Блокировка	• **Заблокировать** – позволяет заблокировать рабочую станцию; • **Разблокировать** – разблокирует ранее заблокированную рабочую станцию. См. «Блокировка/разблокировка рабочих станций», с. 49.
			Содержимое	**Отображать вложенные** – отображает рабочие станции из вложенных контейнеров Active Directory.
Сертификаты		**Действия над контейнером**	**Содержимое**	• **Отображать вложенные** – отображает сертификаты из вложенных контейнеров. • **Отображать удаленные** – отображает удаленные сертификаты. Удаленные сертификаты отображаются красным шрифтом.

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
		Действия	**Основные операции**	• **Свойства** – отображает окно свойств выбранного сертификата; • **Обновить** – обновляет сведения о сертификатах, отображаемые в центральной части интерфейса; • **Удалить** – позволяет удалить выбранный сертификат из JMS (см. «Удаление сертификата », с. 51).
			Управление состоянием	• **Включить** – позволяет восстановить действие сертификата, действие которого было ранее приостановлено (см. «Приостановка/восстановление действия сертификата», с. 52); • **Отключить** – позволяет приостановить действие сертификата (см. «Приостановка/восстановление действия сертификата», с. 52); • **Отозвать** – позволяет отозвать сертификат (см. «Отзыв сертификата», с. 52).
			Резервные копии	• **Импорт** – позволяет импортировать в JMS из файла резервную копию закрытого ключа, связанного с выбранным в интерфейсе сертификатом (см. «Импорт резервной копии закрытого ключа, связанного с сертификатом», с. 53); • **Экспорт** – позволяет экспортировать из JMS копию закрытого ключа, связанного с выбранным в интерфейсе сертификатом, в файл (см. «Экспорт резервной копии сертификата», с. 54); • **Удалить** – позволяет удалить из JMS копию закрытого ключа, связанный с выбранным в интерфейсе сертификатом (см. «Удаление резервной копии сертификата », с. 55).
Ключевые носители		**Действия над контейнером**	**Ключевые носители**	• **Импорт** – позволяет импортировать файл, содержащий список ключевых носителей (см. «Импорт (пакетная регистрация) электронных ключей в JMS», с. 68); • **Установить принудительную смену PIN-кода** - если эта настройка включена, пользователь выбранного электронного ключа должен будет сменить PIN-код электронного ключа для работы с JMS (см. «Установка и отмена принудительной смены PIN-кода», с. 40); • **Отменить принудительную смену PIN-кода** - отменяет предыдущую настройку для выбранного электронного ключа (см. «Установка и отмена принудительной смены PIN-кода», с. 40).
			Содержимое	**Отображать вложенные** – отображает электронные ключи из вложенных контейнеров.

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
		Действия	**Основные операции**	• **Зарегистрировать подключенный** – позволяет зарегистрировать подсоединенный электронный ключ (см. «Регистрация подсоединенных электронных ключей в JMS», с. 57); • **Экспорт выбранных** – позволяет экспортировать сведения об отмеченных электронных ключах в файл (см. «Экспорт электронных ключей», с. 64); • **Экспорт по списку** – позволяет экспортировать сведения об электронных ключах в файл по списку (см. «Подготовка списка электронных ключей для экспорта», с. 60); • **Свойства** – отображает окно свойств выбранного электронного ключа; • **Удалить** – позволяет удалить выбранный электронный ключ или ключи из JMS (см. «Удаление электронного ключа», с. 100); • **Обновить** – обновляет сведения об электронных ключах, отображаемые в центральной части интерфейса; • **Утилита создания списка** – (см. «Подготовка списка электронных ключей для экспорта», с. 60).
			Назначение	• **Назначить пользователю** – позволяет назначить выбранный электронный ключ пользователю (см.» Назначение электронного ключа пользователю», с. 71); • **Отменить назначение** – отменяет назначение электронного ключа пользователю; • **Перенос** – позволяет изменить привязку электронных ключей к контейнеру ресурсной системы (см. «Привязка электронных ключей к контейнерам ресурсной системы», с. 108).
			Вывод из эксплуатации	• **Включить** – позволяет включить возможность использования ранее отключенного электронного ключа (см. «Отключение/включение возможности использования электронного ключа», с. 81); • **Отключить** – позволяет временно отключить возможность использования электронного ключа (см. «Отключение/включение возможности использования электронного ключа», с. 81); • **Отозвать** – позволяет отозвать электронный ключ, например, в случае его утери, поломки или компрометации (см. «Отзыв электронного ключа», с. 88); • **Заменить** – позволяет заменить электронный ключ, например, в связи с истечением срока годности (см. «Замена электронного ключа», с. 91); • **Вернуть в эксплуатацию** – позволяет вернуть в эксплуатацию ранее отозванный электронный ключ (см. «Возврат в эксплуатацию электронного ключа», с. 95).
			Временная блокировка	**Удаленная разблокировка** – позволяет разблокировать электронный ключ в удаленном режиме (см. «Разблокировка электронного ключа в удаленном режиме», с. 97).

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
			Принудительная смена PIN-кода	• **Установить** - если эта настройка включена, пользователь электронного ключа должен будет сменить PIN-код для работы с JMS; • **Отменить** – отменяет предыдущую настройку для выбранного электронного ключа. См. «Установка и отмена принудительной смены PIN-кода», с. 40.
			PIN-код администратора	**Установить** – установка в базе данных JMS PIN-кода администратора для конкретного приложения в электронном ключе (см. «Установка в БД PIN-кода администратора для приложения электронного ключа», с. 109).
			Резервное копирование	**Экспорт** – позволяет экспортировать резервные копии объектов, записанных в память электронных ключей пользователей при выпуске (см. «Экспорт резервных копий объектов, выпущенных на электронный ключ», с. 112).
Ключевые носители		**Действия над контейнером**	**Ключевые носители**	• **Импорт** – позволяет импортировать файл, содержащий список ключевых носителей (см. «Импорт (пакетная регистрация) электронных ключей в JMS», с. 68); • **Установить принудительную смену PIN-кода** - если эта настройка включена, пользователь выбранного электронного ключа должен будет сменить PIN-код электронного ключа для работы с JMS (см. «Установка и отмена принудительной смены PIN-кода», с. 40); • **Отменить принудительную смену PIN-кода** - отменяет предыдущую настройку для выбранного электронного ключа (см. «Установка и отмена принудительной смены PIN-кода», с. 40).
			Содержимое	**Отображать вложенные** – отображает электронные ключи из вложенных контейнеров.

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
		Действия	**Основные операции**	• **Зарегистрировать подключенный** – позволяет зарегистрировать подсоединенный электронный ключ (см. «Регистрация подсоединенных электронных ключей в JMS», с. 57); • **Экспорт выбранных** – позволяет экспортировать сведения об отмеченных электронных ключах в файл (см. «Экспорт электронных ключей», с. 64); • **Экспорт по списку** – позволяет экспортировать сведения об электронных ключах в файл по списку (см. «Подготовка списка электронных ключей для экспорта», с. 60); • **Свойства** – отображает окно свойств выбранного электронного ключа; • **Удалить** – позволяет удалить выбранный электронный ключ или ключи из JMS (см. «Удаление электронного ключа», с. 100); • **Обновить** – обновляет сведения об электронных ключах, отображаемые в центральной части интерфейса; • **Утилита создания списка** – (см. «Подготовка списка электронных ключей для экспорта», с. 60).
			Назначение	• **Назначить пользователю** – позволяет назначить выбранный электронный ключ пользователю (см.» Назначение электронного ключа пользователю», с. 71); • **Отменить назначение** – отменяет назначение электронного ключа пользователю; • **Перенос** – позволяет изменить привязку электронных ключей к контейнеру ресурсной системы (см. «Привязка электронных ключей к контейнерам ресурсной системы», с. 108).
			Вывод из эксплуатации	• **Включить** – позволяет включить возможность использования ранее отключенного электронного ключа (см. «Отключение/включение возможности использования электронного ключа», с. 81); • **Отключить** – позволяет временно отключить возможность использования электронного ключа (см. «Отключение/включение возможности использования электронного ключа», с. 81); • **Отозвать** – позволяет отозвать электронный ключ, например, в случае его утери, поломки или компрометации (см. «Отзыв электронного ключа», с. 88); • **Заменить** – позволяет заменить электронный ключ, например, в связи с истечением срока годности (см. «Замена электронного ключа», с. 91); • **Вернуть в эксплуатацию** – позволяет вернуть в эксплуатацию ранее отозванный электронный ключ (см. «Возврат в эксплуатацию электронного ключа», с. 95).
			Временная блокировка	**Удаленная разблокировка** – позволяет разблокировать электронный ключ в удаленном режиме (см. «Разблокировка электронного ключа в удаленном режиме», с. 97).

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
			Принудительная смена PIN-кода	• **Установить** - если эта настройка включена, пользователь электронного ключа должен будет сменить PIN-код для работы с JMS; • **Отменить** – отменяет предыдущую настройку для выбранного электронного ключа. См. «Установка и отмена принудительной смены PIN-кода», с. 40.
			PIN-код администратора	**Установить** – установка в базе данных JMS PIN-кода администратора для конкретного приложения в электронном ключе (см. «Установка в БД PIN-кода администратора для приложения электронного ключа», с. 109).
			Резервное копирование	**Экспорт** – позволяет экспортировать резервные копии объектов, записанных в память электронных ключей пользователей при выпуске (см. «Экспорт резервных копий объектов, выпущенных на электронный ключ», с. 112).
OTP- и U2F-аутентификаторы	**OTP-токены**	**Действия**	–	Сводная таблица операций с OTP-токенами приведена в разделе «Операции с OTP- и U2F-аутентификаторами», с. .120
	Messaging-токены			
	U2F-аутентификаторы			
Ридеры смарт-карт		**Действия над контейнером**	**Ридеры смарт-карт**	• **Импорт** – позволяет импортировать файл, содержащий список ридеров смарт-карт (см. «Импорт (пакетная регистрация) ридеров смарт-карт в JMS», с. 151)
			Содержимое	**Отображать вложенные** – отображает ридеры смарт-карт из вложенных контейнеров.

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
		Действия	**Основные операции**	• **Зарегистрировать подключенный** – позволяет зарегистрировать подсоединенный ридер смарт-карт (см. «Регистрация подключенных ридеров смарт-карт в JMS», с. 144); • **Экспорт выбранных** – позволяет экспортировать сведения об отмеченных ридеров смарт-карт в файл (см. «Экспорт ридеров смарт-карт», с. 147); • **Экспорт по списку** – позволяет экспортировать сведения об ридерах смарт-карт в файл по списку (см. «Экспорт ридеров смарт-карт», с. 147); • **Свойства** – отображает окно свойств выбранного ридера смарт-карт; • **Удалить** – позволяет удалить выбранный ридер / ридеры смарт-карт из JMS (см. «Удаление ридера смарт-карт», с. 154); • **Обновить** – обновляет сведения о ридерах смарт-карт, отображаемые в центральной части интерфейса; • **Утилита создания списка** – (см. «Подготовка списка ридеров смарт-карт для экспорта», с. 147).
			Назначение	• **Назначить пользователю** – позволяет назначить выбранный ридер смарт-карт пользователю (см. «Назначение ридера смарт-карт пользователю», с. 154); • **Отменить назначение** – отменяет назначение ридера пользователю; • **Перенос** – позволяет изменить привязку ридеров смарт-карт к контейнеру ресурсной системы (см. «Перенос привязки ридеров смарт-карт к контейнерам ресурсной системы?», с. 154).
Подключенные устройства	**Ключевые носители**	**Действия**	**Быстрые операции**	• **Зарегистрировать и выпустить** – позволяет зарегистрировать и выпустить подсоединенный электронный ключ (см. «Регистрация подсоединенных электронных ключей в JMS», с. 57 и «Выпуск электронного ключа администратором», с. 75); • **Зарегистрировать** – позволяет зарегистрировать подсоединенный электронный ключ (см. «Регистрация подсоединенных электронных ключей в JMS», с. 57); • **Очистить** – позволяет удалить из приложений электронного ключа все объекты и проинициализировать их в соответствии с выбранным профилем инициализации (см. «Очистка электронного ключа», с. 82) • **Синхронизация** – позволяет синхронизировать содержимое выбранного электронного ключа с сервером JMS (см. «Синхронизация электронного ключа», 85).
			Основные операции	• **Свойства** – отображает окно свойств выбранного электронного ключа; • **Удалить** – позволяет удалить выбранный электронный ключ или ключи из JMS (см. «Удаление электронного ключа», с. 100); • **Обновить** – обновляет сведения об электронных ключах в центральной части интерфейса.
			Назначение	• **Назначить пользователю** – позволяет назначить выбранный электронный ключ пользователю (см. «Назначение электронного ключа пользователю», с. 71);

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
				• **Отменить назначение** – отменяет назначение электронного ключа пользователю; • **Перенос** - позволяет изменить привязку электронных ключей к контейнеру ресурсной системы (см. «Привязка электронных ключей к контейнерам ресурсной системы», с. 108).
			Вывод из эксплуатации	• **Включить** – позволяет включить возможность использования ранее отключенного электронного ключа (см. «Отключение/включение возможности использования электронного ключа», с. 81); • **Отключить** – отключает возможность использования электронного ключа (см. «Отключение/включение возможности использования электронного ключа», с. 81); • **Отозвать** – позволяет отозвать электронный ключ (см. «Отзыв электронного ключа», с. 88); • **Заменить** – позволяет заменить электронный ключ, например, в случае истечения его срока годности (см. «Замена электронного ключа», с. 91); • **Вернуть в эксплуатацию** – позволяет вернуть в эксплуатацию ранее отозванный электронный ключ (см. «Возврат в эксплуатацию электронного ключа», с. 95).
			Временная блокировка	• **Разблокировать** – позволяет разблокировать заблокированный электронный ключ (см. «Разблокировка подсоединенного электронного ключа», с. 96); • **Заменить отпечатки пальцев (BIO)** – позволяет заменить отпечатки пальцев, хранящиеся в памяти электронного ключа, например, в случае передачи ключа другому пользователю (см. «Замена отпечатков пальцев, сохраненных в памяти JaCarta PKI/BIO», с. 100) • **Сменить PIN-код пользователя** – позволяет сменить PIN-код подсоединенного электронного ключа. Для смены PIN-кода пользователя в приложении ГОСТ 2 следует убедиться, что данный тип PIN-кода был установлен в электронном ключе (устанавливается при инициализации приложения ГОСТ 2 на производстве или с помощью внешнего ПО)
			PIN-код ЭП	**Установить/Сменить** – позволяет установить или сменить PIN-код подписи (ЭП) в электронных ключах JaCarta 2 ГОСТ (см. «Установка и смена PIN-кода подписи в JaCarta-2 ГОСТ», с. 105).
			Принудительная смена PIN-кода	• **Установить** - если эта настройка включена, пользователь выбранного электронного ключа должен будет сменить PIN-код электронного ключа для работы с JMS; • **Отменить** - отменяет предыдущую настройку для выбранного электронного ключа. См. «Установка и отмена принудительной смены PIN-кода», с. 40.
			PIN-код администратора	**Установить** – установка в базе данных JMS PIN-кода администратора для конкретного приложения в электронном ключе (см. «Установка в БД PIN-кода администратора для приложения электронного ключа», с. 109).

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
			Резервное копирование	**Экспорт** – позволяет экспортировать резервные копии объектов, выпущенных в память электронного ключа (см. «Экспорт резервных копий объектов, выпущенных на электронный ключ», с. 112).
Подключенные устройства (продолжение)	**Ридеры смарт-карт**	**Действия**	**Быстрые операции**	**Зарегистрировать** – позволяет зарегистрировать подсоединенный ридер смарт-карт (см. «Регистрация подключенных ридеров смарт-карт в JMS», с. 144)
			Основные операции	• **Свойства** – отображает окно свойств выбранного ридера смарт-карт; • **Удалить** – позволяет удалить выбранный ридер / ридеры смарт-карт из JMS (см. «Удаление ридера смарт-карт», с. 154); • **Обновить** – обновляет сведения о ридерах смарт-карт в центральной части интерфейса.
			Назначение	• **Назначить пользователю** – позволяет назначить выбранный ридер смарт-карт пользователю (см. «Назначение ридера смарт-карт пользователю», с. 154); • **Отменить назначение** – отменяет назначение ридера пользователю; • **Перенос** – позволяет изменить привязку ридеров смарт-карт к контейнеру ресурсной системы (см. «Перенос привязки ридеров смарт-карт к контейнерам ресурсной системы?», с. 154).
Акты и заявки		**Действия**	**Основные операции**	• **Просмотр** – просмотр выбранного акта/заявки в требуемом шаблоне (подробнее см. раздел «Акты и заявки», с. 312); • **Печать** – то же для печати (см. раздел «Акты и заявки», с. 312); • **Свойства** – отображает окно свойств выбранного акта/заявки; • **Обновить** – обновляет сведения о документах в центральной части интерфейса
			Содержимое	**Отображать вложенные** – отображает акты/заявки из вложенных контейнеров.
Профили	**Профили**	**Действия**	**Профили**	• **Создать** – позволяет создать профиль JMS (см. «Настройка профилей JMS», с. 155); • **Удалить** – позволяет удалить профиль JMS; • **Свойства** – Открывает окно свойств профиля JMS; • **Обновить** – обновляет сведения о профилях JMS в центральной части интерфейса; • **Экспорт** – экспортирует созданный профиль JMS (см. «Экспорт/импорт профилей», с. 304); • **Импорт** – импортирует профиль JMS (см. «Экспорт/импорт профилей», с. 304).

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
	Привязка профилей	**Действия**	**Основные операции**	• **Привязать** – позволяет привязать профиль JMS к какому-либо контейнеру ресурсной системы (см. «Привязка профилей», с. 296); • **Создать и привязать профиль** – позволяет создать и привязать профиль JMS; • **Обновить** – обновляет сведения, отображающиеся в центральной части интерфейса; • **Разрешить** – распространяет действие привязанных профилей вышестоящего контейнера на выбранный контейнер и все вложенные в него контейнеры (см. «Наследование профилей», с. 298); • **Запретить** – запрещает действие привязанных профилей вышестоящего контейнера на выбранный контейнер и все вложенные в него контейнеры (см. «Наследование профилей», с. 298).
Пользователи и роли	**Глобальные группы**	**Действия**	**Глобальные группы**	• **Создать** – позволяет создать глобальную группу JMS; • **Удалить** – позволяет удалить глобальную группу JMS; • **Свойства** – открывает окно свойств выбранной глобальной группы JMS; • **Обновить** – обновляет сведения о глобальных группах в центральной части интерфейса.
			Учетные записи	• **Выбрать пользователей** – позволяет добавить пользователей в глобальную группу JMS; • **Выбрать рабочие станции** – позволяет добавить рабочие станции в глобальную группа JMS; • **Исключить** – позволяет исключить пользователей или рабочие станции из глобальной группы JMS.
	Роли	**Действия**	**Роли**	• **Создать** – позволяет создать роль JMS (см. «Создание новой роли JMS», с. 390); • **Удалить** – позволяет удалить роль JMS; • **Свойства** – открывает окно свойств роли JMS; • **Обновить** – обновляет сведения о ролях JMS в центральной части интерфейса.

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
			Операции	• **Развернуть все** – разворачивает списки всех категорий операций в нижней центральной части интерфейса; • **Свернуть все** – сворачивает списки всех категорий операций в нижней центральной части интерфейса; • **Свойства** – отображает окно свойств выбранной роли; • **Обновить** – обновляет сведения о ролях в центральной части интерфейса.
	Назначение ролей	**Действия**	**Роли**	• **Свойства** – отображает окно свойств выбранной роли; • **Обновить** – обновляет сведения о ролях в центральной части интерфейса.
			Пользователи	• **Добавить** – позволяет добавить пользователя в роль (см. «Назначение ролей пользователям JMS», с. 395); • **Удалить** – позволяет удалить пользователя из роли; • **Обновить** – обновляет сведения о ролях и добавленных в них пользователях в центральной части интерфейса.
	Делегирование управления	**Действия**	**Основные операции**	• **Делегировать управление** – позволяет делегировать управление выбранным организационным подразделением определенному пользователю (см. «Делегирование управления», с. 397). • **Обновить** – обновляет сведения в центральной части интерфейса.
Обслуживание	**Планы обслуживания**	**Действия**	**Планы и задачи**	• **Добавить в очередь** – добавляет в очередь на выплонение с последующим запуском выбранный план обслуживания; • **Отменить** – отменяет выполнение запущенного плана обслуживания; • **Свойства** – отображает окно свойств выбранного плана обслуживания; • **Обновить** – обновляет сведения о планах обслуживания в центральной части интерфейса; • **Отчет** – отображает отчет о последнем выполнении выбранного плана обслуживания.
Журналы		**Действия**	**Основные**	Позволяет выполнить следующие действия с записями в журнале: • **Отметить как прочитанное** (только для предупреждений) – событие будет отмечено как прочитанное; • **Отметить как непрочитанное** (только для предупреждений) – событие будет отмечено как непрочитанное; • **Отчет** (только для отчетов планов обслуживания) – отображает отчет о выполнении планов обслуживания; • **Обновить** – обновляет сведения в центральной части интерфейса.

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
			Периоды	В этой секции можно выбрать период, за который будут отображаться события в журнале, доступны следующие варианты: • **Все**, **1 час**, **24 часа**, **7 дней** , **30 дней**, **Сегодня**, **Неделя**, **Месяц**; • **Произвольный период** – позволяет задать период отображения вручную.
			Настройки (только для клиентских событий)	В этой секции выполняется настройка фильтра клиентских событий в случае, если нужно ограничить запись таких событий в журнал. • **Фильтр** – вызов окна настройки фильтрации клиентских событий при их записи в журнал, подробнее см. в разделе «Управление журналом Клиентские события», с. 471
Настройки	**Лицензии**	Не актуально		Отображает сведения об установленных лицензиях JMS.
	Крипто-плагины	Не актуально		Отображает сведения об установленных крипто-плагинах.
	Параметры криптографии	Не актуально		Отображает сведения о текущих параметрах криптографии базы данных JMS.
	Мастер-ключи БД	Не актуально		Отображает сведения о мастер-ключах базы данных JMS.
	Информация о сервере	Не актуально		Отображает сведения о сервере JMS.
	Модели ключевых носителей	Не актуально		Содержит список поддерживаемых ключевых носителей.
	Шаблоны печати	Не актуально		Содержит список шаблонов печати.
	Журналы	Не актуально		Содержит настройки журналов (см. «Ограничение числа записей в журнале клиентских событий», с. 472).

Раздел	Подраздел (если есть)	Вкладка	Секция	Доступные действия
Уведомления	**Шаблоны**	**Действия**	**Основные операции**	• **Создать** – позволяет создать шаблон; • **Свойства** – отображает окно свойств выбранного шаблона; • **Удалить** – позволяет удалить шаблон; • **Обновить** – обновляет сведения о шаблонах в центральной части интерфейса. См. «Уведомления о событиях, связанных с использованием JMS», с. 432.
	Административные правила рассылки			
	Пользовательские правила рассылки			

3.1 Отображение консоли управления JMS в режиме ограниченной функциональности

Существует возможность настроить запуск консоли управления JMS в режиме ограниченной функциональности. В этом режиме в консоли отображаются не все разделы и доступны не все функции.

Примечание. Режим ограниченной функциональности недоступен в версии *CA Edition* продукта JMS (см. «Руководство администратора. Часть 1» [2], раздел «Версии поставки продукта и лицензионные опции»).

Для включения запуска консоли управления JMS с ограниченной функциональностью выполните следующие действия.

1. В редакторе реестра перейдите в следующий раздел реестра:
   - Чтобы настроить запуск консоли управления JMS на уровне компьютера: **HKEY_LOCAL_MACHINE\Software\Aladdin\EAP Administrative Client\Settings**.
   - Чтобы настроить запуск консоль управления JMS на уровне текущего пользователя: **HKEY_CURRENT_USER\Software\Aladdin\EAP Administrative Client\Settings**.
2. Отредактируйте (или создайте, если отсутствует) в этом разделе параметр DWORD **IsLITEVersion** следующим образом:
   - **0** – консоль управления JMS запускается в режиме полной функциональности;
   - **1** – консоль управления JMS запускается в режиме ограниченной функциональности.
3. Перезапустите консоль управления JMS

В режиме ограниченной функциональности доступны следующие разделы и возможности.

- Отображаемые разделы:
  - **Пользователи**;
  - **Ключевые носители**;
  - **Подключенные устройства**.
- В окне свойств пользователя скрыты вкладки:
  - **Учетные записи**;
  - **Группы**;
  - **Роли**;
  - **Ключевые носители**;
  - **Действующие профили**;
  - **Сертификаты** (оператора);
  - **Объекты пользователя**;
- В окне свойств ключевого носителя скрыта вкладка **Содержимое**.
- Элементы управления, которые недоступны пользователю согласно ролевой модели, не отображаются в интерфейсе консоли управления JMS.

3.2 Настройка пользовательского интерфейса консоли управления JMS

Для удобства использования консоль управления JMS позволяет настраивать табличную часть отображения объектов, в частности:

- добавление новых колонок (полей записей);
- скрытие лишних колонок (полей записей);
- перемещение колонок по горизонтали методом перетаскивания;
- восстановление способа отображения по умолчанию;
- сортировку записей по полям.

Так, для того чтобы добавить новую колонку в таблице, например поле телефона (Telephone-Number) в разделе **Пользователи**, в заголовочной части таблицы нажмите правой кнопкой мыши (Рис. 5).

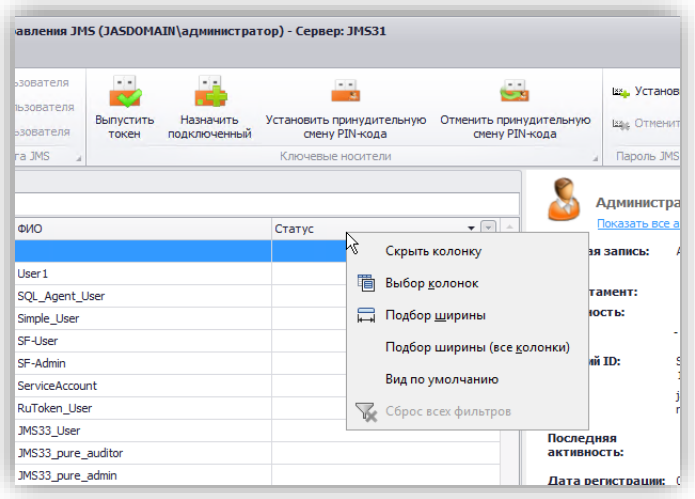


Рис. 5 – Настройка табличной части пользовательского интерфейса консоли управления JMS

В открывшемся меню нажмите **Выбор колонок**, найдите поле Telephone-Number и добавьте его двойным щелчком мыши (Рис. 6).

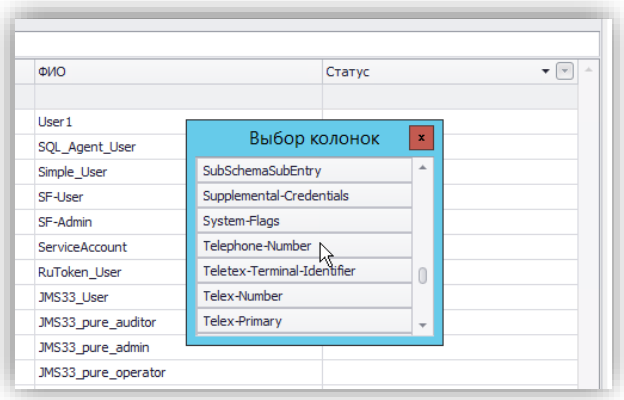


Рис. 6 – Выбор поля для добавления в таблицу

Чтобы скрыть колонку, нажмите на ее заголовочной части левой кнопкой мыши и выберите **Скрыть колонку**.

Для сортировки записей по полю (в прямом или обратном порядке), последовательно нажимайте в заголовочной части данной колонки таблицы левой кнопкой мыши.

3.3 Управление пользователями

3.3.1 Регистрация пользователей в JMS

3.3.1.1 Регистрация пользователей из одного каталога учетных записей

Чтобы зарегистрировать новых пользователей, выполните следующие действия.

4. В консоли управления JMS перейдите в раздел **Пользователи**.
   Окно консоли будет выглядеть следующим образом.

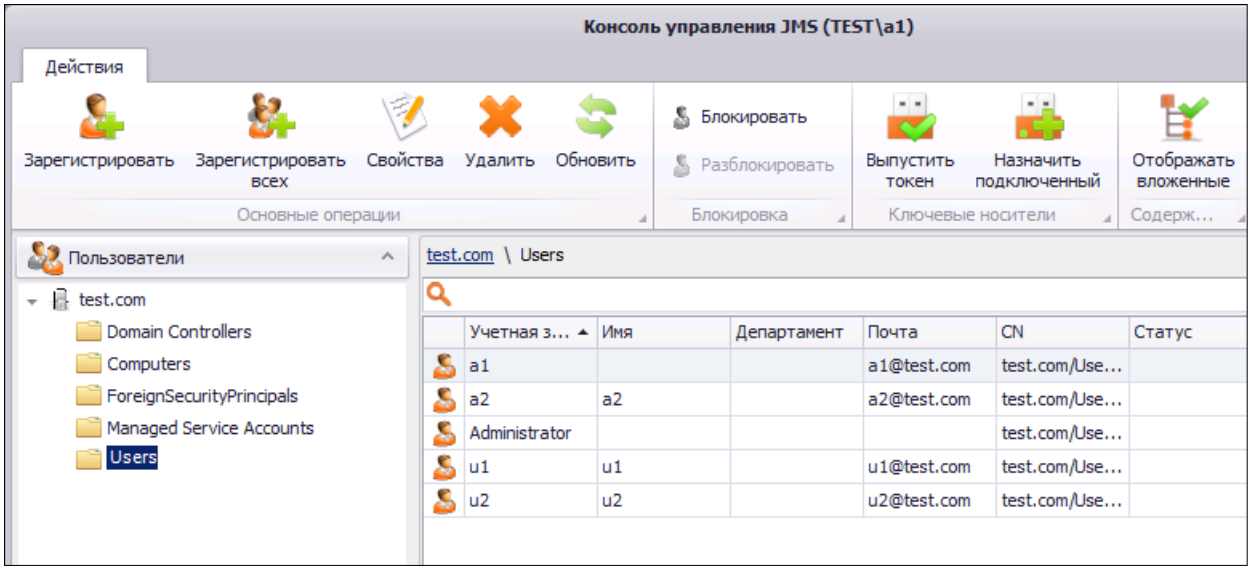


*Рис. 7 – Раздел **Пользователи** консоли управления JMS*

5. Выберите нужный каталог (например, **Users** (Пользователи) или другую организационную единицу) и в верхней панели щелкните на одном из следующих значков:

   - **Зарегистрировать** – чтобы зарегистрировать только некоторых пользователей из выбранного каталога;
   - **Зарегистрировать всех** – чтобы зарегистрировать всех пользователей выбранного каталога.

6. В зависимости от выбранного способа регистрации (**Зарегистрировать** или **Зарегистрировать всех**) выполните следующие действия.

   Если вы выбрали **Зарегистрировать**.

   6.1. В окне **Регистрация новых пользователей** установите флаги напротив пользователей, которых вы хотите зарегистрировать в JMS (чтобы отметить всех пользователей, установите флаг в верхней строке).

   6.2. В нижней части окна нажмите **Зарегистрировать**.

   Если вы выбрали **Зарегистрировать всех**.

   6.3. В отобразившемся сообщении нажмите **Да** для подтверждения операции - после подтверждения произойдет автоматическая регистрация всех пользователей выбранного каталога.

Если при регистрации всех пользователей (**Зарегистрировать всех**) некоторые пользователи из выбранного каталога уже зарегистрированы в JMS, то по завершении регистрации отобразится окно, содержащее список таких (ранее зарегистрированных) пользователей. В этом случае нажмите **Завершить**.

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.

Зарегистрированные пользователи отобразятся в окне консоли управления JMS.

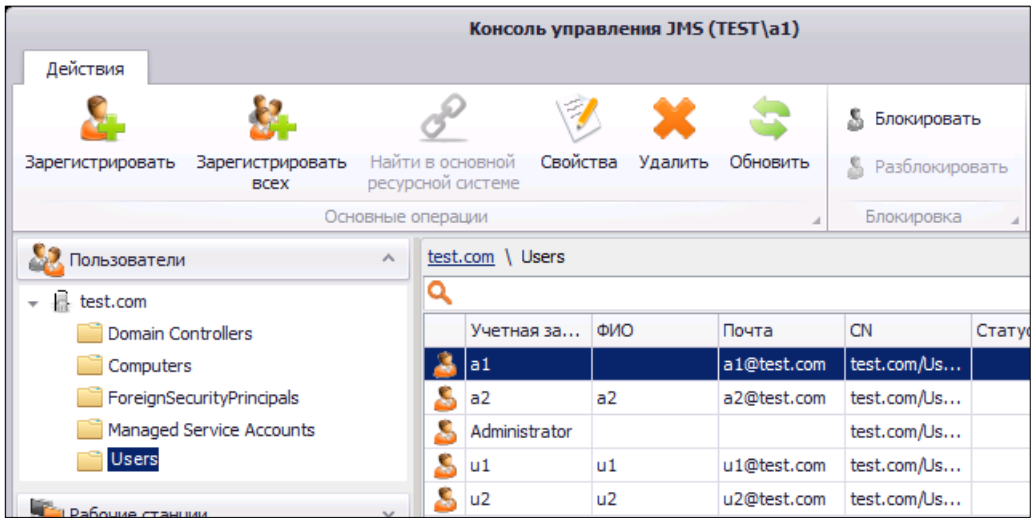


Рис. 8 – Список зарегистрированных пользователей

3.3.1.2 Регистрация пользователей из связанных каталогов учетных записей

Чтобы зарегистрировать пользователей из связанных каталогов учетных записей, выполните следующие действия.

В настоящем документе для примера в качестве основного каталога учетных записей будет использоваться Active Directory, а в качестве зависимого – КриптоПро УЦ 2.0.

1. В консоли управления JMS перейдите в раздел **Пользователи**.
2. В левой панели выберите основной каталог учетных записей (в нашем примере - Active Directory) и в верхней панели нажмите **Зарегистрировать**.

Для успешной регистрации необходимо, чтобы все учетные записи из основного каталога имели совпадающий атрибут (первичный ключ) с учетными записями из зависимого каталога – в противном случае операция не будет завершена.

Отобразится следующее окно.

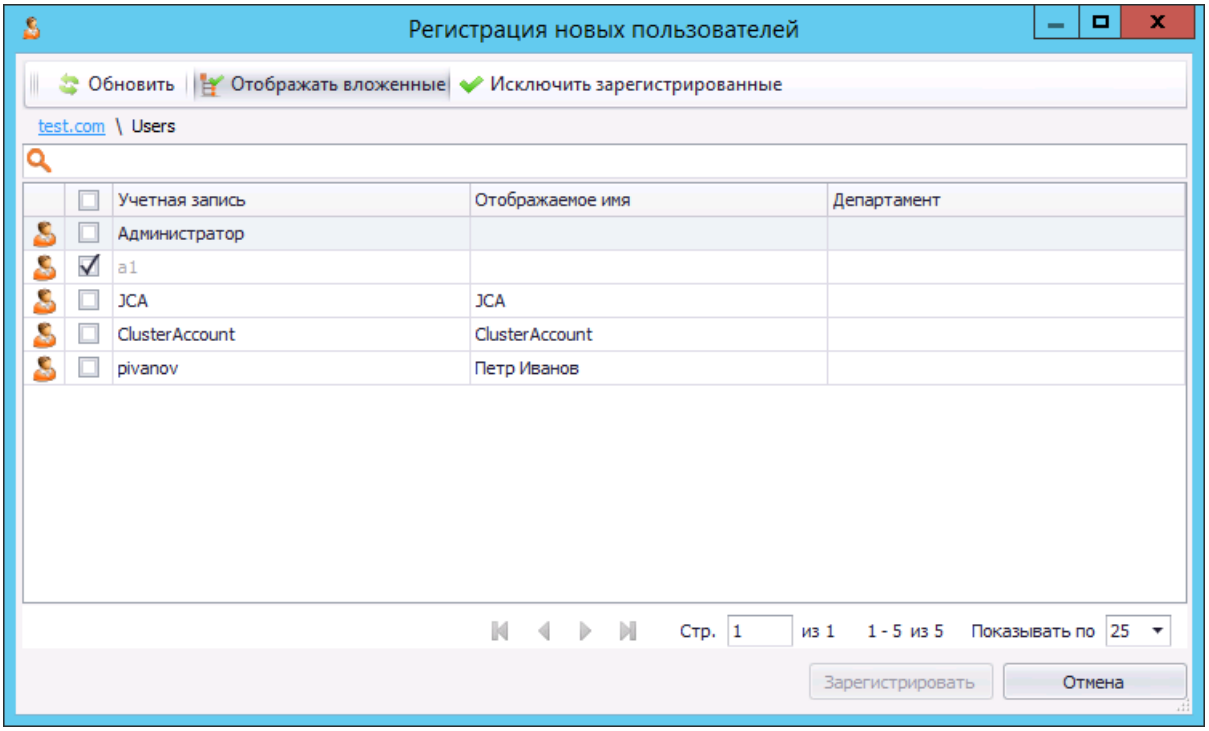


Рис. 9 – Список пользователей каталога учетных записей

3. Отметьте пользователей, которых вы хотите зарегистрировать, и нажмите **Зарегистрировать**. После регистрации новые пользователи отобразятся в центральной части окна консоли управления JMS.

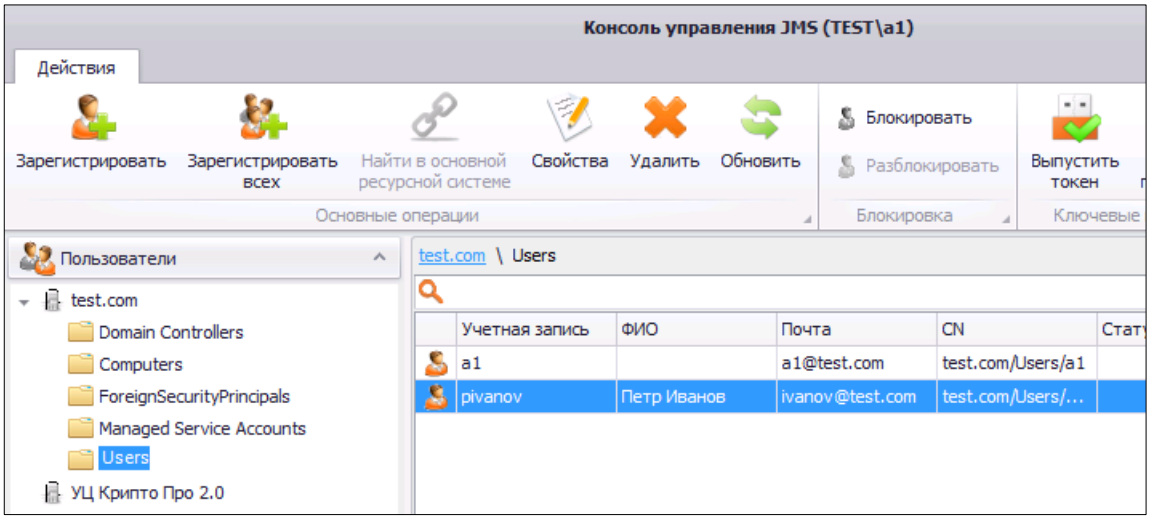


Рис. 10 – Новый пользователь отображен в центральной части окна консоли управления JMS

4. Чтобы убедиться в том, что пользователь с выбранным для связи каталогов учетной записи атрибутом также зарегистрирован из зависимого каталога учетных записей (в нашем случае – КриптоПро 2.0), выберите этот зависимый каталог в левой панели консоли управления JMS.

Пользователи с совпадающим атрибутом отобразятся в центральной части окна.

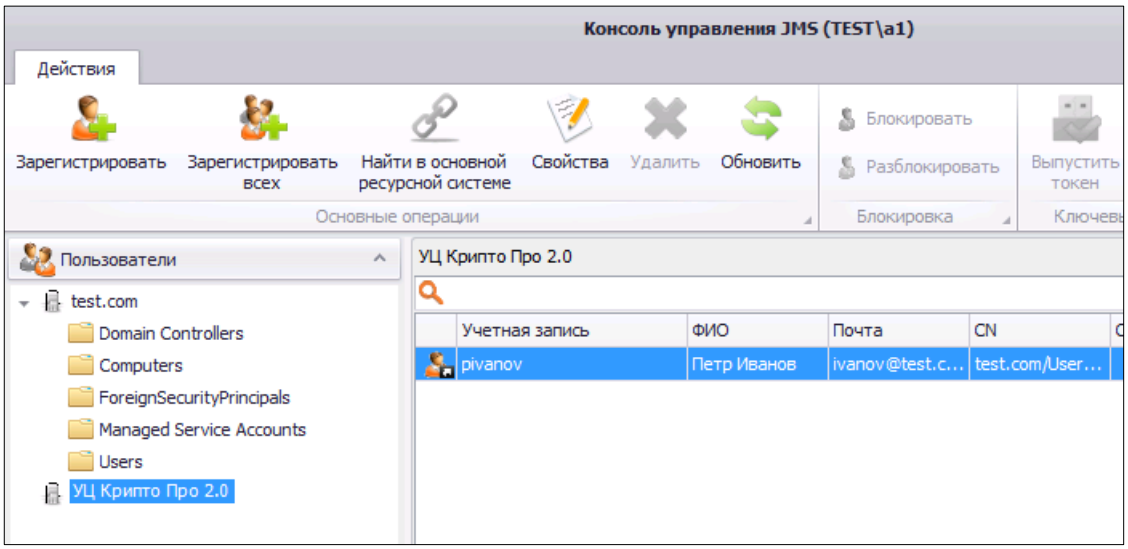


Рис. 11 – Пользователь из зависимого каталога учетных записей был зарегистрирован автоматически

5. Двойным щелчком на записи пользователя откройте свойства этого пользователя.
6. В отобразившемся окне перейдите на вкладку **Учетные записи**.

Окно примет следующий вид.

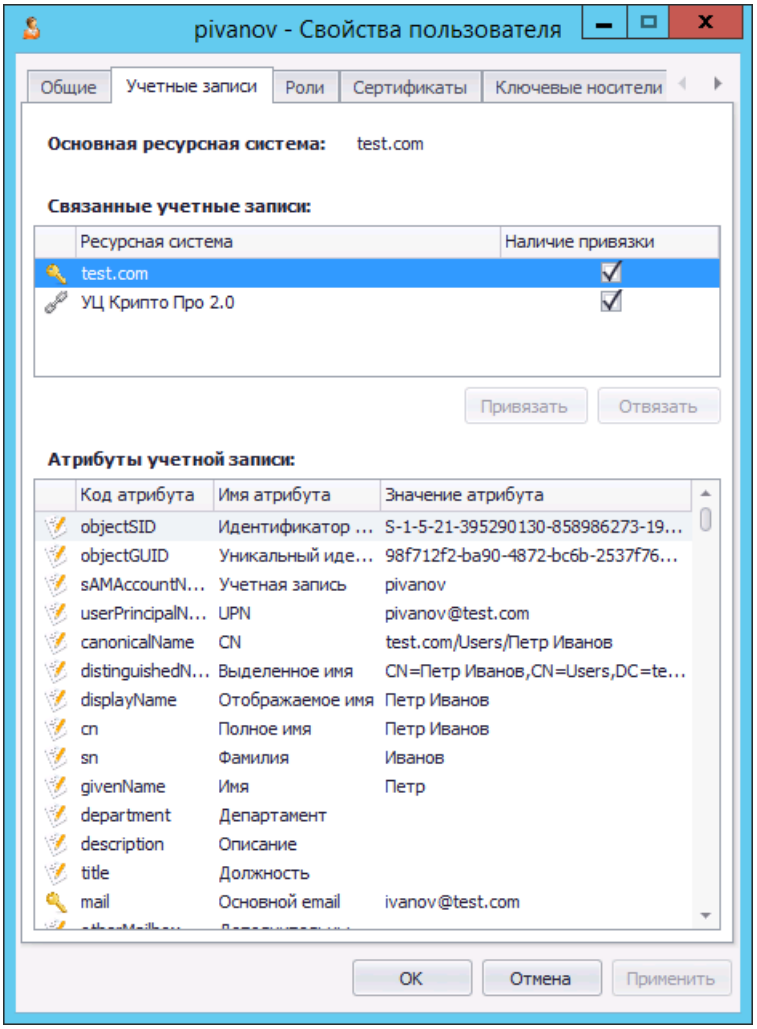


*Рис. 12 – Вкладка **Учетные записи** окна свойств пользователя*

7. В списке **Связанные учетные записи** будут отображаться связанные (основной и зависимый) каталоги учетных записей, при этом основной каталог будет отмечен значком в виде ключа.
8. В списке **Атрибуты учетной записи** первичный ключ (связывающий атрибут) будет отмечен значком в виде ключа.

3.3.2 Установка и отмена принудительной смены PIN-кода

JMS позволяет установить принудительную смену PIN-кода для электронных ключей пользователей JMS. Если такая настройка для пользователя будет включена, то он не сможет воспользоваться Клиентом JMS до тех пор, пока не сменит PIN-код пользователя своей электронной карты. Впоследствии можно отключить такую настройку.

Чтобы установить/отменить принудительную смену PIN-кода электронного ключа для пользователя или пользователей, выполните следующие действия.

1. В левой панели консоли управления JMS перейдите в раздел **Пользователи** и выберите нужный контейнер, содержащий пользователей.
2. В центральной части окна выберите пользователей, для которых вы хотите включить или отключить принудительную смену PIN-кода электронного ключа.
3. В верхней панели щелкните на одном из следующих значков:

- **Установить принудительную смену PIN-кода** – чтобы включить принудительную смену PIN-кода для выбранного пользователя или пользователей;
- **Отменить принудительную смену PIN-кода** – чтобы отключить принудительную смену PIN-кода для выбранного пользователя или пользователей.

Отобразится предупреждающее сообщение.

4. Нажмите **Да**, чтобы подтвердить действие.
   Отобразится сообщение об успешном выполнении операции.
5. Нажмите **ОК** для завершения процедуры.

3.3.3 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.

3.3.3.1 Установка временного пароля

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

1. В левой части консоли управления JMS перейдите в раздел **Пользователи** и выберите контейнер, содержащий нужного пользователя.
2. В центральной части окна выберите нужного пользователя.
3. В верхней панели нажмите **Установить**.
   Отобразится следующее окно.

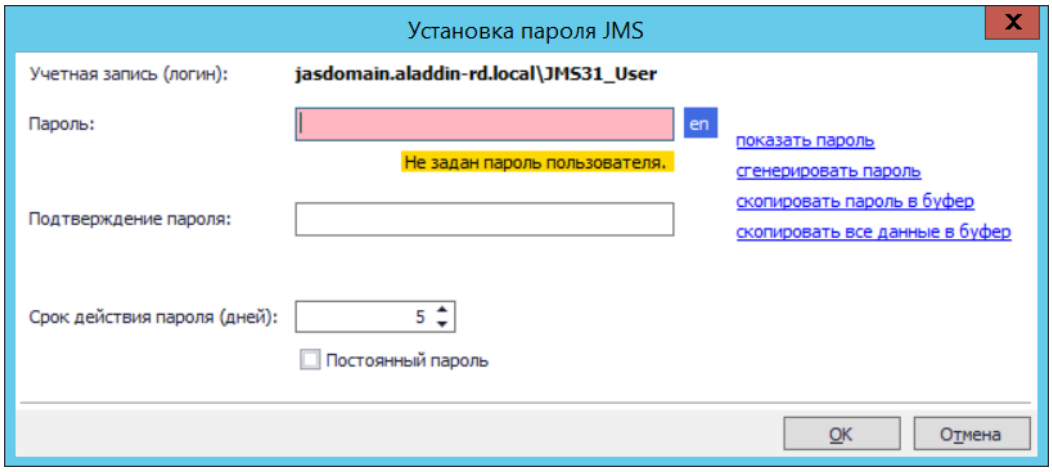


Рис. 13 – Задание временного пароля для работы с JMS

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

Вы также можете воспользоваться ссылкой **сгенерировать пароль**, 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 другими ссылками справа:

- **показать пароль** – отображает значение пароля;
- **скопировать пароль в буфер** – копирует в буфер значение временного пароля, чтобы его можно было передать пользователю;

– **скопировать все данные в буфер** – копирует в буфер имя пользователя и домен, значение временного пароля, а также срок действия временного пароля, чтобы эти данные можно было передать пользователю.

Отобразится сообщение следующего вида.

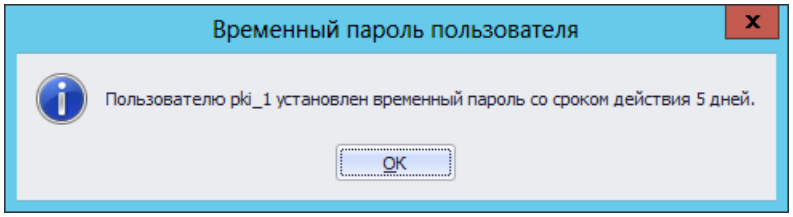


Рис. 14 – Сообщение об успешной установке временного пароля

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

3.3.3.2 Отмена действия временного пароля

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

1. В левой части консоли управления JMS перейдите в раздел **Пользователи** и выберите контейнер, содержащий нужного пользователя.
2. В центральной части окна выберите нужного пользователя.
3. В верхней панели нажмите **Отменить**.
4. В окне предупреждающего сообщения нажмите **Да**, чтобы подтвердить действие.
5. В окне сообщения об успешном выполнении операции нажмите **OK**, чтобы завершить процедуру.

3.3.4 Предоставление и отмена временного доступа в Active Directory по паролю

JMS позволяет установить временный вход с использованием пароля пользователя. Это может понабиться, если пользователь не имеет доступа к своему электронному ключу (например, если электронный ключ утерян или вышел из строя). Также, существует возможность отменить возможность временного входа ранее установленного срока действия такого входа.

Подробнее см. «Руководство администратора. Часть 1» [2], раздел «Разрешения для принудительного входа по смарт-карте и открытия входа по паролю AD».

3.3.4.1 Предоставление временного доступа по паролю

Чтобы предоставить пользователю временный доступ по паролю, выполните следующие действия.

1. В левой части консоли управления JMS перейдите в раздел **Пользователи** и выберите контейнер, содержащий нужного пользователя.
2. В центральной части окна выберите нужного пользователя.
3. В верхней панели нажмите **Предоставить**.

Отобразится следующее окно.

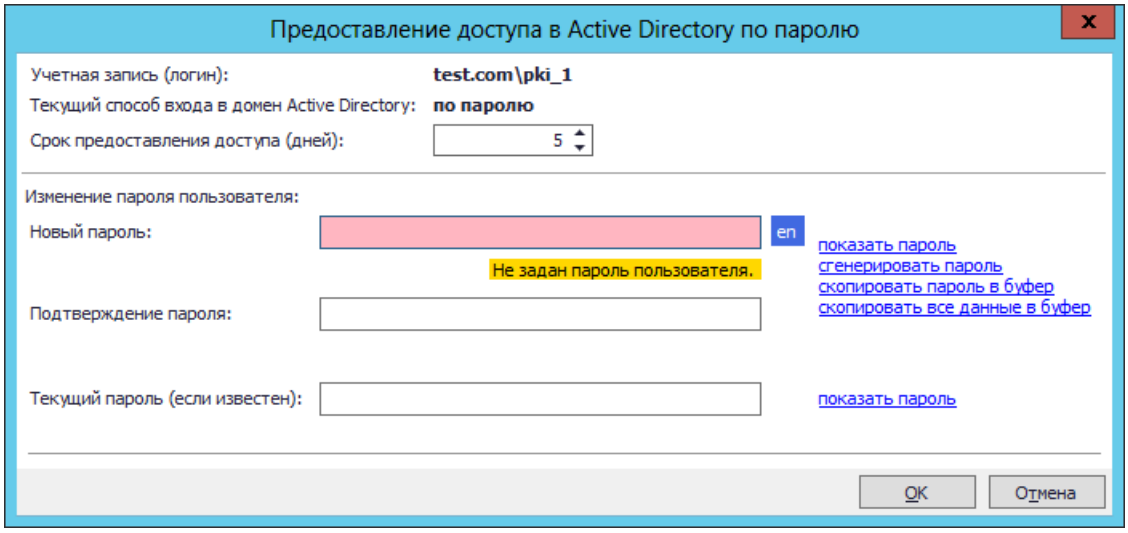


Рис. 15 – Предоставление пользователю временного доступа по паролю

4. Выполните следующие действия:

4.1. В поле **Срок предоставления (дней)** установите число дней, в течение которых выбранный пользователь будет иметь доступ в Active Directory с помощью пароля пользователя - по истечении этого срока возможность входа по паролю пользователя будет отключена;

Важно! Реальный срок действия пароля определяется моментом ближайшего (по истечении указанного в данном поле срока) выполнения *плана обслуживания по умолчанию*, а именно задачи **Проверка истекшего доступа в Active Directory по паролю**, см. раздел «План обслуживания по умолчанию», с. 413. Т.е. реальный срок действия пароля может оказаться больше указанного в диалоге значения.

4.2. В полях **Новый пароль** и **Подтверждение пароля** введите новый пароль пользователя и подтверждение соответственно.

Вы можете воспользоваться ссылкой **сгенерировать пароль**, чтобы создать случайный пароль пользователя. В этом случае поля **Новый пароль** и **Подтверждение пароля** будут заполнены автоматически.

4.3. При необходимости воспользуйтесь следующими ссылками напротив полей **Новый пароль** и **Подтверждение пароля**:

- **показать пароль** – отображает значение нового пароля;
- **скопировать пароль в буфер** – копирует в буфер значение нового пароля для доступа в Active Directory, чтобы его можно было передать пользователю;
- **скопировать все данные в буфер** – копирует в буфер домен и имя пользователя, новый пароль для доступа в Active Directory, а также срок действия нового пароля, чтобы можно было передать эти данные пользователю.

5. В поле **Текущий пароль (если известен)** введите текущий пароль пользователя.

Если в этом поле не вводить текущий пароль пользователя, то впоследствии все данные, которые были зашифрованы на текущем пароле пользователя, невозможно будет расшифровать, т.к. будет выполнен сброс пароля пользователя в Active Directory.

6. При необходимости воспользуйтесь ссылкой показать пароль, которая отобразит в соответствующем поле значение текущего пароля.
7. Нажмите **OK**.

Если вы не заполняли поле **Текущий пароль (если известен)**, отобразится предупреждающее сообщение. (В противном случае переходите к шагу 9 настоящей процедуры.)

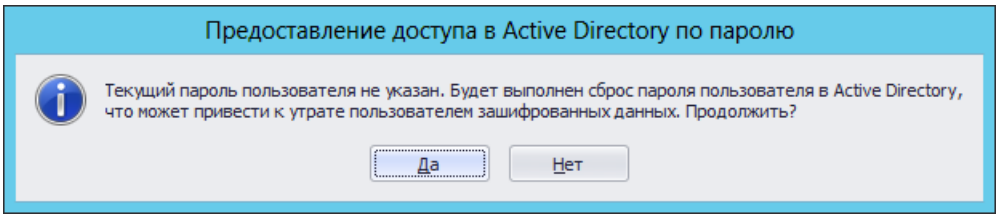


Рис. 16 – Предупреждение об утрате зашифрованных данных

8. Нажмите **Да** для продолжения процедуры.
   Отобразится следующее окно.

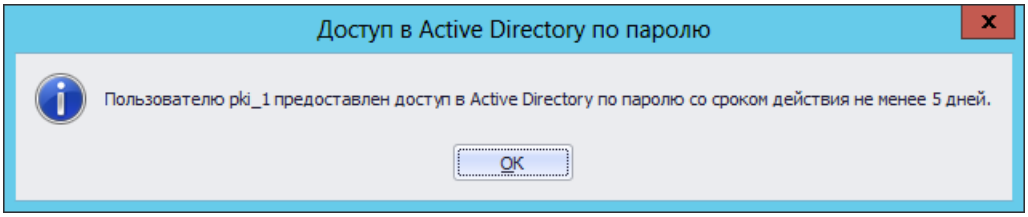


Рис. 17 – Сообщение об успешном предоставлении доступа

9. Нажмите **OK** для завершения процедуры.

3.3.4.2 Отмена временного доступа по паролю

Чтобы отменить временный доступ по паролю пользователя в Active Directory, выполните следующие действия.

1. В левой части консоли управления JMS перейдите в раздел **Пользователи** и выберите контейнер, содержащий нужного пользователя.
2. В центральной части окна выберите нужного пользователя.
3. В верхней панели нажмите **Отменить**.
4. В окне предупреждающего сообщения нажмите **Да**, чтобы подтвердить действие.
5. В окне сообщения о выполнении действия нажмите **OK**, чтобы завершить процедуру.

3.3.5 Добавление нового оператора JMS

В случае если монтирование/демонтирование криптохранилища необходимо выполнять более чем одному оператору, в системе JMS предусмотрена возможность предоставления пользователю JMS права монтирования криптохранилища с назначением ему сертификата открытого ключа и соответствующего закрытого ключа, хранимого на ключевом носителе данного пользователя.

Для добавления нового оператора JMS выполните следующие действия:

1. Для зарегистрированного в JMS пользователя выпустите на его электронном ключе ключевую пару и сертификат открытого ключа. В качестве примера процедуры выпуска такого сертификата можно воспользоваться ее описанием для центра сертификации Microsoft (см. «Руководство администратора. Часть 1» [2], разделы «Шаблон сертификата оператора JMS», «Публикация шаблона сертификата» и «Выпуск сертификатов по подготовленным шаблонам»). В случае если для выпуска сертификата используется удостоверяющий центр другого производителя, то в параметре *Использование ключа (KeyUsage)* выпускаемого сертификата установите значения:

   - Цифровая подпись (digitalSignature);
   - Шифрование ключей (keyEncipherment).

При необходимости экспортируйте выпущенный сертификат в файл.

2. В консоли управления JMS в разделе **Пользователи** выберите пользователя, для которого был выпущен сертификат и в верхней панели нажмите **Свойства**, в диалоговом окне выберите вкладку **Сертификаты** (Рис. 18).

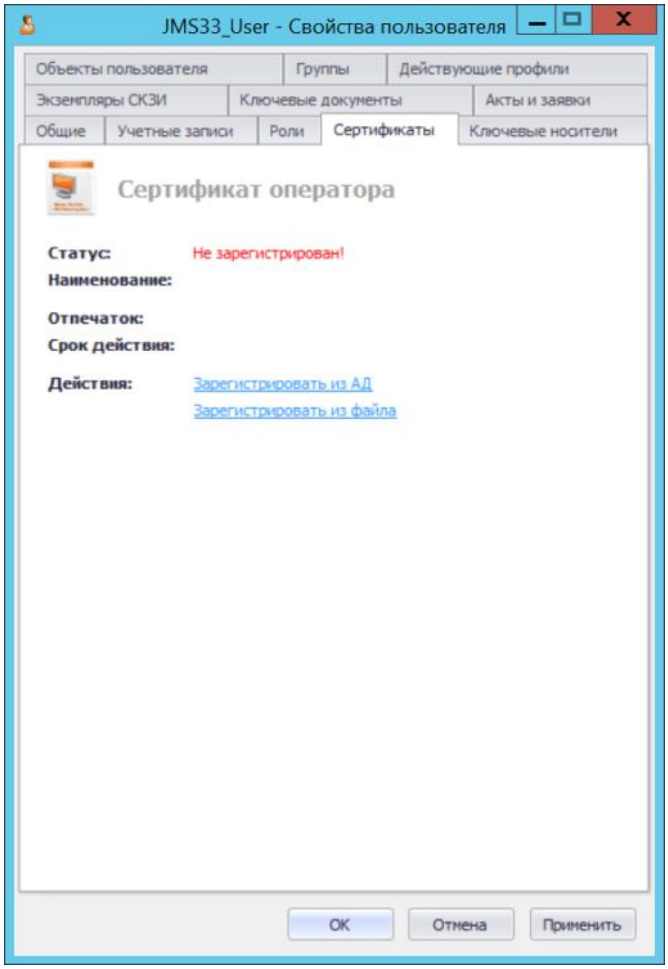


Рис. 18 – Вкладка Сертификаты в свойствах пользователя

3. Зарегистрируйте сертификат, выпущенный на шаге 1, одним из следующих способов:

   - Зарегистрировать сертификат из ресурсной системы (Active Directory). Данный способ может быть использован в случае, если выпущенный для пользователя сертификат опубликован в ресурсной системе.
   - Зарегистрировать сертификат из файла.

3.1. Чтобы зарегистрировать сертификат из ресурсной системы нажмите **Зарегистрировать из АД** (Рис. 18). Отобразится окно выбора сертификата:

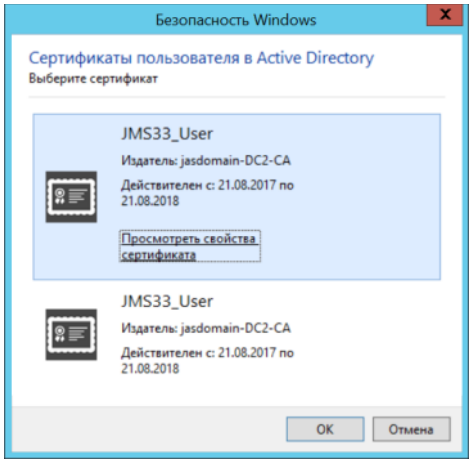


Рис. 19 – Окно выбора сертификата

Выберите нужный сертификат и нажмите **OK**. В случае если выбранный сертификат был выпущен в соответствии с требованиями к сертификату оператора JMS (см. п.1), он будет назначен пользователю в качестве сертификата оператора JMS.

3.2. Чтобы зарегистрировать сертификат из файла нажмите **Зарегистрировать из файла**. Отобразится окно выбора файла сертификата. Выберите нужный файл и нажмите **Открыть**.

Важно! Перед тем как зарегистрировать сертификат из файла, в хранилище доверенных корневых сертификатов (расположение – *Локальный компьютер*) на сервере JMS следует добавить сертификат корневого УЦ и цепочку сертификатов, необходимые для его (сертификата оператора JMS) проверки. В случае если загружаемый сертификат является самоподписанным, его предварительно следует добавить в указанное выше хранилище.

4. Назначьте пользователю роль **Оператор** или другую роль, которой предоставлены права на выполнение операций **Старт/Монтирование хранилища** и **Стоп/Демонтирование хранилища** (см. раздел «Создание, редактирование и назначение ролей JMS», с. 389)

Примечание. Для выполнения операции монтирования криптохранилища серверный агент должен быть запущен от имени пользователя (оператора JMS), для которого были выполнены настройки п.1—п.4.

3.3.6 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 или разблокировать пользователя, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Пользователи**.
2. В списке слева отметьте контейнер ресурсной системы, содержащий пользователей, которые нужно заблокировать или разблокировать (например, **Users** (Пользователи)).
3. В верхней панели выберите вкладку **Действия**.
4. В центральной части окна отметьте пользователя или пользователей, которых необходимо заблокировать или разблокировать.
5. В верхней панели в зависимости от нужного действия щелкните на соответствующем значке (см. рис. 20):

   – **Блокировать** – чтобы заблокировать пользователя;
   – **Разблокировать** - чтобы разблокировать пользователя.

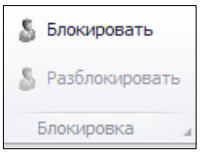


Рис. 20 – Блокировка/разблокировка пользователей

3.3.7 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 Active Directory или удостоверяющем центре КриптоПро УЦ). Поэтому удаленный из JMS пользователь может быть в последующем восстановлен путем процедуры регистрации (см. раздел «Регистрация пользователей в JMS», с. 36).

Чтобы удалить пользователя из JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Пользователи**.
2. В списке слева отметьте контейнер ресурсной системы, содержащий пользователей, которых нужно удалить из JMS (например, **Users** (Пользователи)).
3. В верхней панели выберите вкладку **Действия**.
4. В центральной части окна отметьте пользователя или пользователей, которых необходимо удалить.
5. В верхней панели в секции **Основные операции** нажмите **Удалить**.
6. В запросе на подтверждение удаления нажмите **Да**.

3.4 Управление рабочими станциями

Внимание! Управление рабочими станциями отсутствует в версии *CA Edition* продукта JMS (см. «Руководство администратора. Часть 1» [2], раздел «Версии поставки продукта и лицензионные опции»).

3.4.1 Регистрация рабочих станций в JMS

Чтобы зарегистрировать рабочие станции в JMS, выполните следующие действия.

7. В консоли управления JMS перейдите в раздел **Рабочие станции**.

Окно консоли будет иметь следующий вид.

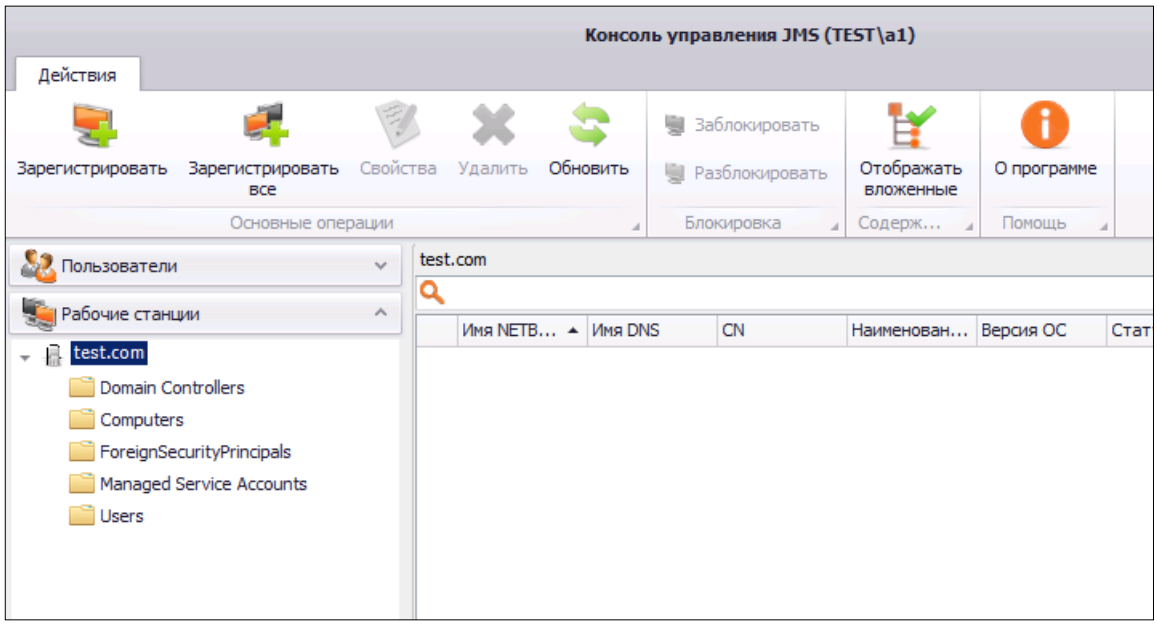


*Рис. 21 – Раздел **Рабочие станции** консоли управления JMS*

8. Выберите нужный каталог (например, **Computers** (Компьютеры)) и в верхней панели щелкните на одном из двух значков:

   - **Зарегистрировать** – чтобы зарегистрировать отдельные рабочие станции;
   - **Зарегистрировать все** – чтобы зарегистрировать все рабочие станции в выбранном каталоге.

9. В зависимости от выбранного способа регистрации (**Зарегистрировать** или **Зарегистрировать все**) выполните следующие действия.

Если вы выбрали **Зарегистрировать**.	Если вы выбрали **Зарегистрировать все**.
9.1. В окне **Регистрация рабочих станций** установите флаги напротив рабочих станций, которые вы хотите зарегистрировать в JMS (чтобы отметить все рабочие станции, установите флаг в верхней строке). 9.2. В нижней части окна нажмите **Зарегистрировать**.	9.1.В отобразившемся сообщении нажмите **Да** для подтверждения операции - после подтверждения произойдет автоматическая регистрация всех рабочих станций выбранного каталога.

⚠ Если при регистрации всех рабочих станций (**Зарегистрировать все**) некоторые рабочие станции из выбранного каталога уже зарегистрированы в JMS, то по завершении регистрации отобразится окно, содержащее список таких (ранее зарегистрированных) рабочих станций. В этом случае нажмите **Завершить**.

Список зарегистрированных рабочих станций отобразится в окне консоли управления JMS.

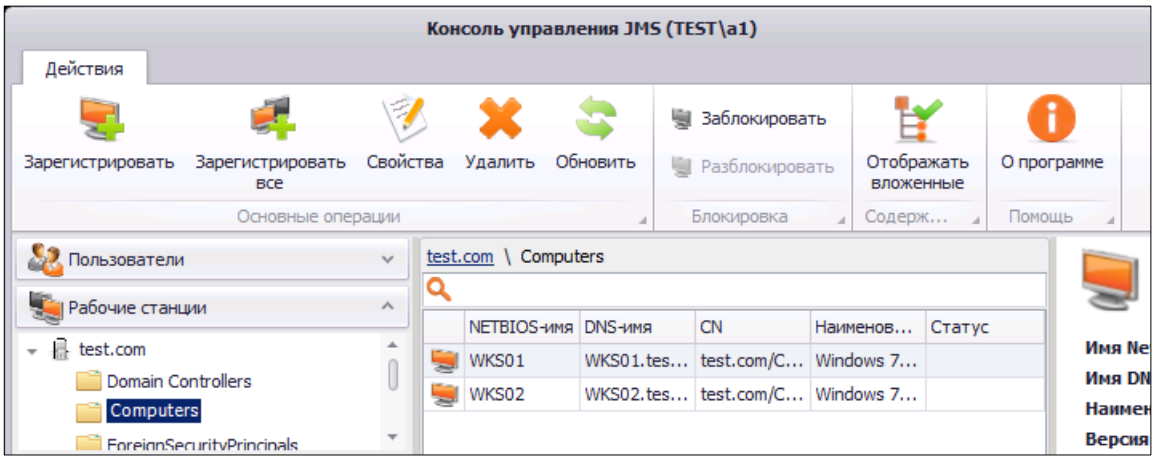


Рис. 22 – Список зарегистрированных рабочих станций

3.4.2 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;
   - на рабочей станции не выполняется обновление ПО JMS Client;
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 **Рабочие станции**.
2. В списке слева отметьте контейнер ресурсной системы, содержащий рабочие станции, которые нужно заблокировать или разблокировать (например, **Computers** (Компьютеры)).
3. В верхней панели выберите вкладку **Действия**.
4. В центральной части окна отметьте рабочую станцию или рабочие станции, которые необходимо заблокировать или разблокировать.
5. В верхней панели в зависимости от нужного действия щелкните на соответствующем значке (см. рис. 23):

   – **Заблокировать** – чтобы заблокировать рабочую станцию;
   – **Разблокировать** - чтобы разблокировать рабочую станцию.

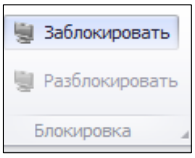


Рис. 23 – Блокировка/разблокировка рабочей станции

3.4.3 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 **Рабочие станции** в отдельной учетной системе с названием **Внедоменные рабочие станции** (отображается последней в списке зарегистрированных учетных систем, Рис. 24).

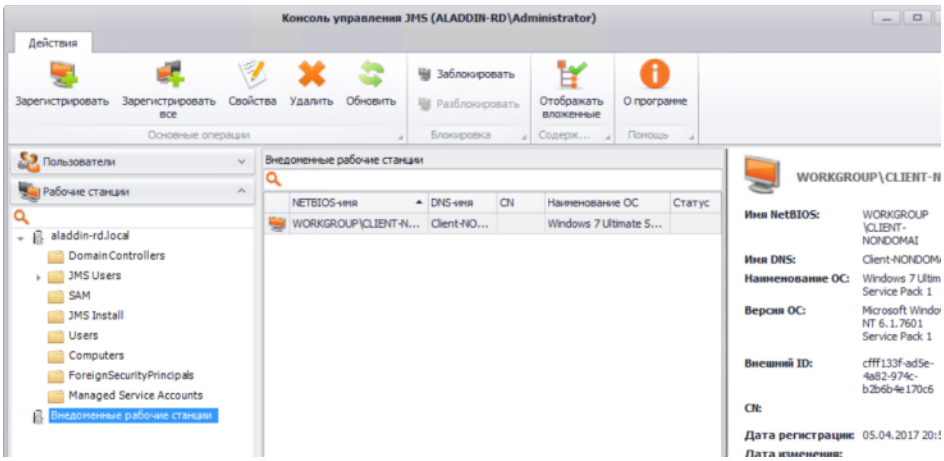


Рис. 24 – Работа с внедоменными рабочими станциями в JMS

Примечание. Чтобы обеспечить регистрацию внедоменной рабочей станции, необходимо выполнить ряд подготовительных действий, см. «Руководство администратора. Часть 1» [2], раздел «Действия, необходимые для работы с внедоменными компьютерами».

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.

3.5 Операции с сертификатами

Операции с сертификатами выполняются в разделе **Сертификаты** консоли управления JMS (Рис. 25).

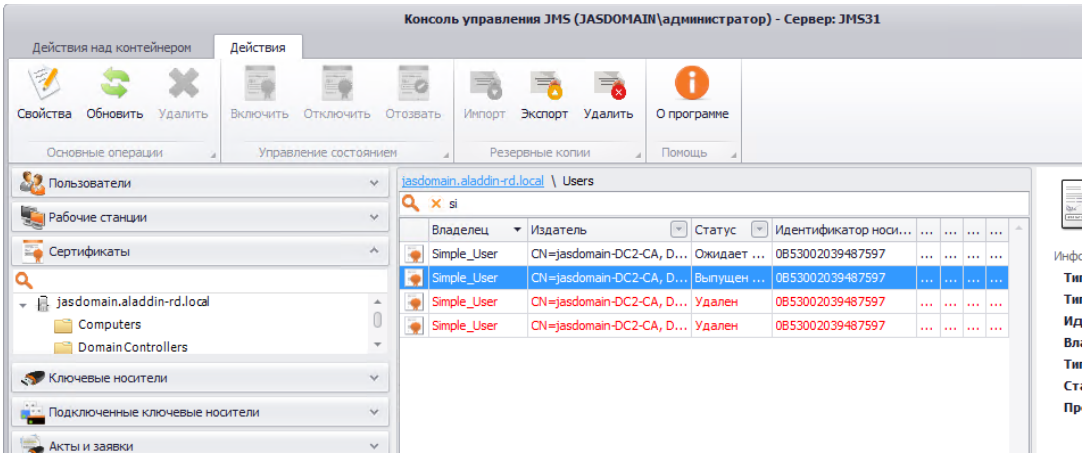


*Рис. 25 – Раздел **Сертификаты** консоли управления JMS*

3.5.1 Удаление сертификата

При удалении сертификата производятся следующие действия:

- сертификат удаляется с его носителя (электронного ключа или рабочей станции);
- сертификат приобретает статус **Удален**;
- выполняется отзыв сертификата в УЦ при условии, что сертификат был выпущен в JMS и в профиле, в соответствии с которым он был выпущен, установлен флаг **Отзывать сертификат в УЦ** (см. например, раздел «Настройки профиля выпуска сертификатов в центре сертификации Microsoft», с. 209).

Примечание. Операция **Удаление** не может быть применена к сертификату, находящемуся в состоянии **Выпущен на КН**. Удаление сертификата станет возможно только после удаления/отзыва в JMS электронного ключа (см. раздел «Операции с электронными ключами», с. 55), на котором он был выпущен, при условии, что он будет сохранен на ЭК в процессе отзыва последнего, в соответствии с настройками профиля выпуска сертификата.

Чтобы удалить сертификат, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Сертификаты.**
2. В центральной части экрана выберите сертификат, который необходимо удалить.
3. В верхней панели, в секции **Основные операции** нажмите **Удалить**.
4. В диалоговом окне с запросом на удаление выбранного сертификата нажмите **Да**.

Удаление производится в два этапа:

1. На предварительном этапе (после нажатия пользователем подтверждения) сертификат приобретает статус **Ожидает удаления**.
2. На заключительном этапе (при выполнении синхронизации электронного ключа или рабочей станции) сертификат физически удаляется из памяти соответствующего устройства, а в консоли управления JMS приобретает статус **Удален.** В случае если включена опция **Отображать удаленные** (на верхней вкладке **Действия над контейнером** консоли управления JMS), удаленные сертификаты отображаются в консоли и выделяются при этом красным шрифтом.

Удаление сертификата можно произвести также из окна свойств электронного ключа (вкладка **Содержимое**) или рабочей станции (вкладка **Сертификаты**), соответственно в разделах **Ключевые носители** и **Рабочие станции** консоли управления JMS, с помощью контекстного меню по нажатию правой клавишей мыши (см. например Рис. 26).

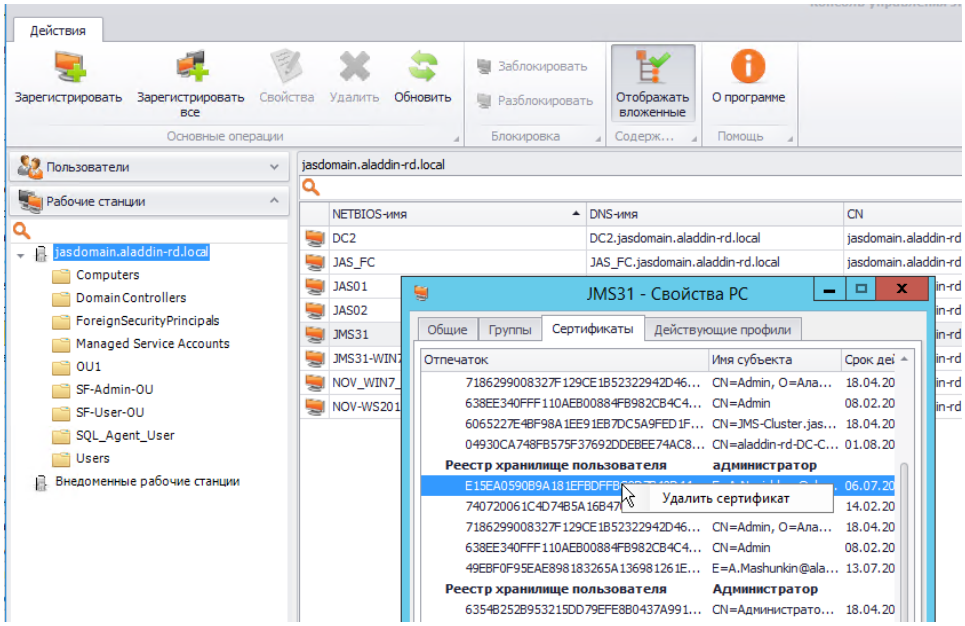


Рис. 26 – Удаление сертификата из окна свойств рабочей станции с помощью контекстного меню

3.5.2 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 **Сертификаты.**
2. В центральной части экрана выберите сертификат, который необходимо отозвать.
3. В верхней панели нажмите **Отозвать**.
4. В диалоговом окне с запросом на отзыв выбранного сертификата нажмите **Да**.

3.5.3 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 **Сертификаты**.
2. В центральной части окна отметьте сертификат, действие которого вы хотите приостановить/возобновить.

3. В верхней панели выберите один из двух пунктов:

   – **Отключить** – чтобы приостановить действие сертификата;
   – **Включить** — чтобы возобновить действие сертификата.

4. В диалоговом окне с запросом на выполняемое действие нажмите **Да**.

3.5.4 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 **Сертификаты**.
2. В центральной части окна отметьте сертификат, копию закрытого ключа для которого необходимо импортировать.
3. В верхней панели нажмите **Импорт**.

Примечание. Для выполнения операции **Импорт** 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. 389)

Отобразится окно мастера импорта резервных копий сертификата.

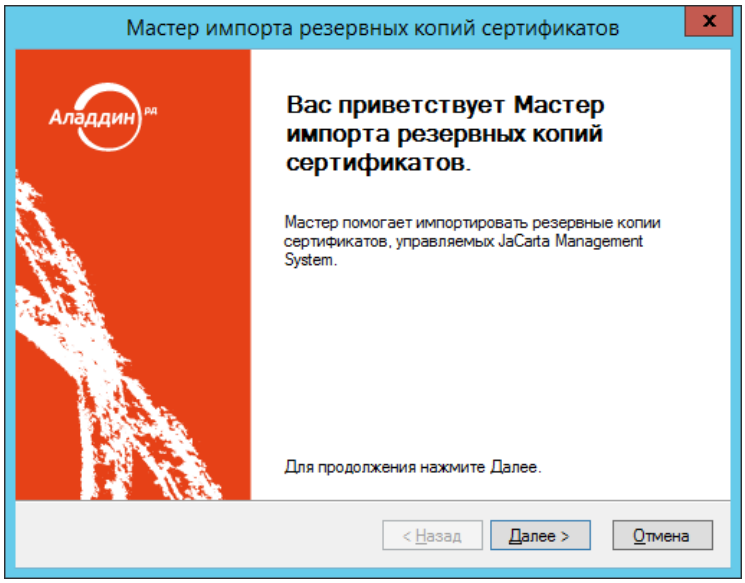


Рис. 27 – Приветственное окно мастера импорта резервных копий сертификатов

4. Следуйте указаниям мастера до завершения процедуры импорта резервной копии закрытого ключа. (В целом процедура соответствует порядку импорта резервной копии сертификата, хранящейся в файловой системе, см. «Импорт резервных копий сертификатов в JMS», с. 479).

3.5.5 Экспорт резервной копии сертификата

В JMS реализована возможность экспортировать резервную копию сертификата в случае, если она была ранее создана при выпуске сертификата или импортирована в JMS. Операция доступна для 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);
- **Ожидает удаления;**
- **Удален**.

Чтобы экспортировать из JMS резервную копию сертификата, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Сертификаты**.
2. В центральной части окна отметьте сертификат, копию закрытого ключа для которого необходимо экспортировать.
3. В верхней панели нажмите **Экспорт**.

Примечание. Для выполнения операции **Экспорт** пользователь должен быть наделен ролью, в которой добавлено право на выполнение операции **Ключевые носители** -> **Экспорт 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. 389)

Отобразится окно мастера экспорта резервных копий сертификата.

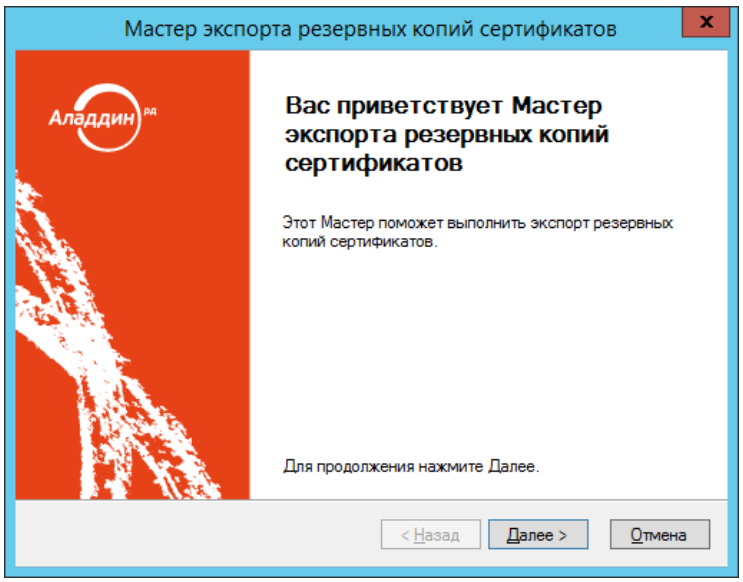


Рис. 28 – Приветственное окно мастера экспорта резервных копий сертификатов

4. Следуйте указаниям мастера до завершения процедуры экспорта резервной копии сертификата. (В целом процедура соответствует порядку экспорта резервной копии

сертификата, описанному в разделе «Экспорт резервных копий объектов, выпущенных на электронный ключ», с. 112).

3.5.6 Удаление резервной копии сертификата

JMS позволяет удалять из своего хранилища резервную копию (если она существует) сертификата.

Чтобы удалить из JMS резервную копию сертификата выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Сертификаты**.
2. В центральной части окна отметьте сертификат, резервную копию которого необходимо удалить.
3. В верхней панели в секции **Резервные копии** нажмите **Удалить**.

Примечание. Для выполнения операции **Удалить** в отношении резервной копии сертификата пользователь должен быть наделен ролью, в которой добавлено право на выполнение операции **Ключевые носители** -> **Удаление 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. 389)

4. В диалоговом окне с запросом на удаление резервной копии сертификата нажмите **Да**.

3.6 Операции с электронными ключами

3.6.1 Жизненный цикл электронного ключа

Обобщенная диаграмма жизненного цикла электронного ключа (ключевого носителя, КН) отображена на Рис. 29. 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.

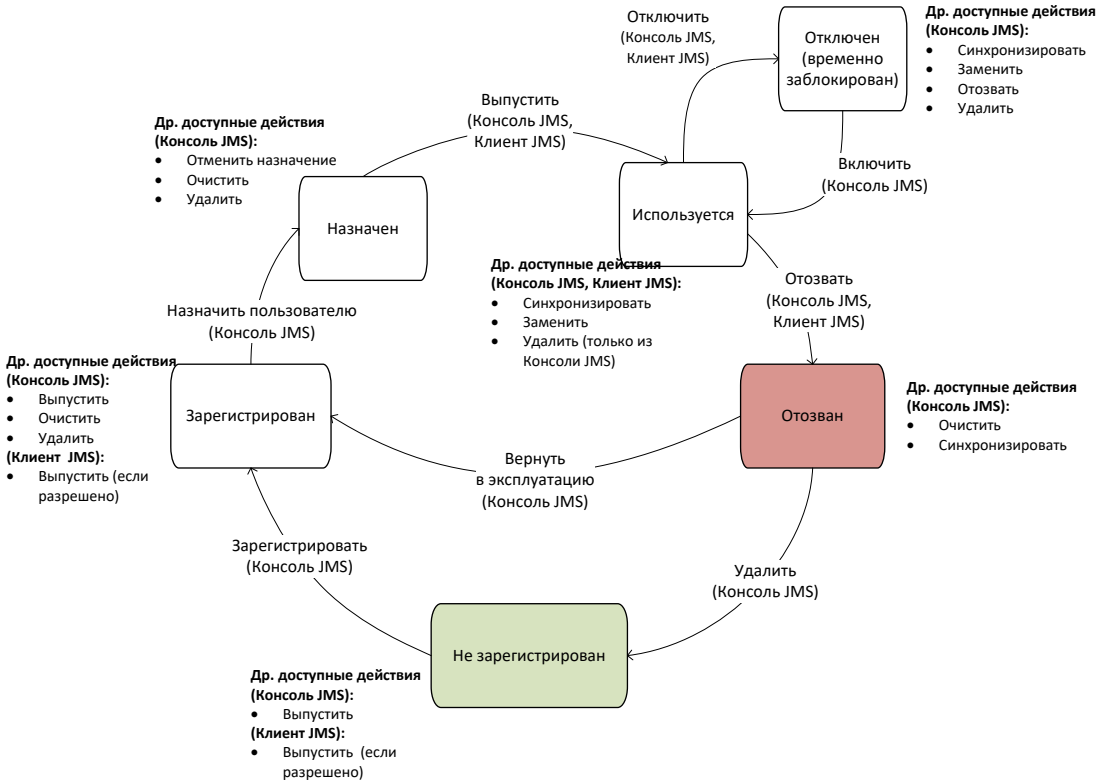


Рис. 29 – Диаграмма жизненного цикла ключевого носителя (электронного ключа)

Ниже приведено краткое описание операций с КН, доступных в зависимости от его текущего состояния в соответствии с Рис. 29.

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 его выпуска (используя профиль клиентского агента, см. «Настройка профиля клиентского агента», с. 164) из клиентского приложения JMS тех КН, которые еще не зарегистрированы в JMS. Подробное описание операции регистрации КН см. в разделе «Регистрация подсоединенных электронных ключей в JMS», с. 57.

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 КН (используя профиль клиентского агента, см. «Настройка профиля клиентского агента», с. 164) из клиентского приложения JMS тех КН, которые еще не назначены пользователю. Подробнее об операции назначения КН см. в разделе «Назначение электронного ключа пользователю», с. 71.

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. 296), 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 электронного ключа администратором», с. 75.

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. 96), после чего пользователю становятся недоступным открытие с помощью данного КН открытие пользовательского сеанса в клиенте JMS. Подробнее см. раздел «Отключение/включение возможности использования электронного ключа», с. 81.

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 электронного ключа», с. 81.

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 электронного ключа», с. 91), 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 электронного ключа», с. 88.

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 **Ключевые носители**). Подробнее об операции удаления КН см. в разделе «Удаление электронного ключа», с. 100.

Описание других операций, приведенных на диаграмме жизненного цикла (**Заменить**, **Синхронизировать**, **Очистить, Отменить назначение**), см. в Табл. 3, с. 20.

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.

3.6.2 Регистрация подсоединенных электронных ключей в JMS

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

1. Подсоедините электронный ключ, который вы хотите зарегистрировать, к компьютеру.
2. Запустите мастер регистрации ключевых носителей любым из следующих способов:

2.1. в консоли управления JMS перейдите в раздел **Ключевые носители**;
2.2. в левой панели выберите группу или организационную единицу, к которой будет привязан электронный ключ (в настоящем документе для примера будет использоваться группа **Users** (Пользователи));
2.3. в верхней панели щелкните на кнопке **Зарегистрировать подключенный**.

Отобразится следующее окно.

2.4. в консоли управления JMS перейдите в раздел **Подключенные устройства**;
2.5. в центральной части окна выберите электронный ключ, который вы хотите зарегистрировать;
2.6. в верхней панели щелкните на кнопке **Зарегистрировать**.

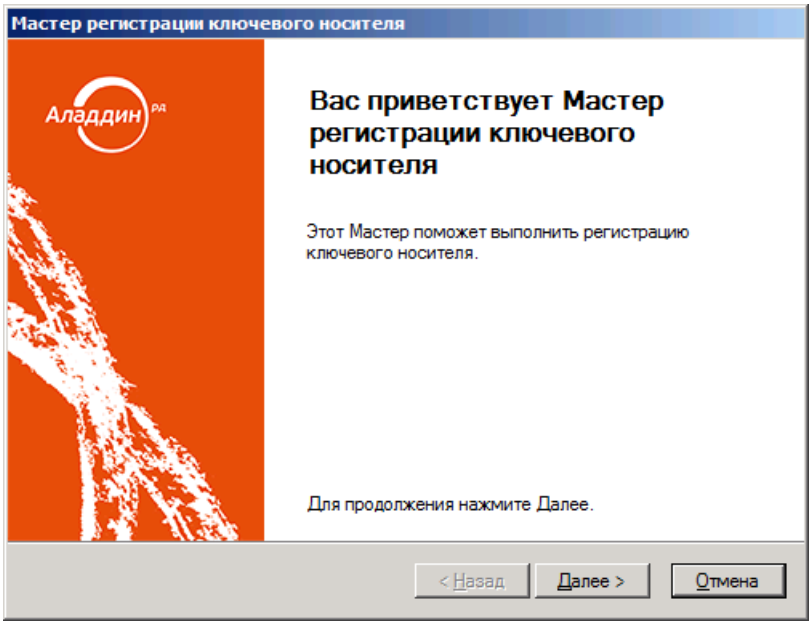


Рис. 30 – Окно приветствия мастера регистрации электронных ключей

3. Нажмите **Далее**.

Если вы регистрируете электронный ключ из раздела **Подключенные устройства** консоли управления JMS, отобразится следующее окно. (В противном случае переходите к шагу 5 настоящей процедуры.)

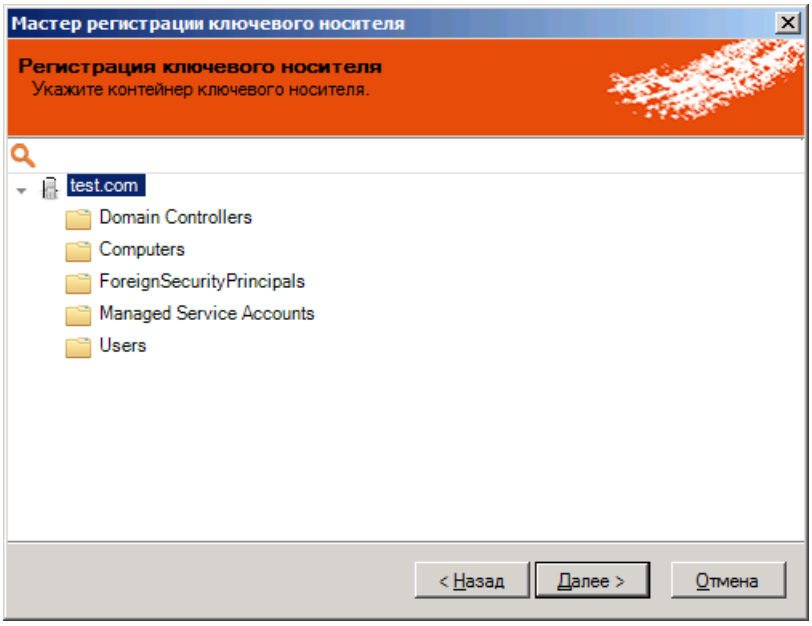


Рис. 31 – Привязка ключевого носителя к группе или организационной единице

4. Выберите группу или организационную единицу, к которой будет привязан зарегистрированный электронный ключ, после чего нажмите **Далее**. Отобразится следующее окно.

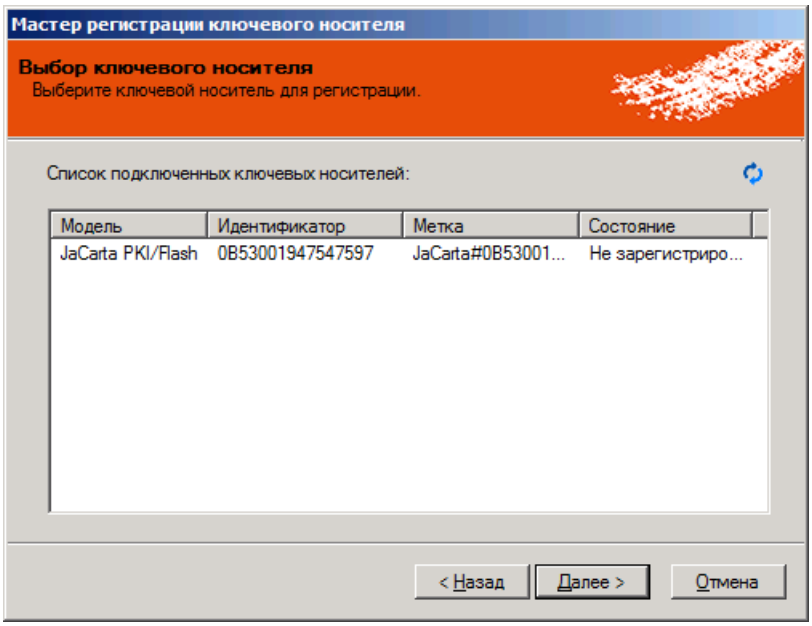


Рис. 32 – Окно выбора ключевого носителя

5. Выберите нужный электронный ключ и нажмите **Далее**.

Отобразится следующее окно.

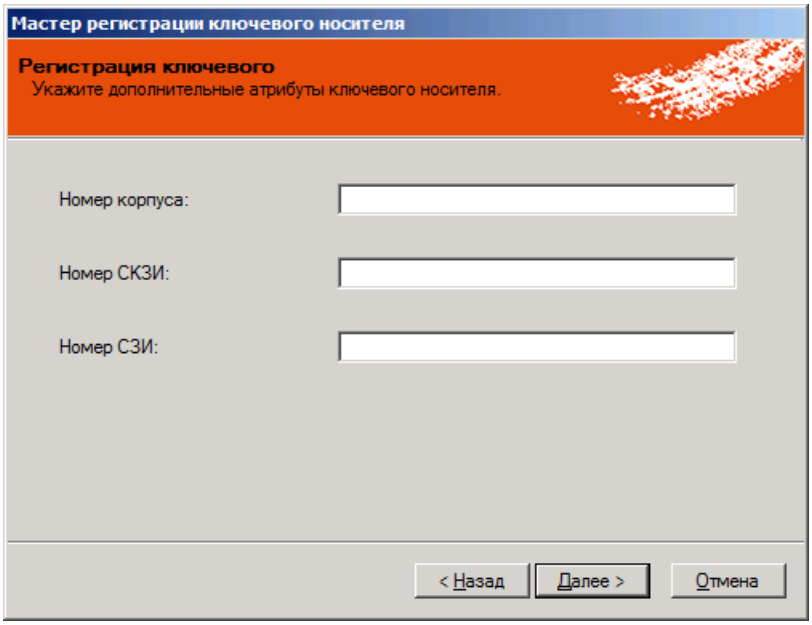


Рис. 33 – Окно дополнительных атрибутов электронного ключа

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.

Отобразится следующее окно.

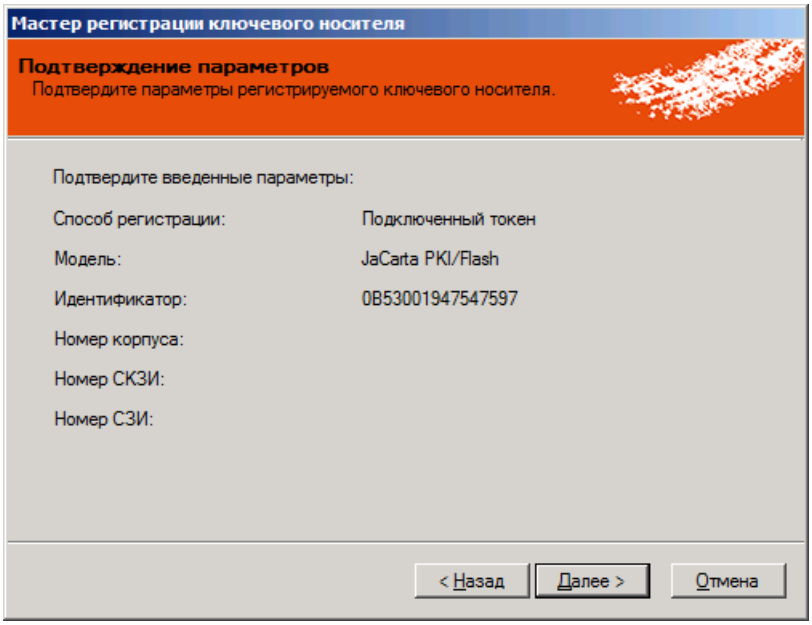


Рис. 34 – Окно подтверждения параметров регистрации электронного ключа

7. Нажмите **Далее**.

Отобразится следующее окно.

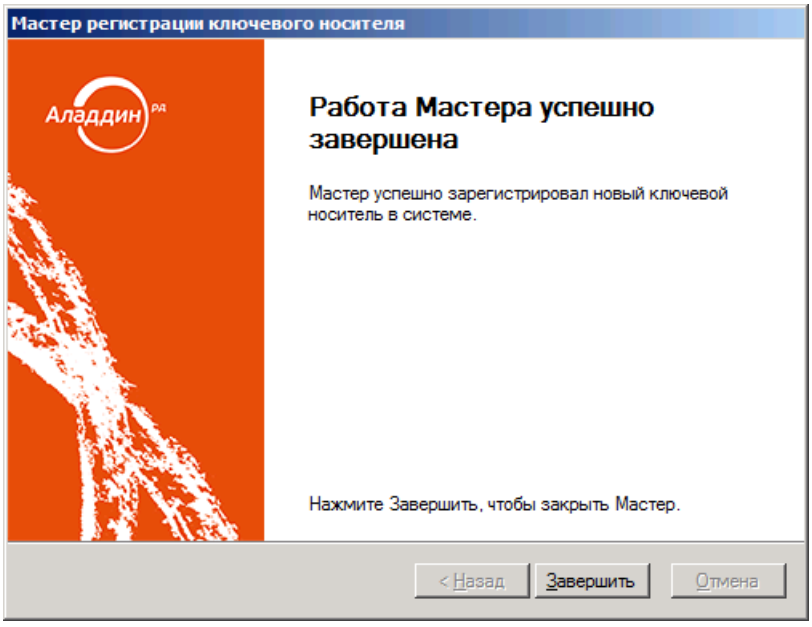


Рис. 35 – Окно завершения работы регистрации ключевых носителей

8. Нажмите **Завершить**.

3.6.3 Экспорт/импорт электронных ключей

JMS позволяет экспортировать электронные ключи с тем, чтобы их можно было импортировать на другом экземпляре JMS. Существует два варианта экспорта:

- экспорт электронных ключей списком – для этого сначала необходимо подготовить список электронных ключей (см. «Подготовка списка электронных ключей для экспорта» ниже), после чего осуществить процедуру экспорта (см. «Экспорт электронных ключей», с. 64);
- экспорт электронных ключей, выбранных в интерфейсе консоли управления JMS (см. «Экспорт электронных ключей», с. 64).

Чтобы импортировать электронные ключи, выполните процедуру «Импорт (пакетная регистрация) электронных ключей в JMS», с. 68.

3.6.3.1 Подготовка списка электронных ключей для экспорта

Чтобы подготовить файл со списком электронных ключей для экспорта из JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Ключевые носители**.
2. В верхней панели выберите вкладку **Действия**.
3. В верхней панели нажмите **Утилита создания списка**.

Отобразится следующее окно.

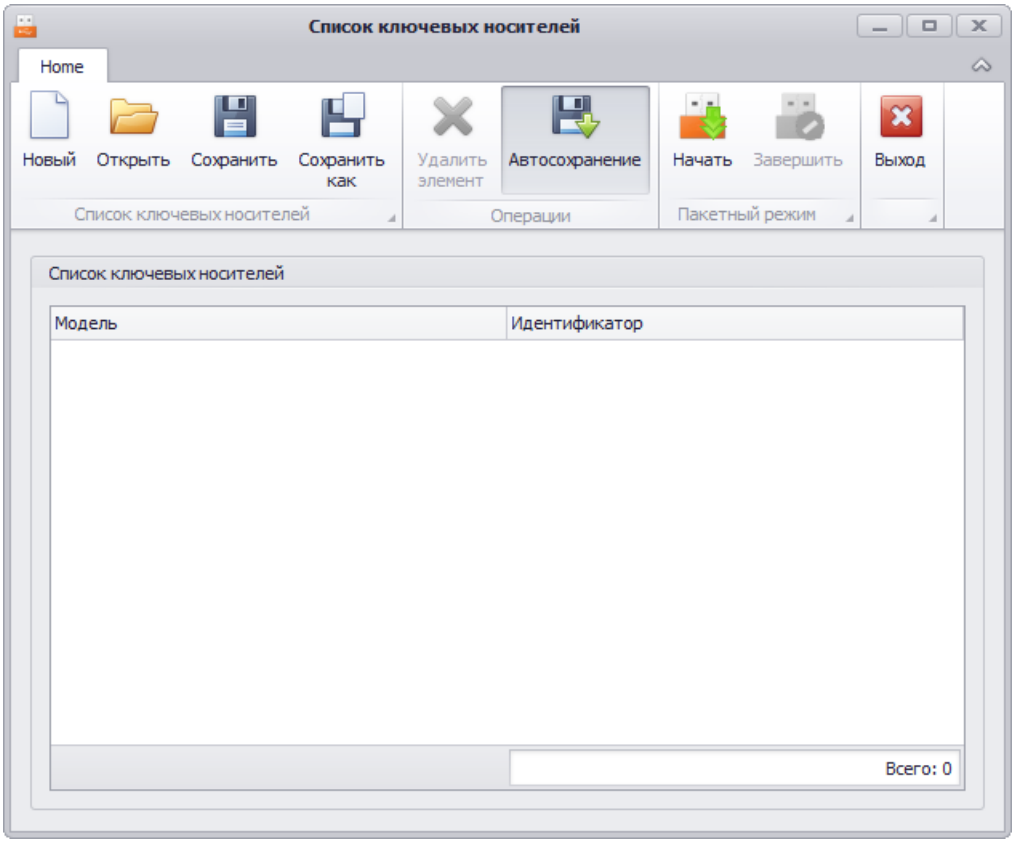


Рис. 36 – Утилита создания списка

4. Нажмите **Начать**.
5. В отобразившемся окне укажите путь и имя файла, в который будут записываться сведения об электронных ключах.

Окно утилиты примет следующий вид.

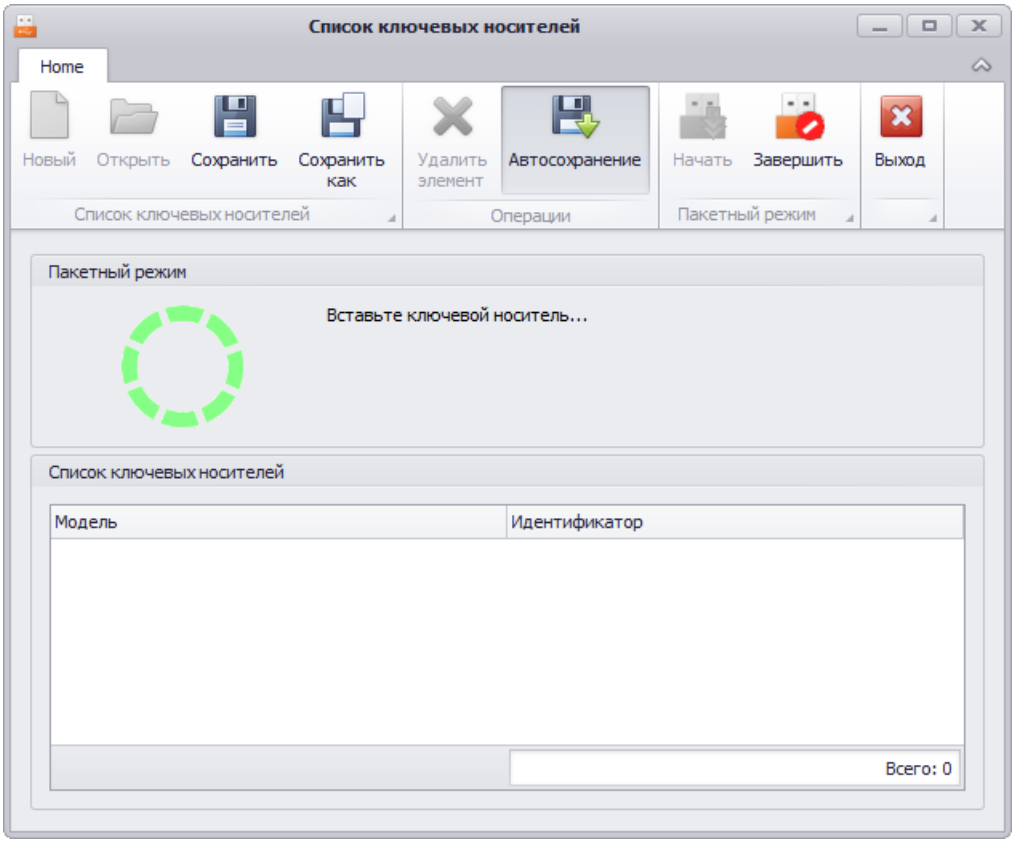


Рис. 37 – Начало процедуры создания списка электронных ключей

6. Подсоедините электронный ключ, который хотите внести в список, к компьютеру.

Спустя некоторое время он будет автоматически добавлен в список (см. изображение ниже).

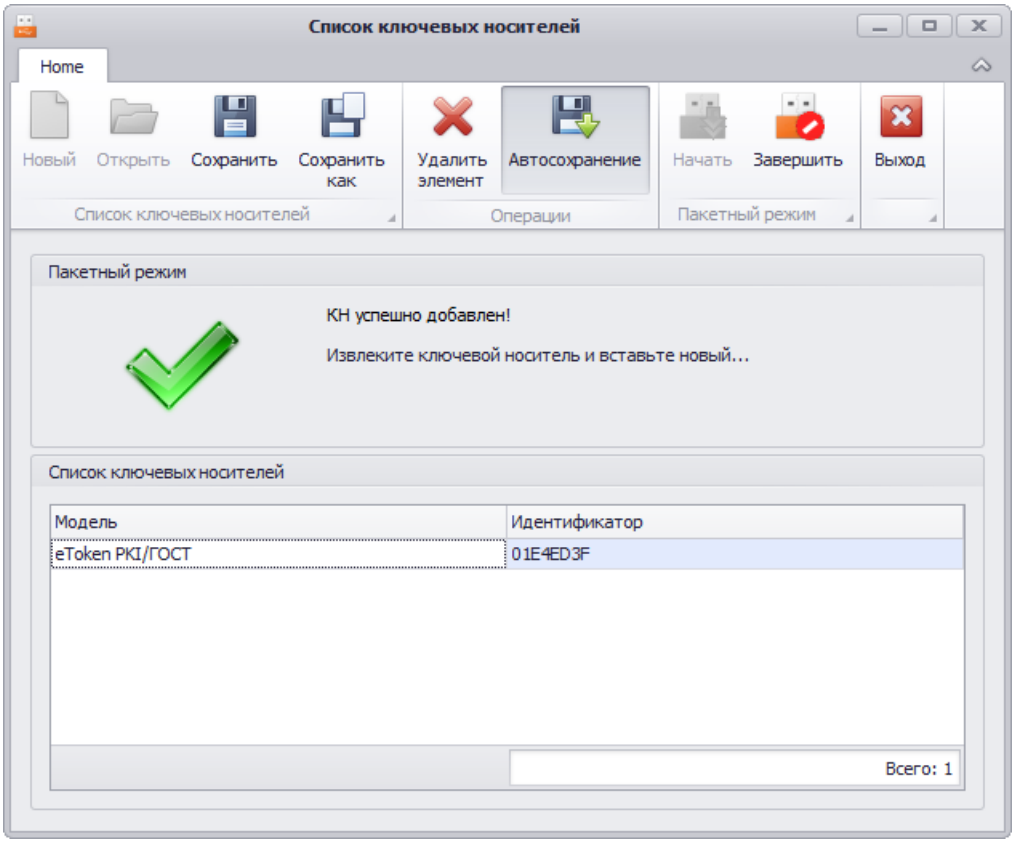


Рис. 38 – Электронный ключ добавлен в список для экспорта

7. Повторите необходимые действия для всех электронных ключей, которые вы хотите добавить в список.
8. В верхней панели утилиты создания списка электронных ключей последовательно щелкните на значках **Сохранить** и **Завершить**.

Окно примет следующий вид.

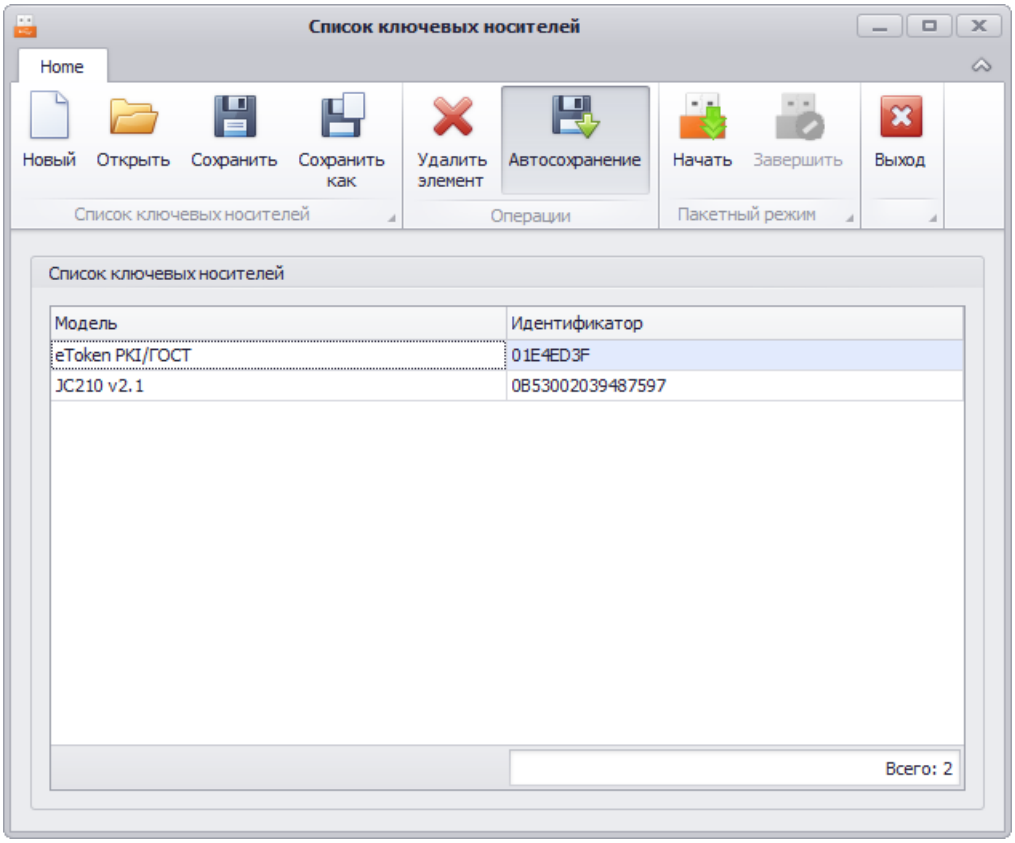


Рис. 39 – Создание списка завершено

9. В верхней панели утилиты создания списка электронных ключей нажмите **Выход**.

3.6.3.2 Экспорт электронных ключей

Чтобы экспортировать список электронных ключей в файл, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Ключевые носители**.
2. В верхней панели выберите вкладку **Действия**.
3. В зависимости от варианта экспорта, выполните следующие действия:

   – *экспорт электронных ключей, выбираемых в интерфейсе JMS* – в левой панели выберите контейнер, из которого вы хотите экспортировать ключи, после чего отметьте нужные ключи в центральной части интерфейса;
   – *экспорт электронных ключей списком* – переходите к следующему шагу процедуры.

4. В верхней панели щелкните на одном из следующих значков:

   – **Экспорт выбранных** – позволяет экспортировать электронные ключи, выделенные в центральной части интерфейса консоли управления JMS;
   – **Экспорт по списку** – позволяет экспортировать электронные ключи по заранее подготовленному списку (см. «Подготовка списка электронных ключей для экспорта», с. 60).

Примечание. Поскольку процедура создания списка позволяет включать в список электронные ключи, не зарегистрированные в JMS, перед тем как начать процедуру в варианте **Экспорт по списку**, следует убедиться, что все электронные ключи из списка зарегистрированы в JMS, в противном случае экспорт завершится с ошибкой.

Отобразится следующее окно.

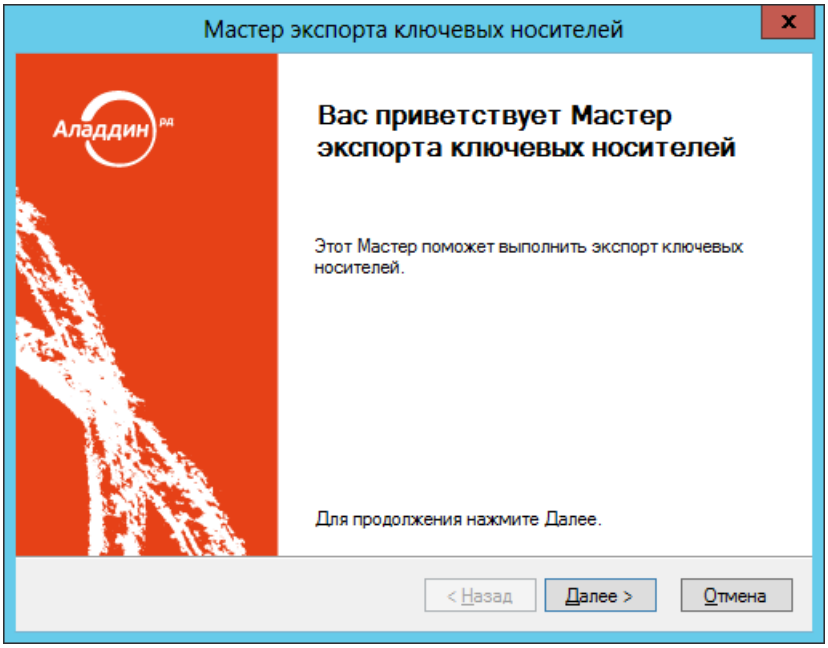


Рис. 40 – Окно приветствия мастера экспорта электронных ключей

5. Нажмите **Далее**.
   Если вы экспортируете электронные ключи по списку, отобразится следующее окно. (Противном случае переходите к шагу 7 настоящей процедуры.)

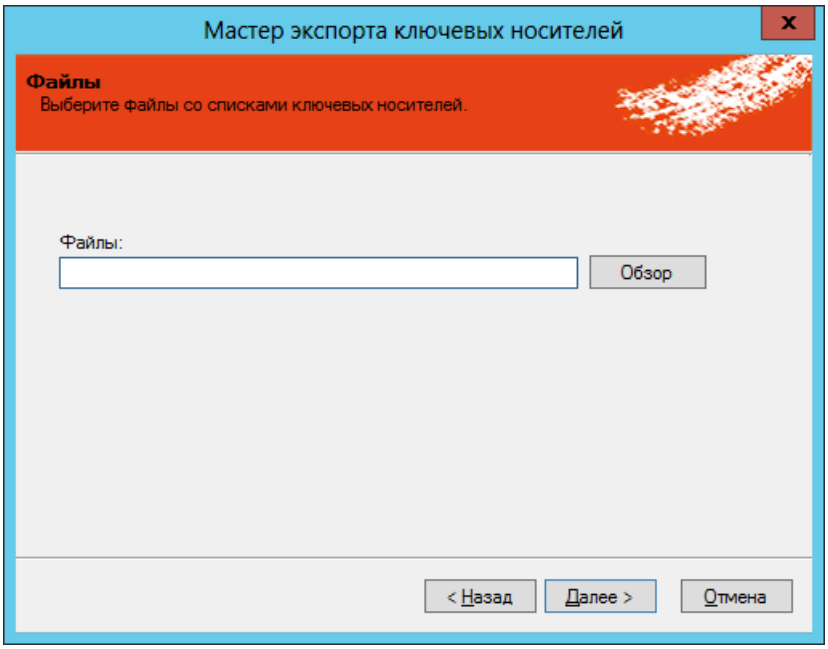


Рис. 41 – Экспорт электронных ключей по списку

6. Воспользуйтесь кнопкой **Обзор**, чтобы указать путь к заранее подготовленному файлу со списком электронных ключей (см. «Подготовка списка электронных ключей для экспорта», с. 60), после чего нажмите **Далее**.
   Отобразится следующее окно.

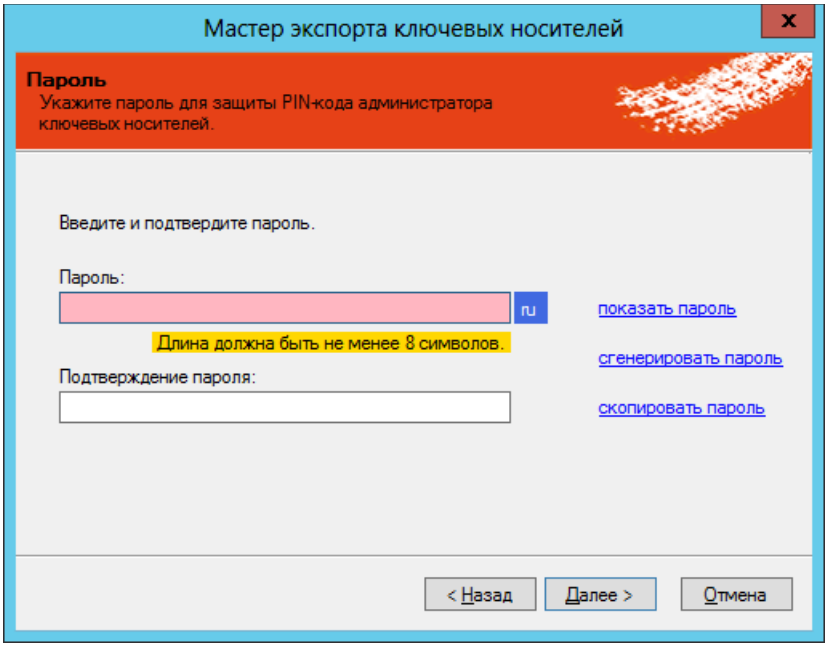


Рис. 42 – Задание пароля

7. В полях **Пароль** и **Подтверждение пароля** введите пароль для защиты экспортируемого файла и подтверждение соответственно.
8. При необходимости воспользуйтесь ссылками справа:

   - **показать пароль** – отображает символы пароля;
   - **сгенерировать пароль** – генерирует случайный пароль;
   - **скопировать пароль** – копирует пароль в буфер.

9. Нажмите **Далее**.
   Отобразится следующее окно.

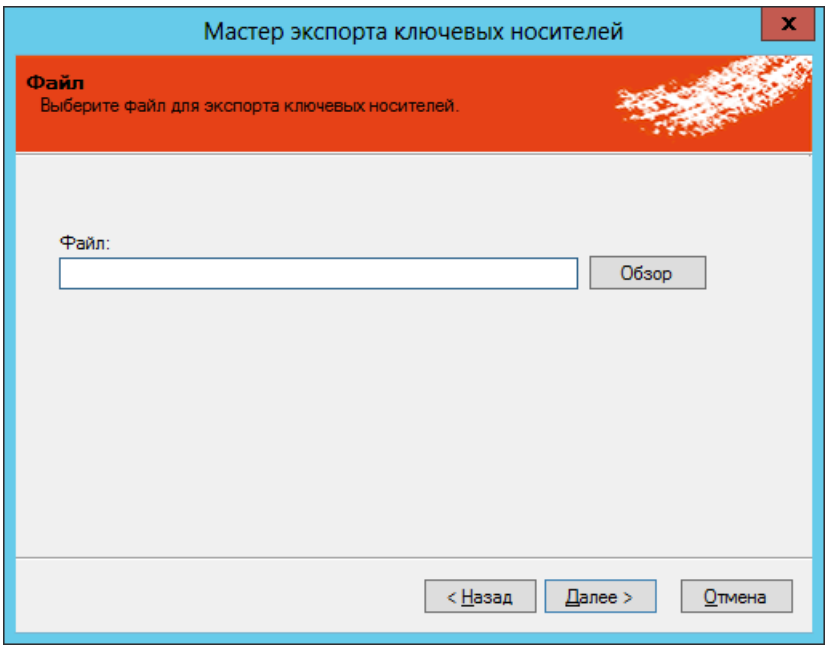


Рис. 43 – Указание пути сохранения файла

10. Воспользуйтесь кнопкой **Обзор**, чтобы указать путь сохранения экспортируемого файла, после чего нажмите **Далее**.

Отобразится следующее окно.

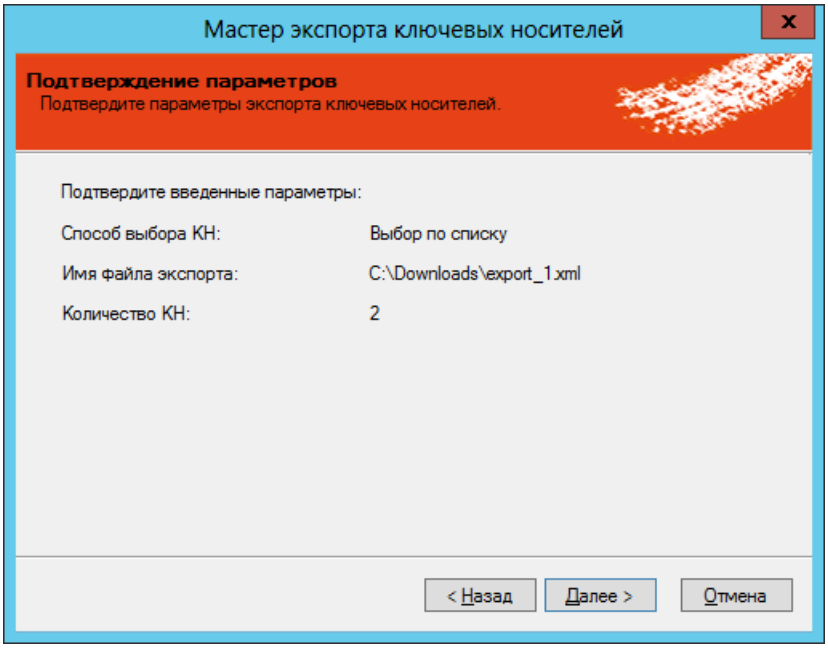


Рис. 44 – Окно подтверждения параметров экспорта

11. Нажмите **Далее**.
Отобразится следующее окно.

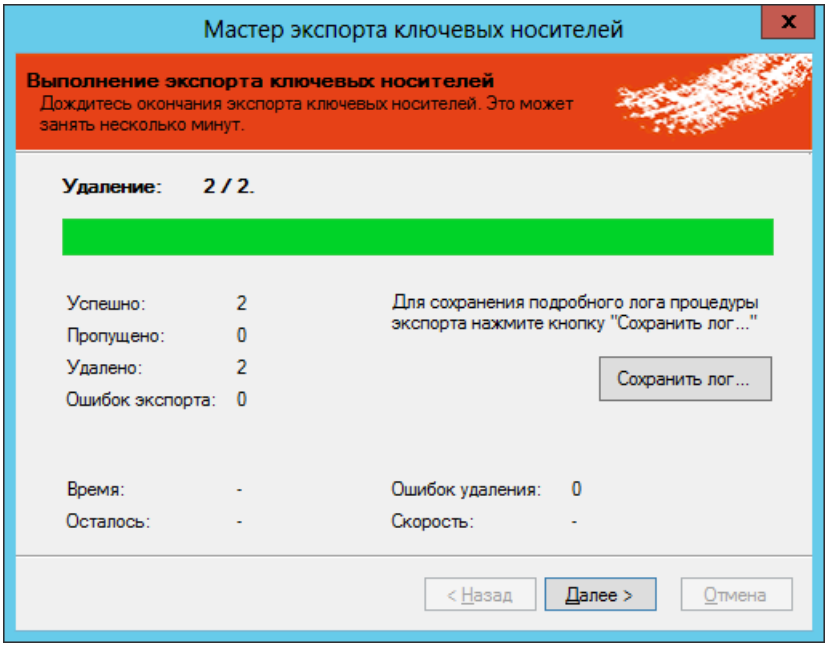


Рис. 45 – Экспорт сведений об электронных ключах в файл

12. Нажмите **Далее**.

Отобразится следующее окно.

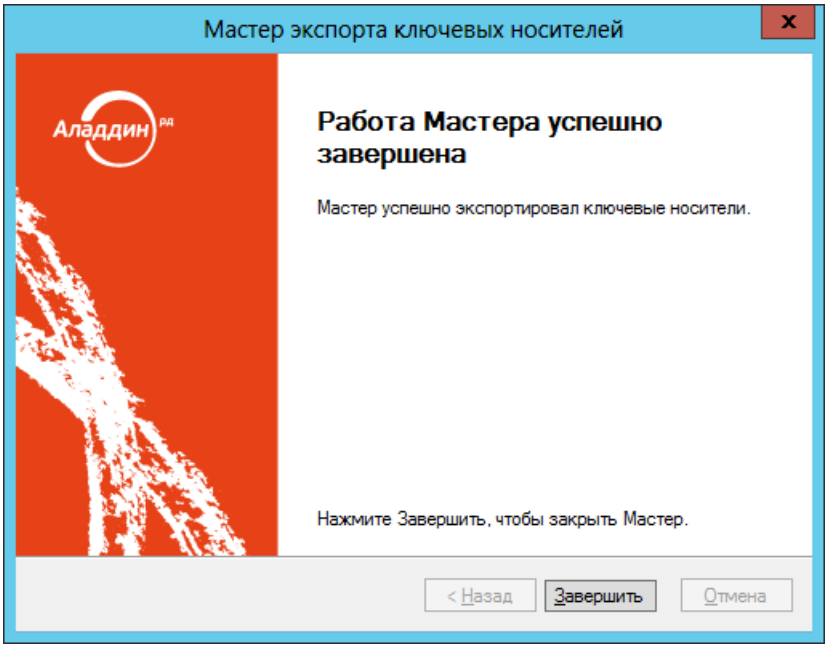


Рис. 46 – Окно завершения процедуры экспорта

13. Нажмите **Завершить** для завершения процедуры.

3.6.3.3 Импорт (пакетная регистрация) электронных ключей в JMS

Для пакетной регистрации электронных ключей в JMS можно воспользоваться файлами следующих типов:

- соответствующим файлом со списком электронных ключей компании-поставщика (предоставляется только компанией Аладдин для электронных ключей JaCarta по запросу заказчика);
- файлом, полученным в результате процедуры экспорта электронных ключей (см. раздел «Экспорт электронных ключей», с. 64);
- файлом, полученным в результате подготовки списка электронных ключей, см. на примере раздела «Подготовка списка электронных ключей для экспорта», с. 60.

Примечание. В последнем случае с помощью процедуры создания списка можно сформировать список электронных ключей, еще не зарегистрированных в JMS. При таком порядке действий регистрация электронных ключей в JMS происходит быстрее, чем их обычная регистрация по одном экземпляру.

Чтобы импортировать электронные ключи в JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Ключевые носители**.
2. В верхней панели выберите вкладку **Действия над контейнером**.
3. В верхней панели щелкните на кнопке Импорт

Отобразится следующее окно.

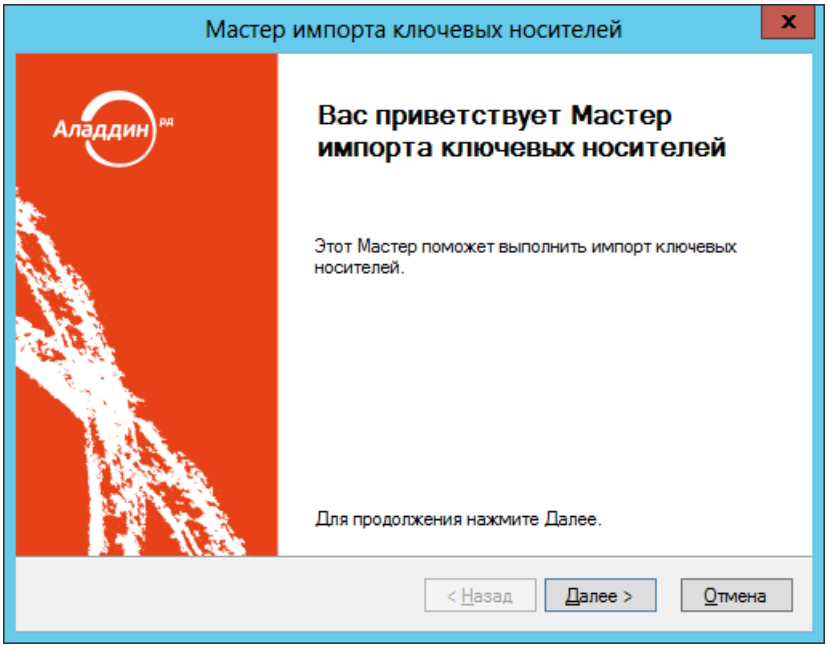


Рис. 47 – Окно приветствия мастера импорта электронных ключей

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

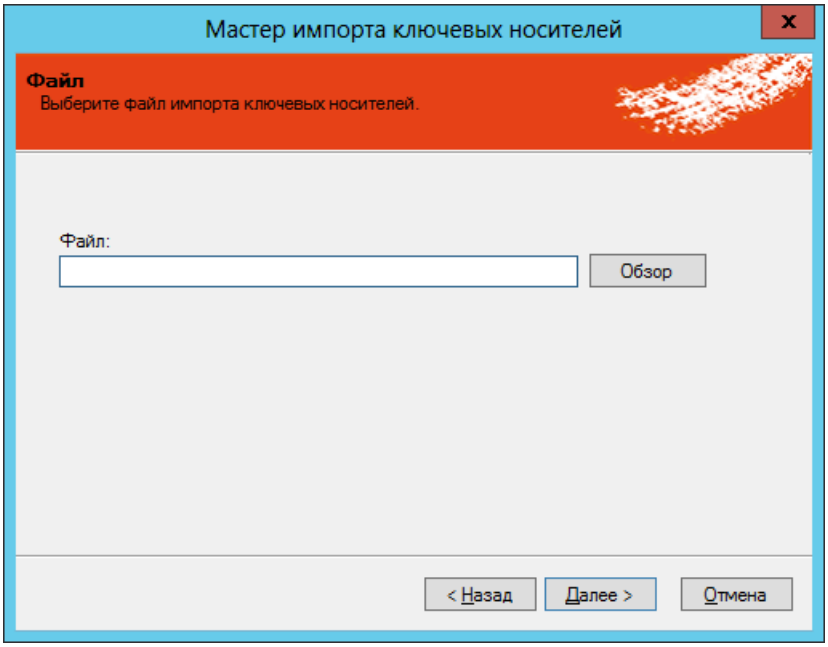


Рис. 48 – Выбор файла, содержащего сведения об импортируемых электронных ключах

5. Воспользуйтесь кнопкой **Обзор**, чтобы указать путь к файлу, содержащему сведения об импортируемых электронных ключах, после чего нажмите **Далее**.

Отобразится следующее окно.

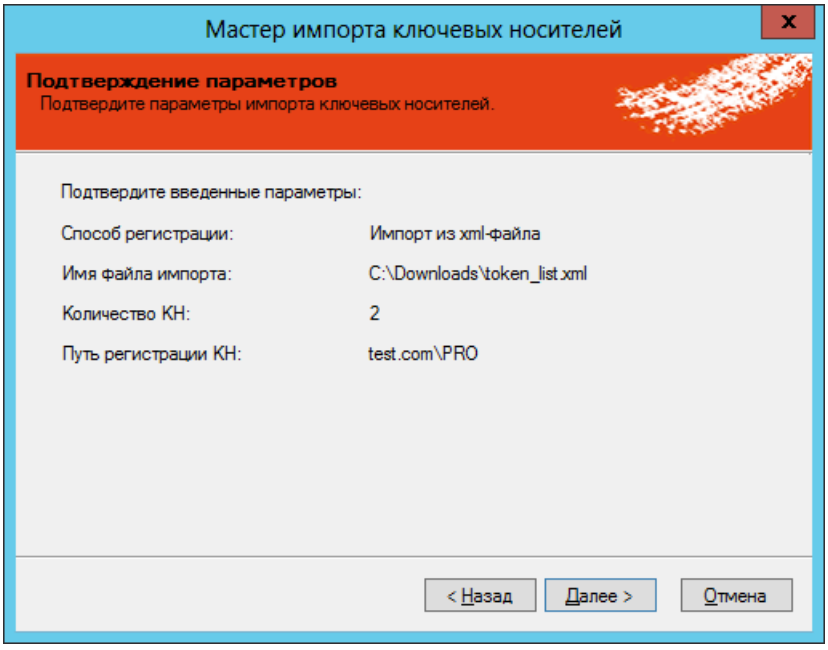


Рис. 49 – Подтверждение параметров импорт

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

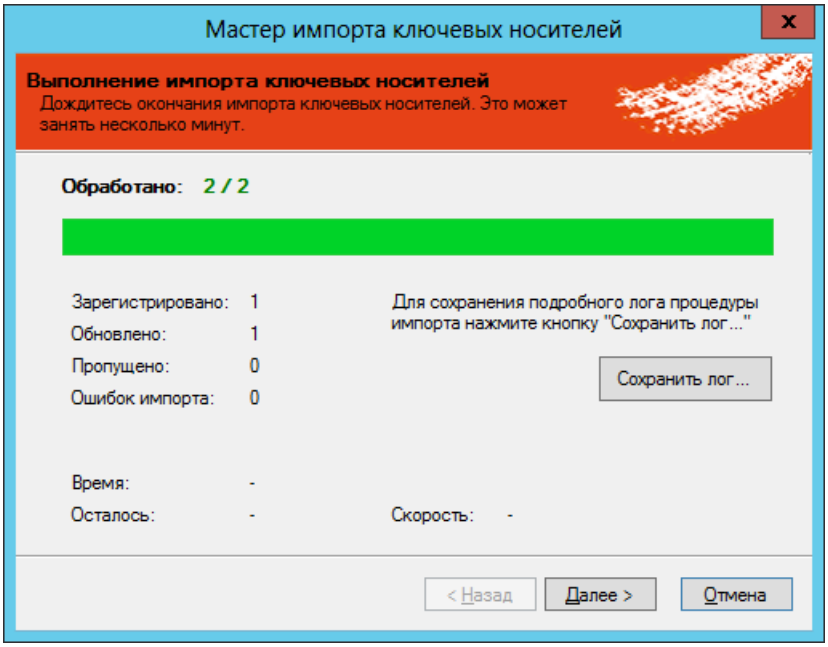


Рис. 50 – Сведения об импорте

7. Нажмите **Далее**.

Отобразится следующее окно.

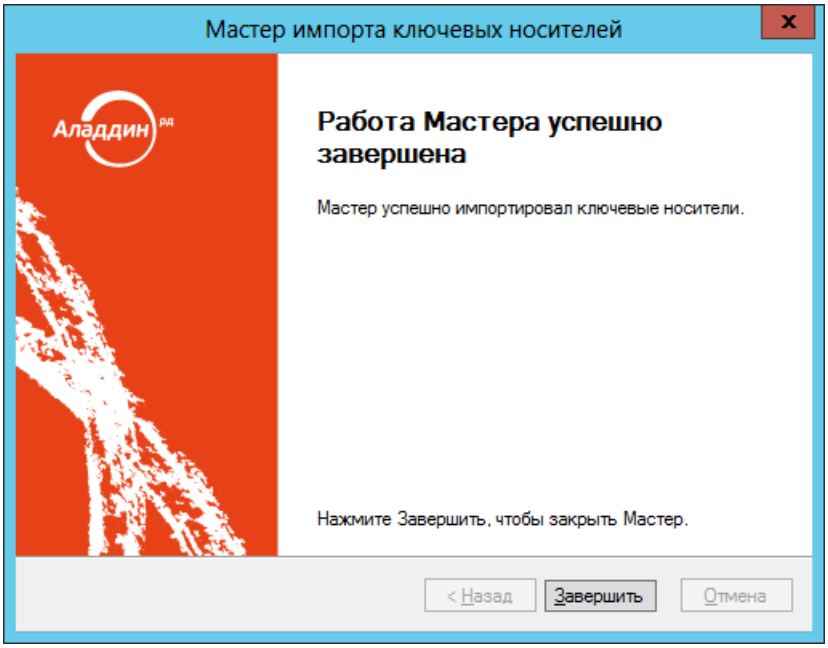


Рис. 51 – Окно завершения работы мастера импорта

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

3.6.4 Назначение электронного ключа 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. 155;
- «Настройка профиля выпуска электронных ключей», с. 158;
- «Привязка профилей», с. 296.

В консоли управления JMS назначить электронный ключ пользователю можно из трех разделов (см. табл. 4).

Табл. 4 – Назначение электронного ключа пользователю

Раздел консоли управления JMS	Условия
Пользователи	Электронный ключ должен быть подсоединен к компьютеру, но необязательно зарегистрирован.
Ключевые носители	Электронный ключ должен быть зарегистрирован в JMS, но необязательно подсоединен к компьютеру.
Подключенные устройства	Электронный ключ должен быть зарегистрирован в JMS и подсоединен к компьютеру.

Чтобы назначить электронный ключ пользователю, выполните следующие действия.

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

- **Пользователи** – в этом случае переходите к следующему шагу процедуры;
- **Ключевые носители** или **Подключенные устройства** -> **Ключевые носители** - в центральной части окна отметьте электронный ключ, которых хотите назначить, после чего в верхней панели нажмите **Назначить пользователю** (или выберите **Назначение -> Назначить пользователю**), в отобразившемся окне отметьте нужного пользователя и нажмите **Выбрать**. Электронный ключ назначен пользователю – процедура завершена.

2. В левой колонке выберите нужный каталог пользователей (например, **Users** (Пользователи)) и в центральной части окна выберите пользователя, которому вы хотите назначить электронный ключ.
3. В верхней панели нажмите **Назначить подключенный**.
   Отобразится окно приветствия мастера назначения ключевого носителя.

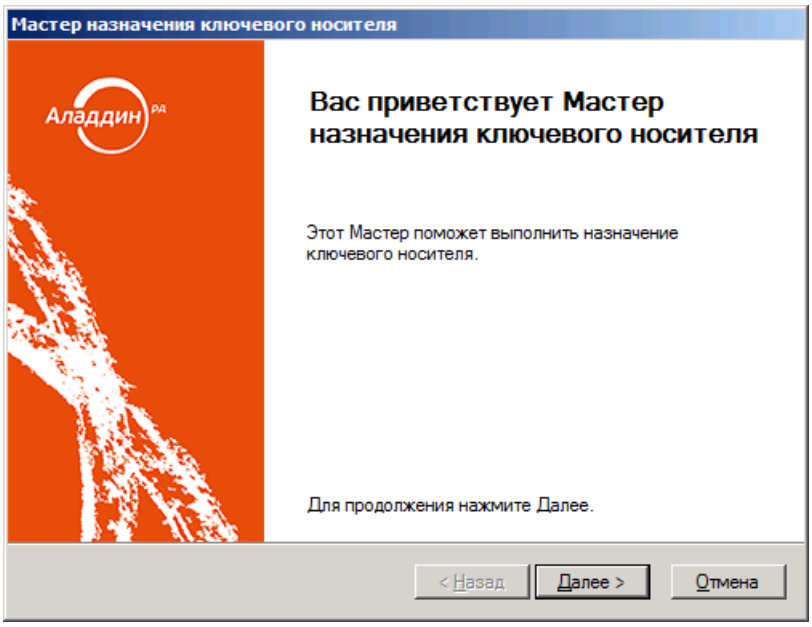


Рис. 52 – Окно приветствия мастера назначения ключевого носителя

4. Нажмите **Далее**.

Отобразится следующее окно.

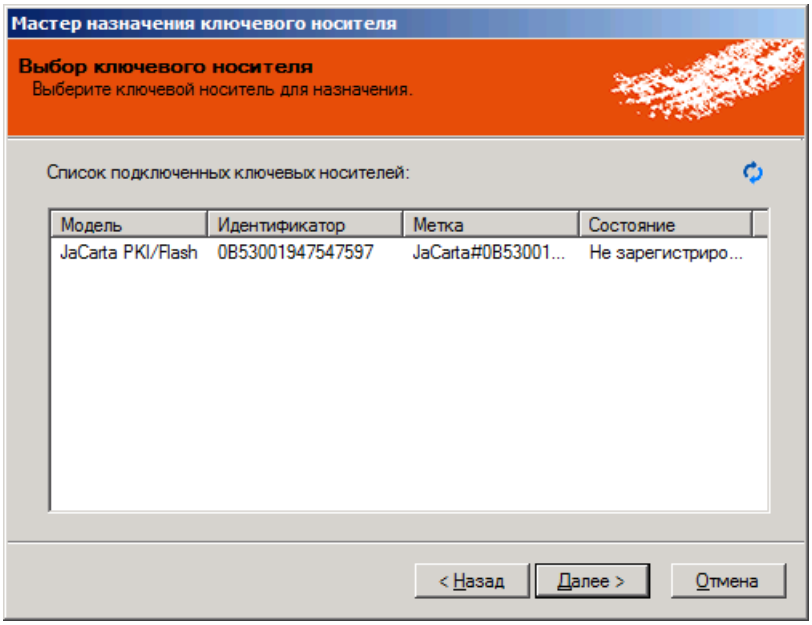


Рис. 53 – Окно выбора ключевого носителя

5. Отметьте в списке нужный электронный ключ и нажмите **Далее**.
Отобразится следующее окно.

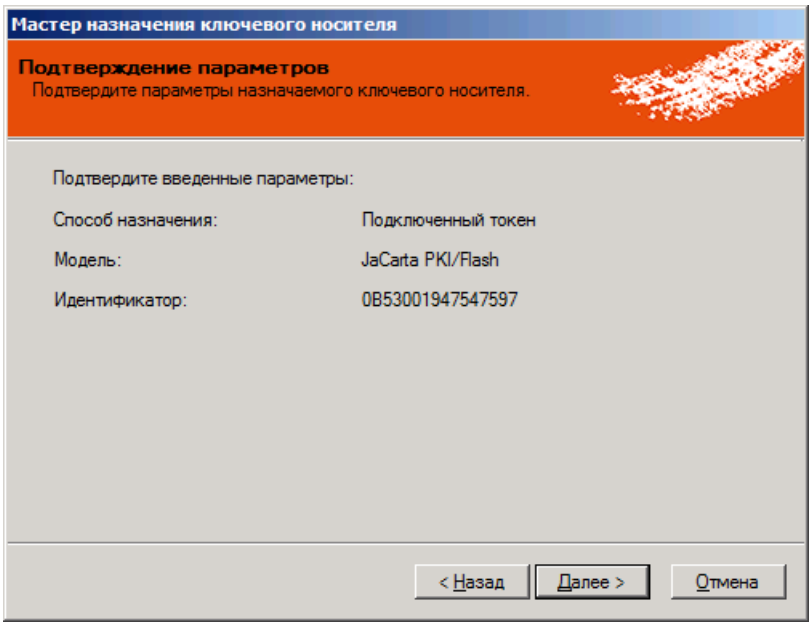


Рис. 54 – Окно подтверждения параметров

6. Нажмите **Далее**.

Отобразится следующее окно.

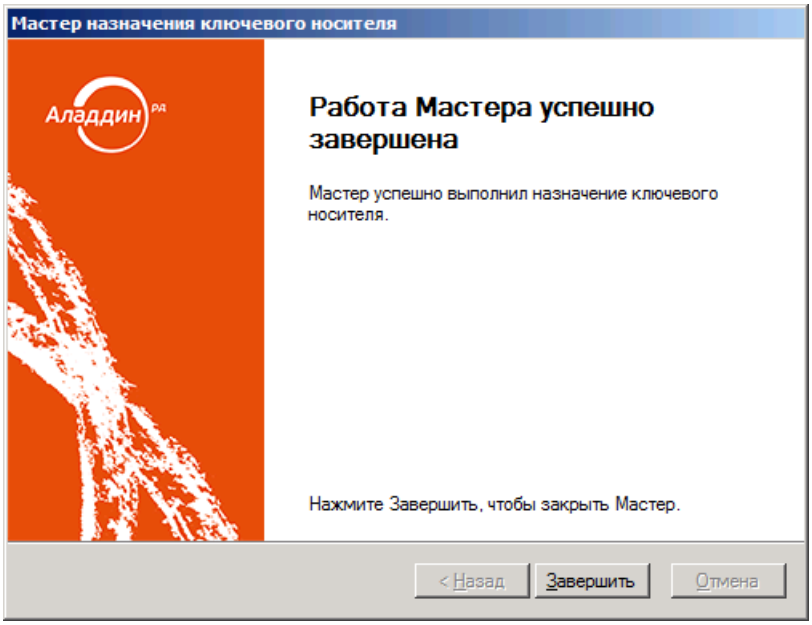


Рис. 55 – Окно завершения работы мастера

7. Нажмите **Завершить** – электронный ключ назначен 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».

Полезная информация. Назначить токен пользователю можно также из окна свойств пользователя, на вкладке **Ключевые носители** (Рис. 56, ниже), нажав в свободном простанстве вкладки правой кнопокой мыши, и выбрав пункт меню **Назначить подключенный**.

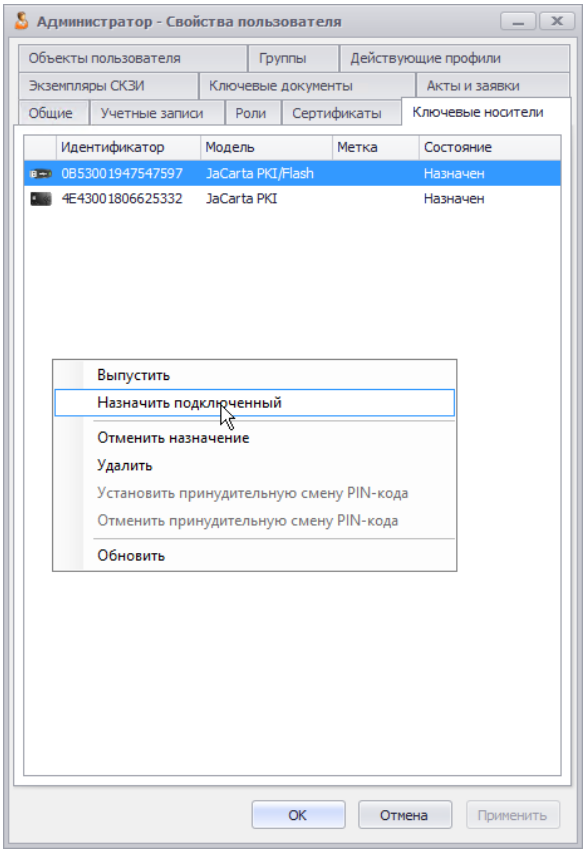


Рис. 56 – Альтернативный способ назначения пользователю электронного ключа

3.6.5 Выпуск электронного ключа администратором

Процедура выпуска электронного ключа может отличаться в зависимости от настроек профилей (см. «Настройка профилей JMS», с. 155).

Если вы настраивали параметры печати документов при выпуске электронного ключа (см. «Настройка параметров печати при выпуске объектов JMS», с. 304), то во время процедуры выпуска, отобразится несколько окон с документами, которые можно распечатать.

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

1. Подсоедините к компьютеру электронный ключ, который вы хотите выпустить.
2. В консоли управления JMS запустите мастер выпуска ключевых носителей одним из следующих способов.

   – В разделе **Пользователи** выберите нужного пользователя и нажмите **Выпустить токен**.
   – В разделе **Подключенные устройства** ->**Ключевые носители** выберите из списка нужный электронный ключ и в верхней панели нажмите **Зарегистрировать и выпустить**.

В последнем случае, если электронный ключ не был назначен пользователю, отобразится окно, в котором необходимо выбрать пользователя, на имя которого этот электронный ключ будет выпущен.

Отобразится окно приветствия мастера выпуска ключевого носителя.

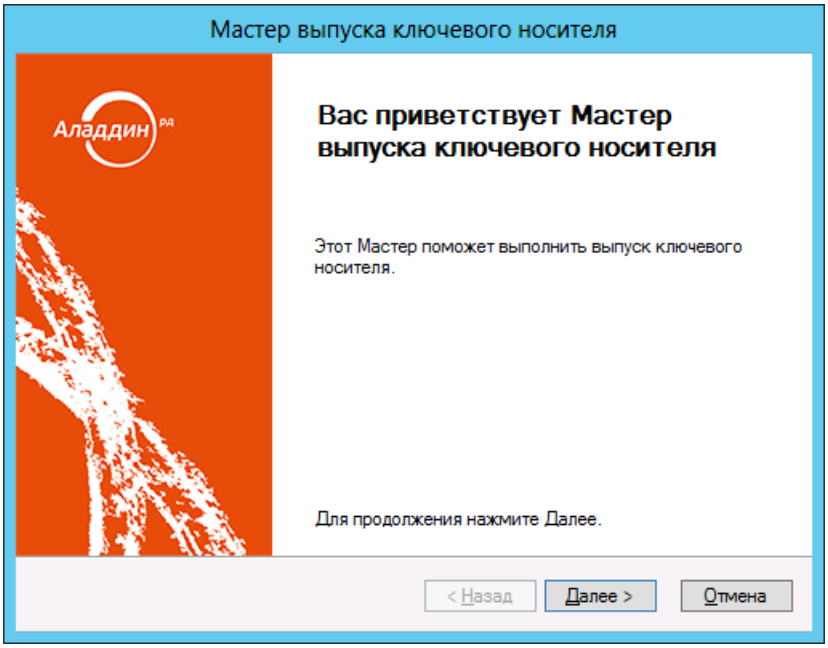


Рис. 57 – Окно приветствия мастера выпуска ключевого носителя

3. Нажмите **Далее**.
4. В зависимости от того, из какого раздела вы начали процедуру выпуска электронного ключа, выполните следующие действия.

   - **Подключенные устройства -> Ключевые носители** - переходите к следующему шагу процедуры.
   - **Пользователи** – отобразится окно выбора электронного ключа. Отметьте в этом окне электронный ключ, который необходимо выпустить, после чего нажмите **Далее**.

5. Если вы запустили процедуру из раздела **Пользователи** и/или к компьютеру подсоединено несколько электронных ключей, отобразится следующее окно. (В противном случае переходите к шагу 7 настоящей процедуры.)

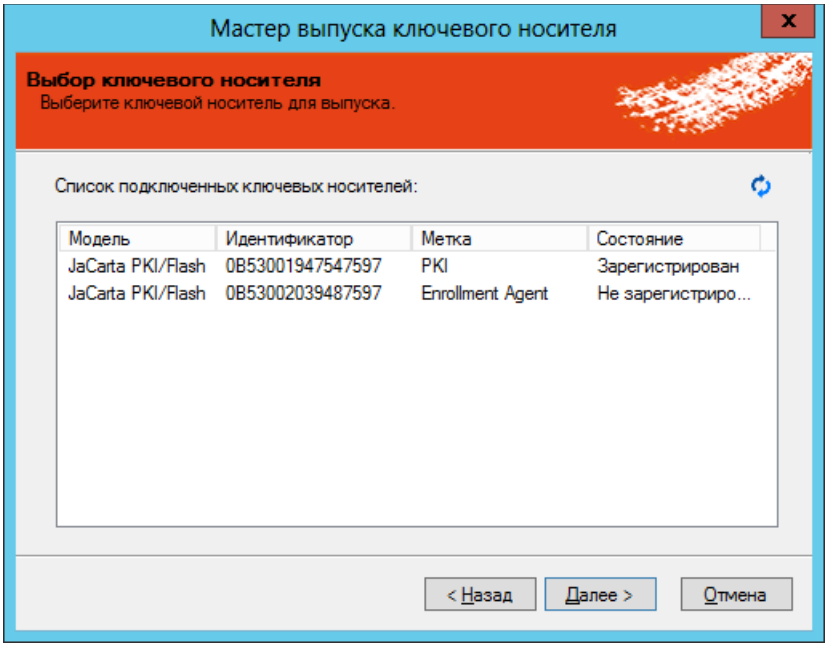


Рис. 58 – Выбор электронного ключа

6. Отметьте электронный ключ, который собираетесь выпустить, после чего нажмите **Далее**. Отобразится следующее окно.

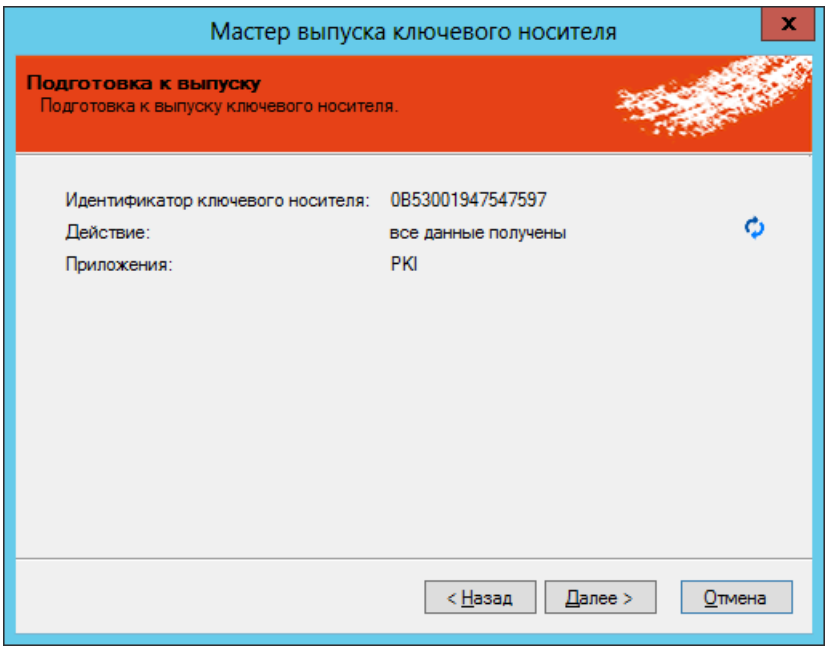


Рис. 59 – Подготовка к выпуску электронного ключа

7. Нажмите **Далее**.

Отобразится следующее окно.

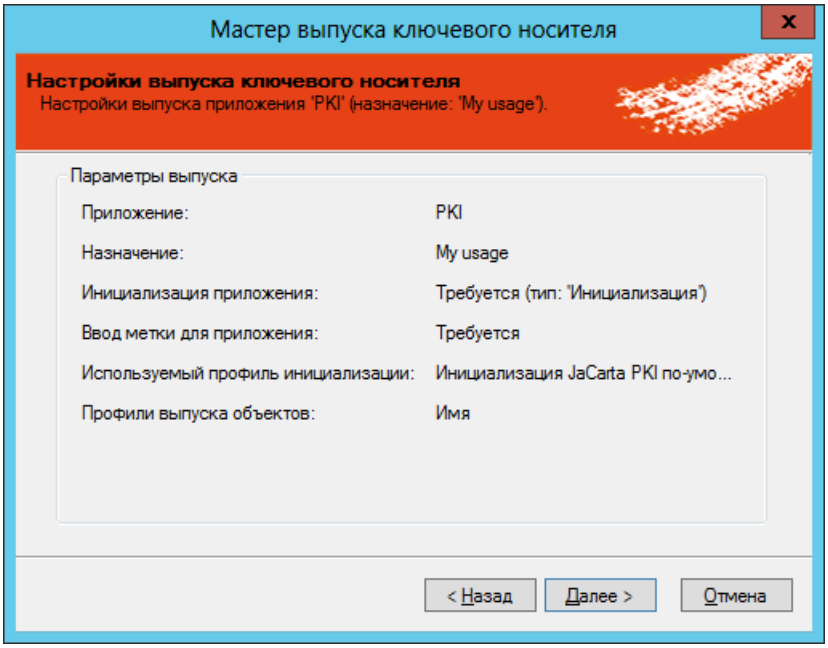


Рис. 60 – Сведения о предстоящем выпуске электронного ключа

Отобразится следующее окно.

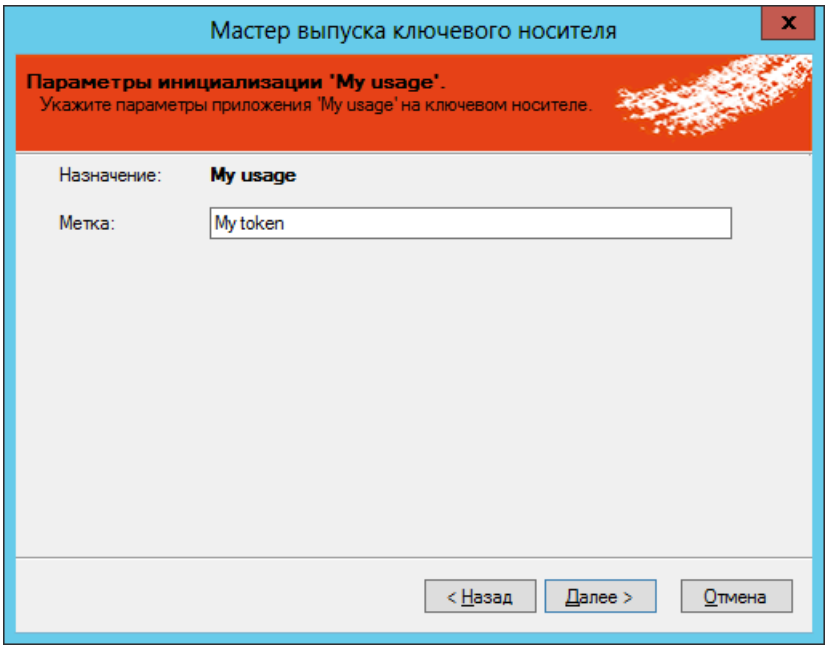


Рис. 61 – Задание метки электронного ключа

8. Задайте метку электронного ключа и нажмите **Далее**.

Отобразится следующее окно.

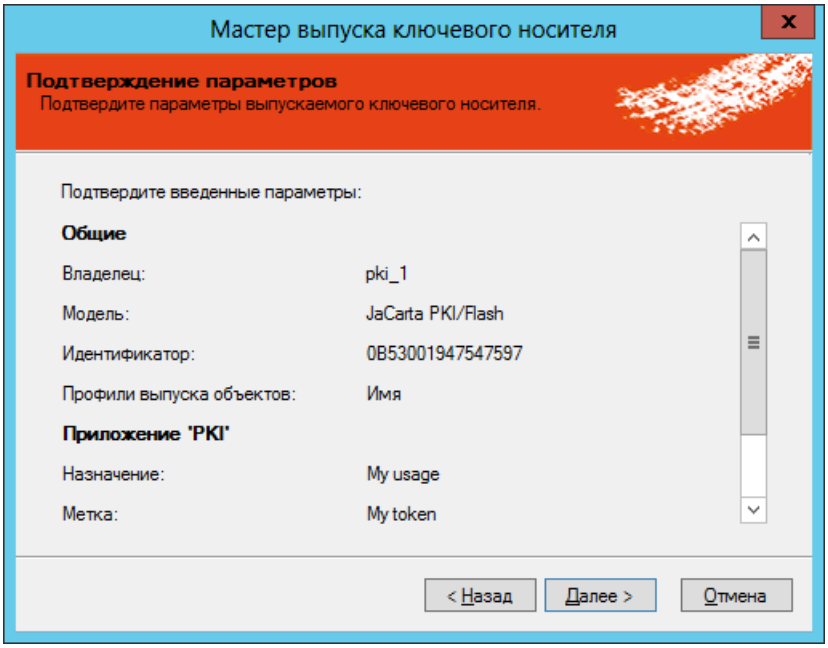


Рис. 62 – Подтверждение параметров выпускаемого электронного ключа

9. Нажмите **Далее**.
10. В зависимости от варианта выпуска электронного ключа выполните действия, указанные в табл. 5.

Табл. 5 – Варианты выпуска электронного ключа

Вариант	Действие
Запись сертификата в память электронного ключа, при этом агентом регистрации является сервер JMS.	Переходите к следующему шагу процедуры.
Запись сертификата в память электронного ключа, при этом агентом регистрации является пользователь, выполняющий функции администратора JMS.	В этом случае отобразится окно выбора сертификата агента регистрации. Выберите в этом окне нужный сертификат и нажмите OK. Если сертификат агента регистрации находится в памяти электронного ключа, подсоедините этот электронный ключ к компьютеру.
Запись в память электронного ключа профиля SecurLogon	

Если вы выполняете выпуск электронного ключа с поддержкой биометрической аутентификации, вы также должны выполнить процедуру, представленную в пункте «Особенности работы с электронными ключами JaCarta PKI/BIO», после чего возвращайтесь к завершению настоящей процедуры.

По завершении выпуска электронного ключа отобразится следующее окно.

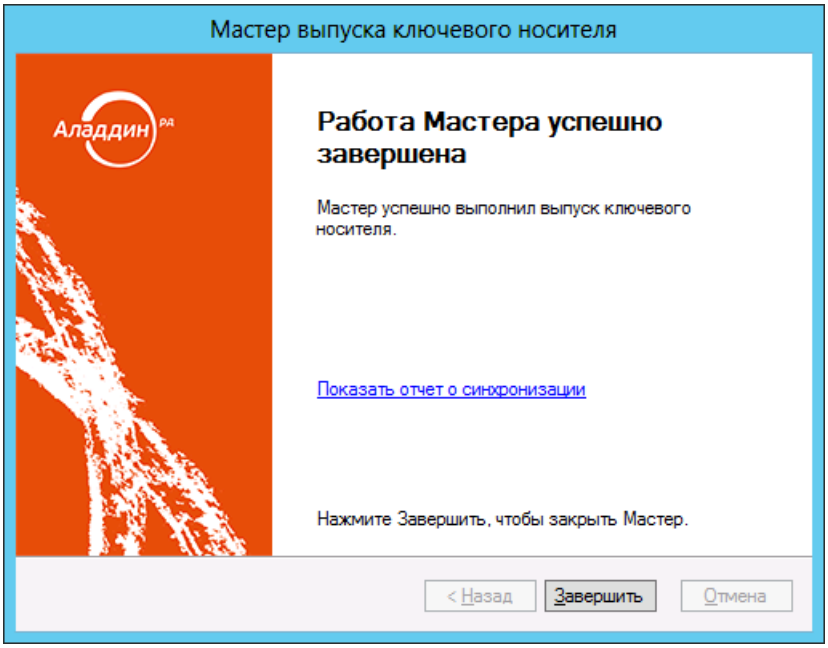


Рис. 63 – Завершение выпуска электронного ключа

11. Нажмите **Завершить**.

Примечания:

1. В случае если электронный ключ был ранее зарегистрирован как СКЗИ, при его выпуске будет сформирован нормативный документ «Акт ввода СКЗИ в эксплуатацию».
2. В случае если при выпуске электронного ключа использовался профиль выпуска сертификатов одного из следующих УЦ:
   - КриптоПро 1.5;
   - КриптоПро 2.0;
   - ViPNet;

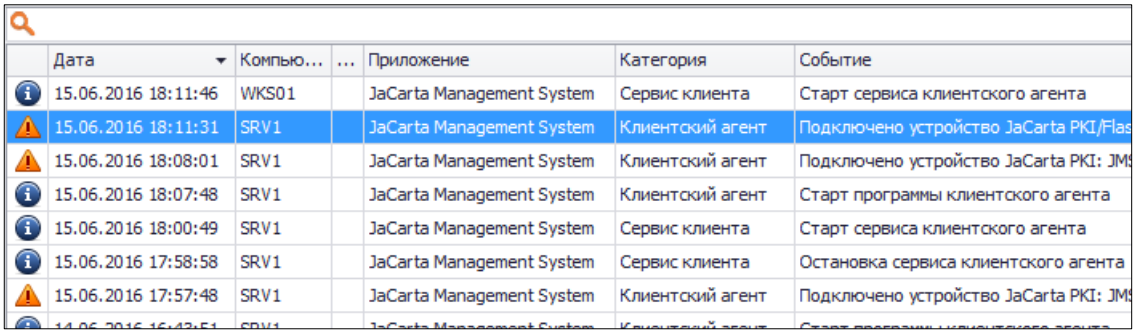
   то по окончании выпуска на данный электронныйо ключ будет записана сформированная ключевая информация, а в системе JMS сгенерированы следующие нормативные документы:
   - «Акт создания ключевой информации»;
   - «Акт ввода ключевой инормации в эксплуатацию»;
   - «Акт создания ключевых документов»;
   - «Акт передачи ключевых документов».

3.6.6 Одобрение администратором использования незарегистрированного электронного ключа, подсоединенного пользователем

Администратор JMS может в интерфейсе консоли управления JMS одобрить использование электронного ключа, который был подсоединен пользователем к своему компьютеру, даже если этот электронный ключ не был ранее зарегистрирован в JMS.

Чтобы зарегистрировать или назначить электронный ключ, подсоединенный пользователем к своему компьютеру, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Журналы** и выберите **Клиентские события** -> **Все события**.
2. В центральной части окна отобразятся события, связанные с деятельности клиентских агентов пользователей.
3. Выберите событие, связанное с подсоединением электронного ключа, например, Подключено устройство (как показано на изображении ниже).



	Дата	Компью...	...	Приложение	Категория	Событие
	15.06.2016 18:11:46	WKS01		JaCarta Management System	Сервис клиента	Старт сервиса клиентского агента
	15.06.2016 18:11:31	SRV1		JaCarta Management System	Клиентский агент	Подключено устройство JaCarta PKI/Flas
	15.06.2016 18:08:01	SRV1		JaCarta Management System	Клиентский агент	Подключено устройство JaCarta PKI: JMS
	15.06.2016 18:07:48	SRV1		JaCarta Management System	Клиентский агент	Старт программы клиентского агента
	15.06.2016 18:00:49	SRV1		JaCarta Management System	Сервис клиента	Старт сервиса клиентского агента
	15.06.2016 17:58:58	SRV1		JaCarta Management System	Сервис клиента	Остановка сервиса клиентского агента
	15.06.2016 17:57:48	SRV1		JaCarta Management System	Клиентский агент	Подключено устройство JaCarta PKI: JMS

Рис. 64 – Событие подсоединение электронного ключа в журнале JMS

4. Если электронный ключ не зарегистрирован, в панели **Действия** справа станут доступны две ссылки:

   - **Зарегистрировать КН** – щелкните на этой ссылке, чтобы запустить процедуру регистрации электронного ключа (см. «Регистрация подсоединенных электронных ключей в JMS», с. 57);
   - **Назначить КН** – щелкните на этой ссылке, что запустить процедуру назначения электронного ключа (см. «Назначение электронного ключа пользователю», с. 71).

3.6.7 Отключение/включение возможности использования электронного ключа

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.

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

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

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

6. В центральной части окна отметьте ключ, возможность использование которого вы хотите включить/отключить.
7. В верхней панели выберите один из двух пунктов:

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

   Отобразится предупреждающее сообщение.
8. Нажмите **Да**, чтобы подтвердить процедуру.

3.6.8 Очистка электронного ключа

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. В центральной части окна выберите электронный ключ, который вы хотите очистить и в верхней панели нажмите **Очистить**.
   Отобразится следующее окно.

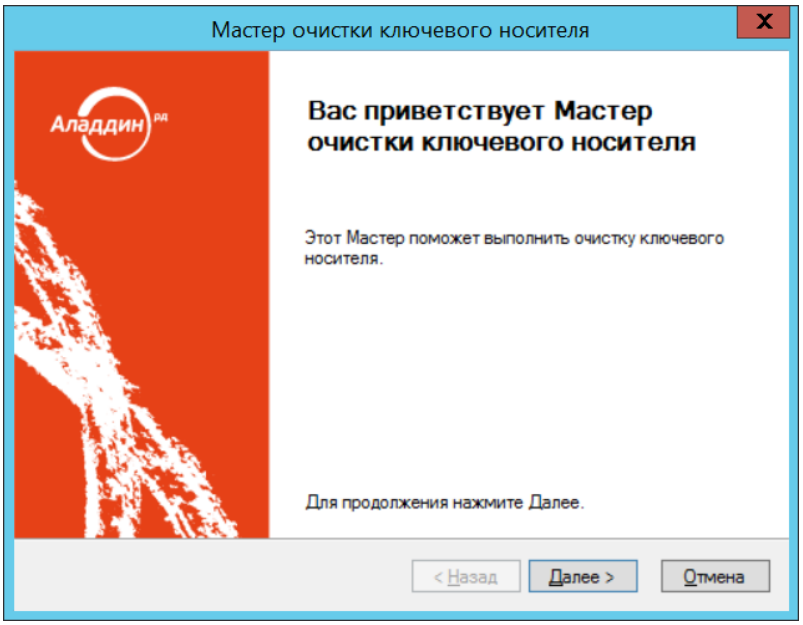


Рис. 65 – Окно приветствия мастера очистки электронного ключа

4. Нажмите **Далее**.

Отобразится следующее окно.

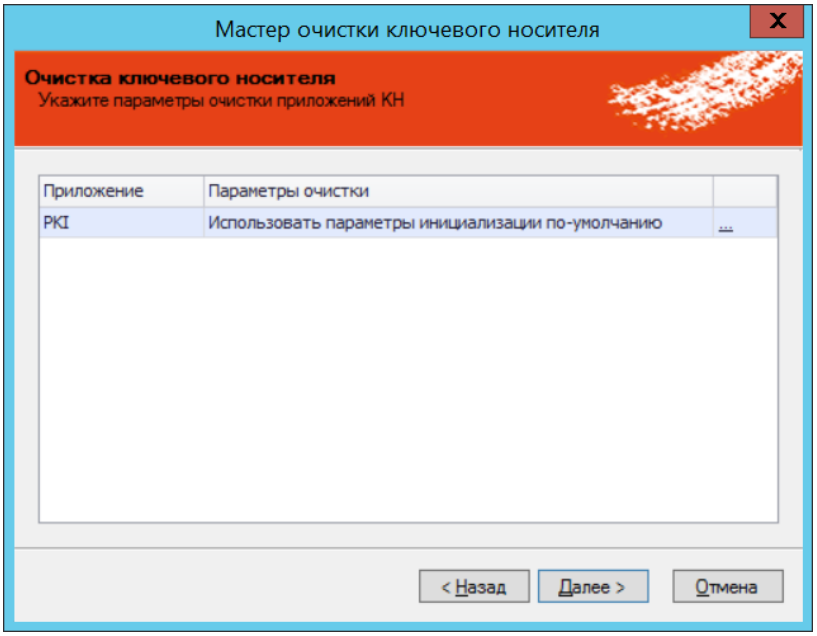


Рис. 66 – Окно настройки параметров очистки электронного ключа

5. Выберите очередное приложение в списке и нажмите «**...**».
Отобразится следующее окно.

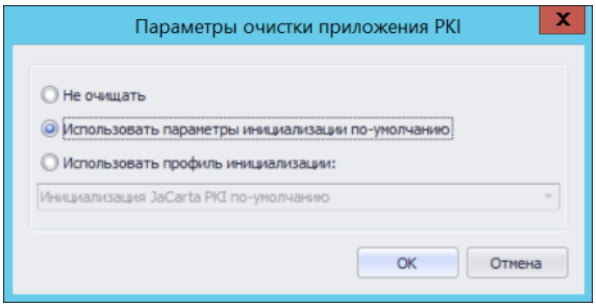


Рис. 67 – Окно выбора способа очистки приложения

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.

6. Выполните предыдущий шаг последовательно для всех приложений в списке (Рис. 66) и нажмите **Далее**.

Отобразится следующее окно.

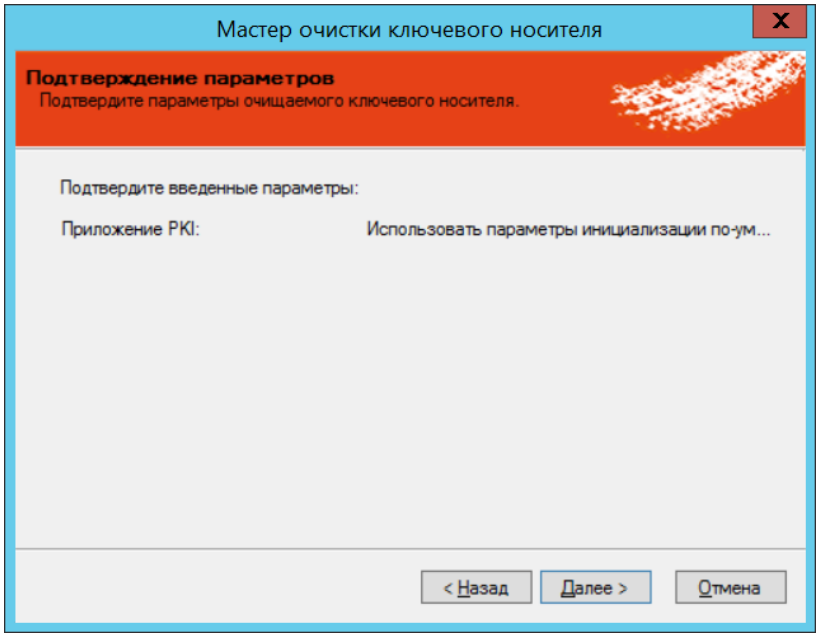


Рис. 68 – Окно подтверждения параметров очистки электронного ключа

Нажмите **Далее**.

7. По окончании процедуры очистки электронного ключа отобразится следующее окно.

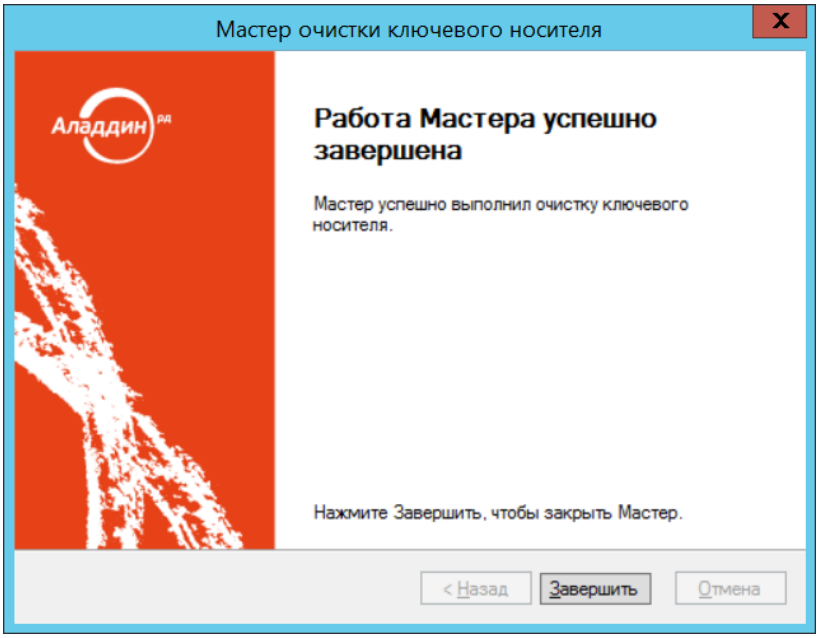


Рис. 69 – Окно завершения работы мастера очистки электронного ключа

8. Нажмите **Завершить**.

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

3.6.9 Синхронизация электронного ключа

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

В процессе синхронизации содержимое электронного ключа приводится в соответствие с привязанными профилями выпуска объектов JMS (например, профили выпуска сертификатов, профили внешних объектов, профиль SecurLogon).

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

Синхронизируемый электронный ключ должен быть при этом подсоединен к компьютеру.

2. В центральной части окна выберите электронный ключ, который вы хотите синхронизировать и в верхней панели нажмите **Синхронизация**.
   Отобразится следующее окно.

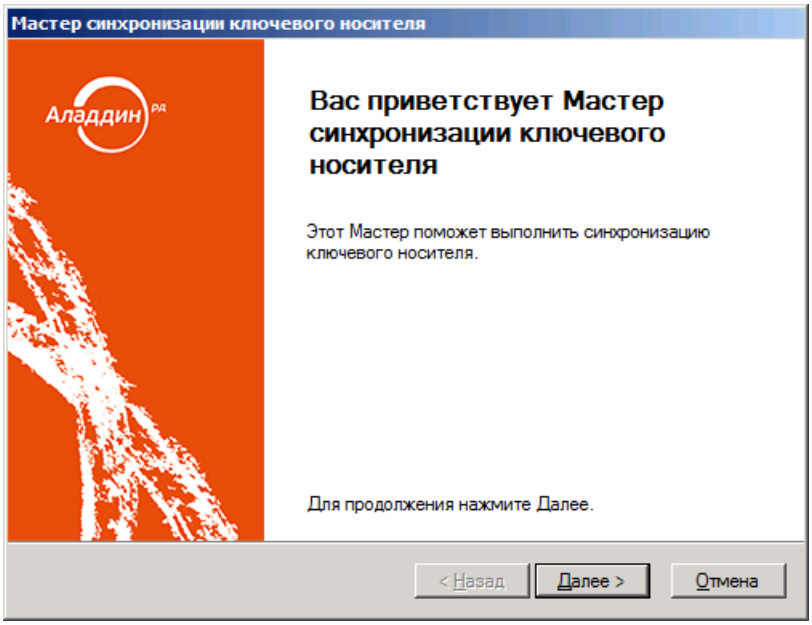


Рис. 70 – Окно приветствия мастера синхронизации ключевого носителя

3. Нажмите **Далее**.

Отобразится следующее окно.

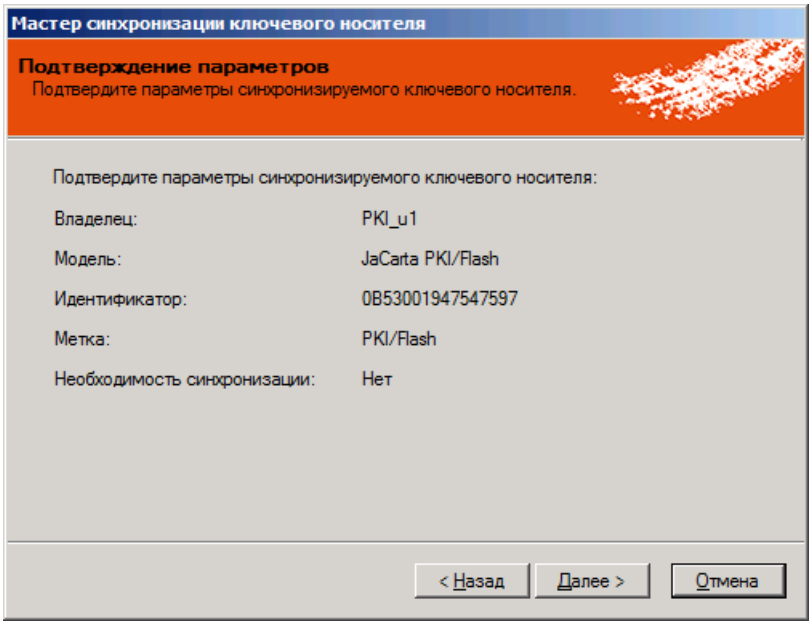


Рис. 71 – Окно подтверждения параметров синхронизируемого ключевого носителя

4. Нажмите **Далее**.
   По окончании процедуры синхронизации отобразится следующее окно.

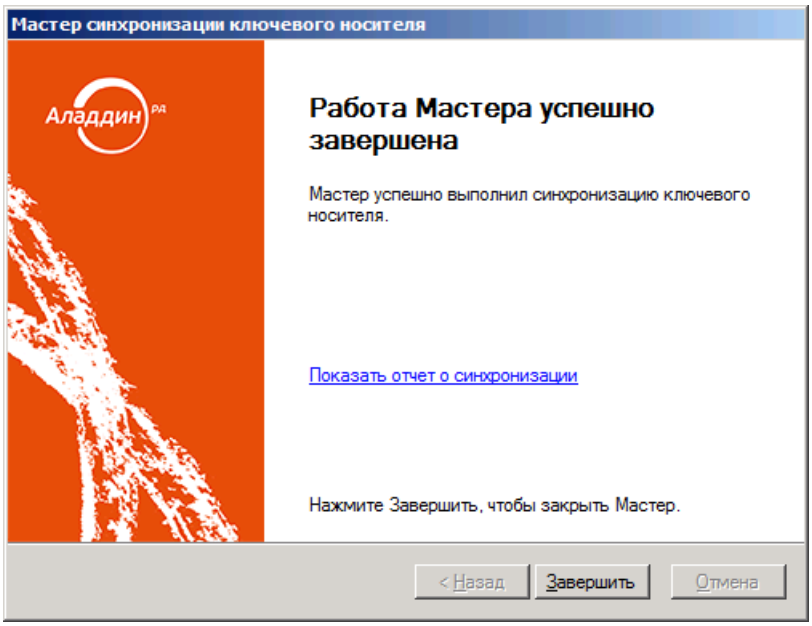


Рис. 72 – Окно завершения работы мастера синхронизации ключевого носителя

5. Нажмите **Завершить**.

3.6.9.1.1 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. 164).

- **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 (за исключением «виртуальных») производится только при нажатии в на ссылку **Синхронизировать** в приложении **Клиент JMS** на вкладке **Ключевые носители** (см. документ «JaCarta Management System. Руководство пользователя», [1]).

Принудительная (расширенная) синхронизация для «виртуальных» электронных ключей (см. «Виртуальный электронный ключ «Хранилище пользователя», с. 118) производится:

- при открытии пользовательского сеанса (сессии) в приложении **Клиент JMS**;
- при нажатии на кнопку **Обновить** в приложении **Клиент JMS**.

Для двух последних случаев синхронизации к рабочей станции не требуется привязывать профиль клиентского агента: при указанных условиях будут использоваться значения профиля клиентского агента по умолчанию (см. Табл. 6).

Примечание. Синхронизацию электронных ключей, производимую в соответствии с профилем настройки клиентского агента, не следует путать с синхронизацией рабочих станций (производится в соответствии с профилем настройки синхронизации рабочей станции, см. «Профиль настройки синхронизации рабочей станции», с. 244). Синхронизация рабочих станций также может включать в себя синхронизацию сертификатов, находящихся в соответствующих хранилищах сертификатов рабочей станции, с хранилищем в БД JMS.

Табл. 6 – 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

Параметр профиля настройки клиентского агента	Значение параметра по умолчанию
Ускоренная синхронизация	5 минут
Количество повторов неудачной синхронизации	5
Настройки автоматической разблокировки	
Разрешать автоматическую разблокировку	Нет
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

3.6.10 Отзыв электронного ключа

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

   В последнем случае отзываемый электронный ключ должен быть подсоединен к компьютеру.
2. В верхней панели нажмите **Отозвать**.

Отобразится следующее окно.

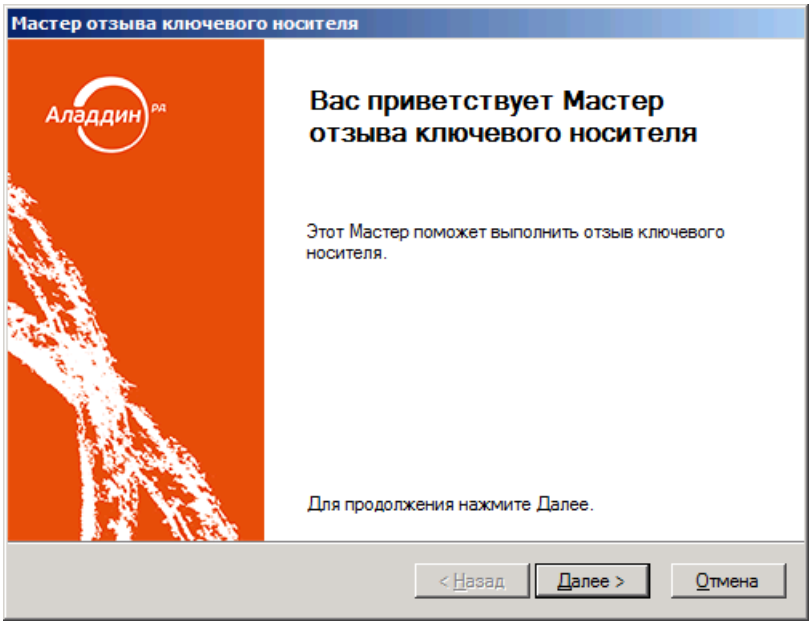


Рис. 73 – Окно приветствия мастера отзыва ключевого носителя

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

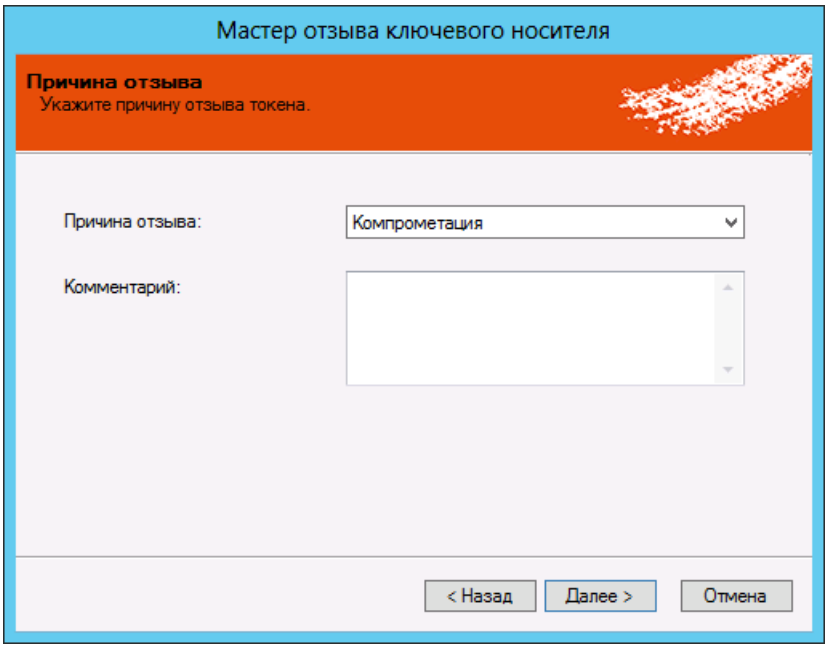


Рис. 74 – Укажите причину отзыва

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

Отобразится следующее окно.

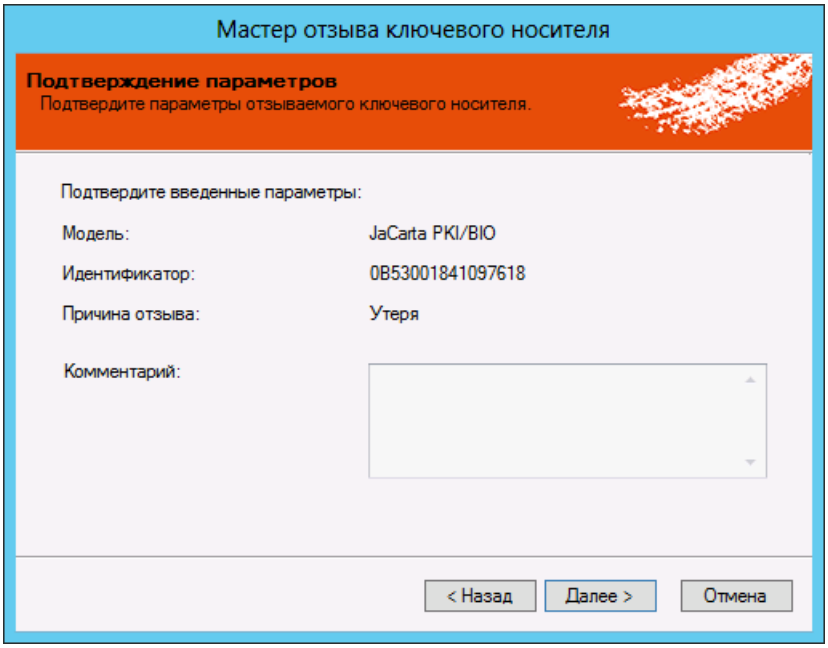


Рис. 75 – Окно подтверждения параметров отзываемого ключевого носителя

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

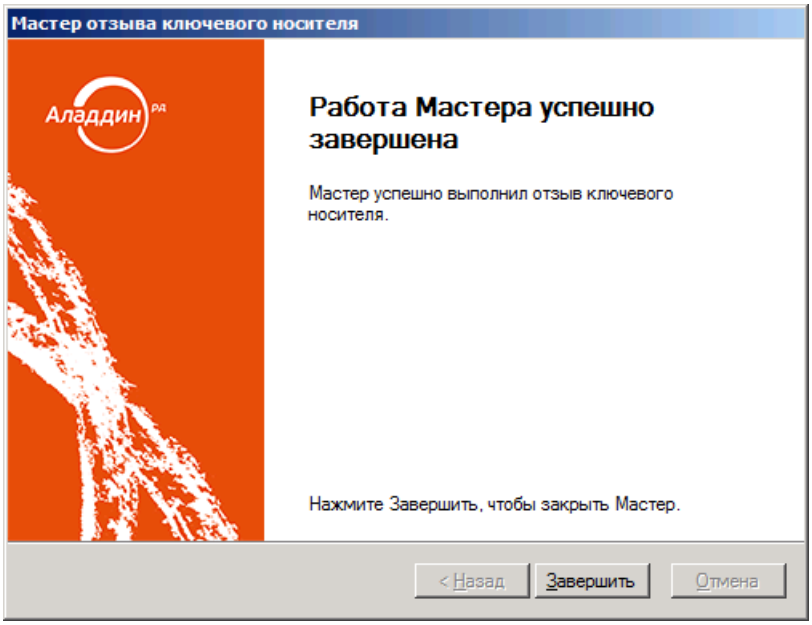


Рис. 76 – Окно завершения работы мастера отзыва ключевого носителя

6. Нажмите **Завершить**.

Примечания:

1. В случае если электронный ключ был ранее зарегистрирован как СКЗИ, при его отзыве будет сформирован нормативный документ «Акт вывода СКЗИ из эксплуатации».
2. Если на электронном ключе хранилась ключевая информация (КИ), при его отзыве данная КИ будет с него удалена, а в системе JMS будет сформирован нормативный документ «Акт вывода ключевой информации из эксплуатации».

3.6.11 Замена электронного ключа

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 центре сертификации Microsoft) 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:
   - **Ключевые носители**;
   - **Подключенные устройства** -> **Ключевые носители**.

В последнем случае заменяемый электронный ключ должен быть подсоединен к компьютеру.

2. Выберите электронный ключ, который требуется заменить.
3. В верхней панели нажмите **Заменить**.
   Отобразится следующее окно.

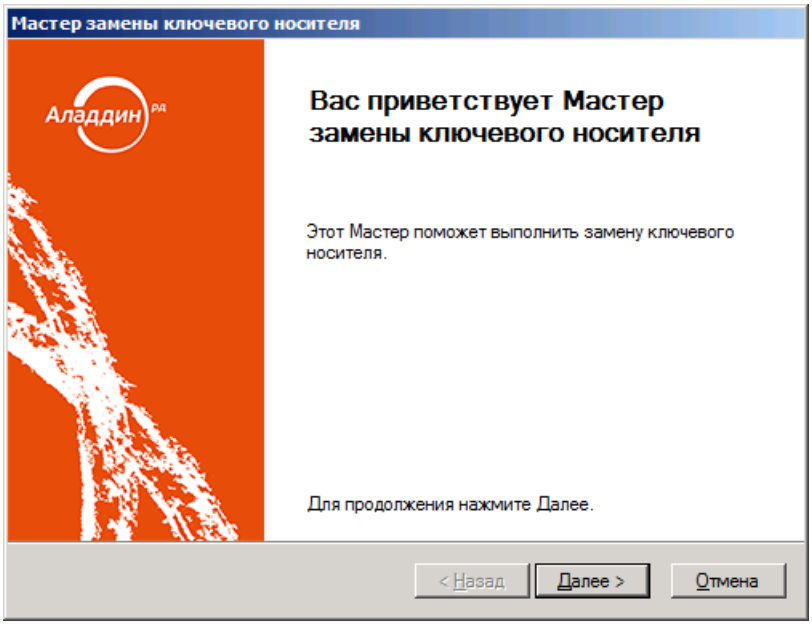


Рис. 77 – Окно приветствия мастера замены ключевого носителя

4. Нажмите **Далее**.

Отобразится следующее окно.

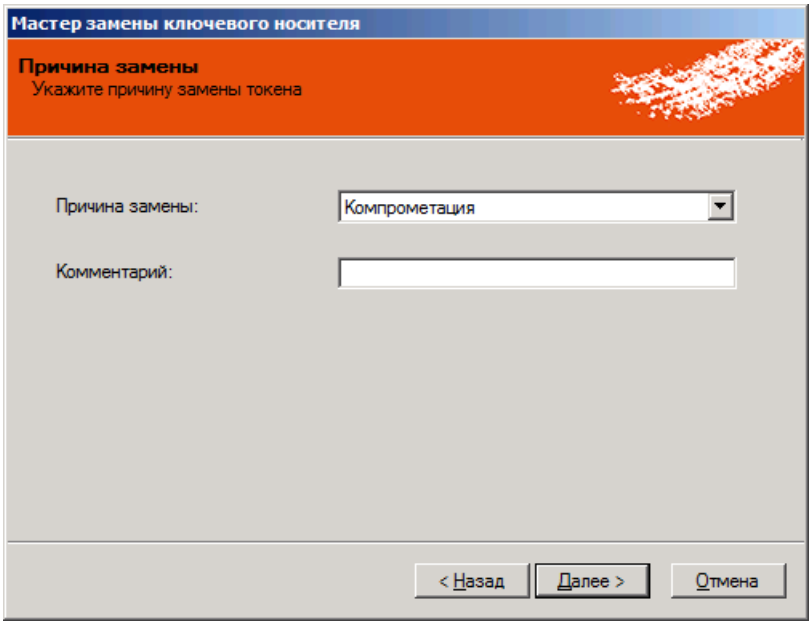


Рис. 78 – Укажите причину замены электронного ключа

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

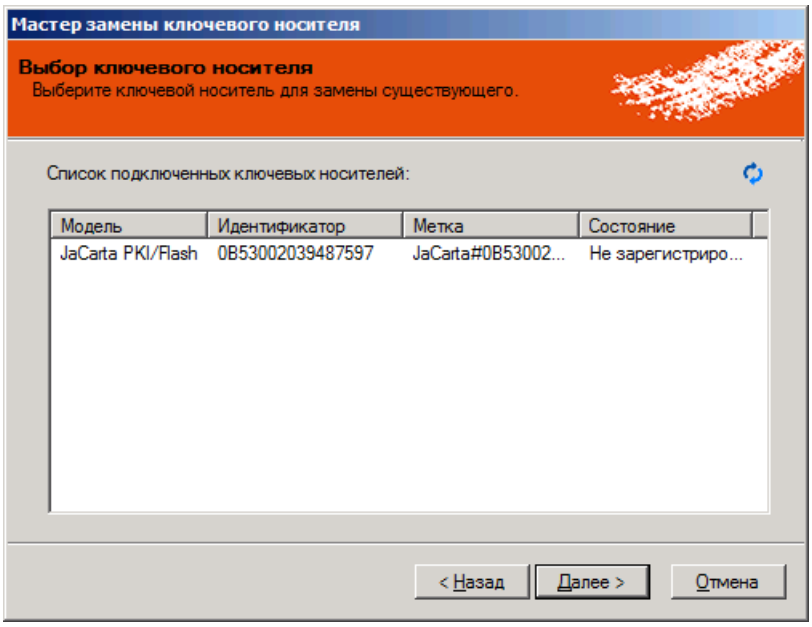


Рис. 79 – Окно выбора нового электронного ключа

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

Отобразится следующее окно.

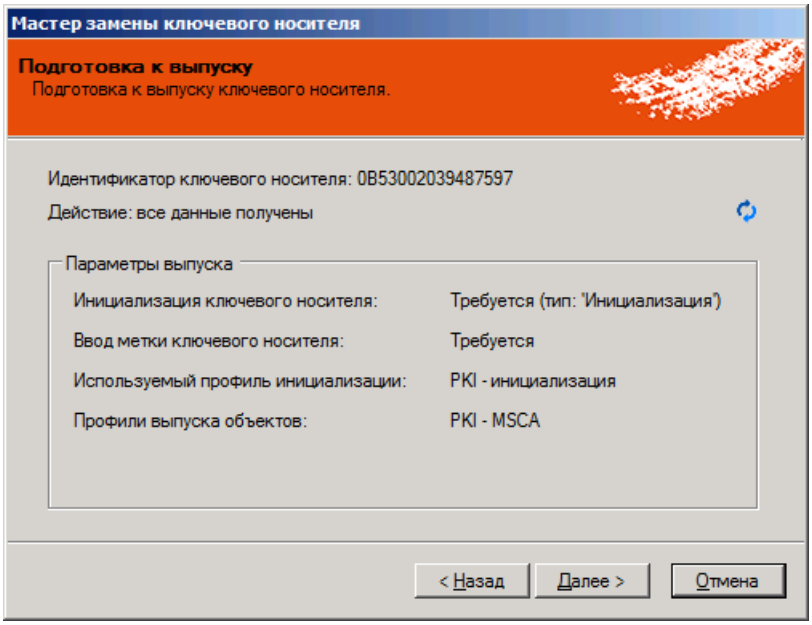


Рис. 80 – Окно подготовки к выпуску ключевого носителя

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

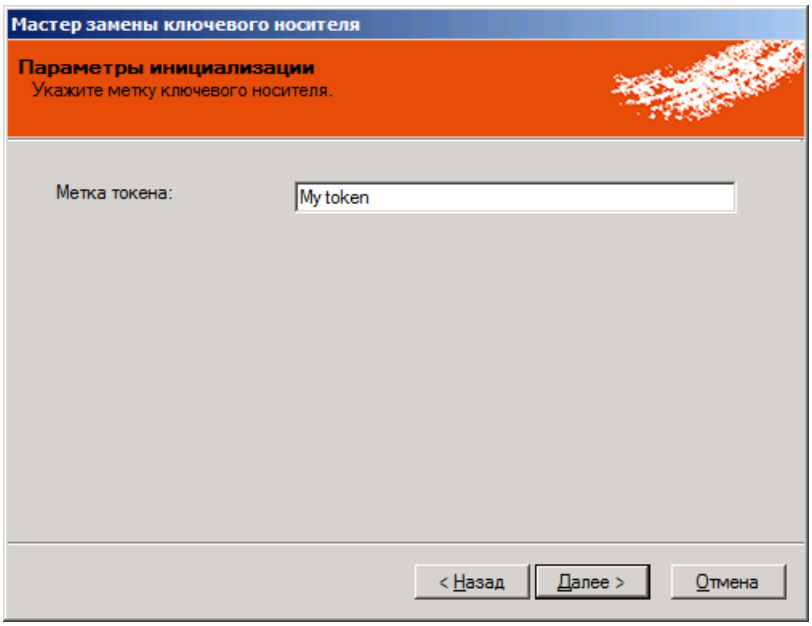


Рис. 81 – Окно настройки параметров инициализации

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

Отобразится следующее окно.

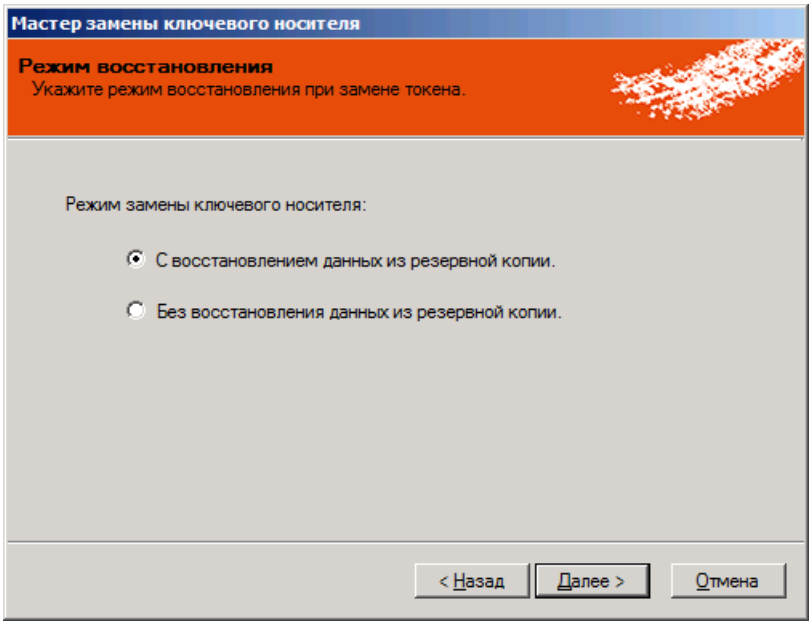


Рис. 82 – Выбор режима замени электронного ключа

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

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

   Отобразится следующее окно.

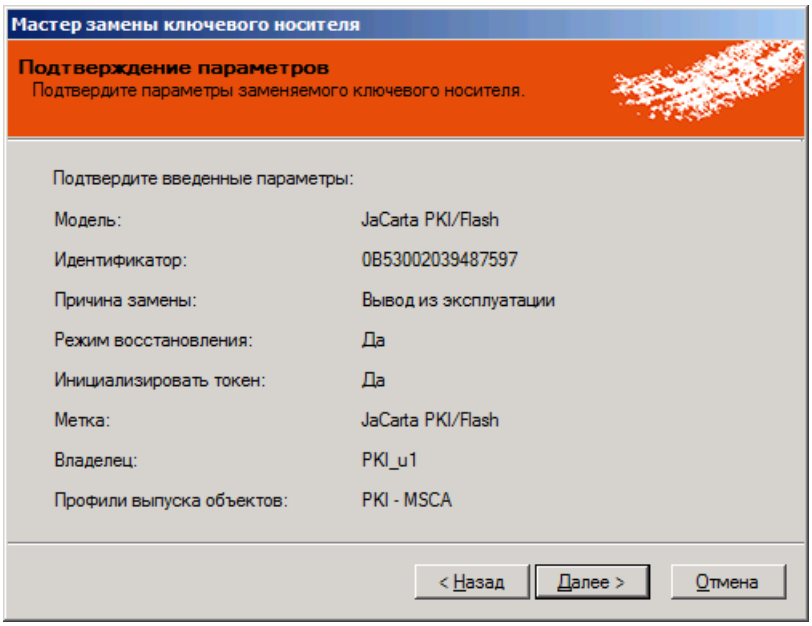


Рис. 83 – Окно подтверждения параметров заменяемого ключевого носителя

10. Нажмите **Далее**.

Если вы выполняете замену электронного ключа с поддержкой биометрической аутентификации, выполните процедуру, представленную в пункте «Особенности работы с электронными ключами JaCarta PKI/BIO», после чего возвращайтесь к завершению настоящей процедуры.

Отобразится следующее окно.

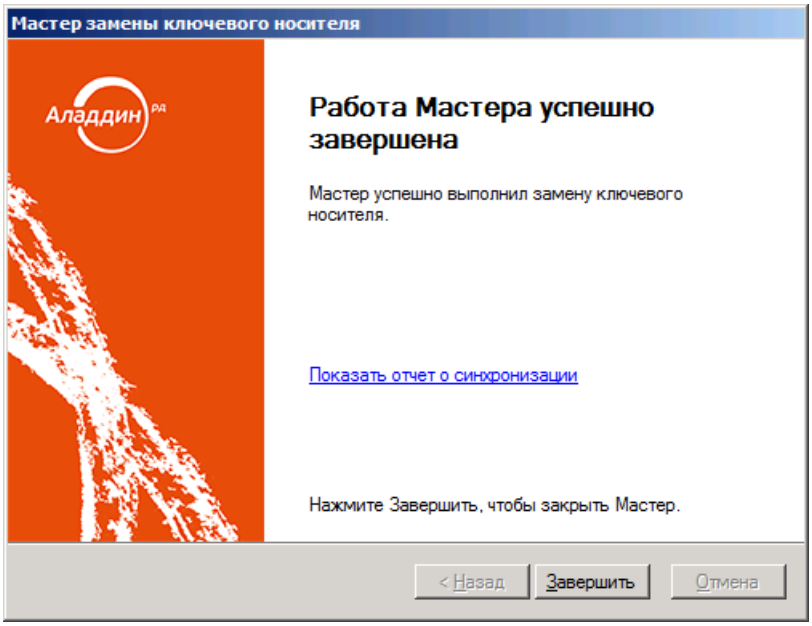


Рис. 84 – Окно завершения работы мастера замены ключевого носителя

11. Нажмите **Завершить**.

3.6.12 Возврат в эксплуатацию электронного ключа

JMS позволяет вернуть отозванный электронный ключ 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:
   - **Ключевые носители**;
   - **Подключенные устройства** -> **Ключевые носители**.

В последнем случае электронный ключ должен быть подсоединен к компьютеру.

2. Выберите электронный ключ, который необходимо вернуть в эксплуатацию.
3. В верхнем меню нажмите **Вернуть в эксплуатацию**.
   Отобразится предупреждающее сообщение.
4. Нажмите **Да**, чтобы подтвердить действие.

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

3.6.13 Разблокировка подсоединенного электронного ключа

3.6.13.1 Предоставление права на разблокировку

По умолчанию встроенная роль **Администратор ИБ** в JMS не наделена правом разблокировки PIN-кодов 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. 390)
- добавить созданной роли право выполнения операции **Разблокировка по PIN-коду администратора** (см. «Приложение 3. Права на выполнение операций», с. 670);
- назначить (добавить) созданную роль пользователю, которому должно быть предоставлено право разблокировки электронных ключей (например, администратору, см. «Назначение ролей пользователям JMS», с. 395).

3.6.13.2 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 панели нажмите **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. Выполните следующие действия в зависимости от того, какой тип доступа заблокирован на электронном ключе.

   - Если на электронном ключе заблокирован PIN-код пользователя, переходите к следующему шагу настоящей процедуры.
   - Если на электронном ключе заблокирована возможность биометрической аутентификации, выполните процедуру, представленную в пункте «Особенности работы с электронными ключами JaCarta PKI/BIO», после чего переходите к последнему шагу настоящей процедуры.
   - Если на электронном ключе заблокирован PIN-код пользователя и возможность биометрической аутентификации, переходите к следующему шагу настоящей процедуры.

Отобразится следующее окно.

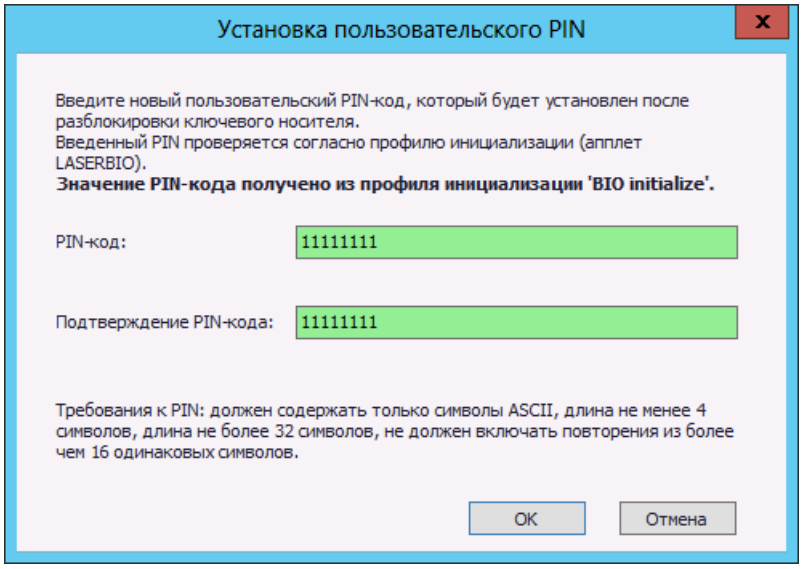


Рис. 85 – Установка пользовательского PIN-кода при разблокировке

Процедура представлена на примере приложения PKI. В случае с приложениями ГОСТ и STORAGE отобразится окно сброса счетчика попыток неверного ввода PIN-кода пользователя. В этом случае нажмите **OK**, чтобы подтвердить действие.

7. В полях **PIN-код** и **Подтверждение PIN-кода** задайте новый PIN-код пользователя и введите подтверждение соответственно, после чего нажмите **OK**.

Если на электронном ключе был заблокирован PIN-код пользователя и возможность биометрической аутентификации, выполните процедуру, представленную в пункте «Особенности работы с электронными ключами JaCarta PKI/BIO», после чего возвращайтесь к завершению настоящей процедуры.

8. В окне сообщения об успешной разблокировке нажмите **OK**.

3.6.14 Разблокировка электронного ключа в удаленном режиме

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

1. В консоли управления JMS перейдите в раздел **Ключевые носители**.
2. Выберите электронный ключ, который нужно разблокировать.
3. В верхней панели выберите **Удаленная разблокировка** (или **Временная блокировка -> Удаленная разблокировка)**.

Отобразится следующее окно.

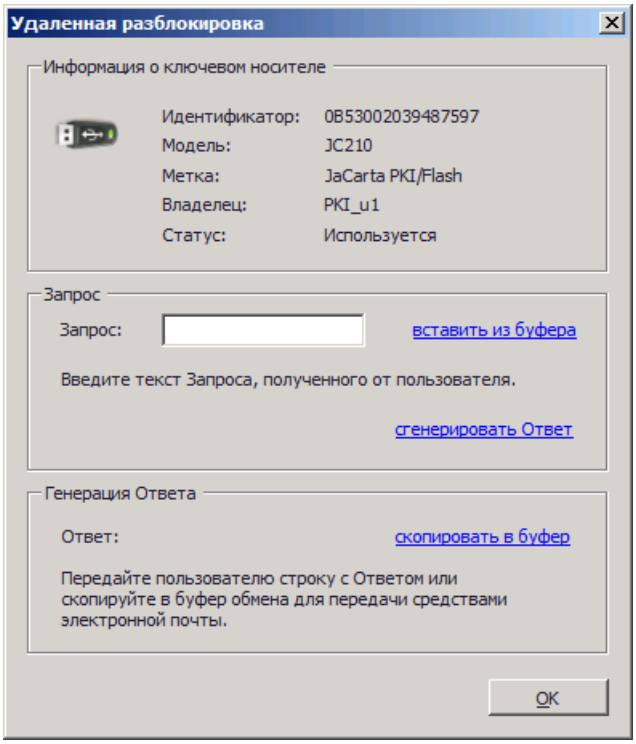


Рис. 86 – Окно удаленной разблокировки

4. Проинструктируйте пользователя (например, по телефону) 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 окно Клиент JMS (например, щелкнув правой кнопкой в области уведомлений на значке и нажав **Открыть**);
4.3. в окне **Клиент JMS** пользователь должен выбрать вкладку **Ключевые носители**, щелкнуть правой кнопкой на значке электронного ключа с заблокированным PIN-кодом пользователя и выбрать **Разблокировать**;
4.4. на экране пользователя отобразится мастер приветствия разблокировки - пользователь должен нажать **Далее**;
4.5. на экране пользователя отобразится окно выбора режима разблокировки - пользователь должен выбрать пункт **Вручную** и нажать **Далее**;
4.6. в отобразившемся окне подтверждения параметров пользователь должен нажать **Далее**;
на экране пользователя отобразится следующее окно.

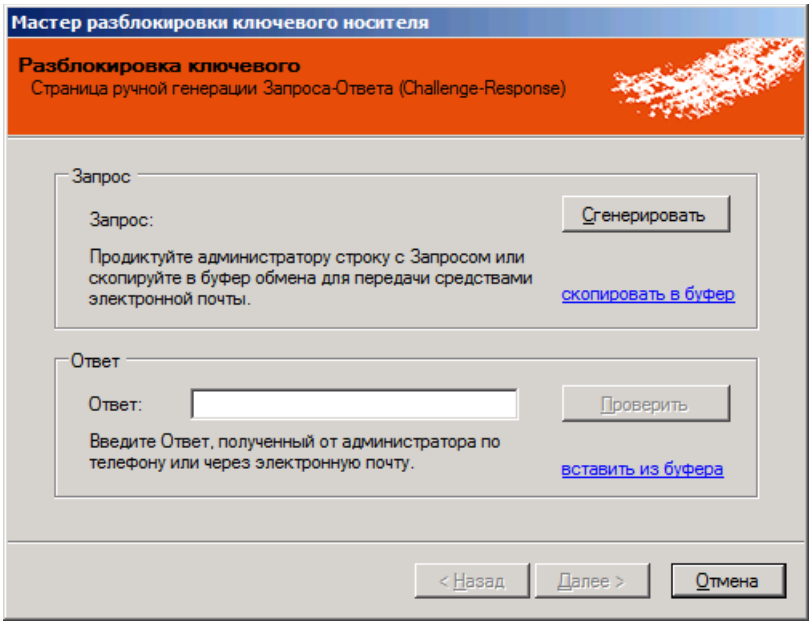


Рис. 87 – Генерация значения запроса

4.7. Пользователь должен нажать **Сгенерировать**.

4.8. В поле **Запрос** отобразится значение запроса - пользователь должен продиктовать это значение вам.

Введите продиктованное пользователем значение запроса в поле **Запрос** окна удаленной разблокировки, после чего щелкните на ссылке **сгенерировать Ответ**. Сгенерированное значение отобразится в поле **Ответ** окна удаленной разблокировки (см. рис. 88).

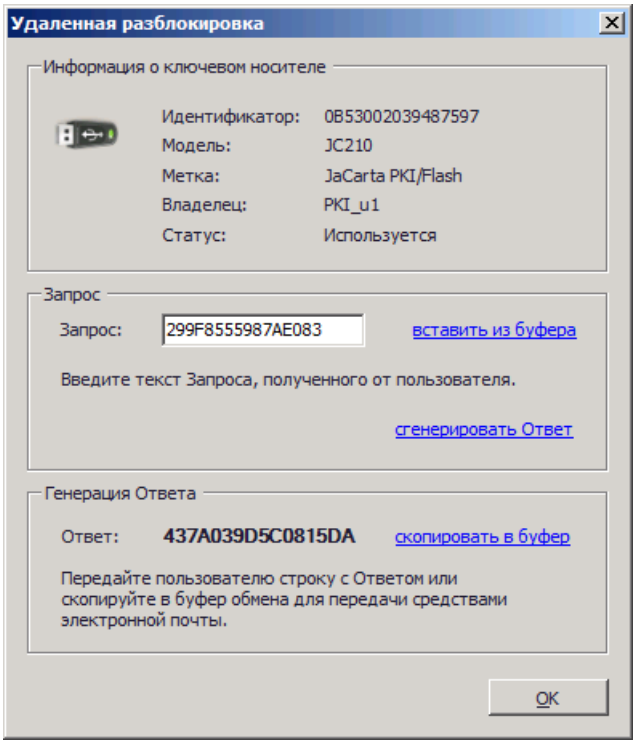


Рис. 88 – Сгенерированный код ответа

5. Продиктуйте пользователю значение ответа - пользователь должен ввести его в поле **Ответ** окна мастера разблокировки, после чего нажать **Проверить**.

Если значение введено верно, на экране пользователя отобразится следующее сообщение.

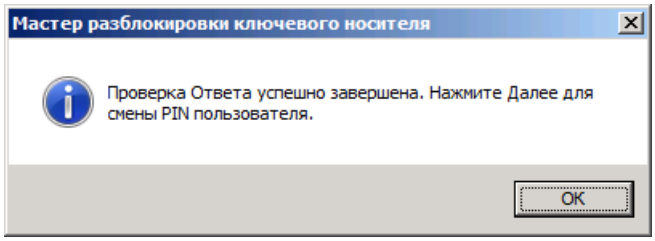


Рис. 89 – Сообщение об успешной проверке значения ответа

6. Пользователь должен закрыть окно сообщения, нажав **OK**, после чего в окне мастера разблокировки нажать **Далее**.
7. На экране пользователя отобразится окно задания нового PIN-кода пользователя – в полях **PIN-код пользователя** и **Подтверждения PIN-кода** пользователь должен ввести новое значение PIN-кода пользователя и подтверждение соответственно, после чего нажать **Далее**.
8. На экране завершения работы мастера разблокировки пользователь должен нажать **Завершить**.
   PIN-код пользователя разблокирован.

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

3.6.15 Замена отпечатков пальцев, сохраненных в памяти JaCarta PKI/BIO

При работе с электронными ключами может возникнуть необходимость заменить отпечатки пальцев пользователя, сохраненные памяти электронного ключа, на другие. Чтобы сделать это, выполните следующие действия.

Важно! Для замены отпечатков пальцев в памяти приложений PKI/BIO пользователю консоли управления JMS должно быть предоставлено право **Разблокировка по PIN-коду администратора**. Процедура предоставления такого права описана в разделе «Предоставление права на разблокировку», с. 96.

1. Подсоедините электронный ключ, в памяти которого необходимо заменить отпечатки пальцев, к компьютеру.
2. В консоли управления JMS перейдите в раздел **Подключенные устройства** -> **Ключевые носители**.
3. В верхней панели нажмите **Заменить отпечатки пальцев (BIO)**.
4. В окне предупреждения нажмите **Да**.
5. Выполните процедуру, представленную в пункте «Особенности работы с электронными ключами JaCarta PKI/BIO», после чего переходите к следующему шагу настоящей процедуры.
6. В окне сообщения об успешной смене отпечатков нажмите **OK**.

3.6.16 Удаление электронного ключа

При удалении электронного ключа в JMS выполняются те же действия, что и при его отзыве (см. «Отзыв электронного ключа», с. 88). 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, профили SecurLogon и др.) рекомендуется предварительно выполнить отзыв и очистку ключа (см. соответственно «Отзыв электронного ключа», с. 88 и «Очистка электронного ключа», с. 82).

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

В последнем случае отзываемый электронный ключ должен быть подсоединен к компьютеру.

8. В верхней панели нажмите **Удалить**.
9. В окне подтверждения запроса на удаление электронного ключа нажмите **Да**.

3.6.17 Особенности работы с электронными ключами JaCarta PKI/BIO

При работе с электронными ключами JaCarta PKI/BIO возникает необходимость сохранять отпечатки пальцев пользователя в памяти электронного ключа при выполнении следующих операций:

- «Выпуск электронного ключа администратором», с. 75;
- «Замена электронного ключа», с. 91;
- «Разблокировка подсоединенного электронного ключа», с. 96;
- «Замена отпечатков пальцев, сохраненных в памяти JaCarta PKI/BIO», с. 100;

Всякий раз, когда такая необходимость возникает, отображается окно мастера сохранения отпечатков пальцев.

Пользователь, которому будет передан электронный ключ, должен участвовать в процедуре для успешного завершения операции.

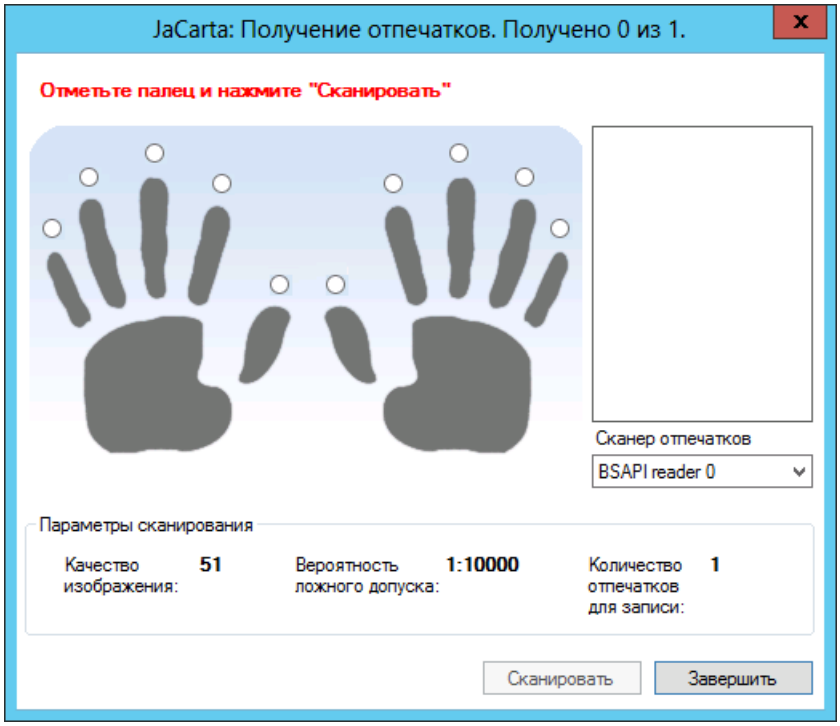


Рис. 90 – Выбор пальцев для сканирования

1. Выберите палец, отпечаток которого будет сохранен в памяти электронного ключа, и нажмите **Сканировать**. (При необходимости выберите нужный сканер отпечатков в соответствующем списке.)

Отобразится следующее окно.

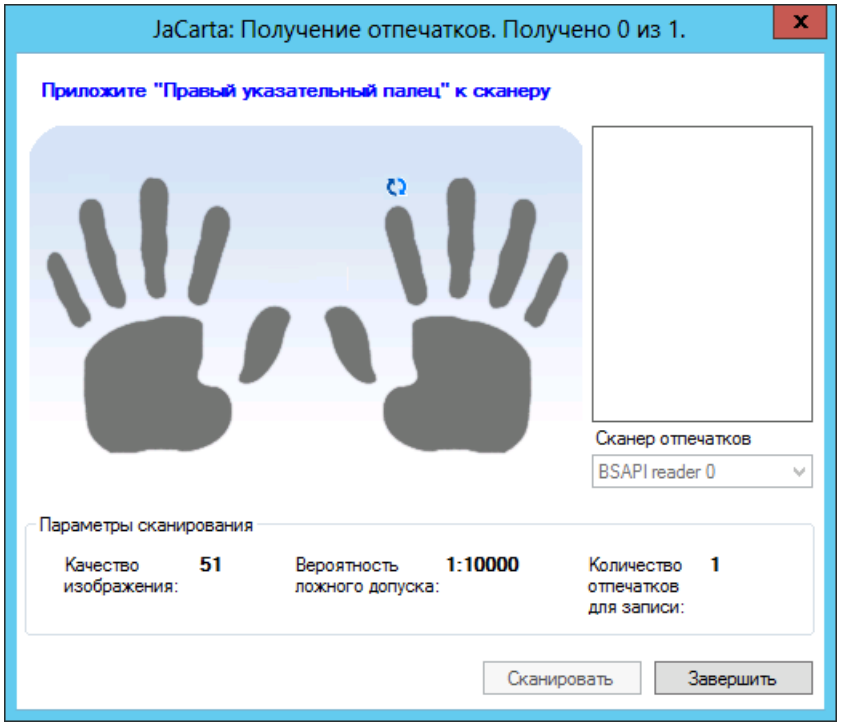


Рис. 91 – Первичное сканирование отпечатка

После первичного сканирования отобразится следующее окно.

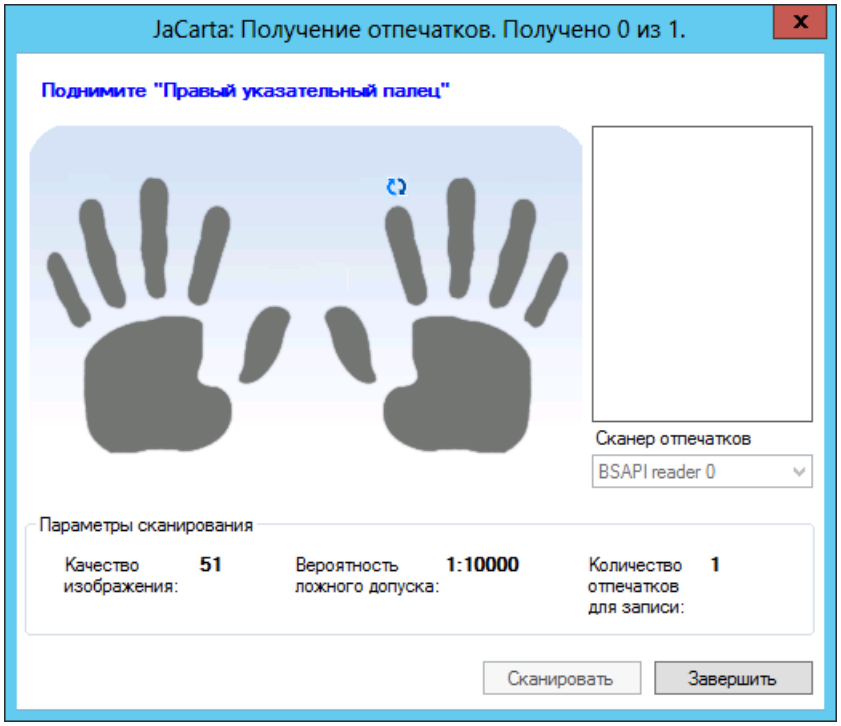


Рис. 92 – Первичное сканирование произведено

2. Пользователь должен убрать палец со сканера отпечатков.

3. После первичного считывания отпечатка необходимо считать тот же отпечаток снова – для этого повторите необходимые шаги настоящей процедуры.

   Двукратного считывания может быть недостаточно – повторяйте необходимые шаги до тех пор, пока отпечатки не будут сохранены в памяти электронного ключа.

   После успешного повторного считывания отобразится следующее окно.

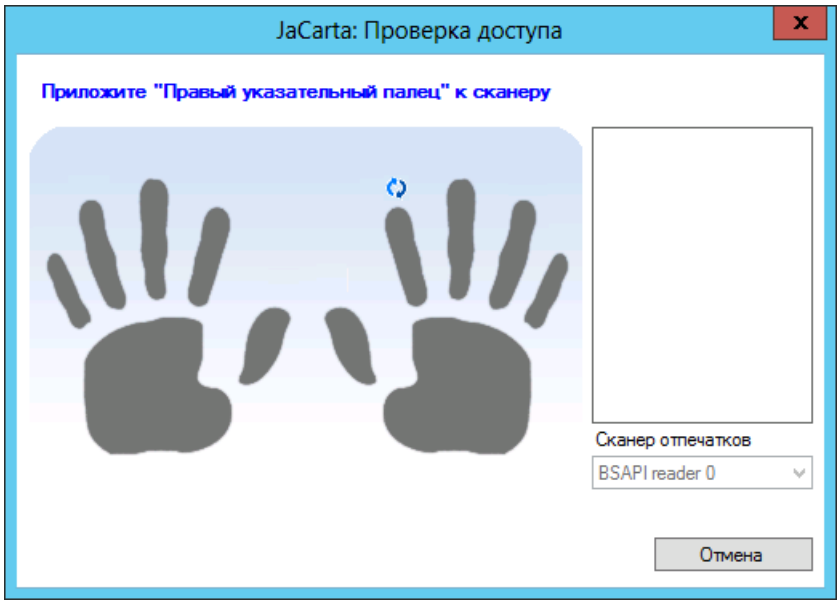


Рис. 93 – Проверка корректности сканирования отпечатков

4. Пользователь должен приложить отсканированный палец к сканеру отпечатков.
5. В зависимости от выполняемой процедуры выполните следующие действия:

   - «Выпуск электронного ключа администратором» - переходите к следующему шагу настоящей процедуры;
   - «Замена электронного ключа» - переходите к следующему шагу настоящей процедуры;
   - «Разблокировка подсоединенного электронного ключа» - возвращайтесь к окончанию процедуры разблокировки (стр. 96);
   - «Замена отпечатков пальцев, сохраненных в памяти JaCarta PKI/BIO» - возвращайтесь к окончанию процедуры замены (стр. 100).

Отобразится следующее окно.

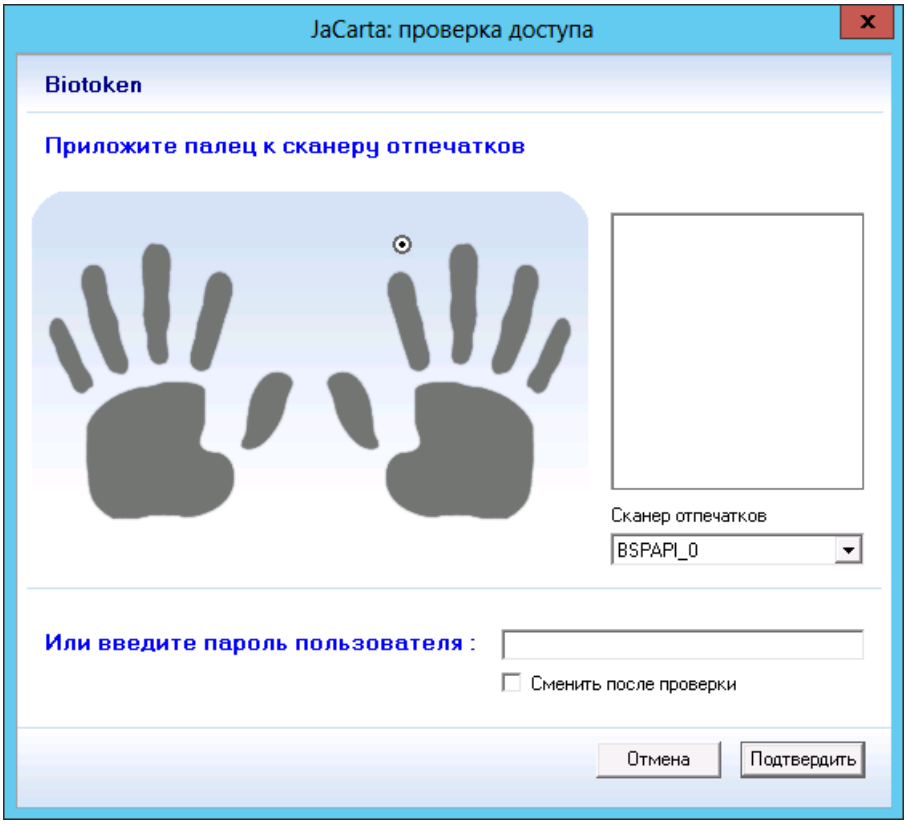


Рис. 94 – Проверка биометрического доступа

6. В зависимости от настроек профиля инициализации пользователь должен приложить палец к сканеру отпечатков и/или ввести PIN-код пользователя в поле **И/Или введите пароль пользователя**.
7. При необходимости установите флаг **Сменить после проверки** – в этом случае пользователь должен будет сменить свой PIN-код пользователя при следующем использовании электронного ключа.
8. Нажмите **Подтвердить**, после чего возвращайтесь к окончанию процедуры («Выпуск электронного ключа администратором», с. 75 или «Замена электронного ключа», с. 91).

3.6.18 Особенности работы с электронными ключами JaCarta-2 ГОСТ

3.6.18.1 Особенности выпуска JaCarta-2 ГОСТ

Порядок выпуска электронных ключей JaCarta-2 ГОСТ в целом соответствует стандартной последовательности действий (см. «Выпуск электронного ключа администратором», с. 75), однако существуют следующие особенности.

1. В текущей версии JMS не предусмотрена процедура инициализации электронных ключей JaCarta-2 ГОСТ, в связи с чем в JMS отсутствует тип профиля инициализации для JaCarta-2 ГОСТ, а в профилях выпуска ключевых носителей для приложения ГОСТ-2 отсутствует опция инициализации.

Примечание. Инициализация электронных ключей *JaCarta-2 ГОСТ* выполняется либо при их производстве, либо на специализированном АРМ администратора безопасности (см. документацию электронных ключей данного типа).

2. В ходе выполнения *Мастера выпуска ключевого носителя* при установке метки электронного ключа в окне соответствующего запроса (Рис. 95) введите PIN-код пользователя и нажмите **ОК**.

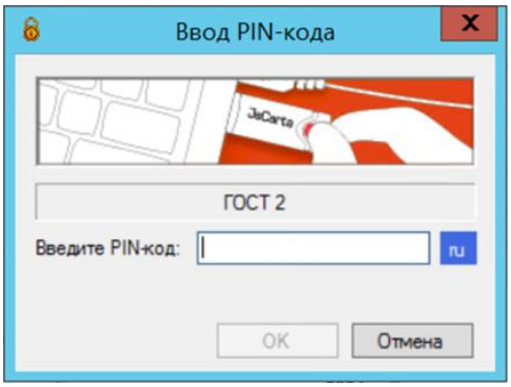


Рис. 95 – Запрос PIN-кода пользователя при выпуске JaCarta-2 ГОСТ

Примечание. В электронных ключах *JaCarta-2 ГОСТ* PIN-код пользователя устанавливается либо при их производстве, либо на специализированном АРМ администратора безопасности.

3. В случае если в профиле выпуска сертификата, применяемом в ходе выпуска *JaCarta-2 ГОСТ*, установлен признак **Применять PIN-код подписи** (см. например «Настройки профиля выпуска сертификатов в центре сертификации Microsoft», с. 209), на этапе генерации ключевых пар мастер выпуска запрашивает PIN-код пользователя и устанавливаемый PIN-код подписи:

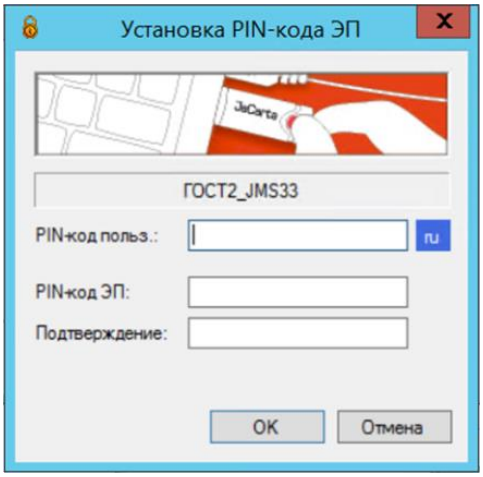


Рис. 96 – Запрос PIN-кодов при генерации ключевых пар на JaCarta-2 ГОСТ

Для завершения данного этапа *Мастера выпуска ключевого носителя* введите PIN-код пользователя, PIN-код подписи (**PIN-код ЭП**) и его подтверждение и нажмите **ОК**.

3.6.18.2 Установка и смена PIN-кода подписи в JaCarta-2 ГОСТ

Для установки PIN-кода подписи (PIN-кода ЭП) в электронном ключе выполните следующие действия:

1. Подсоедините электронный ключ, на котором надо выполнить операцию, к компьютеру.
2. В консоли управления JMS в разделе **Подключенные устройства -> Ключевые носители** выберите электронный ключ в средней части окна (Рис. 97) и в верхней панели нажмите **Установить/Сменить**:

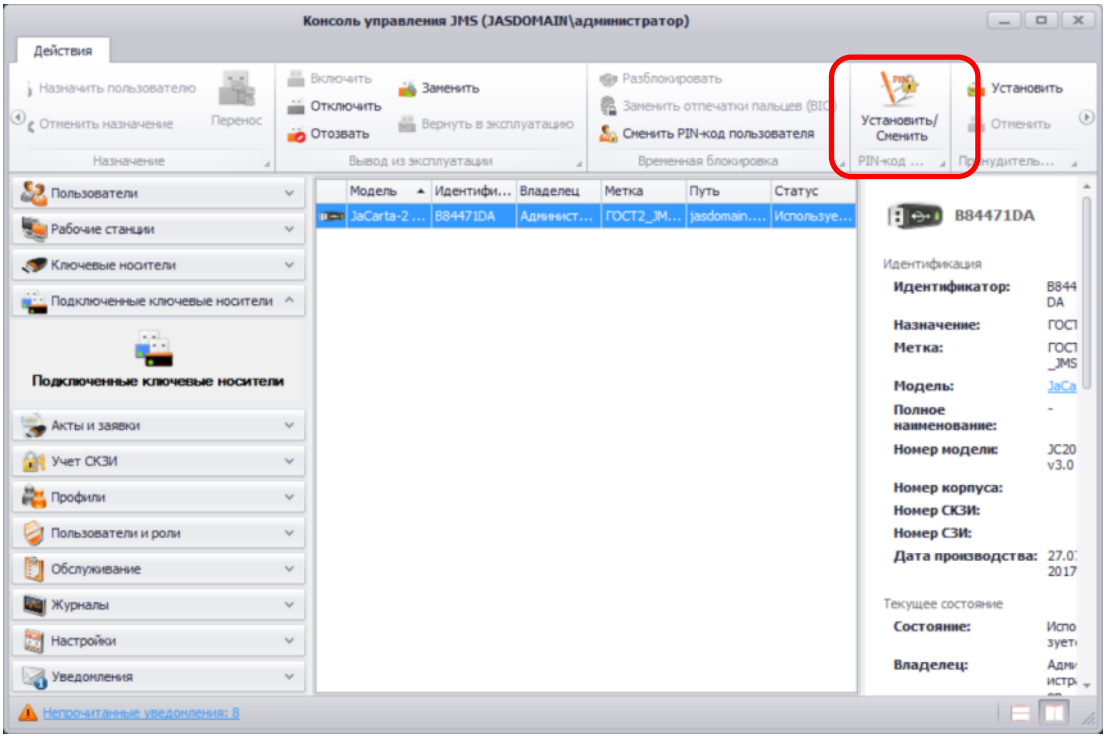


Рис. 97 – Установка/смена PIN-кода подписи в электронном ключе

3. В случае если на электронном ключе установлено несколько приложений, то выберите необходимое приложение, в противном случае переходите к следующему шагу.
4. В отобразившемся окне (Рис. 98) введите **Текущий PIN-код пользователя**, устанавливаемый PIN-код ЭП (**Новый PIN-код**) и его подтверждение (**Подтверждение PIN-кода**) и нажмите **OK**.

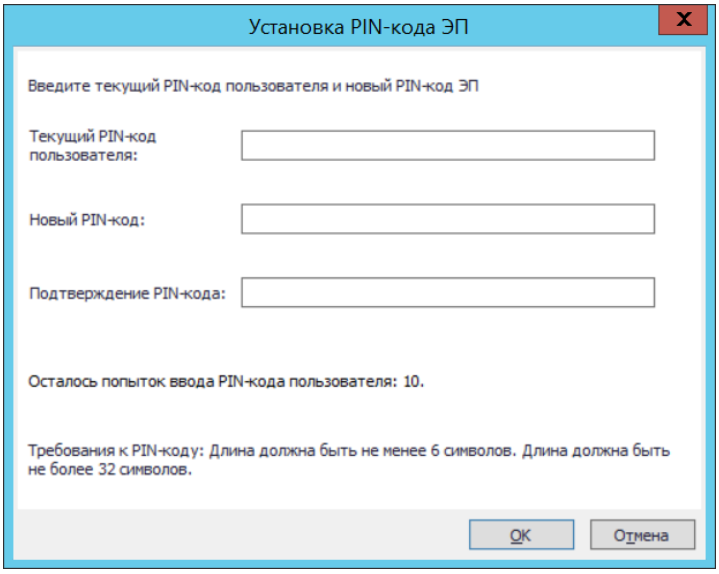


Рис. 98 – Окно установки PIN-кода подписи

5. Нажмите **OK** в окне подтверждения успешной установки PIN-кода подписи (Рис. 99).

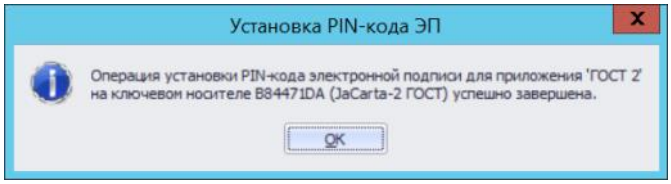


Рис. 99 – Окно подтверждения успешной установки PIN-кода подписи

Для смены PIN-кода подписи в электронном ключе повторите шаги 1—2. В отобразившемся окне (Рис. 100) введите **Текущий PIN-код пользователя**, ранее установленный PIN-код подписи (**Текущий PIN-код ЭП**), новый PIN-код подписи (**Новый PIN-код**) и его подтверждение (**Подтверждение PIN-кода**) и нажмите **OK**.

Рис. 100 – Окно смены PIN-кода подписи

Для завершения операции нажмите **OK** в окне подтверждения успешной смены PIN-кода подписи.

3.6.18.3 Разблокировка PIN-кодов в JaCarta-2 ГОСТ с использованием PUK-кода

Важно! Для разблокировки PIN-кодов в JaCarta-2 ГОСТ с использованием PUK-кода последний должен быть установлен в электронном ключе при его производстве или с помощью специализированного АРМ (см. документацию электронного ключа JaCarta-2 ГОСТ).

Порядок разблокирования PIN-кодов в электронных ключах JaCarta-2 ГОСТ в целом соответствует стандартной последовательности действий (см. «Разблокировка подсоединенного электронного ключа», с. 96), однако существуют следующие особенности.

В процессе разблокировки PIN-кода пользователя, PIN-кода подписи (ЭП) или обоих PIN-кодов в консоли управления JMS отобразится окно следующего вида:

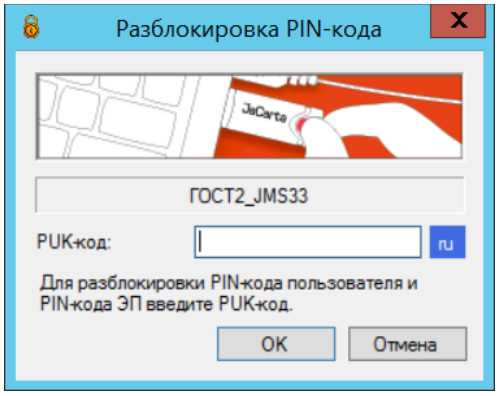


Рис. 101 – Пример окна разблокировки PIN-кодов в JaCarta-2 ГОСТ

Для разблокировки PIN-кодов введите **PUK-код** и нажмите **OK**. В случае успешного разблокирования PIN-кодов отобразится окно следующего вида:

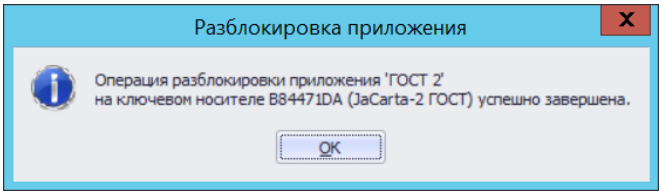


Рис. 102 – Сообщение о разблокировке PIN-кодов в JaCarta-2 ГОСТ

Примечание. Для предоставления права на разблокировку по PUK-коду предварительно следует выполнить действия, описанные в разделе «Предоставление права на разблокировку», с. 96.

3.6.19 Привязка электронных ключей 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, 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:
   - **Ключевые носители**, после чего в правой панели 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.
3. В верхней панели нажмите **Перенос** (см. изображение ниже).

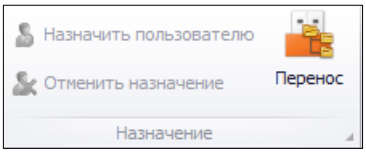


Рис. 103 – Перенос привязки электронного ключа

4. Если вы отметили более одного электронного ключа, отобразится следующее окно. (В противном Случае переходите к шагу 6 настоящей процедуры.)

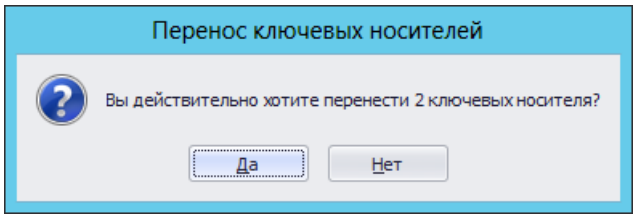


Рис. 104 – Предупреждение об изменении привязки нескольких электронных ключей

5. Нажмите **Да**, чтобы подтвердить действие.
Отобразится следующее окно.

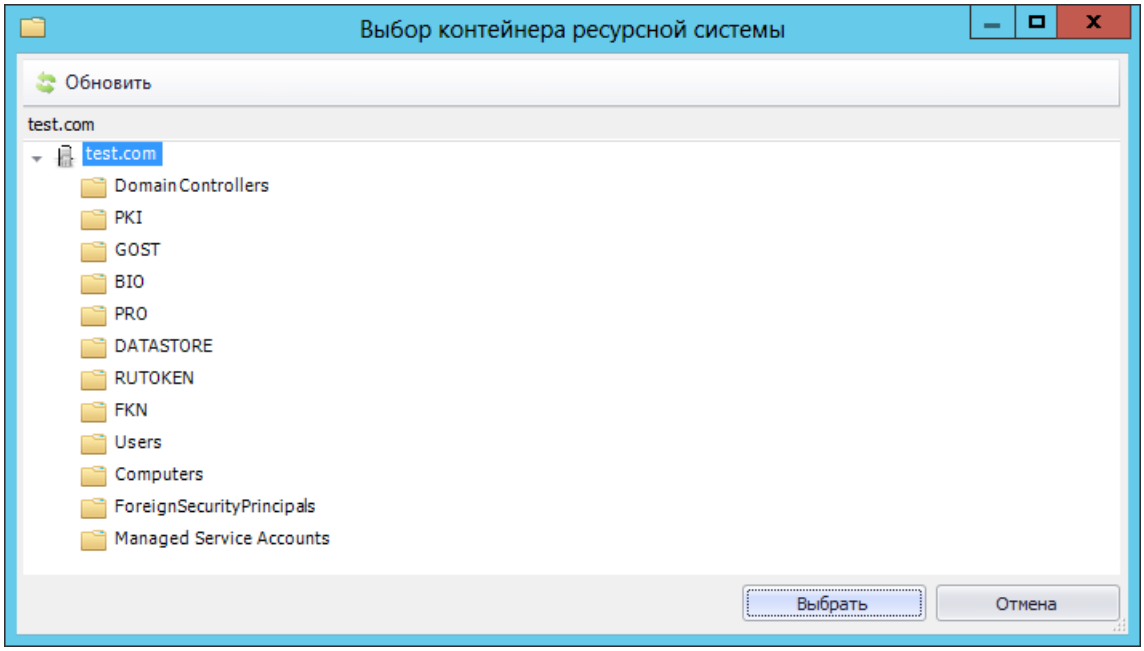


Рис. 105 – Выбор контейнера ресурсной системы для привязки

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

3.6.20 Установка в БД PIN-кода администратора для приложения электронного ключа

JMS позволяет осуществлять установку в базе данных JMS текущего PIN-кода администратора для конкретного приложения электронного ключа.

Если по какой-то причине PIN-код администратора в БД JMS не совпадает с PIN-кодом администратора на электронном ключе, то PIN-код администратора можно поменять.

Например:

- если электронный ключ выпускался без инициализации и в БД JMS нет данных о его PIN-коде администратора, то не будет работать удаленная разблокировка PIN-кода пользователя;

- если электронный ключ проинициализирован без помощи JMS и PIN-код администратора в БД JMS не совпадает с текущим PIN-кодом электронного ключа, то в JMS нет больше возможности этот токен выпускать.

Чтобы установить в базе данных JMS текущий административный PIN-код для конкретного приложения электронного ключа выполните следующие действия:

1. Подсоедините электронный ключ к компьютеру. Электронный ключ должен быть зарегистрирован в БД JMS, в противном случае, необходимо пройти процедуру регистрации (подробнее см. Регистрация подсоединенных электронных ключей в JMS).
2. Запустите приложение Консоль управления JMS.
3. Нажмите **Подключенные устройства** -> **Ключевые носители** и выберите электронный ключ, на котором необходимо установить PIN-код администратора.
4. В верхней панели справа нажмите на значке и нажмите на значке **Установить** (см. Рис. 106).

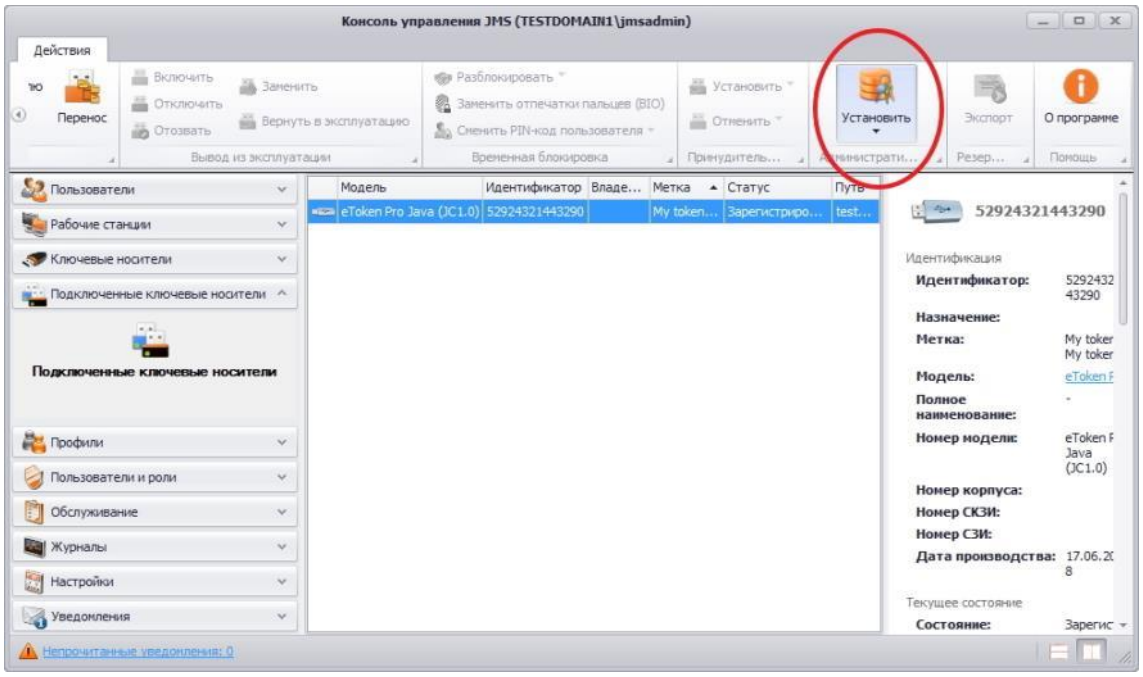


Рис. 106 – Установка PIN-кода администратора

Если приложений несколько, то выберите требуемое приложение (см. рис. 107).

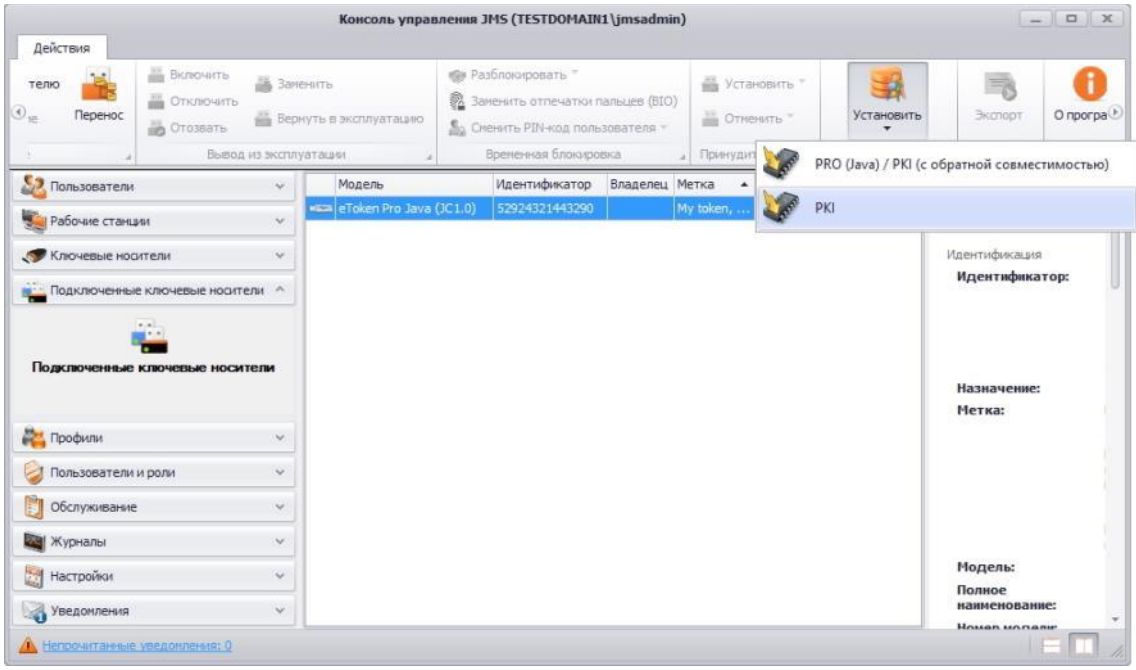


Рис. 107 – Выбор требуемого приложения для установки PIN-кода

5. В появившемся окне (см. рис. 108) введите текущий PIN-код администратора и его подтверждение, после чего нажмите **OK**.

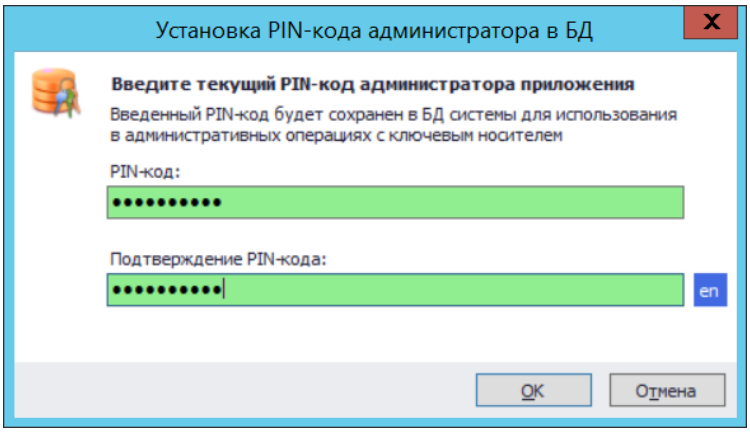


Рис. 108 – Ввод PIN-кода администратора для приложения и его подтверждение

6. В появившемся окне (см. рис. 110) нажмите **Да**.

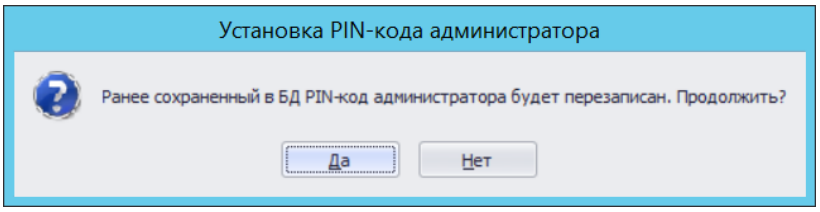


Рис. 109 – Запрос на завершение перезаписи PIN-кода администратора в БД

7. Для завершения операции нажмите **OK**.

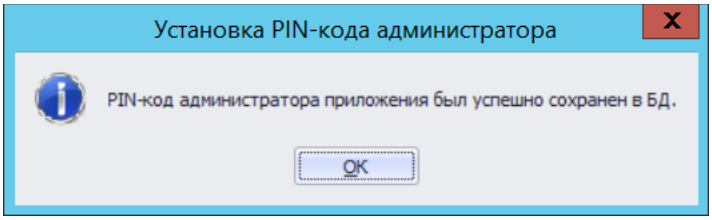


Рис. 110 – Окно успешного сохранения PIN-кода администратора в БД

3.6.21 Экспорт резервных копий объектов, выпущенных на электронный ключ

JMS позволяет выполнить экспорт резервных копий закрытых ключей и соответствующих им сертификатов, выпущенных на электронные ключи, в виде контейнера PFX. Экспортировать можно не только действующие закрытые ключи и сертификаты, но также закрытые ключи и сертификаты, ранее удаленные с электронных ключей. Такая возможность предусмотрена для закрытых ключей и сертификатов, которые были выпущены с помощью центра сертификации Microsoft, КриптоПро УЦ 1.5/2.0.

Чтобы экспорт был возможен, должны быть соблюдены следующие условия.

1. В профиле выпуска сертификатов в JMS должна быть включена возможность экспорта резервных копий объектов, выпущенных на электронные ключи. Подробнее см.:
   - «Настройки профиля выпуска сертификатов в центре сертификации Microsoft», с. 209;
   - «Настройка профиля для выпуска сертификатов в КриптоПро УЦ 1.5», с. 620;
   - «Настройка профиля для выпуска сертификатов в КриптоПро УЦ 2.0», с. 648.
2. Администратор JMS, который будет осуществлять экспорт, должен быть добавлен в роль JMS, содержащую операцию **Ключевые носители -> Выпуск с восстановлением объектов**.

⚠ Ни одна из встроенных ролей JMS не содержит такую операцию, также, встроенные роли JMS невозможно изменить, поэтому соответствующую роль необходимо создать вручную. Подробнее см. «Создание, редактирование и назначение ролей JMS», с. 389.

Чтобы выполнить экспорт резервной копии объектов, выпущенных на электронный ключ, выполните следующие действия.

1. В зависимости от раздела консоли управления JMS , из которого вы хотите начать процедуру, выполните следующие действия.

Пользователи	**Ключевые носители**	**Подключенные устройства -> Ключевые носители**
1.1. Перейдите в раздел **Пользователи** и в левой части интерфейса выберите нужный контейнер, содержащий владельцев электронных ключей. 1.2. В верхней панели выберите вкладку **Действия над контейнером** и нажмите **Экспорт**.	1.1. В левой панели выберите нужный контейнер, содержащий электронные ключи. 1.2. В верхней панели выберите вкладку **Действия**. 1.3. В центральной части выберите электронный ключ, объекты которого нужно экспортировать. 1.4. В верхней панели нажмите **Экспорт**.	1.1. Перейдите в раздел **Подключенные устройства -> Ключевые носители**. 1.2. В центральной части окна выберите нужный ключевой носитель. 1.3. В верхней панели нажмите **Экспорт**.

Отобразится следующее окно.

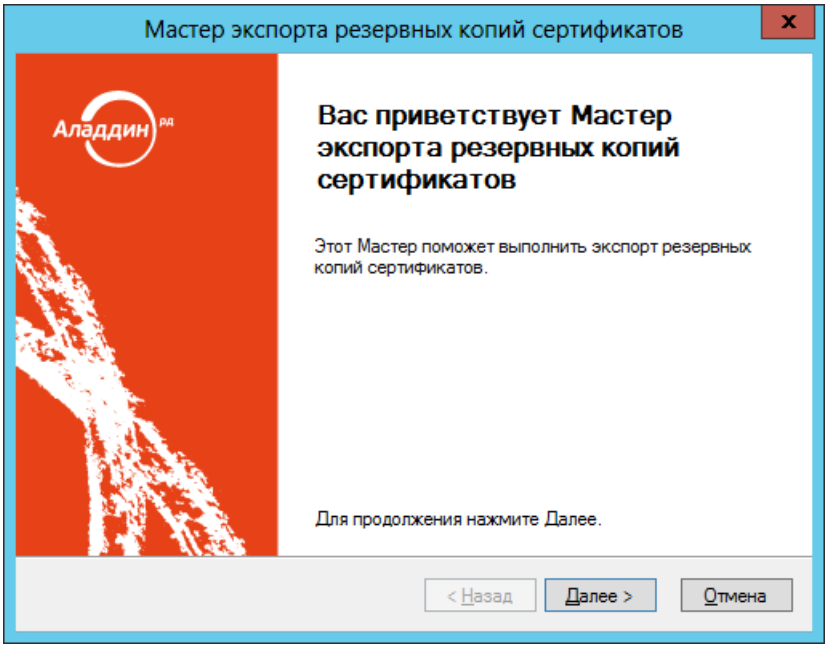


Рис. 111 – Окно приветствия мастера экспорта резервных копий сертификатов

2. Нажмите **Далее**.
3. В зависимости от того, из какого раздела JMS вы запустили процедуру экспорта, выполните следующие действия:

   – **Пользователи** – переходите к следующему шагу процедуры;
   – **Ключевые носители** или **Подключенные устройства** -> **Ключевые носители** – переходите к шагу 6 настоящей процедуры.

   Отобразится следующее окно.

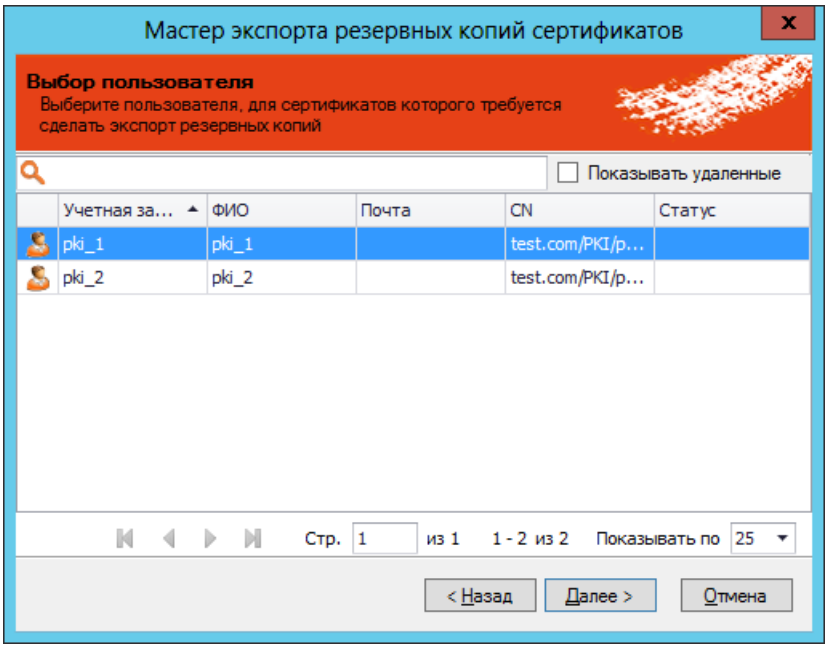


Рис. 112 – Выбор пользователя

4. Выберите пользователя, которому принадлежит электронный ключ, объекты которого вы хотите экспортировать, и нажмите **Далее**. (Вы также можете установить флаг **Показывать удаленные** – в этом случае в окне отобразятся удаленные пользователи.)
Отобразится следующее окно.

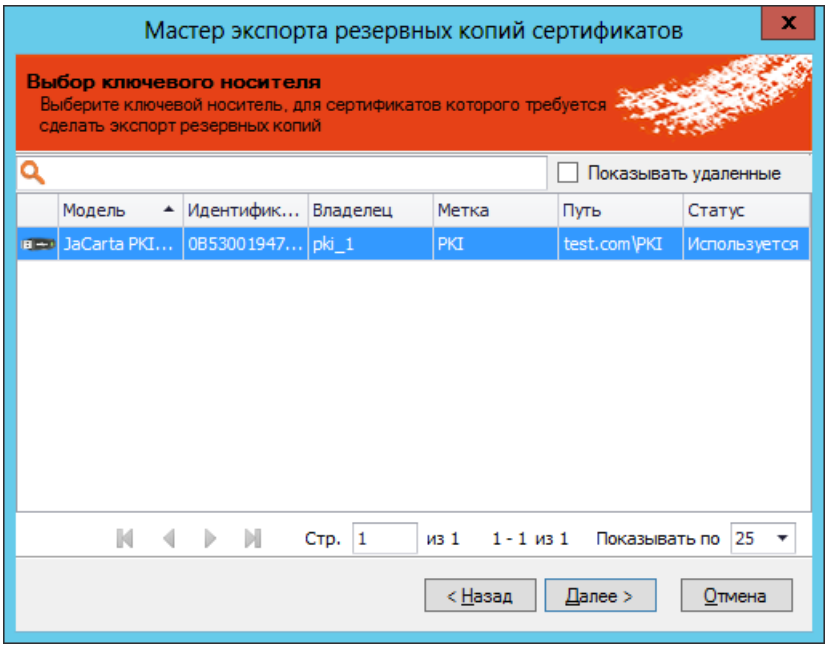


Рис. 113 – Список электронных ключей выбранного пользователя

5. Выберите электронный ключ, объекты которого нужно экспортировать, и нажмите **Далее**. (Вы также можете установить флаг **Показывать удаленные** – в этом случае в окне отобразятся удаленные электронные ключи.)
Отобразится следующее окно.

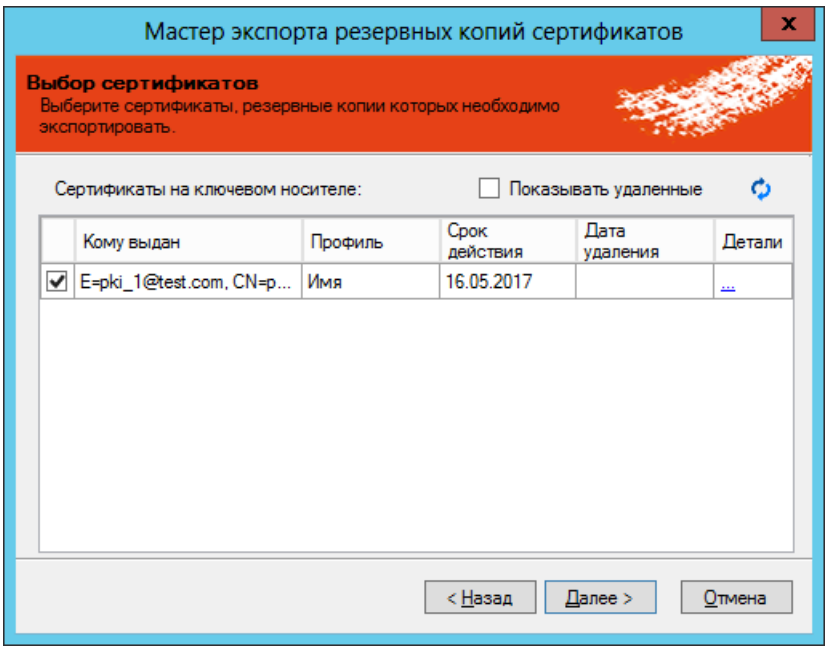


Рис. 114 – Выбор экспортируемых объектов

6. Отметьте сертификаты (объекты), которые нужно экспортировать, после чего нажмите **Далее**. (вы также можете установить флаг **Показывать удаленные** – в этом случае в окне отобразятся удаленные объекты.)
   Отобразится следующее окно.

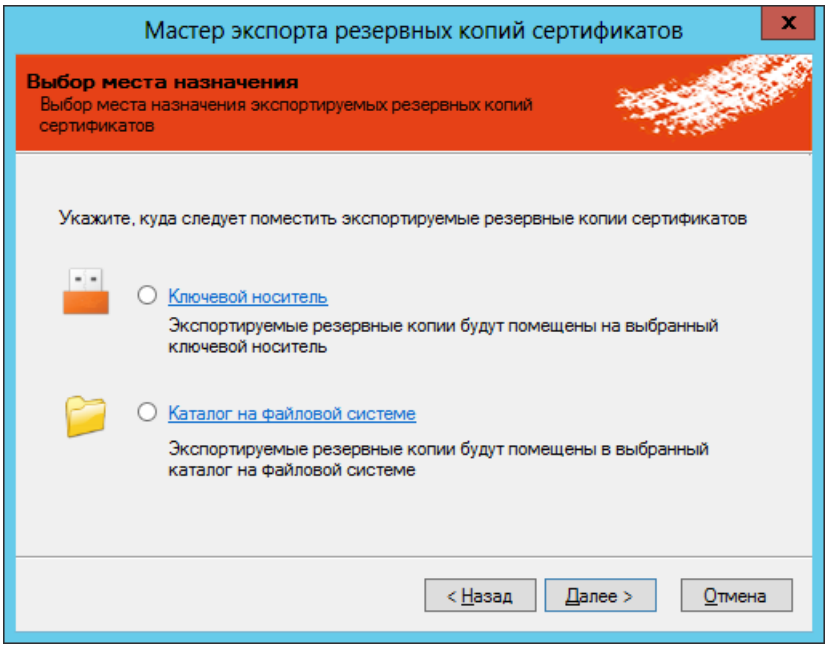


Рис. 115 – Выбора варианта экспорта

7. Выберите один из двух вариантов:

   - **Ключевой носитель** – объект будет экспортирован на другой электронный ключ;
   - **Каталог на файловой системе** – объект будет экспортирован в каталог в файловой системе.

В настоящем документе процедура экспорта описана на примере экспорта в каталог в файловой системе.

Если вы экспортируете объект, который был выпущен на электронный ключ с помощью КриптоПро УЦ 1.5/2.0, то следует выбирать экспорт на электронный ключ. В противном случае в дальнейшем вы не сможете воспользоваться экспортированным объектом.

Отобразится следующее окно.

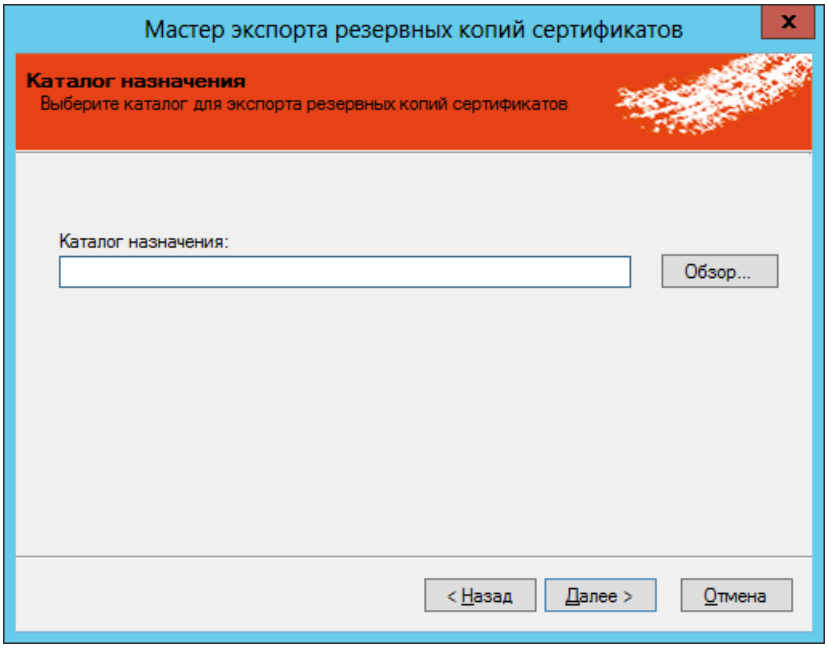


Рис. 116 – Выбора каталога назначения

8. Воспользуйтесь кнопкой обзор, чтобы указать каталог, в который будет сохранена резервная копия экспортируемого объекта, после чего нажмите **Далее**.
   Отобразится следующее окно.

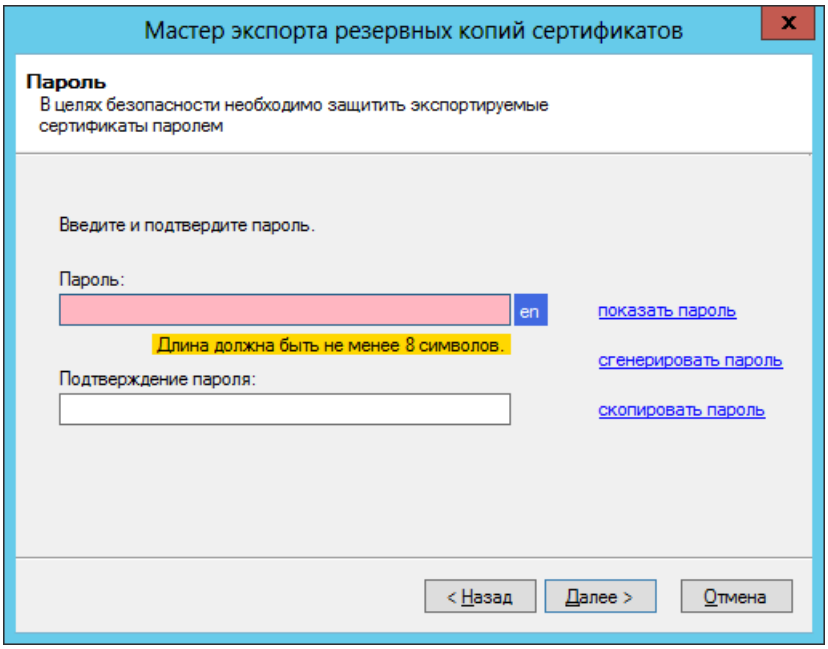


Рис. 117 – Задание пароля для защиты экспортируемого объекта

9. В полях **Пароль** и **Подтверждение** пароля введите пароль для защиты экспортируемого объекта и введите подтверждение соответственно.
10. При необходимости воспользуйтесь ссылками:

- **показать пароль** – отображает заданный пароль;
- **сгенерировать пароль** – генерирует случайный пароль;
- **скопировать пароль** – копирует пароль в буфер.

11. Нажмите **Далее**.
Отобразится следующее окно.

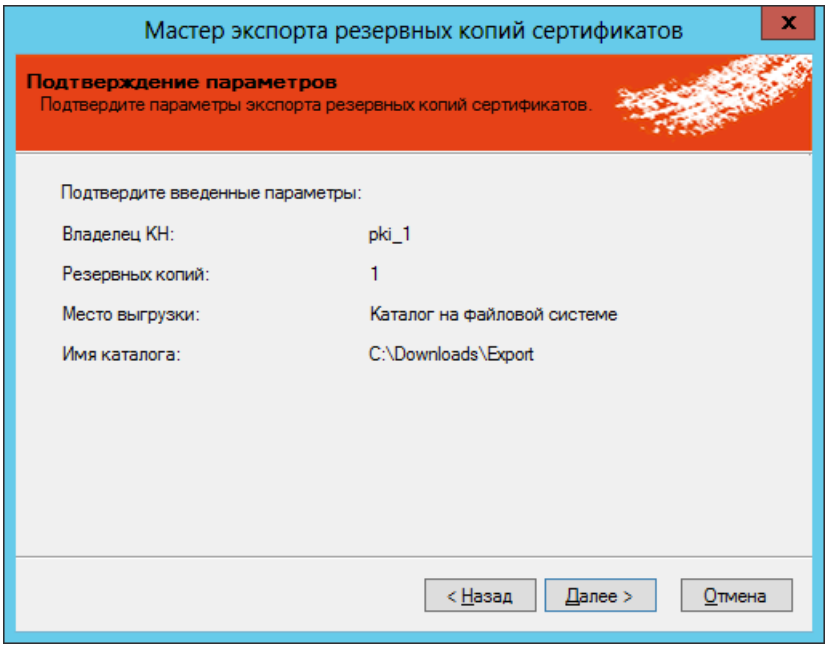


Рис. 118 – Подготовка к экспорту

12. Нажмите **Далее**.
Отобразится следующее окно.

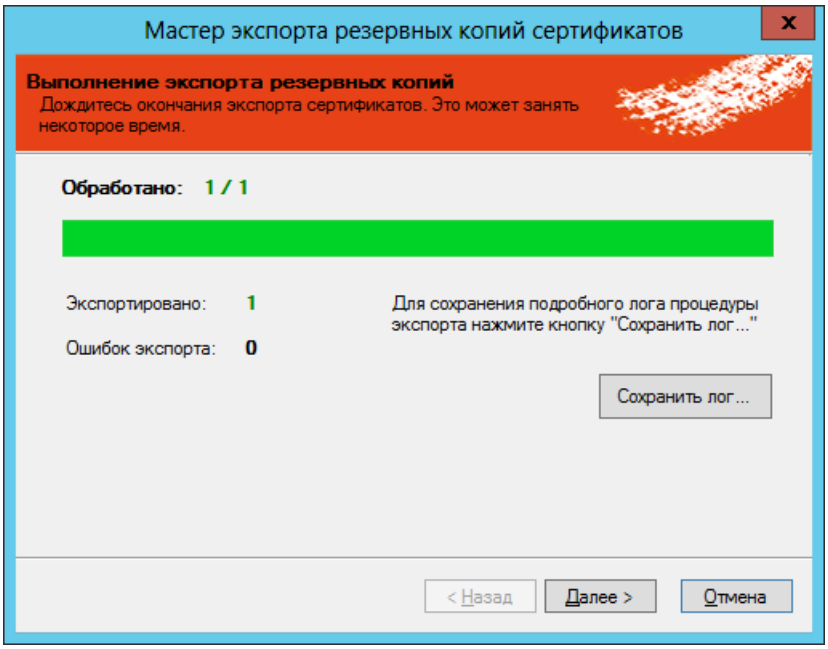


Рис. 119 – Экспорт резервных копий объектов

13. Нажмите **Далее**.

Отобразится следующее окно.

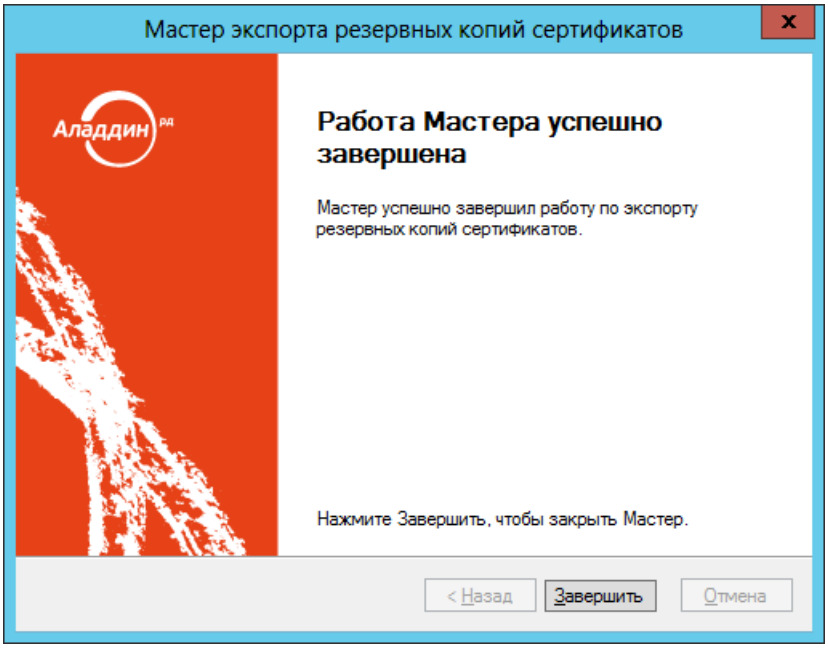


Рис. 120 – Окно завершения работы мастера экспорта объектов

14. Нажмите **Завершить** для завершения процедуры.

3.6.22 Виртуальный электронный ключ «Хранилище пользователя»

JMS поддерживает специальный вид объектов – «виртуальный электронный ключ», представляющий собой способ выпуска или взятия под управления и последующей синхронизации сертификата пользователя в хранилище сертификатов на рабочей станции и связанного с этим сертификатом закрытого ключа.

Выпуск такого «виртуального электронного ключа» происходит в результате выпуска сертификата в хранилище пользователя (см. «Выпуск сертификата в хранилище пользователя», с. 308), либо в результате взятия под управление ранее выпущенного сертификата пользователя (см. «Взятие под управление электронных ключей», с. 458).

После выпуска «виртуальный электронный ключ» отображается в консоли JMS как модель **Хранилище пользователя** с идентификатором, составленным из имени рабочей станции и имени пользователя в формате `<Имя_рабочей_станции>_<Имя_пользователя>`, например *Workstartion_User* (см. Рис. 121).

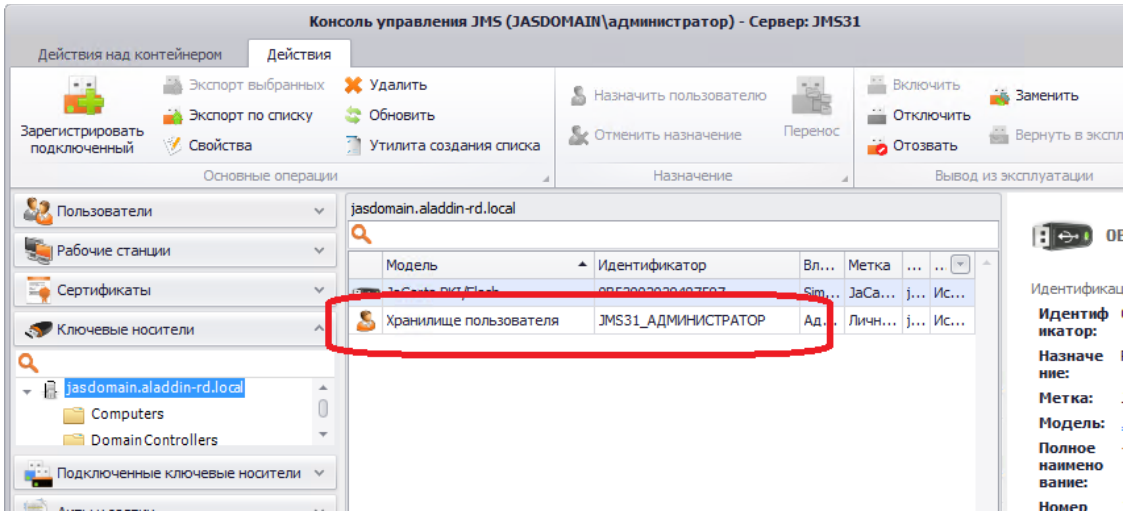


Рис. 121 – Отображение «виртуального электронного ключа» в консоли управления JMS

3.6.23 Виртуальный электронный ключ «Хранилище сервера КриптоПро DSS»

Виртуальный электронный ключ «Хранилище сервера КриптоПро DSS», представляет собой способ выпуска (или взятия под управления и последующей синхронизации) сертификата пользователя в хранилище на сервере КриптоПро DSS и связанного с этим сертификатом закрытого ключа.

Выпуск такого виртуального электронного ключа происходит в результате выпуска сертификата в хранилище КриптоПро DSS (см. «Выпуск сертификата в хранилище сервера КриптоПро DSS», с. 309), либо в результате взятия под управление ранее выпущенного сертификата пользователя в хранилище КриптоПро DSS (выполняется при взятии под управление пользователей КриптоПро DSS, см. «Взятие под управление пользователей КриптоПро DSS», с. 459, и «Взятие под управление электронных ключей», с. 458).

После выпуска «виртуальный электронный ключ» отображается в консоли JMS как модель **Хранилище сервера КриптоПро DSS** (см. Рис. 122).

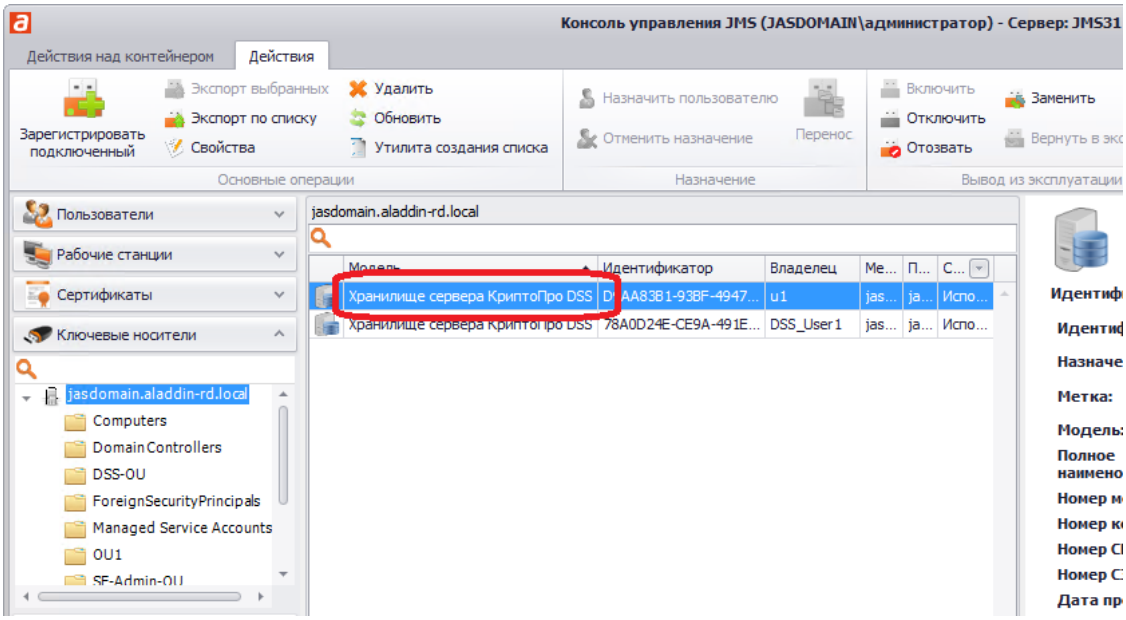


Рис. 122 – Отображение «виртуального электронного ключа» ***Хранилище сервера КриптоПро DSS***

3.7 Операции с OTP- и U2F-аутентификаторами

Операции, связанные с управлением жизненным циклом OTP- и U2F-аутентификаторов осуществляются в разделе **OTP- и U2F-аутентификаторы** (Рис. 123) 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]).

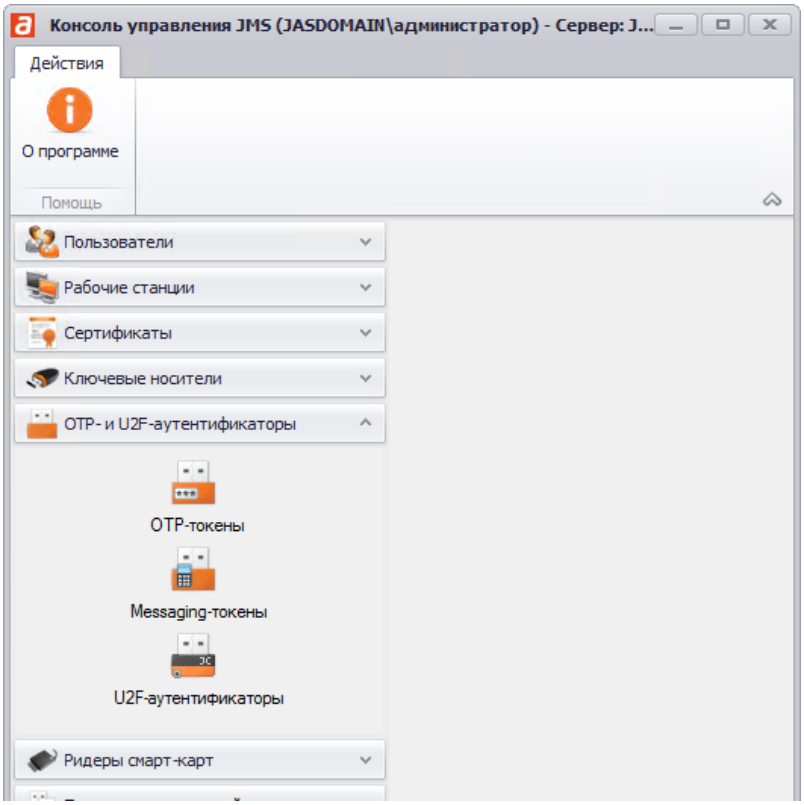


*Рис. 123 – Общий вид раздела **OTP- и U2F-аутентификаторы** консоли управления JMS*

В табл. 7 (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. 7 – 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. 122	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. 127	Да (Email)	мобильное приложение Aladdin 2FA компании Аладдин
OTP- и U2F-аутентификаторы -> OTP-токены	«Установка и изменение PIN-кода для OTP», с. 128	Да (Email)	• eToken PASS; • eToken NG OTP; • eToken NG OTP (Java); • JC-WebPass; • Другие OTP-токены, реализующие спецификации RFC 4226 и 6238 • мобильное приложение Aladdin 2FA компании Аладдин
OTP- и U2F-аутентификаторы -> OTP-токены	«Включение и отключение OTP-токена», с. 129	Нет	
OTP- и U2F-аутентификаторы -> OTP-токены	«Синхронизация значений OTP», с. 130		
OTP- и U2F-аутентификаторы -> OTP-токены	«Просмотр и редактирование свойств OTP-токена», с. 132		
OTP- и U2F-аутентификаторы -> OTP-токены	«Удаление сведений об OTP-токене», с. 135		
OTP- и U2F-аутентификаторы -> Messaging-токены	«Управление PIN-кодом для Messaging-токена», с. 137	Да (SMS)	Messaging-токен
OTP- и U2F-аутентификаторы -> Messaging-токены	«Включение и отключение Messaging-токена», с. 137	Нет	
OTP- и U2F-аутентификаторы -> Messaging-токены	«Просмотр свойств Messaging-токена», с. 137	Нет	
OTP- и U2F-аутентификаторы -> Messaging-токены	«Удаление сведений о Messaging-токене», с. 140	Нет	
OTP- и U2F-аутентификаторы -> U2F-аутентификаторы	«Включение и отключение U2F-аутентификатора», с. 141	Нет	U2F-аутентификатор
OTP- и U2F-аутентификаторы -> U2F-аутентификаторы	« Просмотр и редактирование свойств U2F-аутентификатора», с. 141		
OTP- и U2F-аутентификаторы -> U2F-аутентификаторы	«Удаление сведений о U2F-аутентификаторе», с. 143		

3.7.1 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. 310.

3.7.1.1 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. 675).

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. 124).

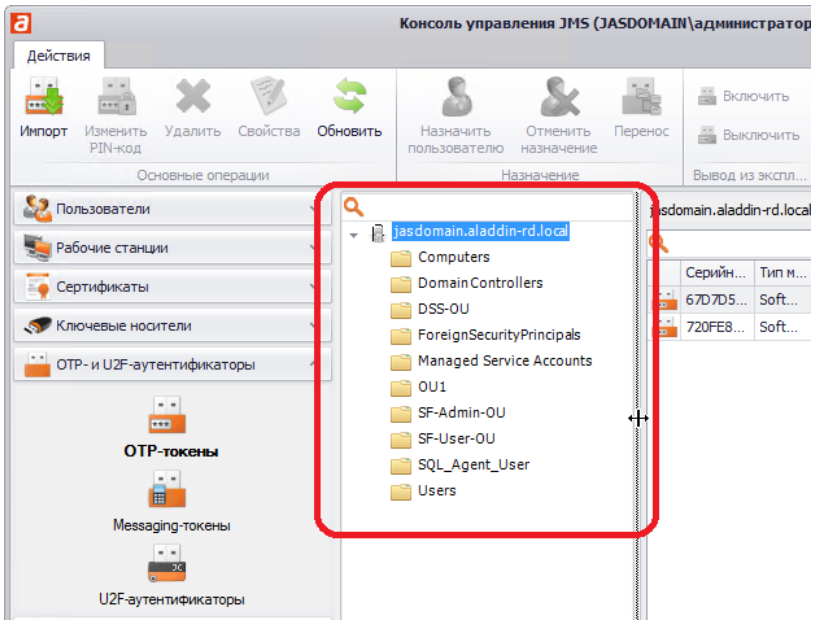


Рис. 124 – Выбор контейнера для привязки импортируемых OTP-токенов

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

Отобразится следующее окно.

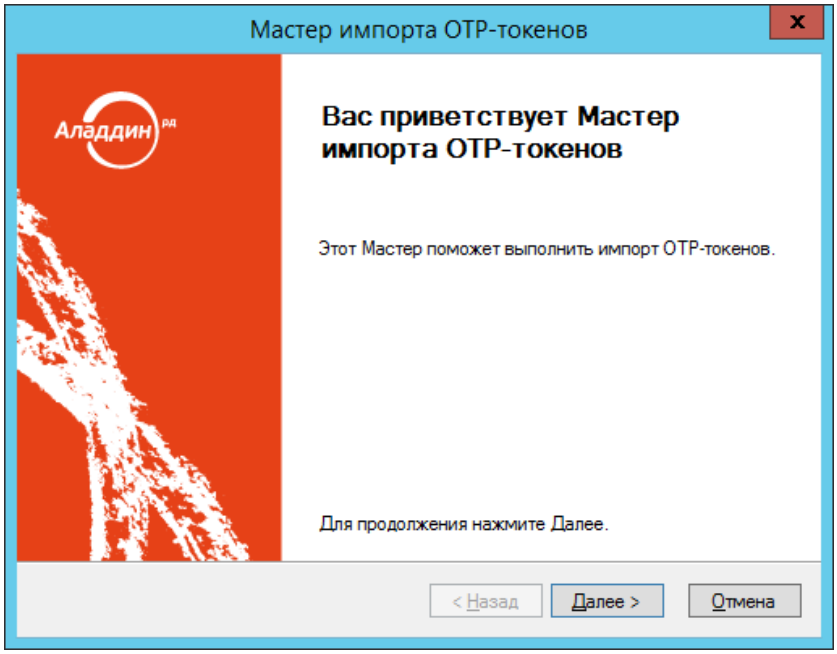


Рис. 125 – Окно приветствия мастера импорта ключевых носителей

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

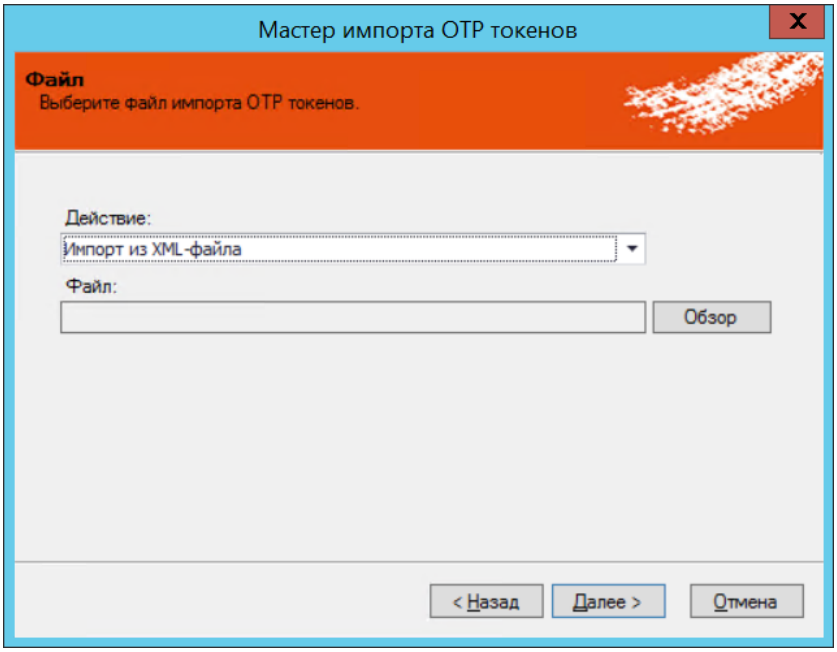


Рис. 126 – Указание пути к инвентарному файлу

5. Воспользуйтесь кнопкой **Обзор**, чтобы указать путь к инвентарному файлу, после чего нажмите **Далее**.

По завершении импорта отобразится следующее окно.

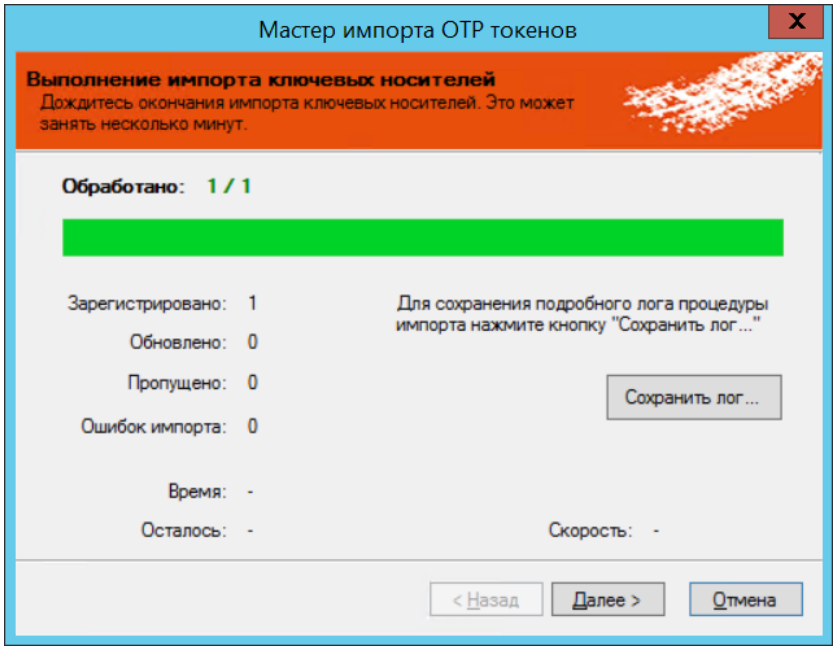


Рис. 127 – Импорт завершён

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

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

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

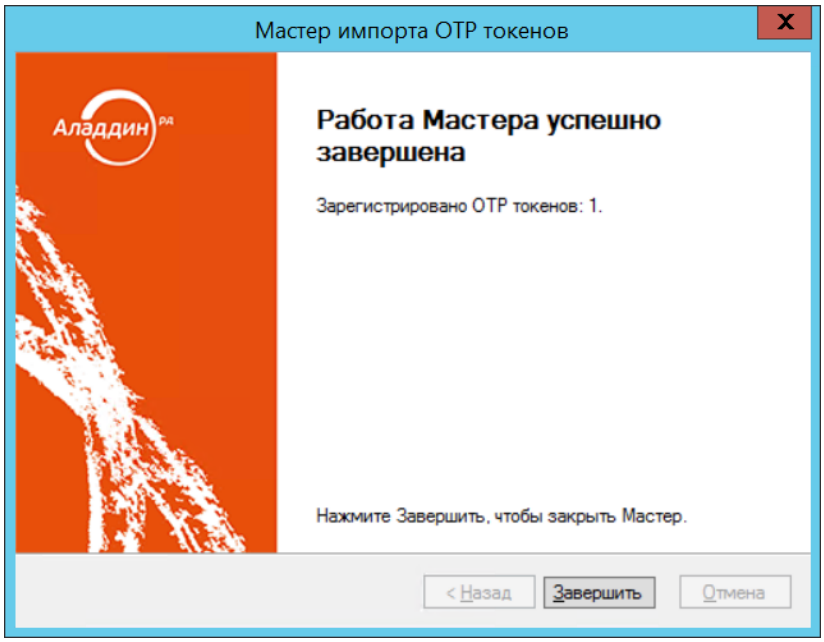


Рис. 128 – Окно завершения процедуры импорта

8. Нажмите **Завершить**.

Сведения об импортированных OTP-токенах отобразятся в центральной части окна консоли управления JMS (рис. 129). После регистрации токены имеют статус *Зарегистрирован*.

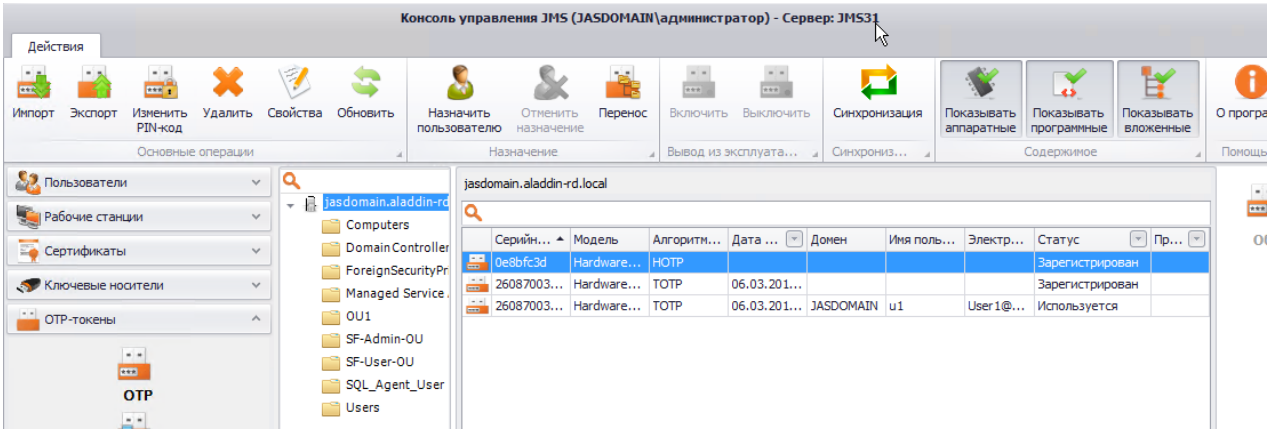


Рис. 129 – Сведения об импортированных OTP-токенах в консоли управления JMS

3.7.1.2 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. 122).

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 **Назначить пользователю** на верхней панели. Отобразится окно следующего вида.

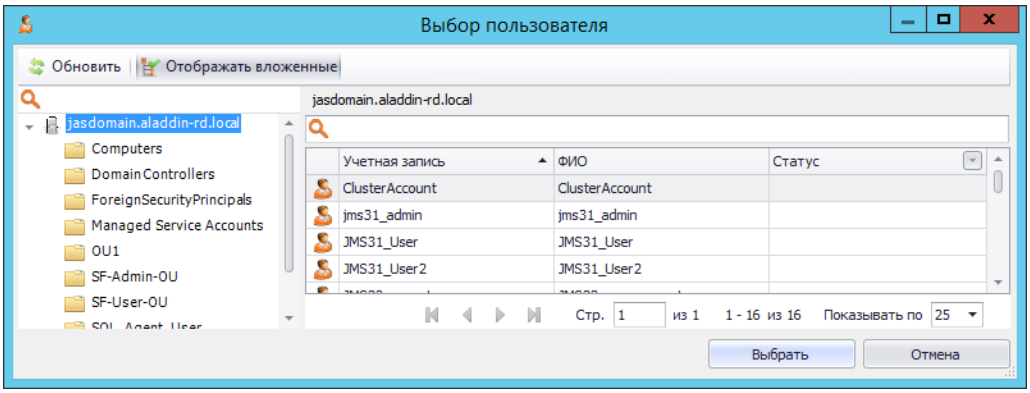


Рис. 130 – Окно выбора пользователя для назначения

2. В центральной части окна выберите пользователя и нажмите **Выбрать**.
3. В окне подтверждения нажмите **Ок**.

В результате OTP-токен меняет статус с *Зарегистрирован* на *Назначен*.

Для отмены назначения токена пользователю выполните следующие действия.

1. В верхней панели нажмите **Отменить назначение**. При этом будет отображено окно с контейнерами ресурсной системы (Рис. 131).

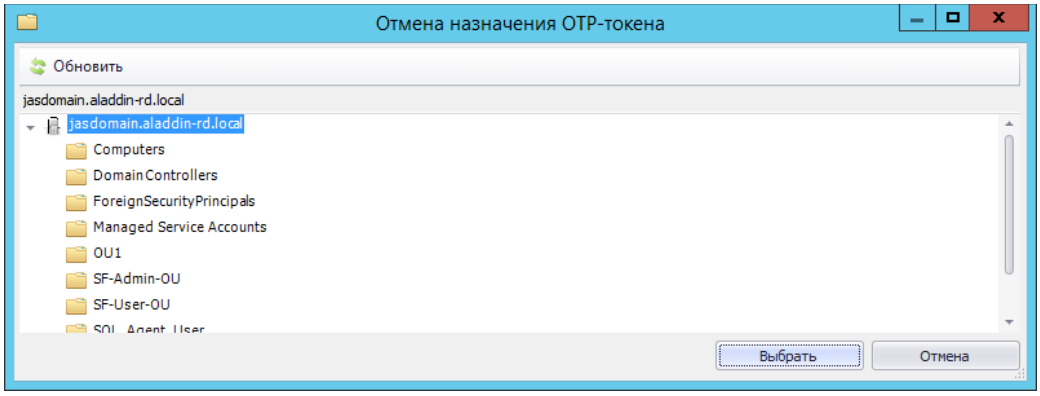


Рис. 131 – Окно выбора контейнера для привязки токена при отмене его назначения пользователю

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

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

3.7.1.3 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. 122.
2. Выполните назначение аппаратных OTP-токенов пользователям, руководствуясь разделом «Назначение / отмена назначения аппаратного OTP-токена», с. 125.
3. Создайте профиль выпуска аппаратных OTP-токенов, руководствуясь разделом «Настройка профиля выпуска аппаратных OTP-токенов», с. 254.
4. Настройте для выпуска аппаратных OTP-токенов и запустите на выполнение соответствующий план обслуживания, руководствуясь разделами «План обслуживания жизненного цикла OTP-токенов», с. 410 и «Запуск и просмотр результатов планов обслуживания из Консоли управления JMS», с.405.
5. Выпущенные и готовые к использованию (статус *Используется*) экземпляры аппаратных OTP-токенов отобразятся в консоли управления JMS со значением *HardwareOTP* в поле **Модель** (Рис. 132).

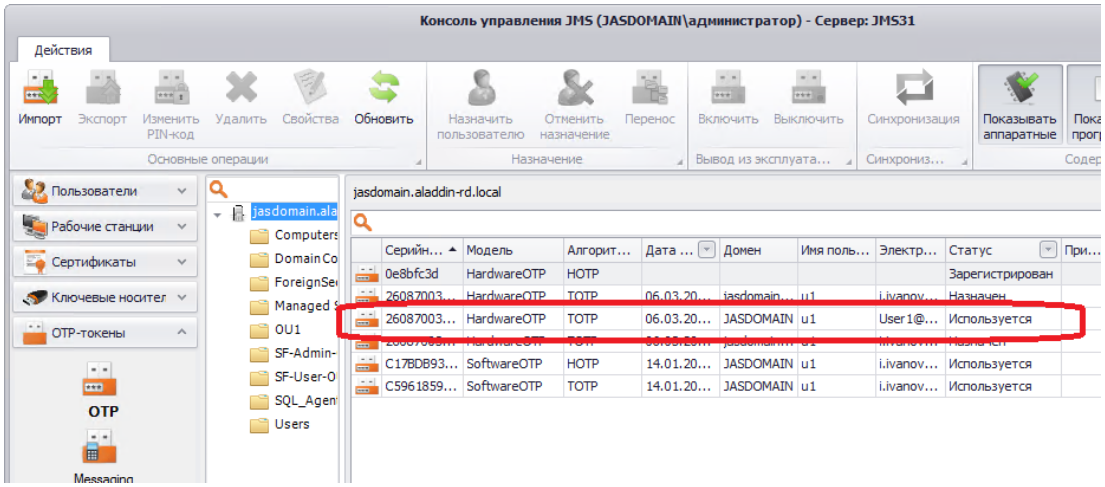


Рис. 132 – Отображение выпущенного экземпляра аппаратного OTP-токена

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 Active Directory должен быть настроен адрес электронной почты.
2. В серверном агенте JMS (приложение *Сервер JMS*) должен быть настроен транспортный сервис SMTP (вкладка **Настройка -> Настройка транспорта -> Настройка SMTP**). Подробнее см. руководство по установке и настройке JMS [2].

3.7.1.4 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 Active Directory должен быть настроен адрес электронной почты.
2. В серверном агенте JMS (приложение *Сервер JMS*) должен быть настроен транспортный почтовый сервис (вкладка **Настройка -> Настройка транспорта -> Настройка SMTP**). Подробнее см. руководство по установке и настройке JMS [2].

Чтобы выпустить для группы пользователей JMS программные OTP-токены, такие как Aladdin 2FA компании Аладдин (или аналогичные мобильные приложения других поставщиков), выполните следующие действия.

1. Создайте профиль выпуска программных OTP-токенов, руководствуясь разделом «Настройка профиля выпуска программных OTP-токенов», с. 262.
2. Настройте для выпуска программных OTP-токенов и запустите на выполнение соответствующий план обслуживания, руководствуясь разделами «План обслуживания жизненного цикла OTP-токенов», с. 410 и «Запуск и просмотр результатов планов обслуживания из Консоли управления JMS», с.405.
3. Выпущенные и готовые к использованию (статус *Используется*) экземпляры программных OTP-токенов отобразятся в консоли управления JMS со значением *SoftwareOTP* в поле **Модель (**Рис. 133**)**.

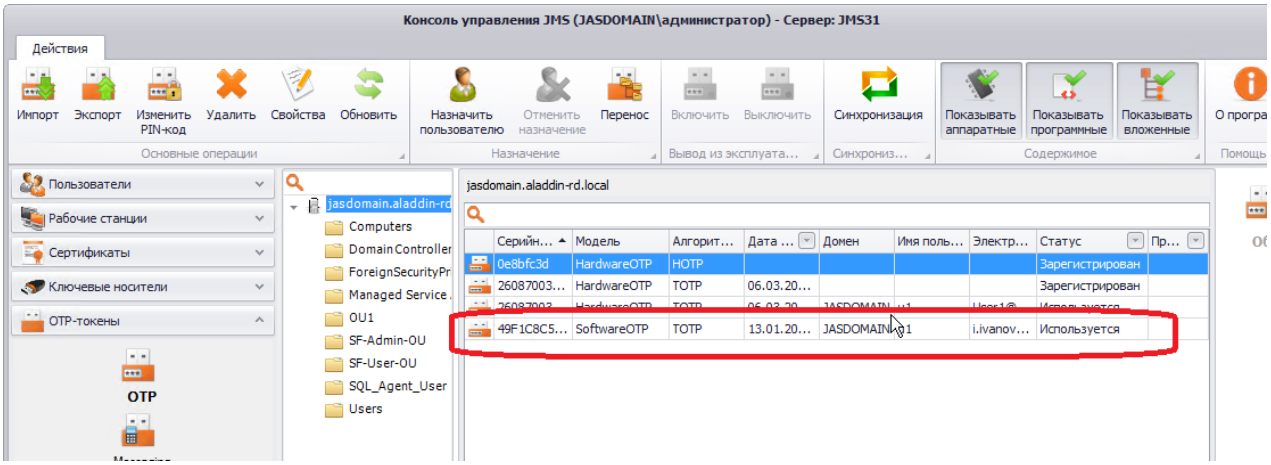


Рис. 133 – Отображение выпущенного экземпляра программного OTP-токена

4. Пользователи, для которых были выпущены токены получат на свой электронный адрес сообщение, содержащее PIN-код для OTP и QR-код (Рис. 134).

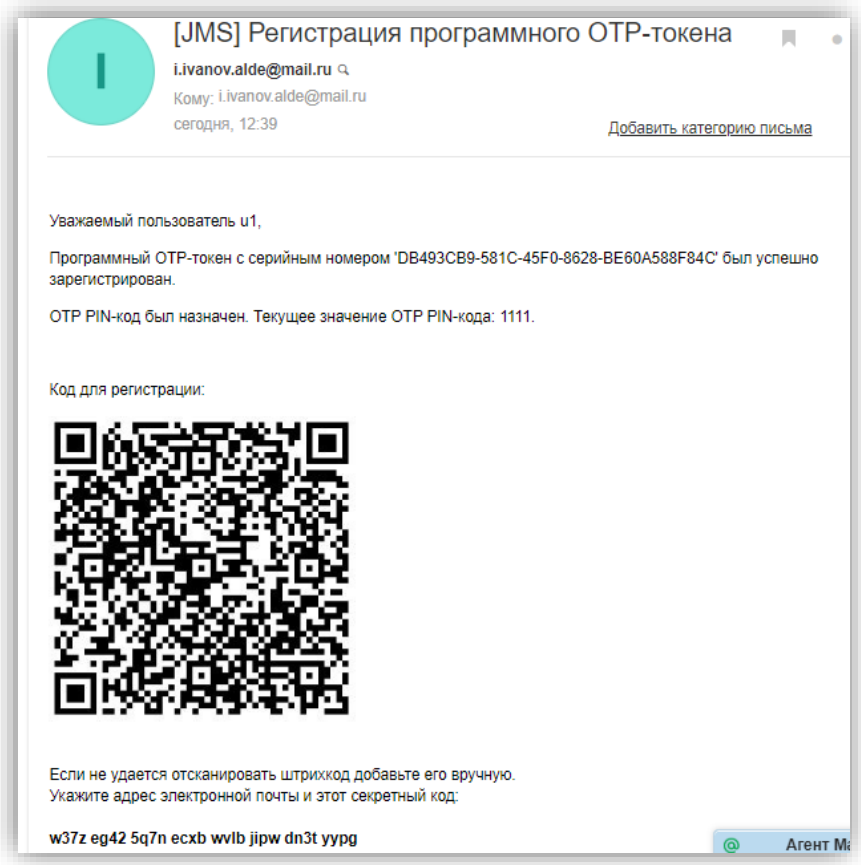


Рис. 134 - сообщение, содержащее PIN-код для OTP и QR-код

15. 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.

3.7.1.5 Установка и изменение PIN-кода для OTP

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

1. В консоли управления JMS отметьте токен, PIN-код для OTP которого вы хотите изменить.
2. В верхней панели выберите **Изменить PIN-код**.

Отобразится следующее окно.

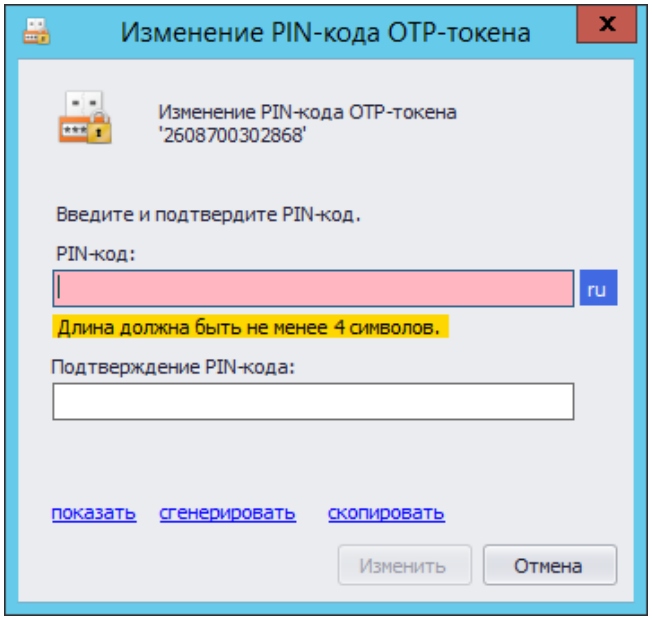


Рис. 135 – Установка или изменение PIN-кода для OTP

3. Выполните необходимые действия, руководствуясь табл. 8 ниже.

Табл. 8 – Параметры установки или изменения PIN-кода для OTP

Настройка	Описание
PIN-код	Введите значение нового PIN-кода для OTP
Подтверждение PIN-кода	Введите подтверждение PIN-кода для OTP
Показать	Отображает содержимое поля **PIN-код**, при этом поле **Подтверждение PIN-кода** становится неактивным
Сгенерировать	Генерирует случайный PIN-код для OTP и автоматически подставляет его в оба поля: **PIN-код** и **Подтверждение PIN-кода**
Скопировать	Копирует текущее значение поля **PIN-код** в буфер

4. Нажмите **Изменить**.
   При успешной установке/изменении PIN-кода для OTP отобразится соответствующее сообщение. 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 системе Active Directory должен быть настроен адрес электронной почты, а также в серверном агенте JMS должен быть настроен транспортный почтовый сервис.

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

3.7.1.6 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. 126 и «Выпуск программных OTP-токенов (мобильное приложение Aladdin 2FA)», с. 127.

1. В консоли управления JMS выберите OTP-токен, возможность использования которого вы хотите включить или отключить.

2. В зависимости от нужного действия в верхней панели 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** центральной части консоли управления JMS (см. рис. 136 ниже).

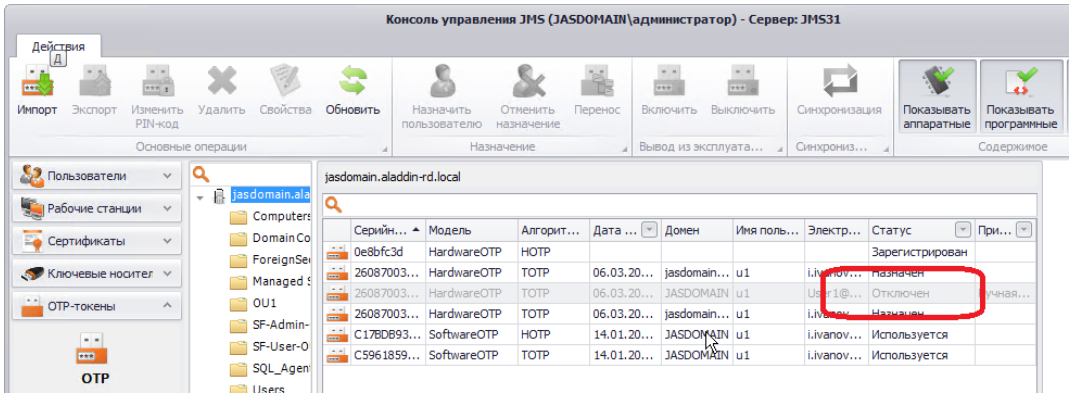


*Рис. 136 – Текущий статус OTP-токена отображается в столбце **Статус***

3.7.1.7 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. 254 и «Настройка профиля выпуска программных OTP-токенов», с. 262).

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

1. В консоли управления JMS выберите OTP-токен, который вы хотите синхронизировать с JMS.
2. В верхней панели выберите **Синхронизировать**.

Отобразится следующее окно.

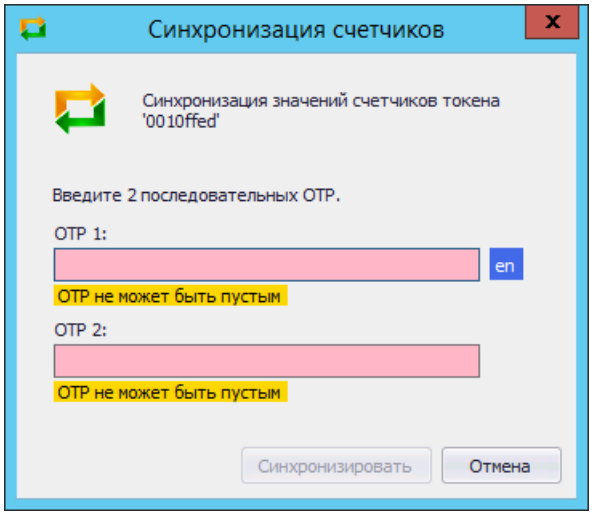


Рис. 137 – Синхронизация OTP-токена

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**.
   После ввода двух значений окно будет иметь следующий вид.

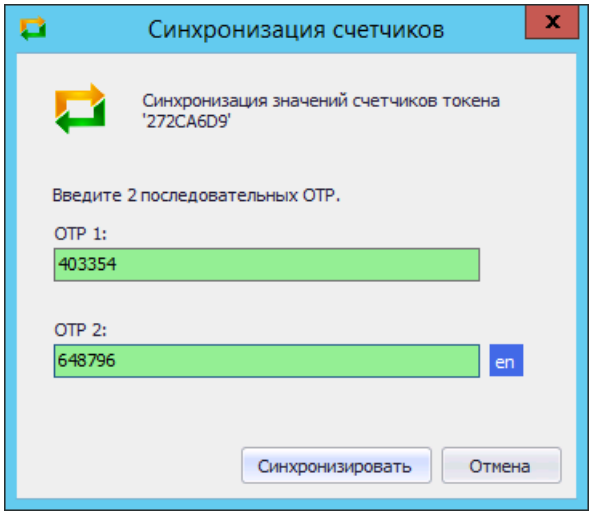


Рис. 138 – Ввод двух последовательных значений OTP

5. Нажмите **Синхронизировать**.
   При успешной синхронизации отобразится следующее сообщение.

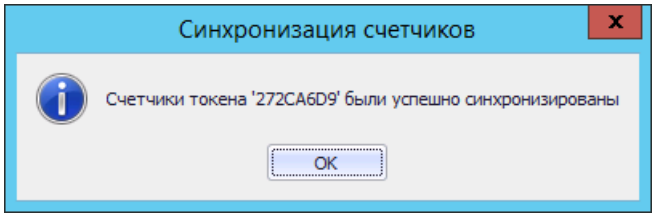


Рис. 139 – Сообщение об успешной синхронизации OTP-токена

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

3.7.1.8 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. В верхней панели нажмите **Свойства**.
   Отобразится следующее окно.

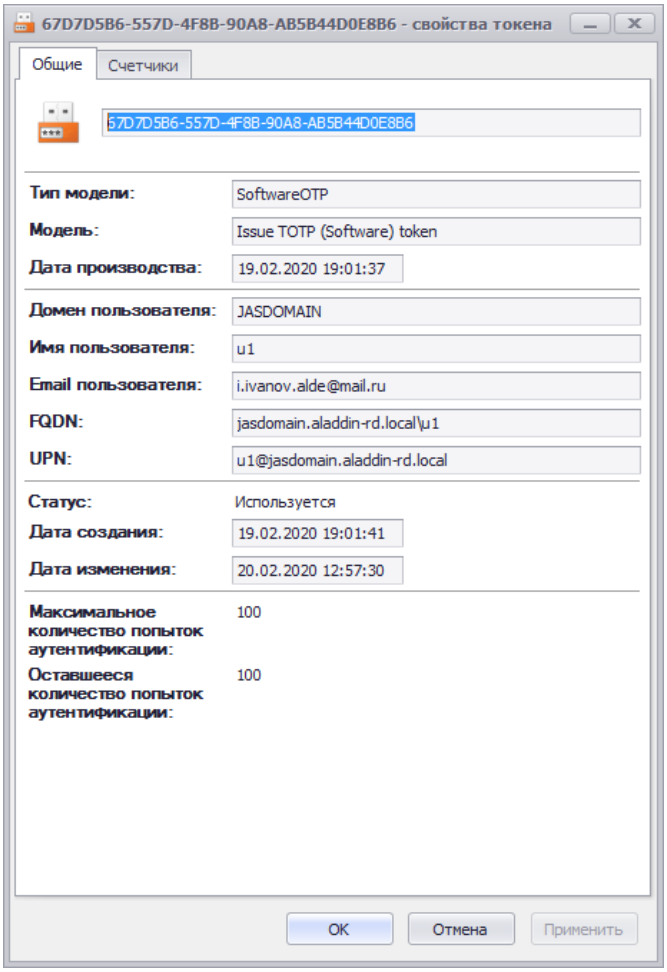


*Рис. 140 – Вкладка **Общие** свойств OTP-токена*

3. На вкладке отображаются поля в соответствии с табл. 9.

Табл. 9 – Общие параметры OTP-токена

Поле	Описание
Тип модели	Тип OTP-токена (программный/аппаратный). Возможные варианты: • **SoftwareOTP** • **HardwareOTP**
Модель	Отображает название модели OTP-токена.
Дата производства	Отображает дату производства OTP-токена.

Поле	Описание
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. Настройка рассылки уведомлений производится в серверном агенте JMS (приложение Сервер JMS), в транспортном почтовом сервисе (вкладка **Настройка**, пункт **Настройка транспорта**). 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.
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 настройке **Максимальное количество неудачных попыток аутентификации** серверного агента JAS (приложение *Сервер JAS*) на вкладке **Настройка** -> **Прикладные настройки сервера** -> **Настройки аутентификации**, подробнее см. руководство по установке и настройке сервера JAS [3], раздел *«Прикладные настройки сервера»* -> *«Настройки аутентификации»*.
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.

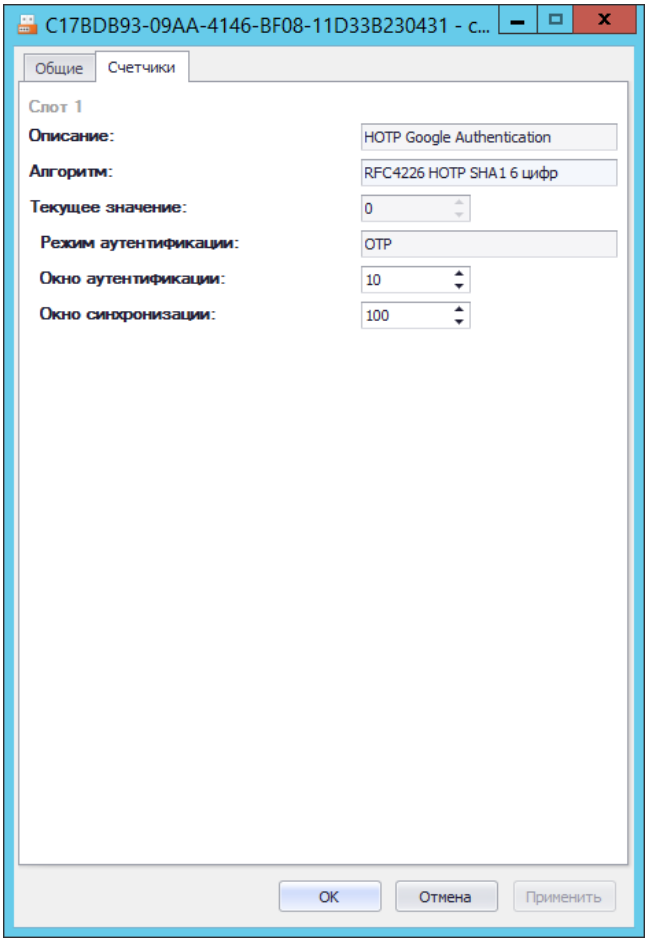


*Рис. 141 – Вкладка **Счетчики** окна свойств OTP-токена с алгоритмом генерации HOTP*

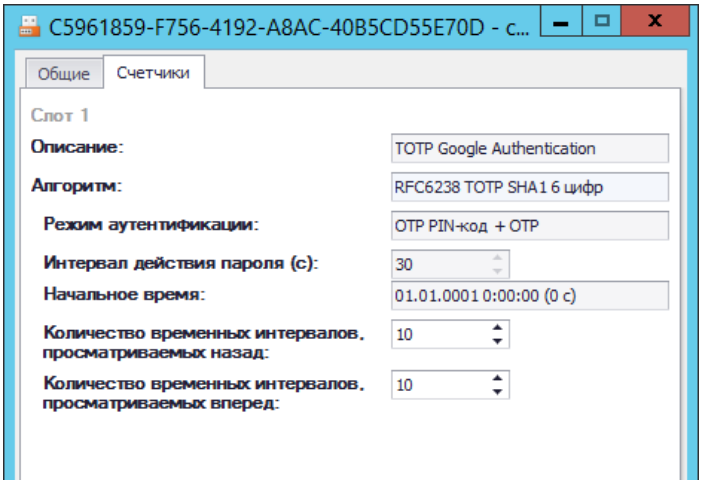


*Рис. 142 – Вкладка **Счетчики** окна свойств OTP-токена с алгоритмом генерации TOTP*

5. Выполните настройки, руководствуясь табл. 10 ниже.

Табл. 10 – Дополнительные параметры OTP-токена

Настройка/поле	Описание
Описание	Отображает описание выбранного OTP-токена, задается в профиле выпуска OTP-токенов (см. Табл. 46, с. 256). Неизменяемое поле.
Алгоритм	Отображает алгоритм формирования одноразовых паролей, используемый на OTP-токене. Задается в профиле выпуска OTP-токенов (см. Табл. 46, с. 256). 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. 46, с. 256) Неизменяемое поле.
Окно аутентификации **Окно синхронизации** (только для токенов с алгоритмом HOTP)	Описание параметров приведено в Табл. 48, с. 260. Параметры позволяют выполнить индивидуальную настройку для отдельного токена (после выпуска токена со значениями параметров, определенных в профиле выпуска).
Интервал действия пароля (с) **Начальное значение** (только для токенов с алгоритмом TOTP)	Описание параметров приведено в Табл. 51, с. 267. Неизменяемые поля.
Количество временных интервалов, просматриваемых назад **Количество временных интервалов, просматриваемых вперед** (только для токенов с алгоритмом TOTP)	Описание параметров приведено в Табл. 51, с. 267. Параметры позволяют выполнить индивидуальную настройку для отдельного токена (после выпуска токена со значениями параметров, определенных в профиле выпуска).

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

3.7.1.9 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. В верхней панели выберите **Удалить**.
3. Отобразится диалоговое окно подтверждения выбора.
4. Нажмите **Да** для завершения процедуры.

3.7.2 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.

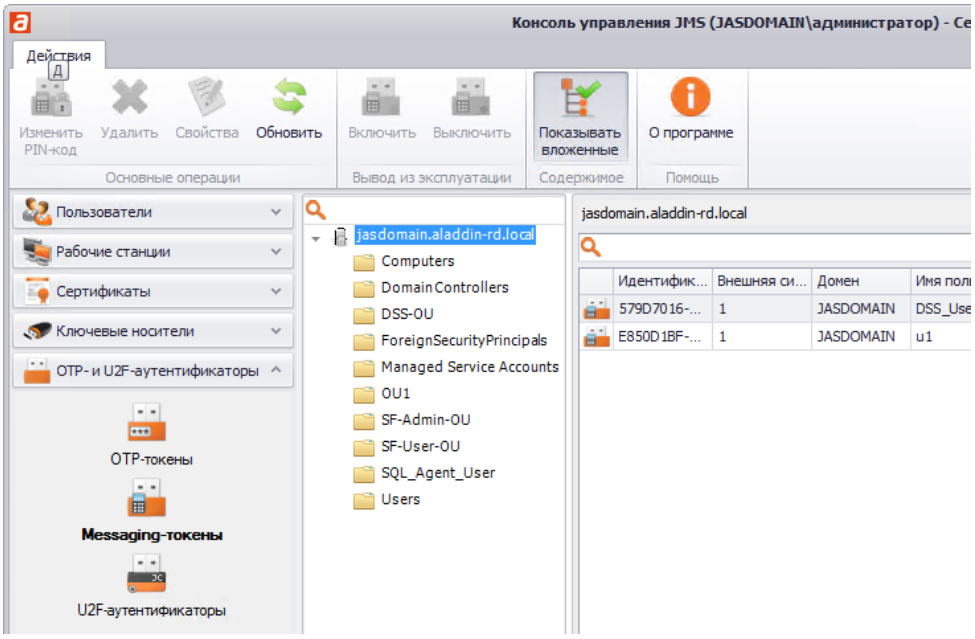


Рис. 143 – Раздел управления Messaging-токенами в консоли управления JMS

3.7.2.1 Выпуск messaging-токенов

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

1. У пользователей, зарегистрированных в JMS, для которых выпускаются токены, в ресурсной системе Active Directory в заданном атрибуте должен быть указан номер телефона, на который будут присылаться сообщения с OTP, подробнее см. описание параметра **Атрибут с номером телефона**, Табл. 53, с. 271.
2. В серверном агенте JAS (приложение *Сервер JAS*) должен быть настроен транспортный сервис для отправки сообщений пользователям (вкладка **Настройки** -> **Прикладные настройки сервера** -> вкладка **Настройки Messaging**, подробнее см. руководство по установке и настройке сервера JAS [3]).

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. 269 выполните его привязку к соответствующему контейнеру ресурсной системы, руководствуясь разделом «Привязка профилей», с. 296.
2. Настройте для выпуска messaging-токенов и запустите на выполнение соответствующий план обслуживания, руководствуясь разделами «План обслуживания жизненного цикла OTP-токенов», с. 410 (проверьте факт включения задачи «Обслуживание Messaging-токенов») и «Запуск и просмотр результатов планов обслуживания из Консоли управления JMS», с.405.
3. Выпущенные и готовые к использованию (статус *Используется*) экземпляры messaging-токенов отобразятся в консоли управления (Рис. 143, выше).

3.7.2.2 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. 128).

3.7.2.3 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. 129).

3.7.2.4 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. В верхней панели выберите **Свойства**.
   Отобразится следующее окно.

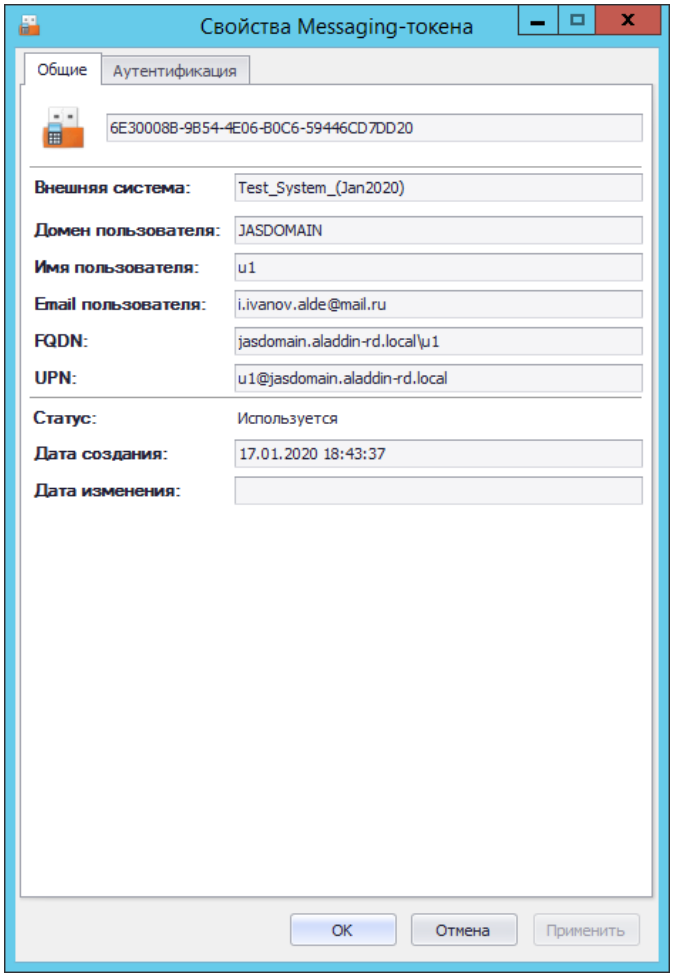


*Рис. 144 – Вкладка **Общие** свойств Messaging-токена*

3. Окно содержит параметры, описанные в Табл. 11.

Табл. 11 – Просмотр общих свойств Messaging-токена

Поле	Описание
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. 53, с. 271.
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 создания	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. 137).

4. Перейдите на вкладку **Аутентификация**.

Окно примет следующий вид.

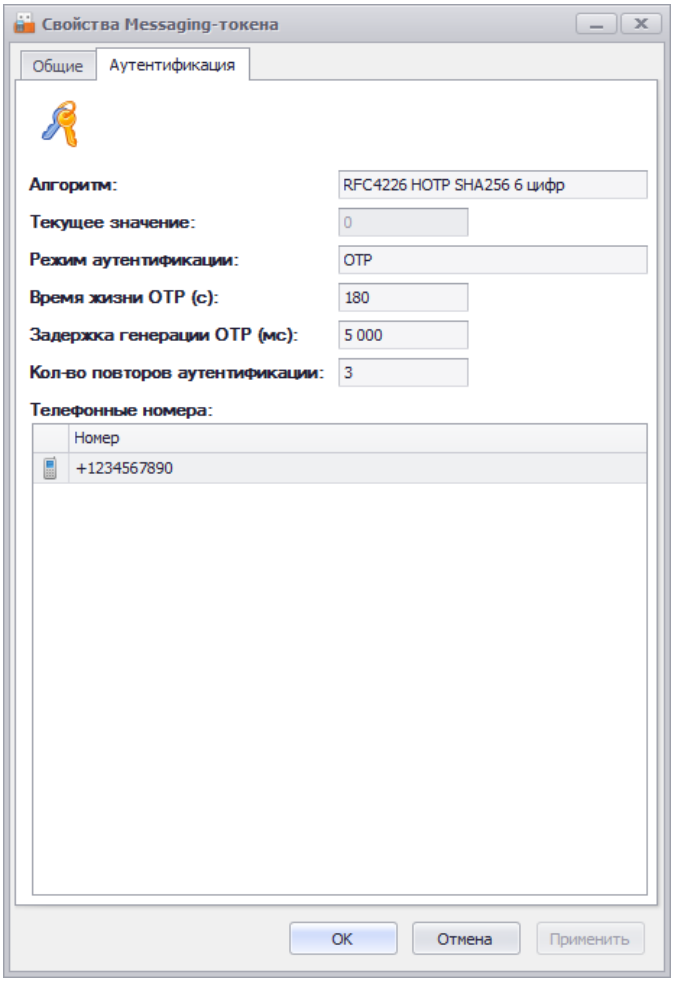


*Рис. 145 – Вкладка **Аутентификация** окна свойств Messaging-токена*

5. Окно содержит параметры токена, описанные в Табл. 12.

Табл. 12 – Параметры аутентификационной информации Messaging-токена

Настройка/поле	Описание
Алгоритм	Отображает алгоритм генерации одноразового пароля аутентификации (OTP). (Задается профилем выпуска messaging-токенов, см. Табл. 53, с. 271)
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)** • **Кол-во повторов аутентификации**	В полях отображаются значения настроек, выполненных в соответствии с профилем выпуска messaging-токенов, см. Табл. 53, с. 271
Телефонные номера	Отображает телефонные номера в соответствии с параметром профиля выпуска **Атрибут с номером телефона** (см. Табл. 53, с. 271).

3.7.2.5 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. 135).

3.7.3 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. 146).

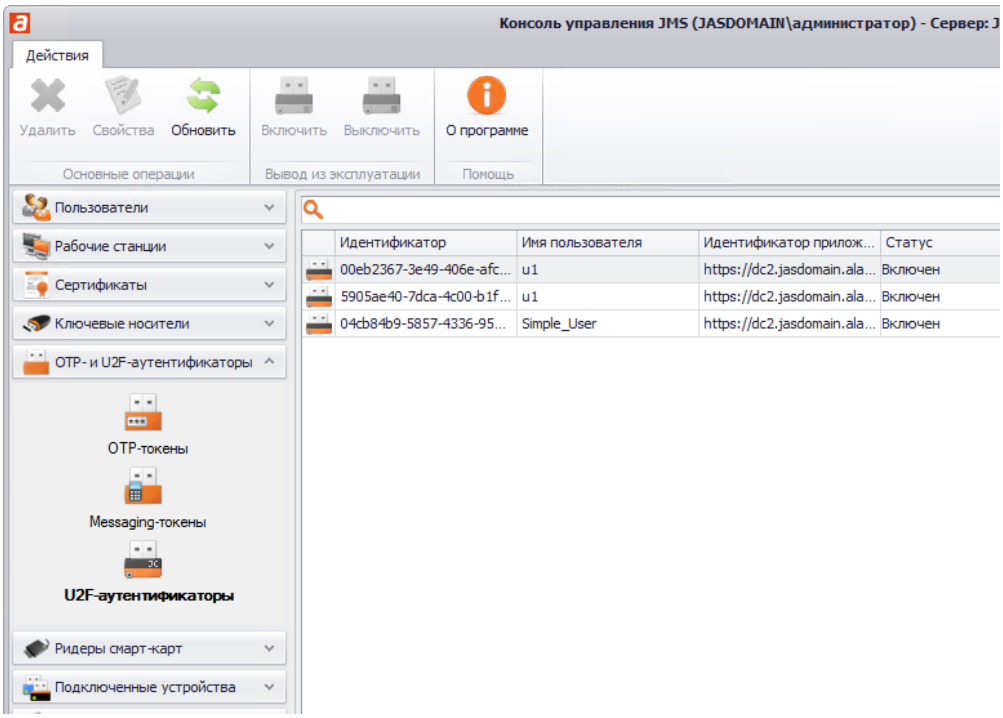


Рис. 146 – Раздел управления U2F-аутентификаторами в консоли управления JMS

3.7.3.1 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. 129).

3.7.3.2 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. В верхней панели выберите **Свойства**.
   Отобразится следующее окно.

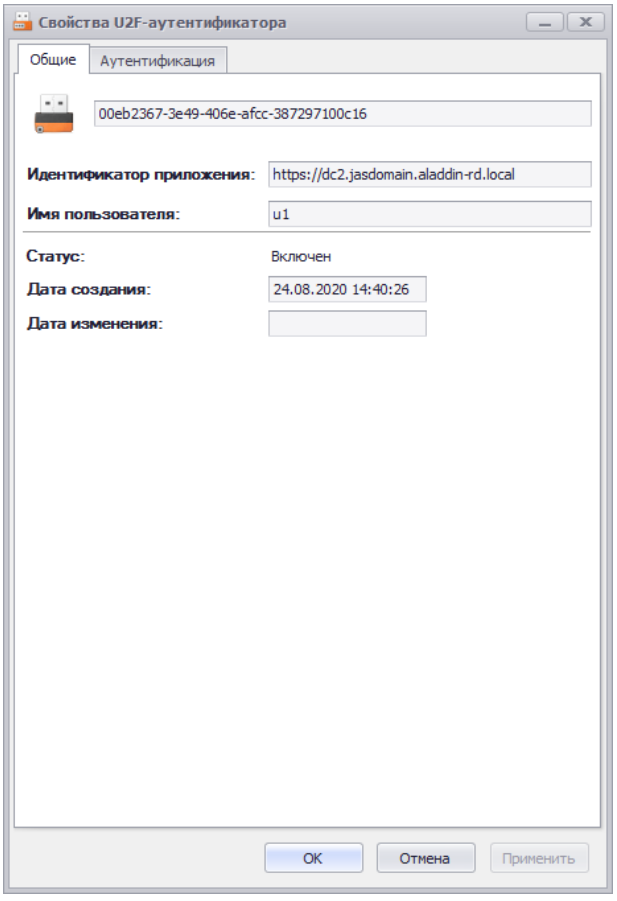


*Рис. 147 – Вкладка **Общие** свойств U2F-аутентификатора*

3. Отображаемые параметры описаны в Табл. 13.

Табл. 13 – 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

Поле	Описание
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**.
Окно примет следующий вид.

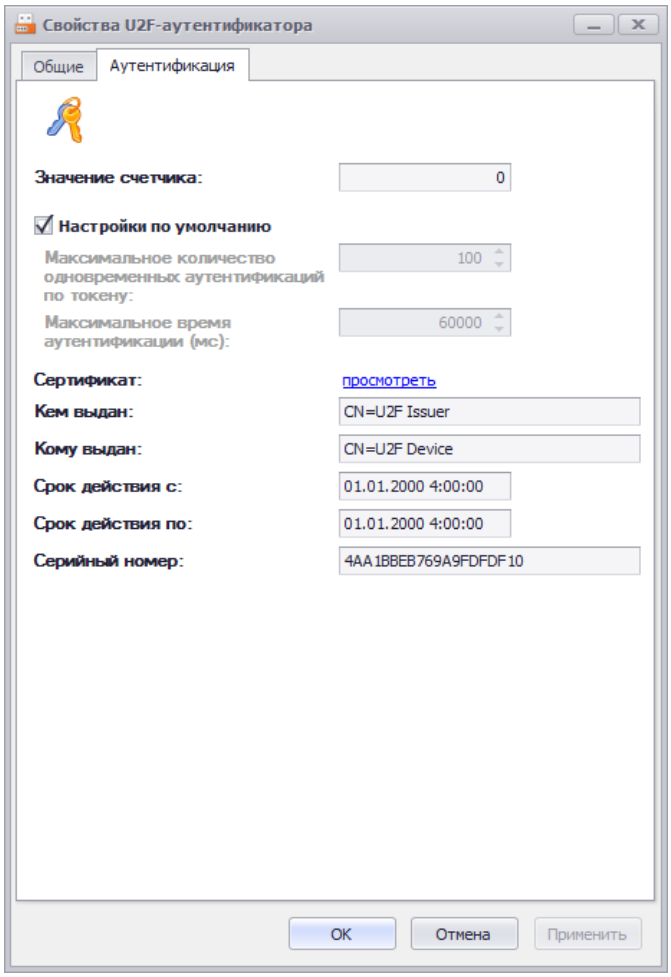


*Рис. 148 – Вкладка **Аутентификация** окна свойств U2F-аутентификатора*

5. Выполните настройки, руководствуясь Табл. 14.

Табл. 14 – Параметры аутентификационной информации U2F-аутентификатора

Настройка/поле	Описание
Значение счетчика	Значение счетчика аутентификаций, сохраняемое на стороне U2F-сервера согласно спецификациям протокола U2F. Неизменяемое поле.

Настройка/поле	Описание
Настройки по умолчанию	Если флажок установлен, для аутентификации пользователей будут применяться настройки по умолчанию, установленные в серверном агенте JAS (приложение Сервер JAS), на вкладке **Настройка** -> **Прикладные настройки сервера** -> **Настройки U2F**, подробнее см. руководство по установке и настройке сервера JAS [3], раздел *«Прикладные настройки сервера» -> «Настройки U2F».* Снятие этого флажка позволяет переопределить следующие настройки по умолчанию для выбранного U2F-аутентификатора: • Максимальное количество одновременных аутентификаций по токену; • Максимальное время аутентификации (мс)
Максимальное количество одновременных аутентификаций по токену	Максимальное количество одновременных аутентификаций по данному U2F-аутентификатору. **Примечание.** При создании аутентификатора параметр принимает значение по умолчанию, задаваемое в серверном агенте JAS, на вкладке **Настройка** -> **Прикладные настройки сервера** -> **Настройки U2F,** подробнее см. руководство по установке и настройке сервера JAS [3].
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 в серверном агенте JAS, на вкладке **Настройка** -> **Прикладные настройки сервера** -> **Настройки U2F,** подробнее см. руководство по установке и настройке сервера JAS [3].
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.

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

3.7.3.3 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. 135).

3.8 Операции с ридерами смарт-карт

3.8.1 Регистрация подключенных ридеров смарт-карт в JMS

Чтобы зарегистрировать подключенный ридер смарт-карт в JMS, выполните следующие действия.

1. Подключите ридер смарт-карт, который вы хотите зарегистрировать, к компьютеру.

   Примечание. Для того чтобы карт-ридер мог отображаться в консоли управления и быть зарегистрированным в JMS, в него должна быть вставлена смарт-карта.

2. Запустите мастер регистрации ридеров смарт-карт любым из следующих способов:

   2.1. в консоли управления JMS перейдите в раздел **Ридеры смарт-карт**;
   2.2. в левой панели выберите группу или организационную единицу, к которой будет привязан ридер смарт-карт (в настоящем документе для примера будет использоваться группа **Users** (Пользователи));
   2.3. в верхней панели щелкните на кнопке **Зарегистрировать подключенный**.

   Отобразится следующее окно.

   2.1. в консоли управления JMS перейдите в раздел **Подключенные устройства** -> **Ридеры смарт-карт**;
   2.2. в центральной части окна выберите ридер смарт-карт, который вы хотите зарегистрировать;
   2.3. в верхней панели щелкните на кнопке **Зарегистрировать**.

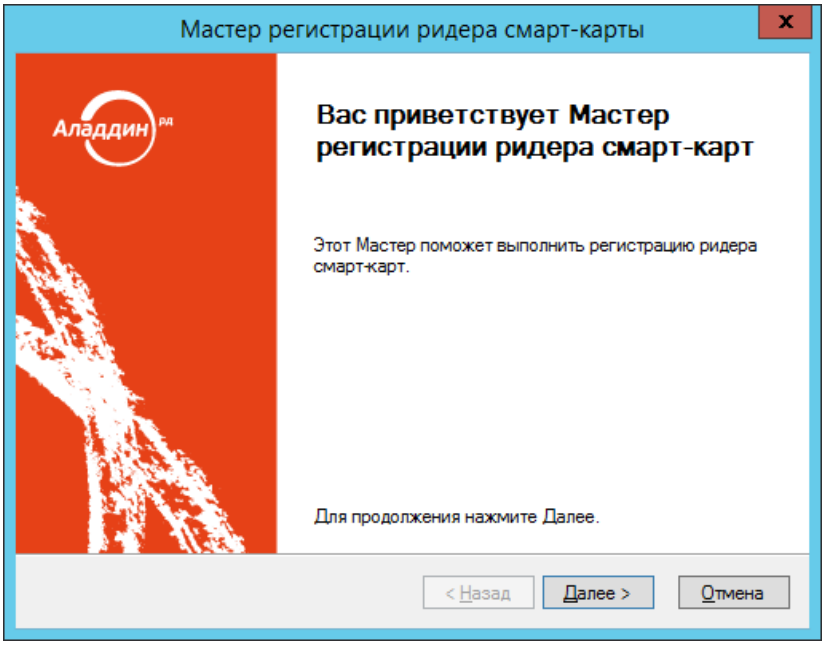


Рис. 149 – Окно приветствия мастера регистрации ридеров смарт-карт

3. Нажмите **Далее**.
   Если вы регистрируете карт-ридер из раздела **Подключенные устройства** -> **Ридеры смарт-карт** консоли управления JMS, отобразится следующее окно (Рис. 150) . Выберите в нем группу или организационную единицу, к которой будет привязан зарегистрированный карт-

ридер, после чего нажмите **Далее**. (В противном случае переходите к шагу 6 настоящей процедуры.)

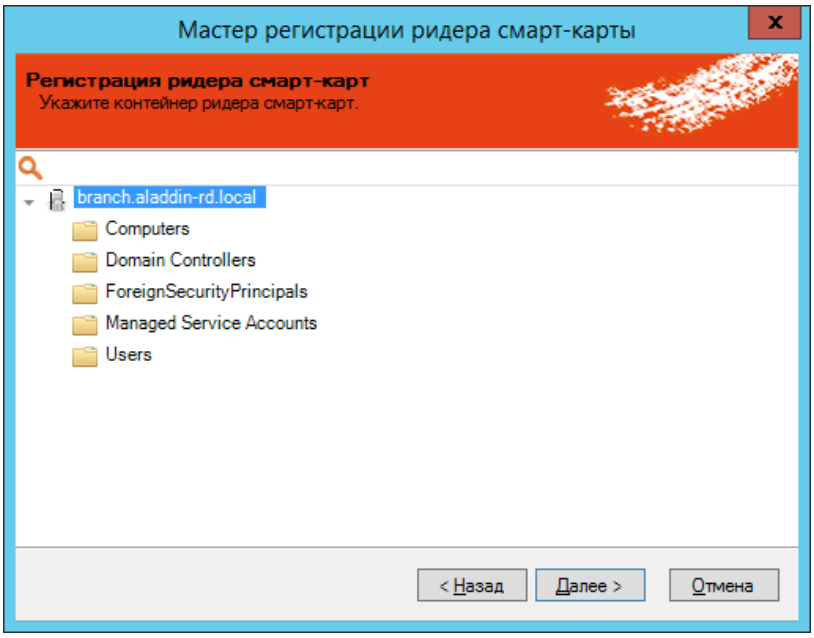


Рис. 150 – Привязка карт-ридера к группе или организационной единице

4. Отобразится следующее окно.

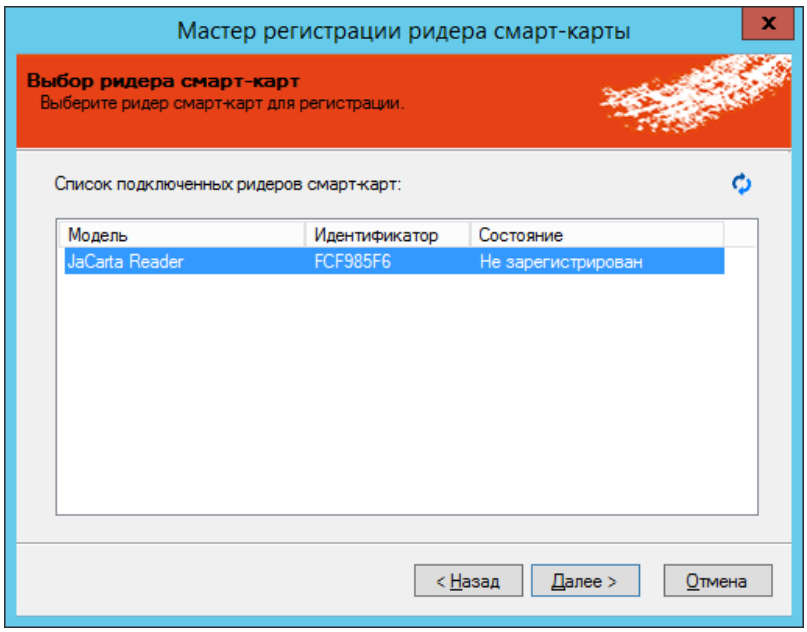


Рис. 151 – Окно выбора карт-ридера

5. Выберите нужный карт-ридер и нажмите **Далее**.

6. Отобразится следующее окно.

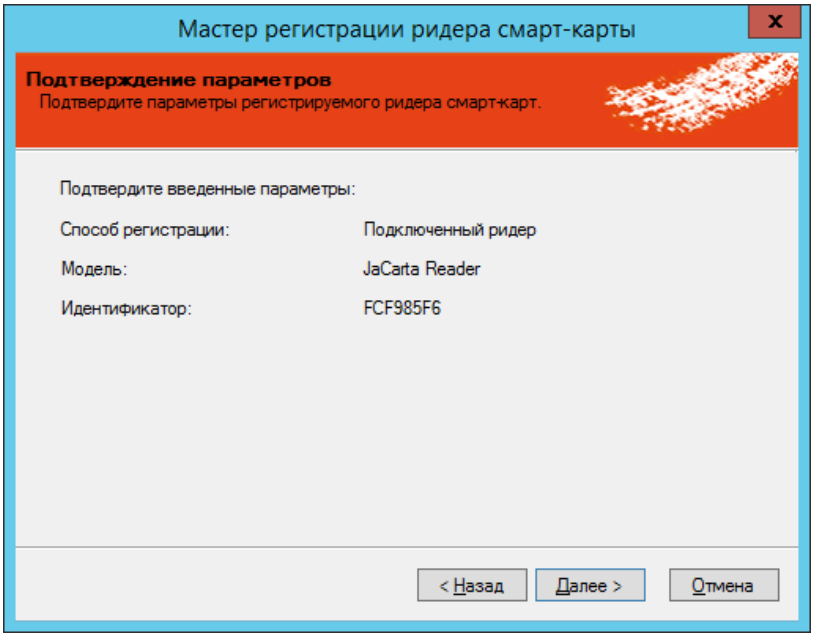


Рис. 152 – Окно подтверждения параметров регистрации карт-ридера

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

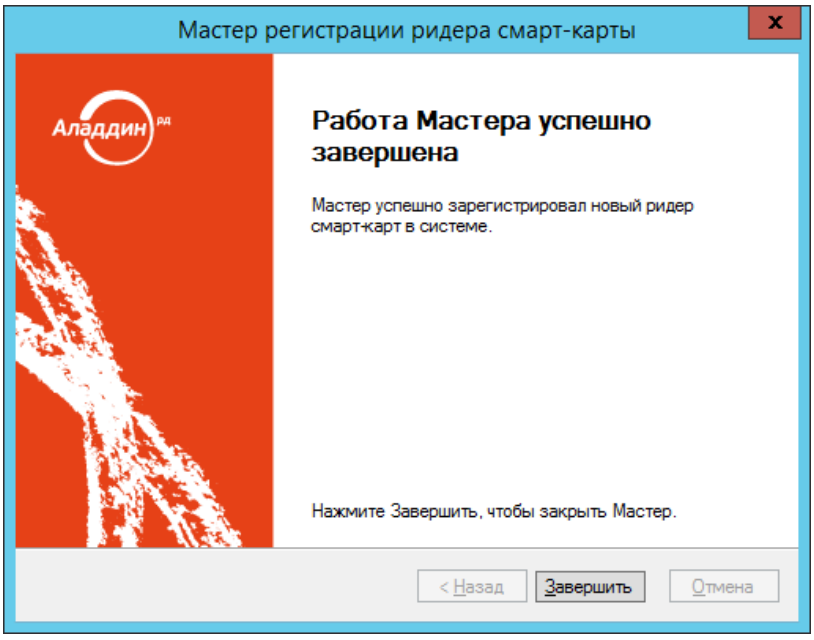


Рис. 153 – Окно завершения работы регистрации ридера смарт-карт

8. Нажмите **Завершить**.

3.8.2 Экспорт/импорт ридеров смарт-карт

JMS позволяет экспортировать ридеры смарт-карт с тем, чтобы их можно было импортировать на другом экземпляре JMS. Существует два варианта экспорта:

- экспорт карт-ридеров списком – для этого сначала необходимо подготовить список карт-ридеров (см. «Подготовка списка ридеров смарт-карт для экспорта» ниже), после чего осуществить процедуру экспорта (см. «Экспорт ридеров смарт-карт», с. 147);
- экспорт карт-ридеров, выбранных в интерфейсе консоли управления JMS (см. «Экспорт ридеров смарт-карт», с. 147).

Чтобы импортировать карт-ридеры, выполните процедуру «Импорт (пакетная регистрация) ридеров смарт-карт в JMS», с. 151.

3.8.2.1 Подготовка списка ридеров смарт-карт для экспорта

Чтобы подготовить файл со списком ридеров смарт-карт для экспорта из JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Ридеры смарт-карт**.
2. В верхней панели выберите вкладку **Действия**.
3. В верхней панели нажмите **Утилита создания списка**.
   Отобразится следующее окно.

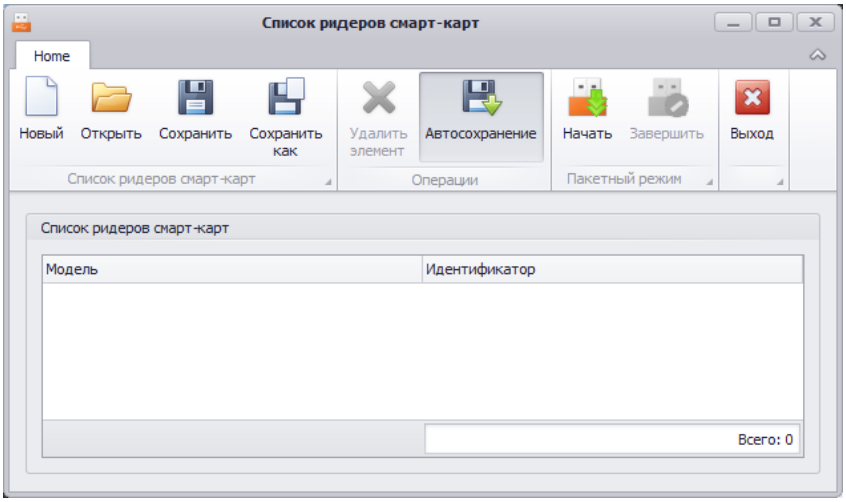


Рис. 154 – Утилита создания списка

4. Порядок работы с утилитой аналогичен порядку работы с утилитой для создания списка электронных ключей (см. «Подготовка списка электронных ключей для экспорта», с. 60). Для регистрации всех ридеров необходимо последовательно подключать их к USB-порту компьютера.

Примечание. Для корректной регистрации ридера, в него должна быть вставлена смарт-карта.

3.8.2.2 Экспорт ридеров смарт-карт

Чтобы экспортировать список ридеров смарт-карт в файл, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Ридеры смарт-карт**.
2. В верхней панели выберите вкладку **Действия**.
3. В зависимости от варианта экспорта, выполните следующие действия:

- *экспорт карт-ридеров, выбираемых в интерфейсе JMS* – в левой панели выберите контейнер, из которого вы хотите экспортировать ридеры, после чего отметьте нужные ридеры в центральной части интерфейса;
- *экспорт карт-ридеров списком* – переходите к следующему шагу процедуры.

4. В верхней панели щелкните на одном из следующих значков:

   - **Экспорт выбранных** – позволяет экспортировать карт-ридеры, выделенные в центральной части интерфейса консоли управления JMS;
   - **Экспорт по списку** – позволяет экспортировать ридеры по заранее подготовленному списку (см. «Подготовка списка ридеров смарт-карт для экспорта», с. 147).

Примечание. Поскольку процедура создания списка позволяет включать в список карт-ридеры, не зарегистрированные в JMS, перед тем как начать процедуру в варианте **Экспорт по списку**, следует убедиться, что все карт-ридеры из списка зарегистрированы в JMS, в противном случае экспорт завершится с ошибкой.

   Отобразится следующее окно.

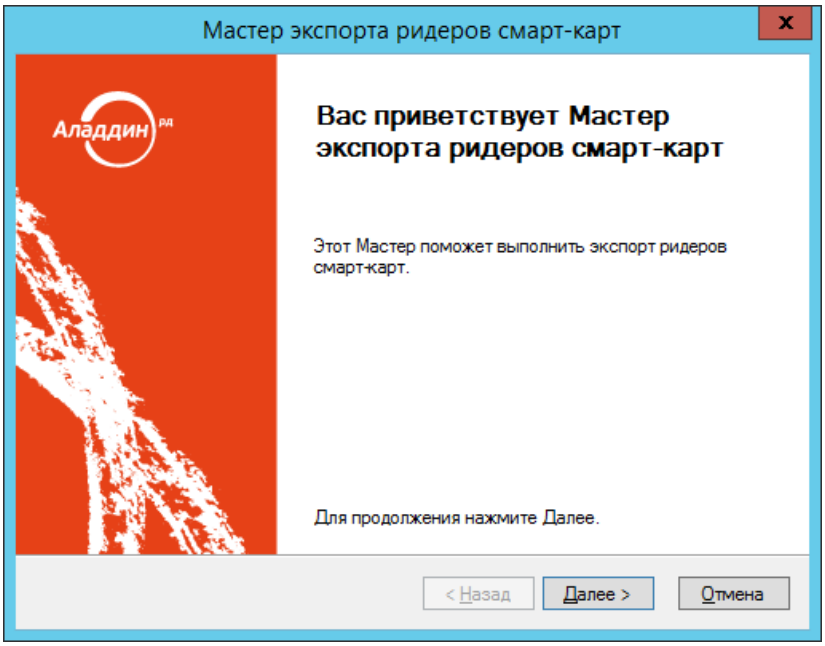


Рис. 155 – Окно приветствия мастера экспорта карт-ридеров

5. Нажмите **Далее**.
   Если вы экспортируете карт-ридеры по списку, отобразится следующее окно. (Противном случае переходите к шагу 7 настоящей процедуры.)

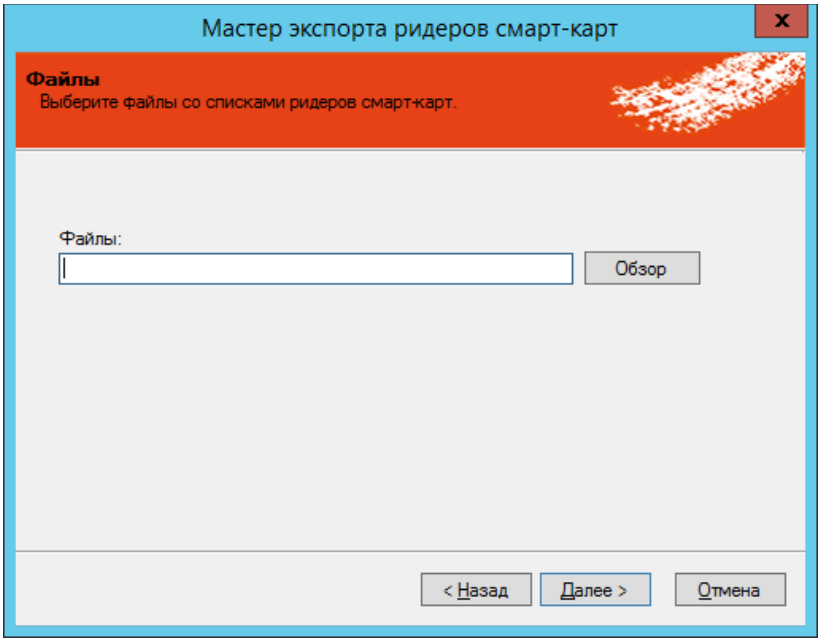


Рис. 156 – Экспорт карт-ридеров по списку

6. Воспользуйтесь кнопкой **Обзор**, чтобы указать путь к заранее подготовленному файлу со списком электронных ключей (см. «Подготовка списка ридеров смарт-карт для экспорта», с. 147), после чего нажмите **Далее**.

7. Отобразится следующее окно.

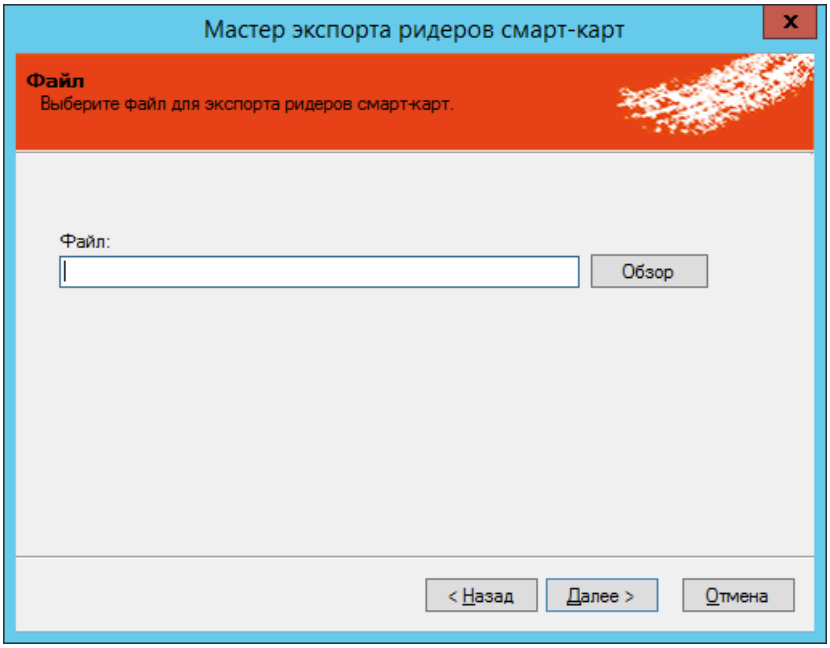


Рис. 157 – Указание пути сохранения файла

8. Воспользуйтесь кнопкой **Обзор**, чтобы указать путь сохранения экспортируемого файла, после чего нажмите **Далее**.

Отобразится следующее окно.

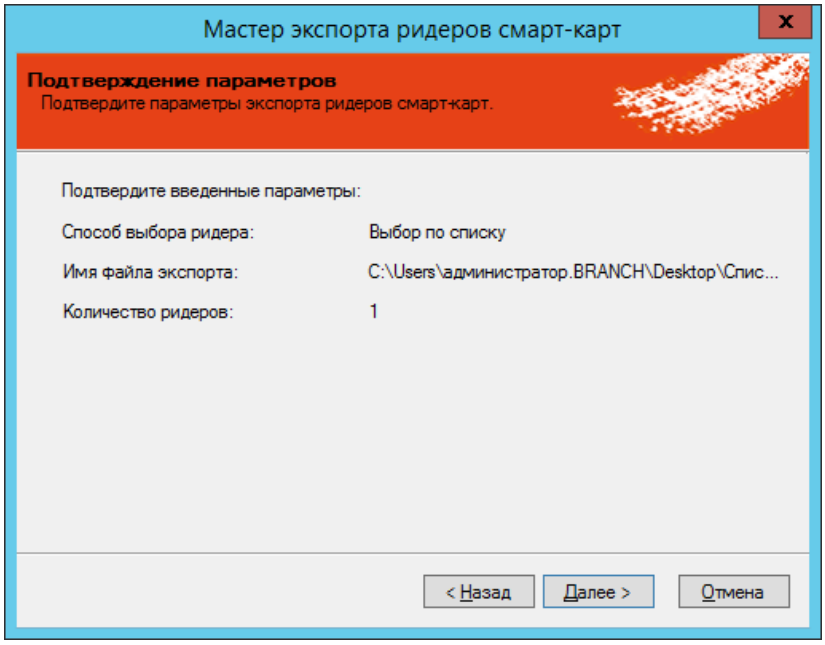


Рис. 158 – Окно подтверждения параметров экспорта

9. Нажмите **Далее**.
Отобразится следующее окно.

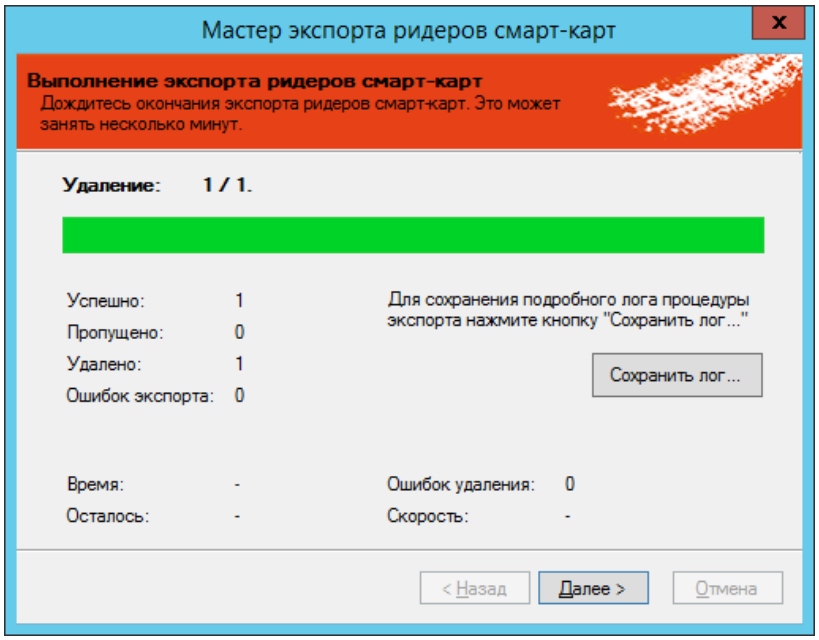


Рис. 159 – Экспорт сведений о карт-ридерах в файл

10. Нажмите **Далее**.

Отобразится следующее окно.

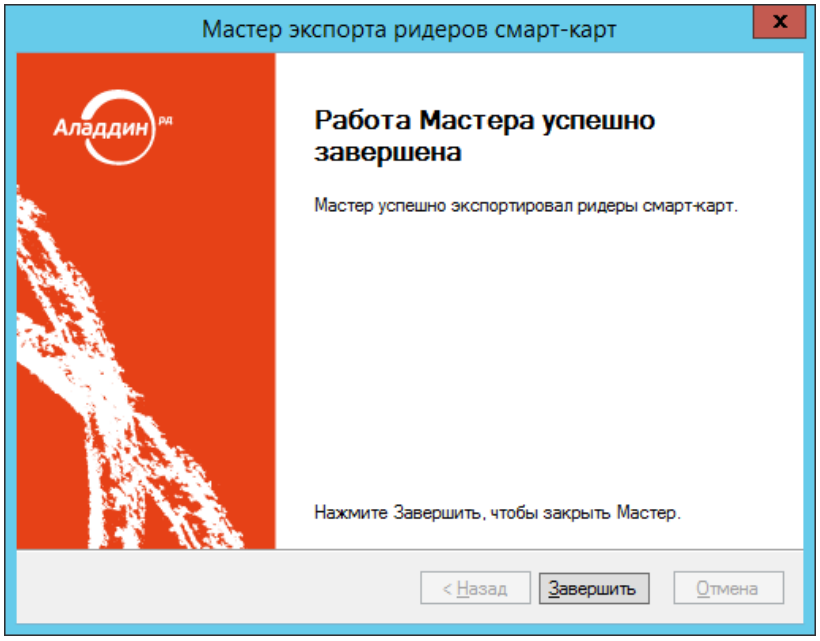


Рис. 160 – Окно завершения процедуры экспорта

11. Нажмите **Завершить** для завершения процедуры.

3.8.2.3 Импорт (пакетная регистрация) ридеров смарт-карт в JMS

Для пакетной регистрации карт-ридеров в JMS можно воспользоваться файлами следующих типов:

- соответствующим файлом со списком карт-ридеров компании-поставщика (предоставляется только компанией Аладдин для карт-ридеров её производства по запросу заказчика);
- файлом, полученным в результате процедуры экспорта карт-ридеров (см. «Экспорт ридеров смарт-карт», с. 147);
- файлом, полученным в результате подготовки списка карт-ридеров, см. на примере раздела «Подготовка списка ридеров смарт-карт для экспорта», с. 147.

Примечание. В последнем случае с помощью процедуры создания списка можно сформировать список карт-ридеров, еще не зарегистрированных в JMS. При таком порядке действий регистрация карт-ридеров в JMS происходит быстрее, чем их обычная регистрация по одному экземпляру.

Чтобы импортировать карт-ридеры в JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Ридеры смарт-карт**.
2. В верхней панели выберите вкладку **Действия над контейнером**.
3. В верхней панели нажмите **Импорт**.

Отобразится следующее окно.

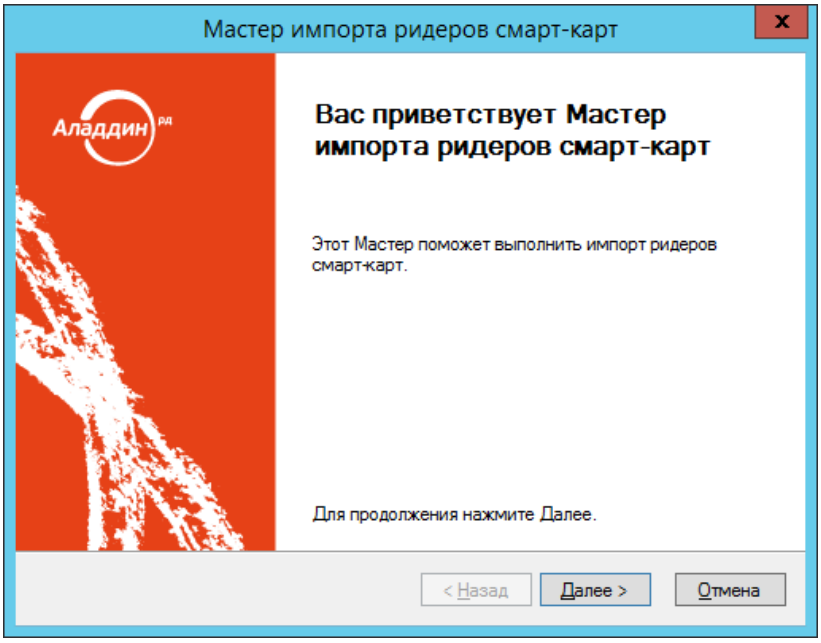


Рис. 161 – Окно приветствия мастера импорта карт-ридеров

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

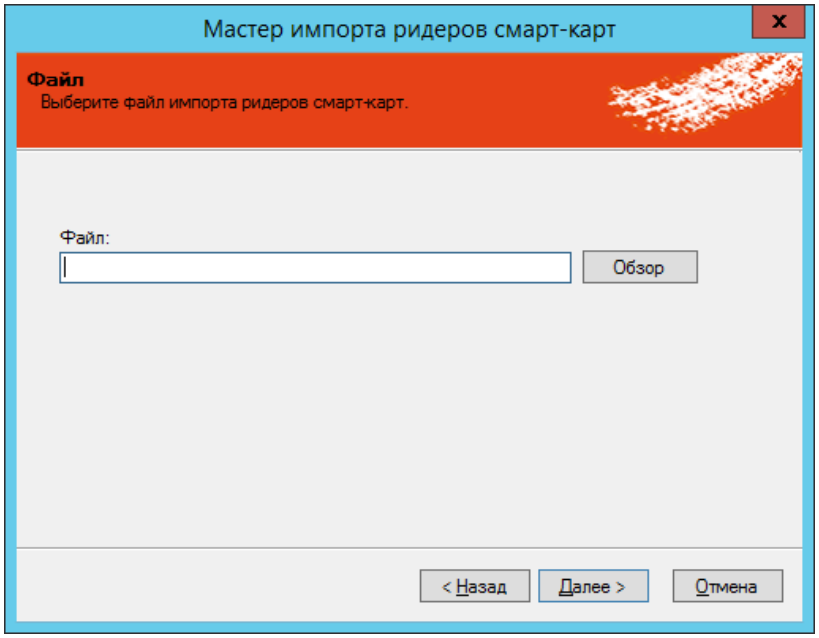


Рис. 162 – Выбор файла, содержащего сведения об импортируемых карт-ридерах

5. Воспользуйтесь кнопкой **Обзор**, чтобы указать путь к файлу, содержащему сведения об импортируемых карт-ридерах, после чего нажмите **Далее**.

Отобразится следующее окно.

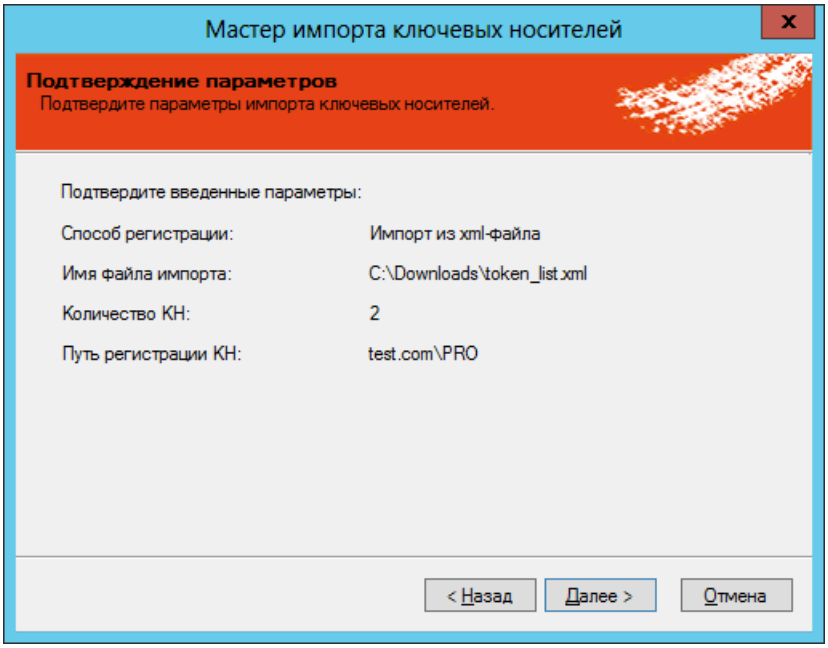


Рис. 163 – Подтверждение параметров импорт

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

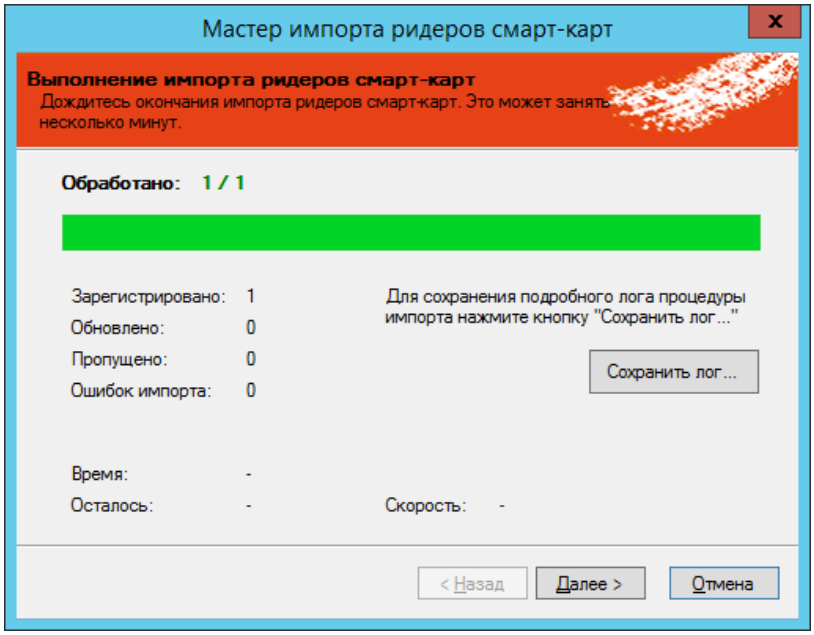


Рис. 164 – Сведения об импорте

7. Нажмите **Далее**.

Отобразится следующее окно.

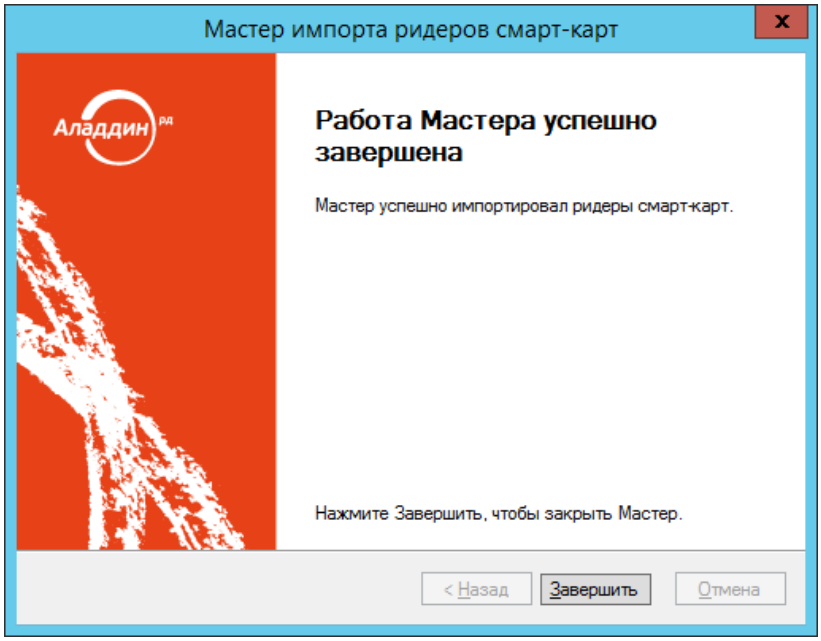


Рис. 165 – Окно завершения работы мастера импорта

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

3.8.3 Назначение ридера смарт-карт пользователю

Чтобы назначить карт-ридер пользователю в консоли управления JMS перейдите в один из следующих разделов: **Ридеры смарт-карт** или **Подключенные устройства** -> **Ридеры смарт-карт**; и в центральной части окна отметьте карт-ридер, который хотите назначить, после чего в верхней панели нажмите **Назначить пользователю.** В отобразившемся окне отметьте нужного пользователя и нажмите **Выбрать**.

3.8.4 Удаление ридера смарт-карт

Чтобы удалить карт-ридер из JMS, выполните следующие действия.

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

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

   В последнем случае удаляемый карт-ридер должен быть подключен к компьютеру.

2. В верхней панели нажмите **Удалить**.
3. В окне подтверждения запроса на удаление электронного ключа нажмите **Да**.

3.8.5 Перенос привязки ридеров смарт-карт к контейнерам ресурсной системы

Управление привязкой карт-ридеров к контейнерам ресурсной системы осуществляется по аналогии с привязкой электронных ключей (см. «Привязка электронных ключей к контейнерам ресурсной системы», с. 108).

3.9 Настройка профилей JMS

Профили JMS классифицируются в соответствии с группами, перечисленными в табл. 15.

Табл. 15 – 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. 158.
Профили выпуска OTP-токенов **Примечание.** Профили данной группы доступны в консоли, только если в лицензии JMS указана опция на поддержку сервера JAS.	**Выпуск программных OTP-токенов** - позволяет настроить общие параметры выпуска программных генераторов OTP, предлагаемых различными поставщиками приложений для мобильных устройств на базе ОС Android и iOS (например, мобильное приложение Aladdin 2FA компании Аладдин). Настройка профиля данного типа приведена в разделе «Настройка профиля выпуска программных OTP-токенов», с. 262. **Выпуск аппаратных OTP-токенов** - позволяет настроить общие параметры выпуска аппаратных OTP-токенов, таких как JaCarta WebPass, eToken PASS, eToken NG OTP и других, реализующих спецификации RFC 4226 и 6238. Настройка профиля данного типа приведена в разделе «Настройка профиля выпуска аппаратных OTP-токенов», с. 254. **Выпуск messaging-токенов** - позволяет настроить общие параметры выпуска messaging-токенов – виртуальный объектов, которые регистрируются в JMS с привязкой к пользователям и осуществляют процедуру передачи значения OTP на мобильный телефон пользователя посредством службы SMS. Настройка профиля данного типа приведена в разделе «Настройка профиля выпуска Messaging-токенов», с. 269.
Профили настроек клиентского агента (Профили не предусмотрены в версии продукта JMS *CA Edition*)	**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. 164.
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 PKI (с обратной совместимостью), eToken Pro (Card OS)», с. 174; • **Инициализация eToken Pro (Card OS)** – позволяет настроить параметры инициализации электронных ключей eToken Pro - см. «eToken Pro (Java) / JaCarta PKI (с обратной совместимостью), eToken Pro (Card OS)», с. 174; • **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, JaCarta PKI/BIO», с. 183; • **Инициализация JaCarta PKI / BIO** – позволяет настроить параметры инициализации электронных ключей JaCarta PKI/BIO, см. «JaCarta PKI, JaCarta PKI/BIO», с. 183;

Группа профилей JMS	Типы профилей в группе
	• **Инициализация JaCarta ГОСТ / eToken ГОСТ** – позволяет настроить параметры инициализации электронных ключей с апплетом «Криптотокен», как то: JaCarta ГОСТ, JaCarta ГОСТ/Flash, eToken ГОСТ – см. «JaCarta ГОСТ / eToken ГОСТ», с. 192; • **Инициализация ФКН** – позволяет настроить параметры инициализации электронных ключи JaCarta CryptoPro – см. «JaCarta Cryptopro», с. 203; • **Инициализация RuToken** (S, ЭЦП/ЭЦП 2.0, Lite) – позволяет настроить параметры инициализации электронных ключей Рутокен – см. раздел «RuToken S/RuToken ЭЦП/ RuToken ЭЦП 2.0/ RuToken Lite», с. 195; • **Инициализация ESMART** и ESMART ГОСТ – позволяет настроить параметры инициализации электронных ключей ESMART – см. раздел «ESMART / ESMART ГОСТ», с. 205. 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. 209); • **Выпуск сертификатов – КриптоПро УЦ 1.5** – позволяет настроить параметры выпуска сертификатов в центре сертификации КриптоПро версии 1.5 (см. «Работа с КриптоПро УЦ 1.5», с. 591 и «Настройка профиля для выпуска сертификатов в КриптоПро УЦ 1.5», с. 620); • **Выпуск сертификатов – КриптоПРО УЦ 2.0** – позволяет настроить параметры выпуска сертификатов в центре сертификации КриптоПро 2.0 (см. «Работа с КриптоПро УЦ 2.0», с. 628 и «Настройка профиля для выпуска сертификатов в КриптоПро УЦ 2.0», с. 648); • **Выпуск сертификатов – ViPNet УЦ** – позволяет настроить параметры выпуска сертификатов в центре сертификации ViPNet (см. «Работа с ViPNet УЦ», с. 565 и «Настройка профиля для выпуска сертификатов в ViPNet УЦ», с. 585); • **Выпуск электронного ключа для использования в SecurLogon** – позволяет настроить параметры записи профиля Windows в электронный ключ во время выпуска (подробнее см. «Коннектор SecurLogon», с. 554 и «Создание и настройка профиля SecurLogon», с. 561).
Профили коннектора КриптоПро DSS **Примечание.** Профили данной группы доступны в консоли, только если в лицензии JMS указана соответствующая опция на поддержку КриптоПро DSS.	• **Профиль пользователя КриптоПро DSS** - позволяет настроить общие параметры создания и последующего подержания в актуальном состоянии объектов **Пользователь** в системе «КриптоПро DSS», соответствующих пользователям, зарегистрированным в JMS. Настройка профиля данного типа приведена в разделе «Настройка профиля пользователя КриптоПро DSS», с.281. • **Профиль выпуска сертификата на КриптоПро DSS** - позволяет настроить общие параметры выпуска сертификатов в системе «КриптоПро DSS» для пользователей, добавленных в «КриптоПро DSS» (а также взятых под управление) с помощью системы JMS. Настройка профиля данного типа приведена в разделе «Настройки профиля выпуска сертификатов на КриптоПро DSS», с. 223.
Профили синхронизации рабочей стации (Профили не предусмотрены в версии продукта JMS *CA Edition*)	**Настройки синхронизации рабочей стации** – содержит набор параметров, которые могут с заданной периодичностью быть автоматически загружены на сервер JMS с рабочей станции с установленным клиентским агентом JMS (подробнее см. «Профиль настройки синхронизации рабочей станции», с. 244).
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 электронных ключей», с. 458

Для успешного выпуска электронных ключей после создания и настройки профилей необходимо выполнить привязку этих профилей к пользователям JMS (см. «Привязка профилей», с. 296).

3.9.1 Общие операции с профилями

Общее управление профилям осуществляется в разделе **Профили -> Профили** Консоли управления JMS (Рис. 167).

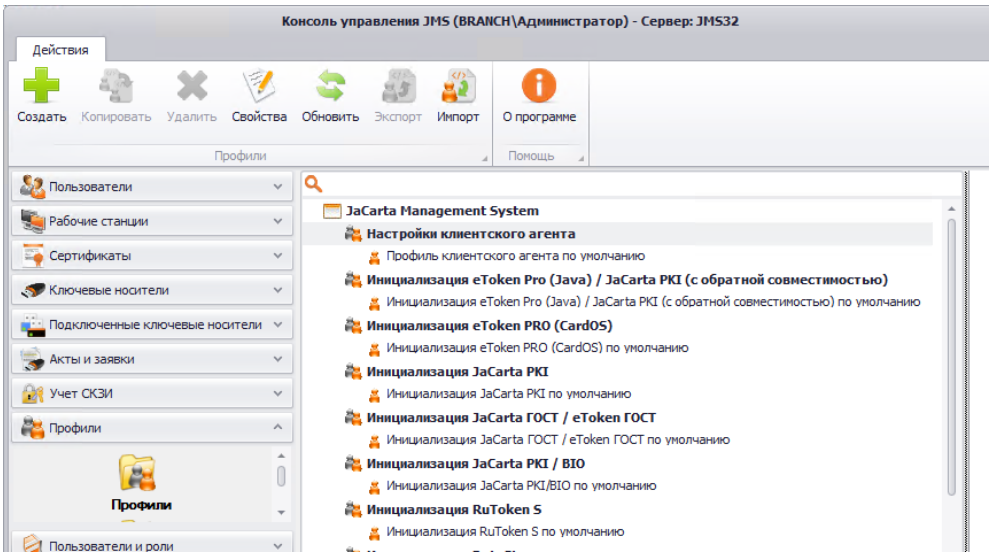


*Рис. 166 – Общий вид раздела **Профили -> Профили** Консоли управления JMS*

Общая информации по управлению профилями содержится в Табл. 16.

Табл. 16 – Общие операции с профилями

Операция	Описание
Создать	Для создания профиля в таблице профилей выберите строку с названием раздела (например **Настройки клиентского агента**) и в верхней панели нажмите **Создать**. Подробно процедура создания профиля описано в разделах, посвященным соответствующим типам профилей
Копировать	Для копирования профиля выберите его в таблице профилей и на верхней панели нажмите **Копировать**. В появившемся окне введите необходимые изменения и сохраните получившийся профиль с другим именем.
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 центре сертификации Microsoft», с. 209; • «Настройка профиля для выпуска сертификатов в ViPNet УЦ», с. 585; • «Настройка профиля для выпуска сертификатов в КриптоПро УЦ 1.5», с. 620; • «Настройка профиля для выпуска сертификатов в КриптоПро УЦ 2.0», с. 648; Удаленные *профили выпуска сертификата* сохраняются в системе

Операция	Описание
Свойства	Операция служит для просмотра свойств типов профилей, либо для редактирования свойств самих профилей.
Обновить	Обновляет отображения информации в таблице профилей
Экспорт	См. раздел «Экспорт/импорт профилей», с. 304
Импорт	См. раздел «Экспорт/импорт профилей», с. 304
 (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.

3.9.2 Настройка профиля выпуска электронных ключей

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

   – если вы хотите создать новый профиль выпуска электронных ключей, в центральной части окна консоли управления JMS отметьте **Выпуск ключевых носителей** и в верхней панели нажмите **Создать**, отобразится окно следующего вида (см. рис. 167);
   – если вы хотите отредактировать существующий профиль, в центральной части окна консоли управления JMS отметьте этот профиль и в верхней панели нажмите **Свойства**.

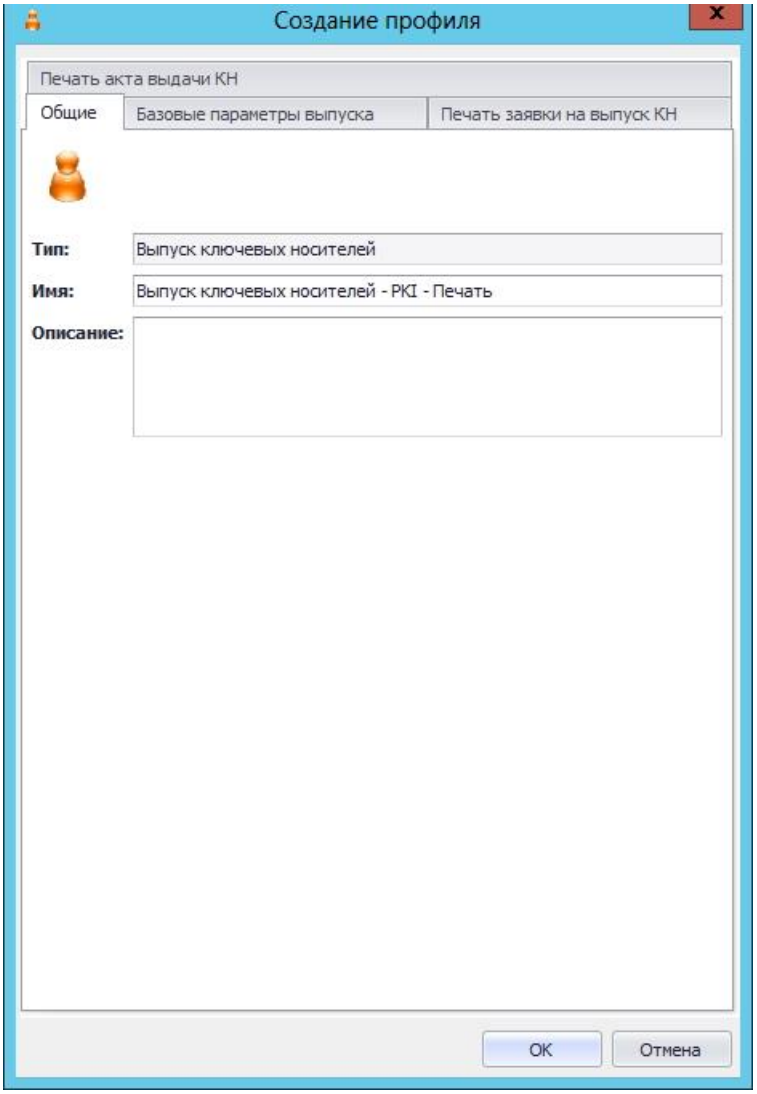


*Рис. 167 – Вкладка **Общие** свойств профиля настройки параметров выпуска ключевых носителей*

3. Введите необходимые данные (или измените существующие), после чего перейдите на вкладку **Базовые параметры выпуска**.

Окно примет следующий вид.

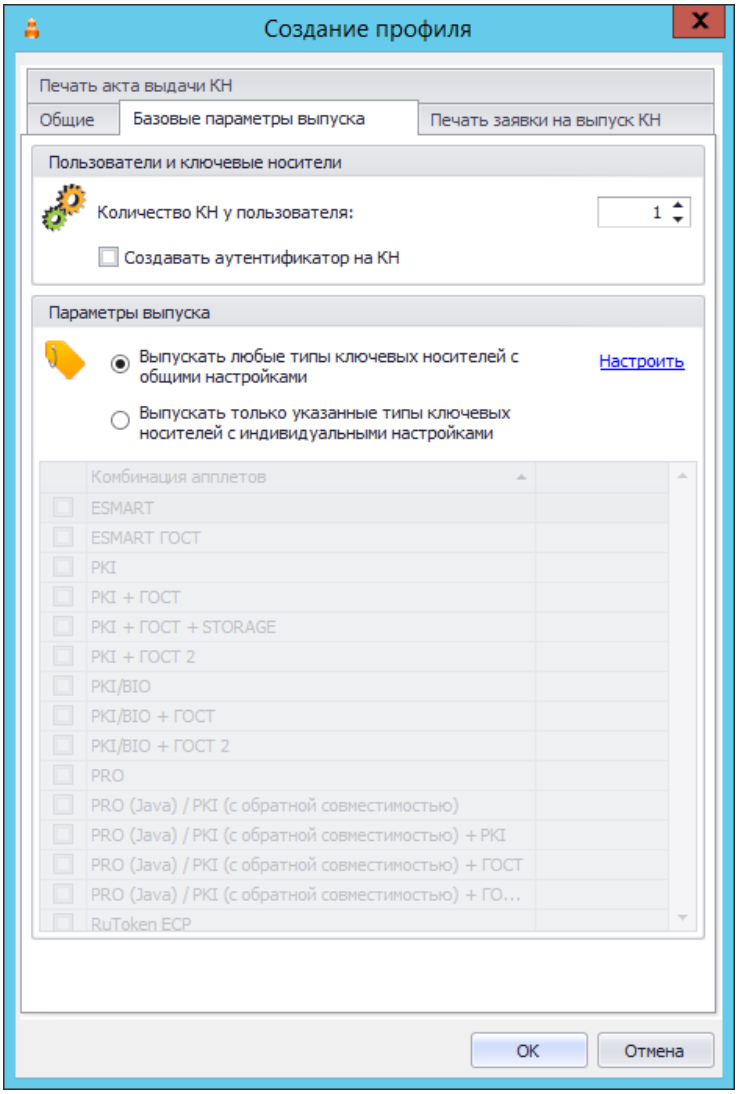


*Рис. 168 – Вкладка **Базовые параметры выпуска***

4. Выполните настройки, руководствуясь табл. 17.

Табл. 17 – Параметры выпуска электронных ключей

Настройка	Описание
Количество КН у пользователя	В поле следует указать максимальное количество электронных ключей, которое можно выпустить для одного пользователя
Создавать аутентификатор на КН	При установленной настройке на электронном ключе будет создаваться аутентификатор – ключевая пара, по которой осуществляется аутентификация пользователя в клиентском приложении JMS (Клиент JMS). **Примечания:** 1. Настройка доступна только в версии продукта JMS Enterprise Edition. 2. Если флаг не установлен, аутентификация в клиентском приложении (открытие сессии пользователя) с использованием электронного ключа, выпущенного по этому профилю, будет невозможна (необходимо будет использовать другие способы аутентификации).

Настройка	Описание
Выпускать любые типы ключевых носителей с общими настройками	В этом случае 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	Этот пункт позволяет задать индивидуальные настройки в зависимости от типа выпускаемого электронного ключа. Отметьте комбинации апплетов (приложений), соответствующие нужным вам моделям электронных ключей. • **PKI** - электронные ключи JaCarta с приложением PKI; • **PKI + ГОСТ** - электронные ключи JaCarta с приложениями PKI и ГОСТ; • **PKI + ГОСТ + STORAGE** - электронные ключи JaCarta с приложениями PKI, ГОСТ и STORAGE; • **PKI/BIO** - электронные ключи JaCarta с приложением PKI/BIO; • **PKI/BIO + ГОСТ** - электронные ключи JaCarta с приложениями PKI/BIO и ГОСТ; • **PRO** - электронные ключи eToken PRO; • **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; • **PRO (Java) / PKI (с обратной совместимостью) + ГОСТ** - электронные ключи eToken ГОСТ, а также электронные ключи JaCarta с приложениями PKI (с обратной совместимостью) и ГОСТ; 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.» • **RuToken ECP** – электронные ключи Рутокен ЭЦП; • **RuToken Lite** – электронные ключи Рутокен Lite; • **RuToken S** – электронные ключи Рутокен S; • **STORAGE** – электронные ключи JaCarta LT; • **ГОСТ** – электронные ключи eToken ГОСТ, а также электронные ключи JaCarta с приложением ГОСТ; • **ГОСТ + STORAGE** – электронные ключи JaCarta с приложениями ГОСТ и STORAGE; • **ГОСТ 2** – электронные ключи JaCarta ГОСТ 2, а также электронные ключи JaCarta с приложением ГОСТ 2; • **ФКН** – электронные ключи JaCarta CryptoPro; • **ESMART** – электронные ключи ESMART; • **ESMART ГОСТ** – электронные ключи ESMART ГОСТ. Чтобы настроить индивидуальные параметры выпуска, щелкните на ссылке **Настроить** напротив каждой комбинации апплетов (приложений).

Окно настроек параметров выпуска выглядит следующим образом.

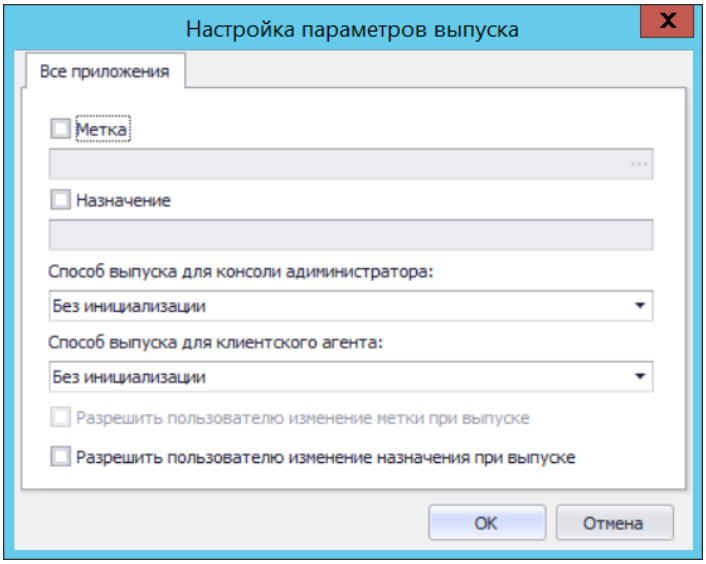


Рис. 169 – Окно настройки параметров выпуска

Если электронный ключ содержит несколько апплетов (приложений), то в отобразившемся окне будет несколько вкладок, как показано на рис. 170. Каждая вкладка соответствует апплету (приложению) в памяти электронного ключа. В этом случае необходимо выполнить настройку для каждого из этих апплетов (приложений).

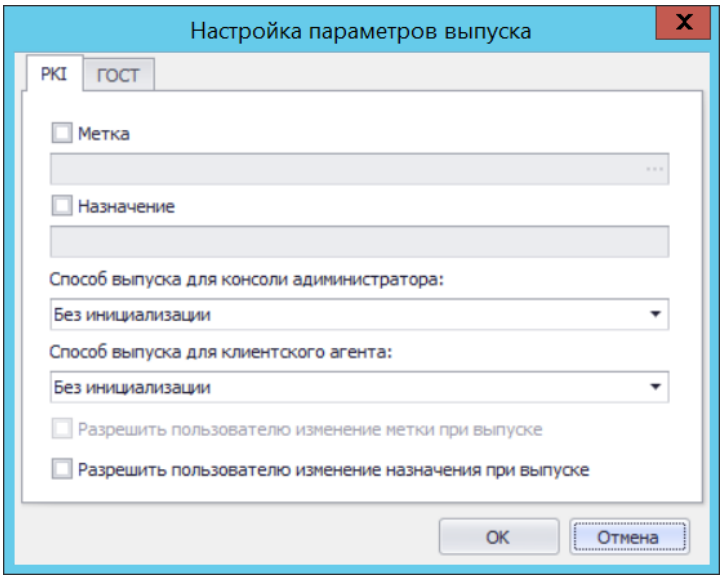


Рис. 170 – Окно настройки параметров выпуска электронных ключей с несколькими приложениями

5. Выполните необходимые настройки, руководствуясь табл. 18.

Табл. 18 – Настройка базовых параметров выпуска

Настройка	Описание
Метка	Позволяет задать метку выпускаемого электронного ключа.

Настройка	Описание
	В случае установки флага (**Метка**) вы можете ввести значение метки вручную или воспользоваться кнопкой [...]. В последнем случае отобразится окно, где 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.
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 (см. «Руководство администратора. Часть 1» [2], раздел «Смена языка пользовательского интерфейса JMS»).
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 электронных ключей», с. 458), 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. 164). 2. Если вы планируете взять под контроль JMS электронные ключи, выпущенные до установки и настройки JMS (см. «Взятие под управление электронных ключей», с. 458), вам следует выбрать пункт **Без инициализации**. В противном случае все существующие объекты в памяти электронного ключа будут удалены.
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. 164).
Разрешить пользователю изменение назначения при выпуске	Позволяет разрешить или запретить менять описание назначения электронного ключа в процессе самостоятельного выпуска пользователем.

6. 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. 304).
7. Последовательно нажмите **ОК** в окне настройки параметров выпуска и в окне настроек профиля, чтобы сохранить изменения.

3.9.3 Настройка профиля клиентского агента

Внимание! Профиль клиентского агента не предусмотрен в версии *CA Edition* продукта JMS (см. «Руководство администратора. Часть 1» [2], раздел «Версии поставки продукта и лицензионные опции»).

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. 296), 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 -> Профили**.
2. Выполните одно из следующих действий:

- если вы хотите создать новый профиль настроек клиентского агента, в центральной части окна консоли управления JMS отметьте **Настройки клиентского агента** и в верхней панели нажмите **Создать**;
- если вы хотите отредактировать существующий профиль, в центральной части окна консоли управления JMS отметьте этот профиль и в верхней панели нажмите **Свойства**.

Отобразится следующее окно.

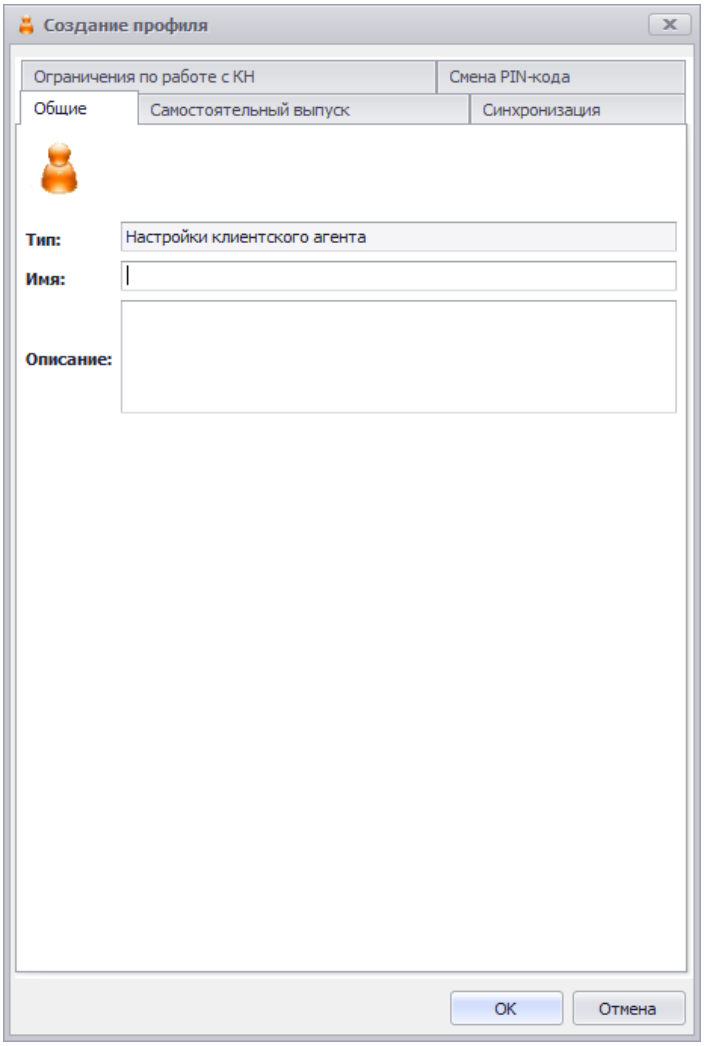


*Рис. 171 – Вкладка **Общие** свойств профиля настроек клиентского агента*

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

Окно примет следующий вид.

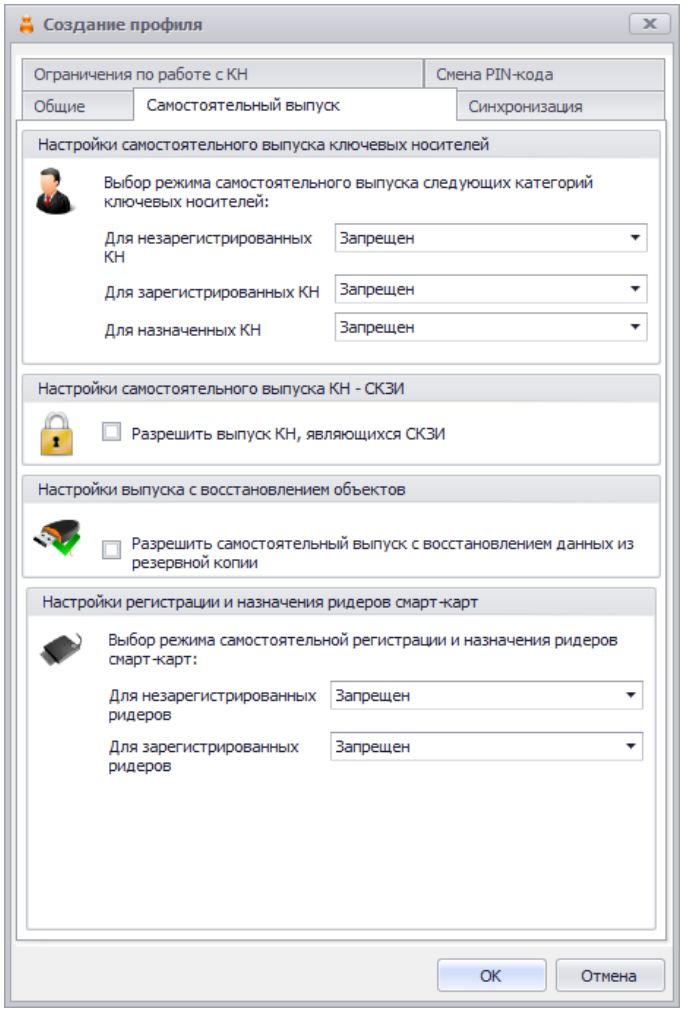


*Рис. 172 – Вкладка **Самостоятельный выпуск***

4. Выполните настройку, руководствуясь табл. 19.

Табл. 19 – 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 «JaCarta Management System. 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

Секция	Настройка	Описание
		не назначенных конкретным пользователям. Доступны следующие варианты: • **Запрещен** – пользователи не могут самостоятельно выпускать электронные ключи, зарегистрированные в JMS; • **Разрешен вручную** – пользователи могут вручную выпускать электронные ключи, на свое имя, если эти электронные ключи зарегистрированы в JMS (см. документ «JaCarta management System. 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 «JaCarta Management System. 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. 314)	**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 клиентский агент JMS, пользователи смогут выпускать электронные ключи в режиме восстановления данных.
Настройки регистрации и назначения ридеров смарт-карт	**Для незарегистрированных ридеров**	Доступны следующие варианты выбора режима настройки: • **Запрещен** – пользователь не может самостоятельно назначить себе карт-ридер, не зарегистрированный в JMS; • **Разрешен вручную** – пользователь на свое имя может назначить подключенный карт-ридер. Предварительная регистрация ридера при данной опции выполняется автоматически; • **Разрешен автоматически** – карт-ридера на имя пользователя, вошедшего в систему, произойдет автоматически после подсоединения этого карт-ридера к компьютеру.

Секция	Настройка	Описание
	Для зарегистрированных ридеров	Доступны следующие варианты выбора режима настройки: • **Запрещен** – пользователь не может самостоятельно назначить себе карт-ридер, зарегистрированный в JMS; • **Разрешен вручную** – пользователь на свое имя может назначить подключенный карт-ридер, если только он не был назначен другому пользователю администратором JMS из консоли управления; **Примечание**. В случае если подключенный к пользовательскому компьютеру карт-ридер ранее был уже назначен другому пользователю, текущий пользователь не сможет назначить данный ридер на свое имя из клиентского агента, пока прежнее назначение не будет отменено администратором из консоли управления JMS. • **Разрешен автоматически** – назначение зарегистрированного карт-ридера на имя пользователя, вошедшего в систему, произойдет автоматически после подсоединения этого карт-ридера к компьютеру.

5. Перейдите на вкладку **Синхронизация**.

Окно примет следующий вид.

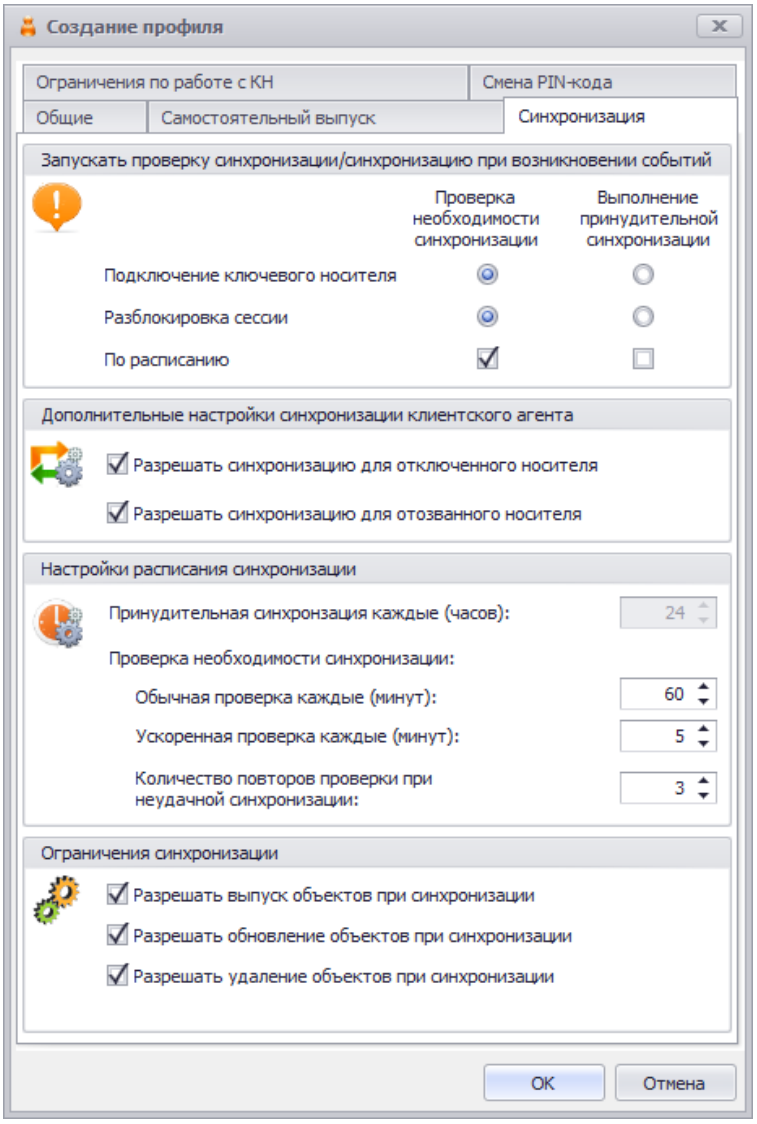


*Рис. 173 – Вкладка **Синхронизация***

6. Выполните необходимые настройки, руководствуясь табл. 20.

Табл. 20 – Настройки автоматической синхронизации

Настройка	Описание
<Секция> **Запускать проверку синхронизации /синхронизацию при возникновении событий**	

Настройка	Описание	
	<Столбец> **Проверка необходимости синхронизации** Под «проверкой необходимости синхронизации» понимается как сама проверка, так и выполнение такой синхронизации. Действия в данном столбце выполняются только при условии, что произошли изменения на стороне сервера JMS (например, в профиле типа **Выпуск ключевых носителей** или в профилях выпуска сертификатов). **Примечание.** В случае обнаружения необходимости обновления сертификата на электронном ключе данный сертификат будет обновлён, подробнее см. раздел «Настройка автоматического перевыпуска сертификата на электронном ключе», с. 312	<Столбец> **Выполнение принудительной синхронизации** Действия в данном столбце выполнятся независимо от появления изменений на стороне сервера JMS. Производимые действия аналогичны нажатию на ссылку **Синхронизировать** для соответствующего электронного ключа в клиенте JMS, благодаря чему объекты, содержащиеся в электронном ключе, будут зарегистрированы (взяты под управление) на сервере JMS. **Важно!** 1. Частая принудительная синхронизация электронного ключа может приводить к его преждевременному износу. 2. Регулярная принудительная синхронизация ведет к повышенной нагрузке на сервер JMS и требует специального анализа для предотвращения состояния отказа в обслуживании.
Подключение ключевого носителя	Синхронизация запускается при подсоединении к компьютеру электронного ключа (установите необходимый тип синхронизации с помощью элемента «радиокнопка»)	то же
Разблокировка сессии	Синхронизация производится по факту разблокировки пользовательского сеанса Windows (установите необходимый тип синхронизации с помощью элемента «радиокнопка»)	то же
По расписанию	Синхронизация проводится по расписанию. (Установите флаг, если требуется синхронизация с предварительной проверкой ее необходимости. Настройка расписания осуществляется в секции **Настройки расписания синхронизации**)	Синхронизация проводится по расписанию. (Установите флаг, если требуется безусловная синхронизация. Настройка расписания осуществляется в секции **Настройки расписания синхронизации**, в подсекции **Проверка необходимости синхронизации**)
<Секция> **Дополнительные настройки синхронизации клиентского агента**		
Разрешать синхронизацию для отключенного носителя	Позволяет применять синхронизации к электронным ключам, действие которых было приостановлено	
Разрешать синхронизацию для отозванного носителя	Позволяет применять синхронизацию к электронным ключам, которые были отозваны	

Настройка	Описание
<Секция> **Настройки расписания синхронизации**	
Принудительная синхронизация каждые (часов)	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/синхронизацию при возникновении событий** включена настройка **По расписанию** в столбце **Выполнение принудительной синхронизации**
<Подсекция > **Проверка необходимости синхронизации**	
Обычная проверка 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/синхронизацию при возникновении событий** включена настройка **По расписанию** в столбце **Проверка необходимости синхронизации**
Ускоренная проверка 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/синхронизацию при возникновении событий** включена настройка **По расписанию** в столбце **Проверка необходимости синхронизации**
Количество повторов проверки при неудачной синхронизации	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/синхронизацию при возникновении событий** включена настройка **По расписанию** в столбце **Проверка необходимости синхронизации**
<Секция > **Ограничения синхронизации**	
Разрешать выпуск объектов при синхронизации	Позволяет выпускать записывать объекты в память электронного ключа во время синхронизации
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**.

Окно примет следующий вид.

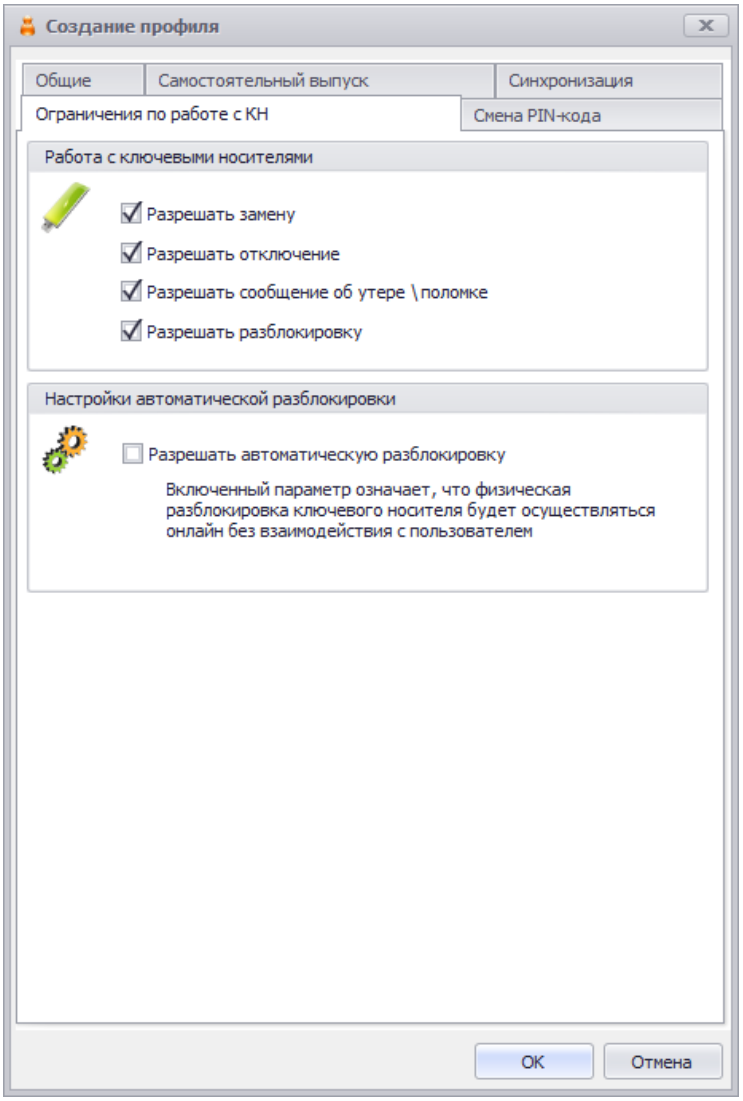


*Рис. 174 – Вкладка **Ограничения по работе с КН***

8. Выполните настройку, руководствуясь табл. 21.

Табл. 21 – 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

Секция	Настройка	Описание
		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. 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**.

9. Перейдите на вкладку **Смена PIN-кода**.

Окно примет следующий вид.

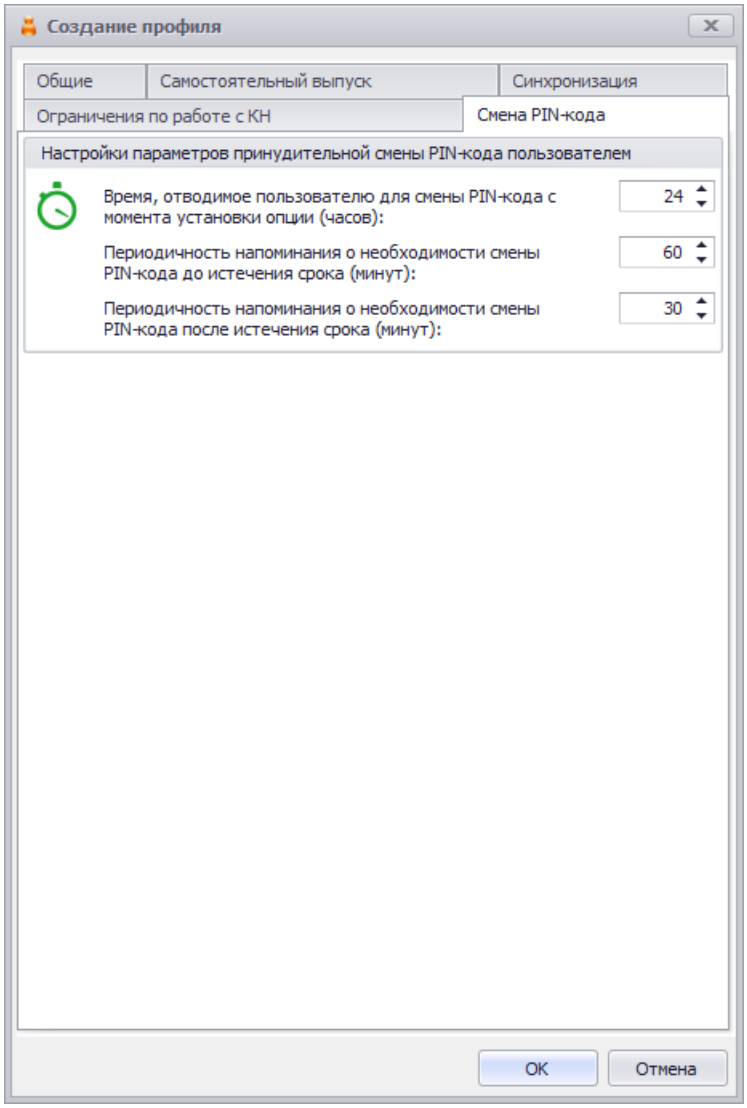


*Рис. 175 – Вкладка **Смена PIN-кода***

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.

3.9.4 Настройки параметров инициализации

3.9.4.1 eToken Pro (Java) / JaCarta PKI (с обратной совместимостью), eToken Pro (Card OS)

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

2. Выполните одно из следующих действий:

   – чтобы создать новый профиль, выберите нужный тип профиля (**Инициализация eToken Pro (Java) / JaCarta PKI (с обратной совместимостью)** или **Инициализация eToken Pro (Card OS)**) и в верхней панели нажмите **Создать**.
   – чтобы изменить существующий профиль, отметьте этот профиль (например, **Инициализация eToken Pro (Java) / JaCarta PKI (с обратной совместимостью) по умолчанию** или **Инициализация eToken Pro (Card OS) – по умолчанию**) в центральной части окна консоли управления JMS, после чего в верхней панели нажмите **Свойства**.

   Отобразится окно следующего вида.

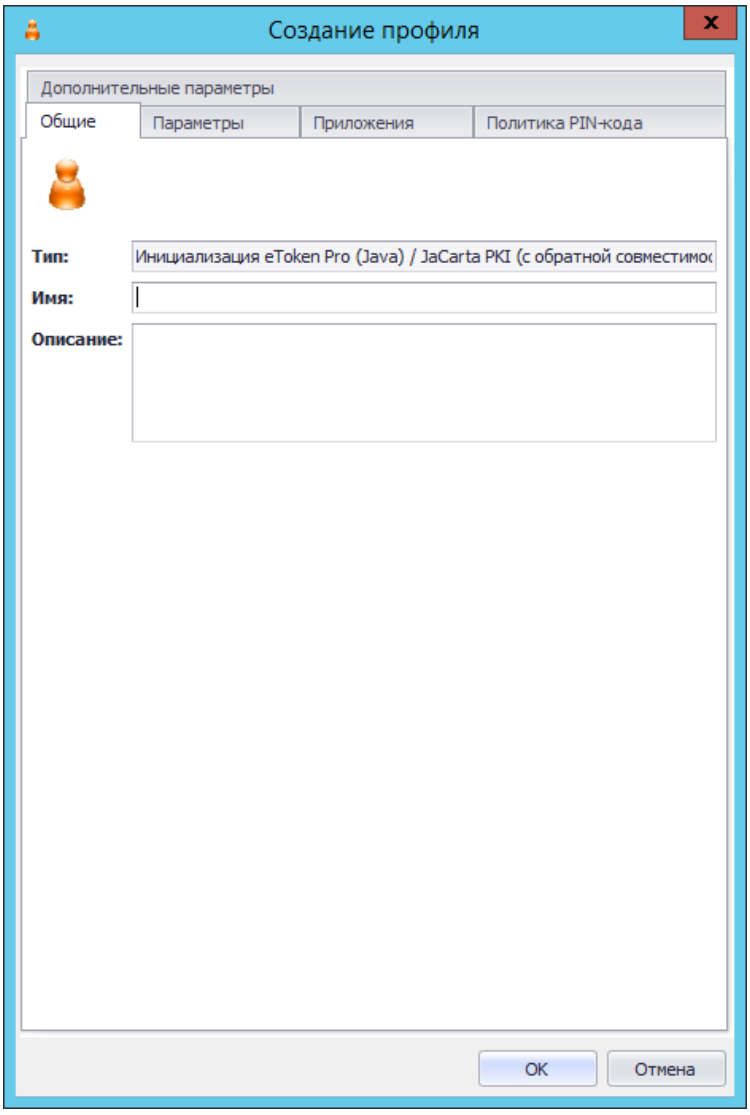


*Рис. 176 – Вкладка **Общие** свойств профиля инициализации*

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

Окно примет следующий вид.

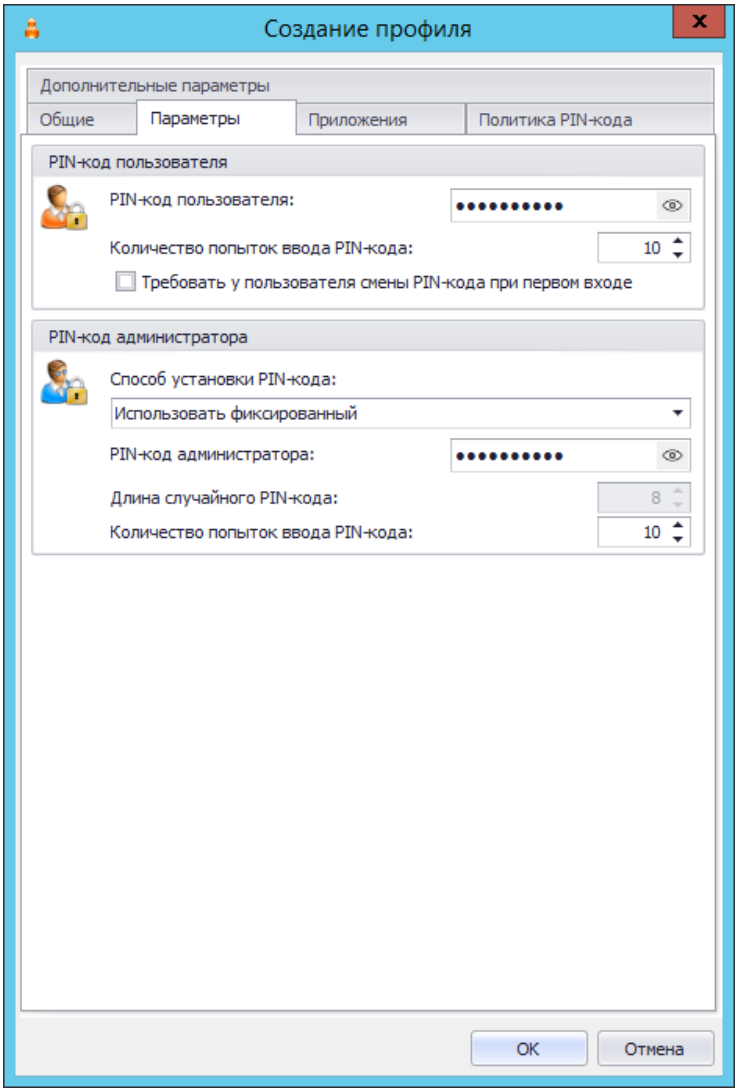


*Рис. 177 – Вкладка **Параметры** окна свойств профиля инициализации*

4. Выполните необходимые настройки, руководствуясь табл. 22.

Табл. 22 - 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.

Секция	Настройка	Описание
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 **Приложения**.

Окно примет следующий вид.

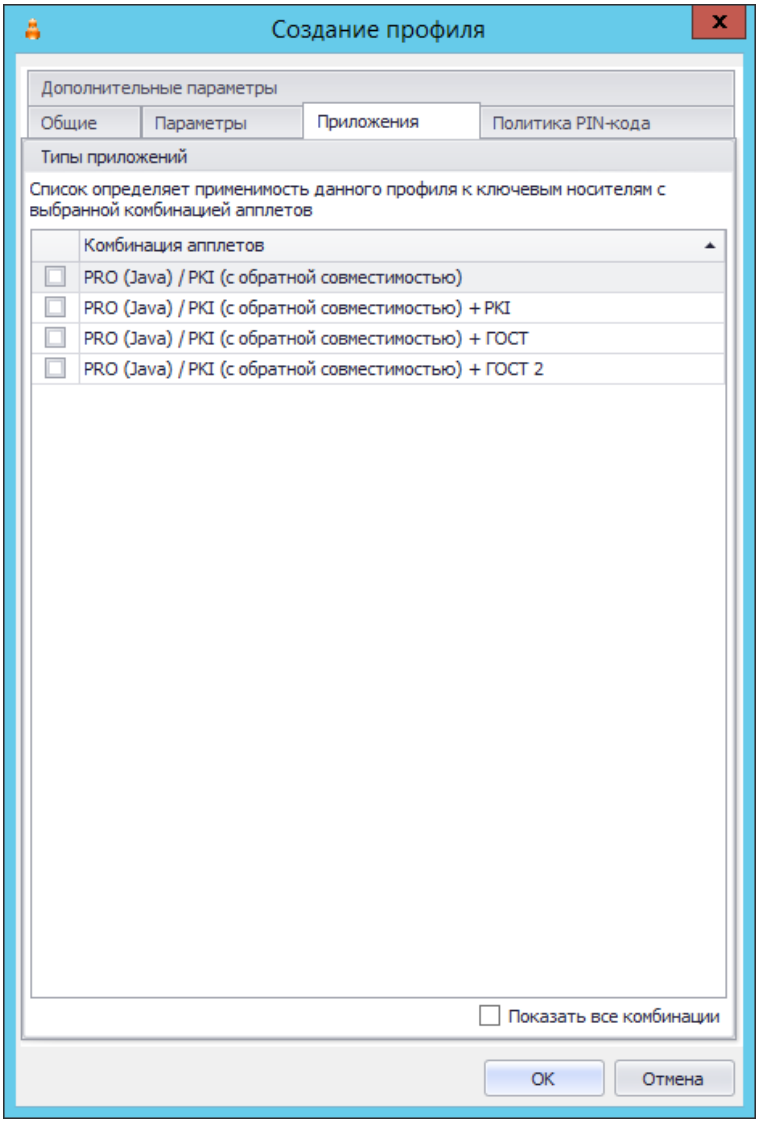


Рис. 178 – Список приложений

6. Отметьте нужные комбинации приложений, после чего перейдите на вкладку **Политика PIN-кода**.

Окно примет следующий вид.

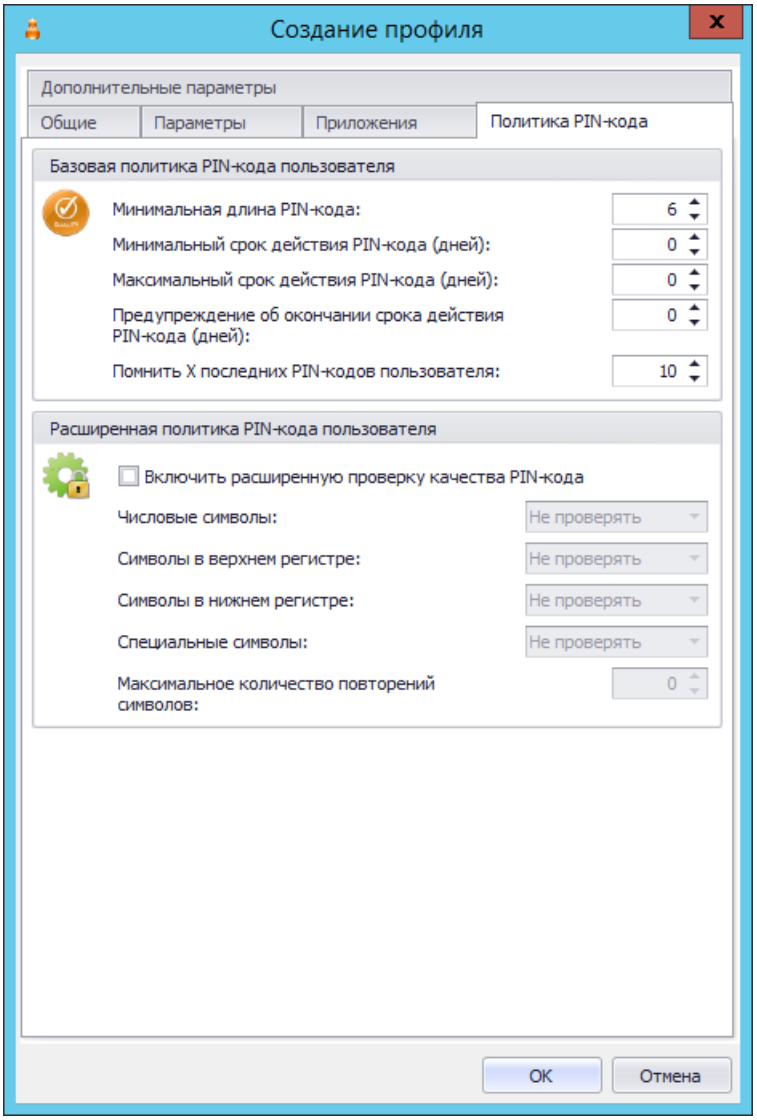


*Рис. 179 – Вкладка **Политика PIN-кода** окна свойств профиля инициализации*

7. Выполните необходимые настройки, руководствуясь табл. 23.

Табл. 23 – 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.

Секция	Настройка	Описание
	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.
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;

Секция	Настройка	Описание
		• **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: • **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.

8. Перейдите на вкладку **Дополнительные параметры**.

Окно примет следующий вид.

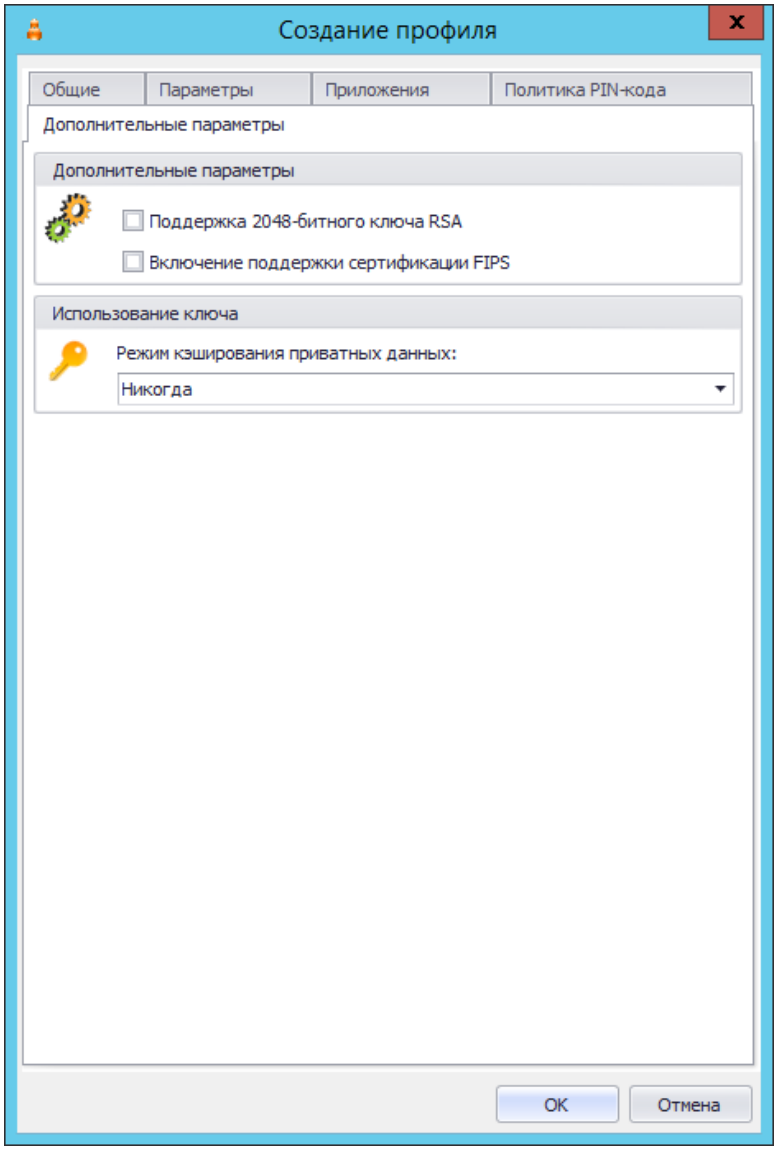


*Рис. 180 – Вкладка **Дополнительные параметры** окна свойств профиля инициализации*

9. Выполните необходимые настройки, руководствуясь табл. 24.

Табл. 24 – Настройка дополнительных параметров инициализации электронных ключей

Настройка	Описание
Поддержка 2048-битного ключа RSA	Установите этот флаг для поддержки 2048-битных ключей RSA. Настройка актуальна только для электронных ключей eToken PRO (Card OS) – у остальных моделей электронных ключей такая поддержка всегда включена.
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 управления и использования компьютерных и телекоммуникационных систем связи.

Настройка	Описание
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.

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

3.9.4.2 JaCarta PKI, JaCarta PKI/BIO

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

   – чтобы создать новый профиль, выберите нужный тип профиля (**Инициализация JaCarta PKI** или **Инициализация JaCarta PKI/BIO**) и в верхней панели нажмите **Создать**.
   – чтобы изменить существующий профиль, отметьте этот профиль (например, **Инициализация JaCarta PKI по умолчанию** или **Инициализация JaCarta PKI/BIO по умолчанию**) в центральной части окна консоли управления JMS, после чего в верхней панели нажмите **Свойства**.

Отобразится следующее окно.

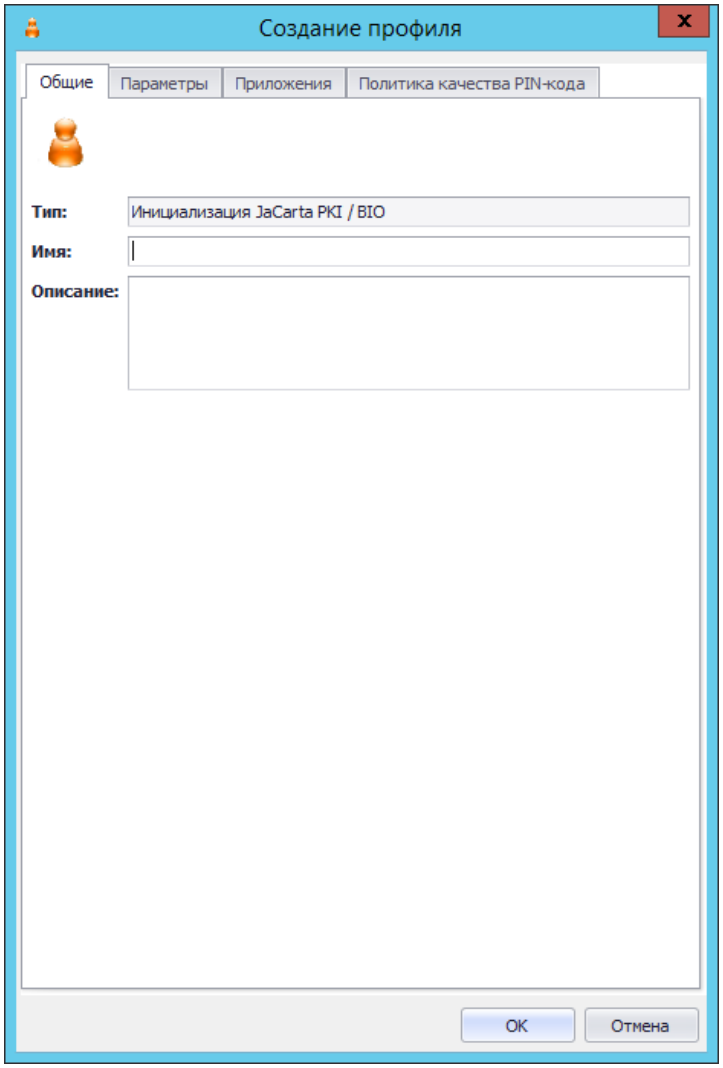


*Рис. 181 – Вкладка **Общие***

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

Окно примет следующий вид.

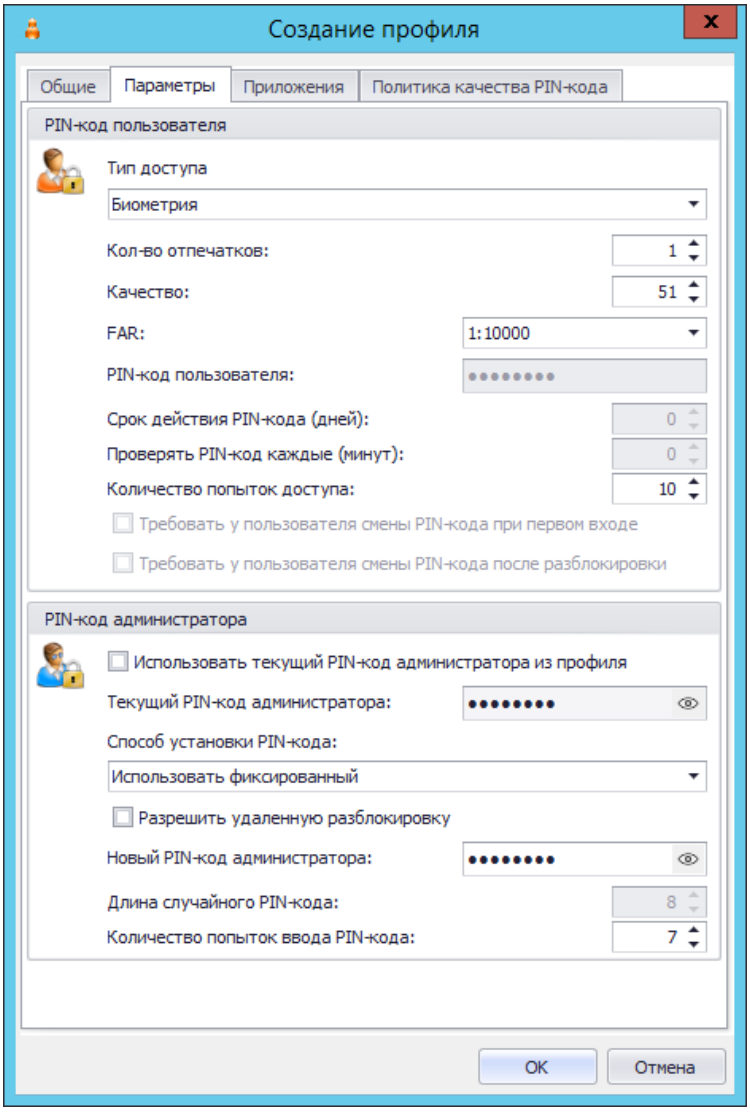


*Рис. 182 – Вкладка **Параметры***

Настройки **Тип доступа**, **Кол-во отпечатков**, **Качество** и **FAR** (false acceptance rate - вероятность ложного доступа) отображаются, только если вы редактируете профиль инициализации JaCarta PKI/BIO.

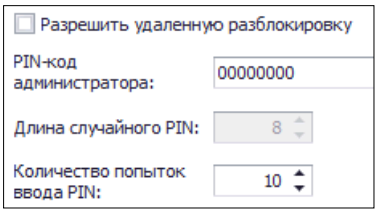
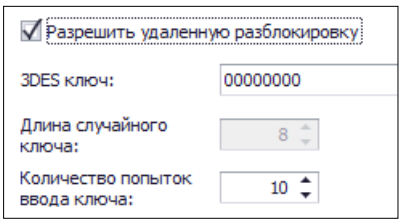
4. Выполните настройку, руководствуясь табл. 25.

Табл. 25 - Настройка параметров инициализации

Секция	Настройка	Описание
PIN-код пользователя	**Тип доступа**	Позволяет выбрать из списка четыре варианта: • **PIN** – для аутентификации пользователь должен ввести только PIN-код пользователя электронного ключа, биометрическая аутентификации может быть включена только при следующей инициализации электронного ключа; • **Биометрия** – аутентификация пользователя происходит по результату сканирования отпечатка пальца пользователя, PIN-код пользователя при аутентификации не задействуется; • **PIN или Биометрия** – для аутентификации пользователю нужно выполнить одно из двух: либо ввести PIN-код пользователя электронного ключа, либо приложить палец к сканеру отпечатков – если хотя бы один из этих методов успешен, пользователь проходит аутентификацию;

Секция	Настройка	Описание
		• **PIN и Биометрия** – для аутентификации пользователь должен как ввести PIN-код пользователя, так и приложить палец к сканеру отпечатков пальцев. Настройка отображается при редактировании профилей инициализации электронных ключей с возможностью биометрической аутентификации.
	Кол-во отпечатков	Определяет максимальное количество отпечатков пальцев пользователя, которое можно сохранить в памяти электронного ключа JaCarta (от 1 до 10). В каждом конкретном случае пользователь сможет выбрать, какой отпечаток пальца использовать при аутентификации. Настройка отображается при редактировании профилей инициализации электронных ключей с возможностью биометрической аутентификации. Минимальное рекомендуемое значение: 2.
	Качество	Определяет граничное значение качества изображения. Если качество изображения ниже данного значения, сохранение отпечатков пальцев пользователя не будет производиться. Допустимые значения – от 1 до 100. Чем больше установленное значение, тем больше попыток может потребоваться пользователю, чтобы сохранить отпечаток в памяти электронного ключа или аутентифицироваться по результатам сканирования отпечатка пальца. Значение по умолчанию: 51. Настройка отображается при редактировании профилей инициализации электронных ключей с возможностью биометрической аутентификации.
	FAR	False Acceptance Rate (Вероятность ложного допуска) - определяет вероятность ложного допуска (т.е. вероятность, с которой система считывания отпечатков пальцев ошибочно аутентифицирует пользователя). Вероятность ложного допуска определяется как соотношение возможного количества ошибочной идентификации к числу попыток аутентификации. Соответственно, вероятность должного допуска 1:100 выше, чем вероятность ложного допуска 1:1000. Настройка отображается при редактировании профилей инициализации электронных ключей с возможностью биометрической аутентификации.
	PIN-код пользователя	Позволяет задать значение PIN-кода пользователя. Настройка не активна при выбранной настройке Тип доступа – Биометрия.
	Срок действия PIN-кода	Число дней, спустя которое пользователь должен будет сменить PIN-код пользователя.
	Проверять PIN-код каждые	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.

Секция	Настройка	Описание
	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.
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. (см. также «Установка в БД PIN-кода администратора для приложения электронного ключа», с. 109)
	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**.

Секция	Настройка	Описание
	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). • 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.

5. Перейдите на вкладку **Приложения**.

Окно примет следующий вид.

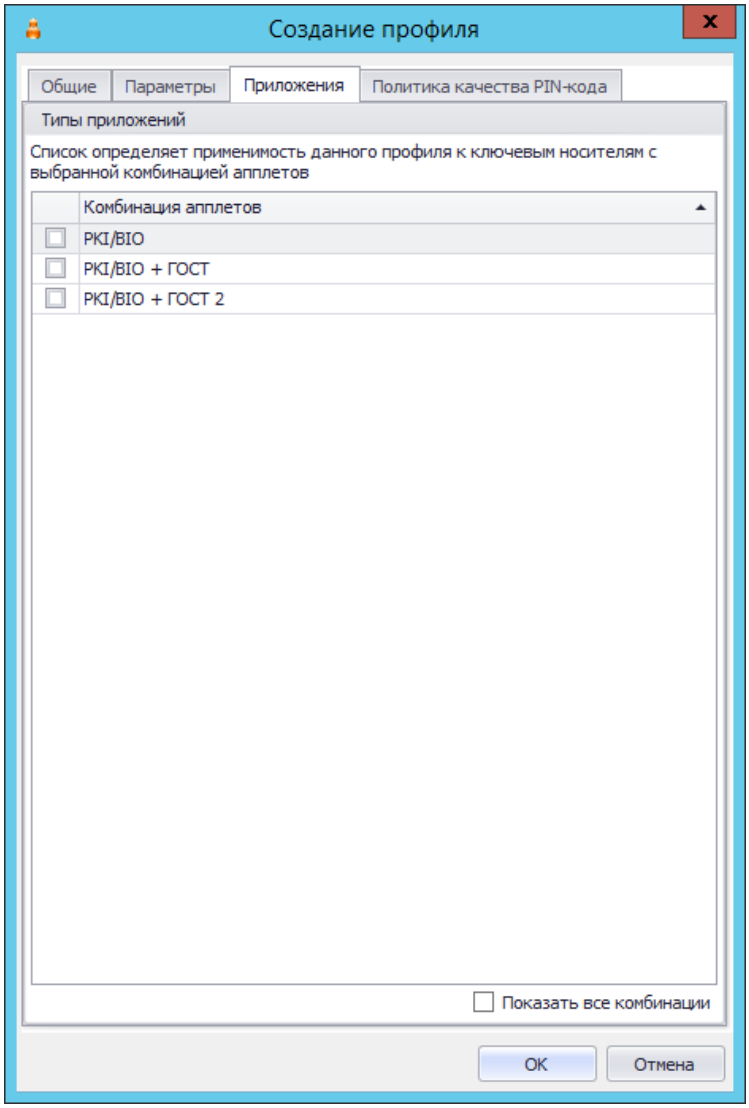


*Рис. 183 – Вкладка **Приложения***

6. Отметьте нужные комбинации приложений, после чего переходите на вкладку **Политика качества PIN-кода**.

Окно примет следующий вид.

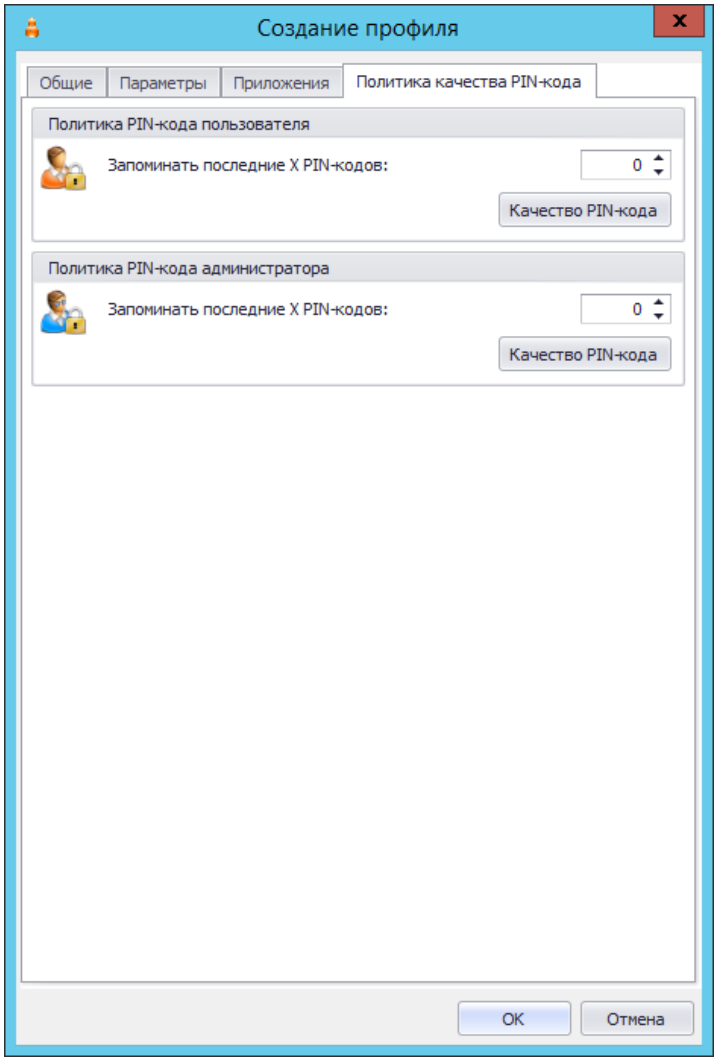


*Рис. 184 – Вкладка **Политика качества PIN-кода***

7. Эта вкладка позволяет настроить качество PIN-кодов, используемых с электронными ключами, которые будут инициализированы с настраиваемым профилем.
8. Выполните настройку, руководствуясь табл. 26.

Табл. 26 – Политики качества PIN-кодов

Секция	Настройка	Описание
Политика PIN-кода пользователя / Политика 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.
	Качество PIN-кода	При нажатии на кнопку отображается окно, которое позволяет настроить качество PIN-кода (см. следующий шаг настоящей процедуры).

9. Чтобы настроить качество PIN-кода, в нужной секции нажмите **Качество PIN-кода**.

Настройки для каждого типа PIN-кода (PIN-код пользователя, PIN-код администратора) аналогичны – в настоящем руководстве для примера будет приведена настройка качества PIN-кода пользователя.

Отобразится следующее окно.

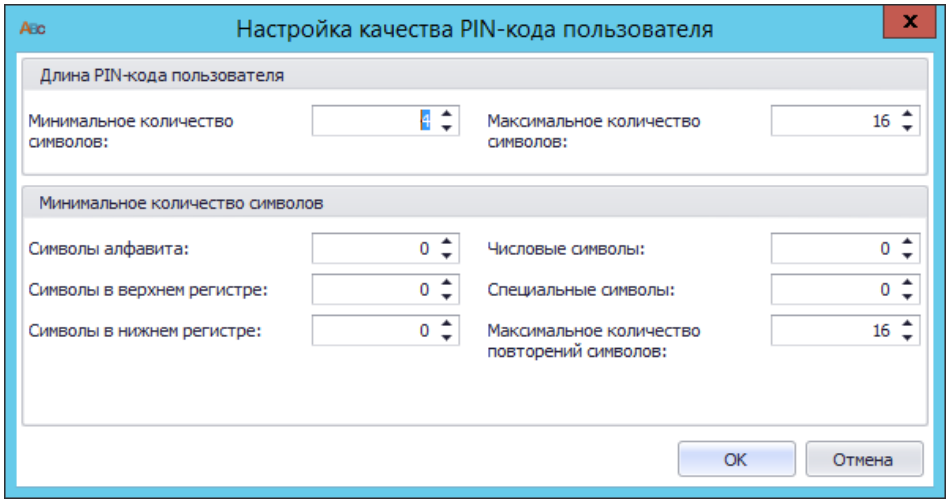


*Рис. 185 – **Настройка качества PIN-кода пользователя***

10. Выполните настройку, руководствуясь табл. 27.

Табл. 27 – Настройка качества PIN-кода

Секция	Настройка	Описание
Длина PIN-кода пользователя/ администратора	**Минимальное количество символов**	Позволяет задать минимальное необходимое число символов в PIN-коде.
	Максимальное количество символов	Позволяет задать максимальное возможное число символов в PIN-коде.
Минимальное количество символов	**Символы алфавита**	Позволяет задать минимальное необходимое число символов алфавита в PIN-коде.
	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.

11. При необходимости настройте параметры другого PIN-кода, после чего последовательно нажмите **OK**, чтобы закрыть окно настройки качества PIN-кода и окно настройки профиля инициализации.

3.9.4.3 JaCarta ГОСТ / eToken ГОСТ

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

   – чтобы создать новый профиль, выберите нужный тип профиля (**Инициализация JaCarta ГОСТ/eToken ГОСТ**) и в верхней панели нажмите **Создать**.
   – чтобы изменить существующий профиль, отметьте этот профиль (например, **Инициализация JaCarta ГОСТ/eToken ГОСТ по умолчанию**) в центральной части окна консоли управления JMS, после чего в верхней панели нажмите **Свойства**.

   Отобразится следующее окно.

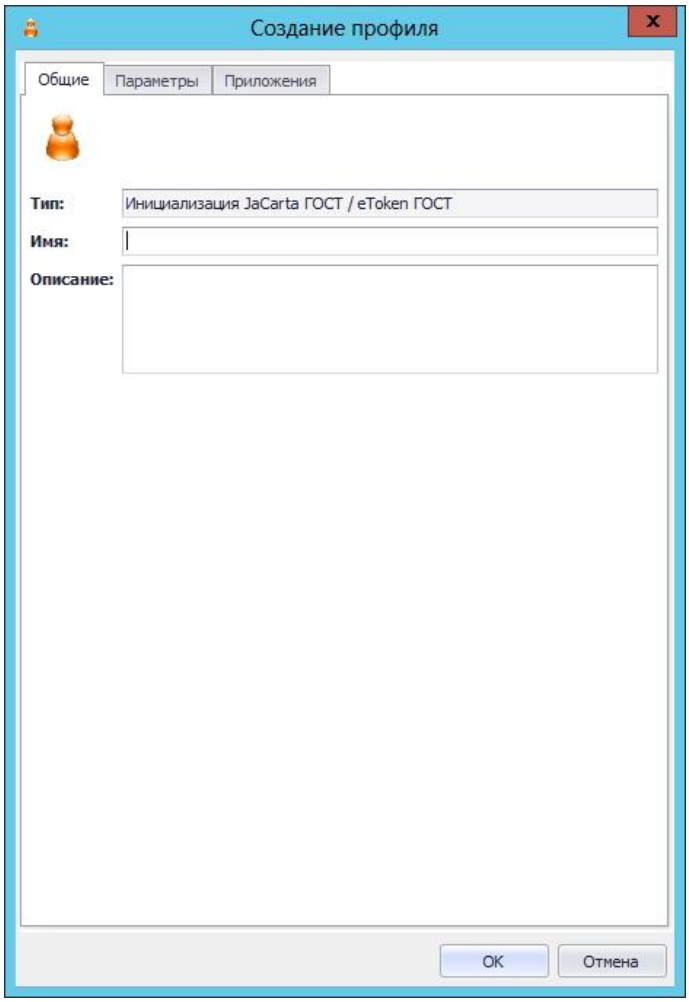


*Рис. 186 – Вкладка **Общие***

3. В соответствующих полях введите (или отредактируйте) имя и описание профиля, после чего выберите вкладку **Параметры**.

Окно примет следующий вид.

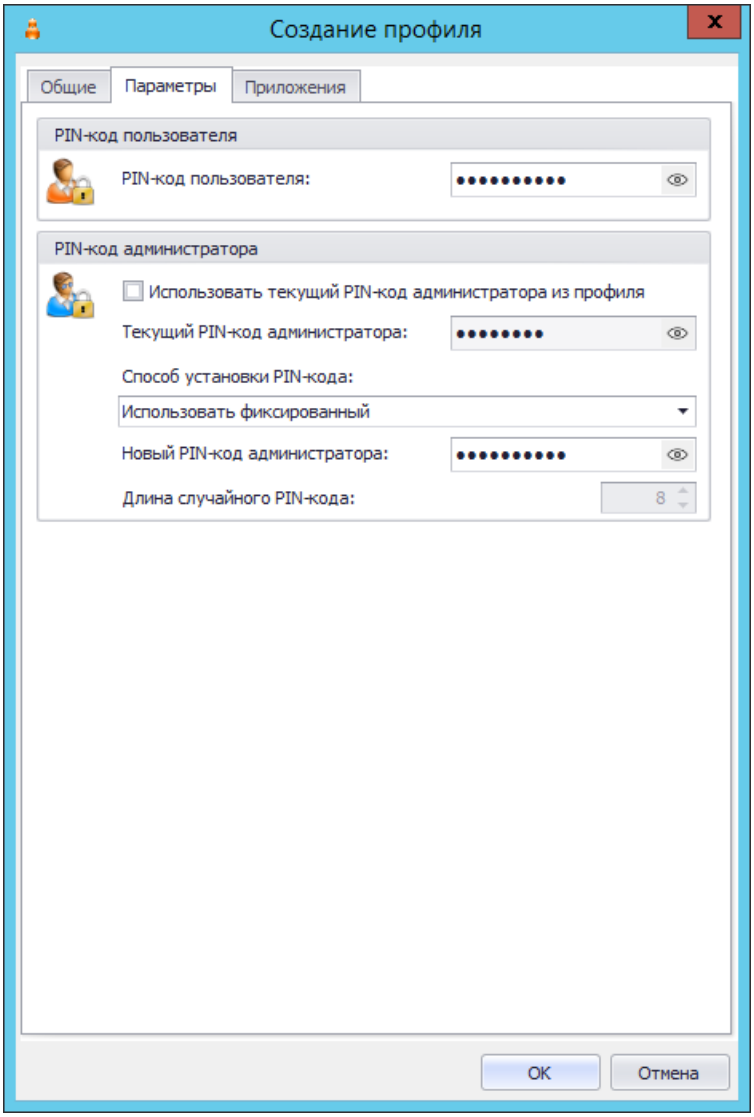


Рис. 187 – Вкладка Параметры

4. Выполните настройку, руководствуясь табл. 28.

Табл. 28 – Настройка параметров профиля инициализации

Секция	Настройка	Описание
PIN-код пользователя	**PIN-код пользователя**	Позволяет задать PIN-код 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

Секция	Настройка	Описание
		умолчанию, недоступен администратору для настройки). **Примечание.** При применении профиля к ранее 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. (см. также «Установка в БД PIN-кода администратора для приложения электронного ключа», с. 109)
	Текущий PIN-код администратора	Поле позволяет указать текущий PIN-код администратора в электронном ключе. Используется только при включенном флаге **Использовать текущий PIN-код администратора из профиля**
	Способ установки PIN-кода	Этот список позволяет задать способ формирования PIN-кода администратора: • **Использовать фиксированный** – необходимо указать значение PIN-кода в поле **PIN-код администратора**; • **Генерировать случайный** – необходимо указать длину случайного PIN-кода, используя настройку **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	Если в списке **Способ установки PIN-кода** был выбран пункт **Генерировать случайный**, то эта настройка позволяет задать длину случайного PIN-кода администратора.

5. Перейдите на вкладку **Приложения**.

Окно примет следующий вид.

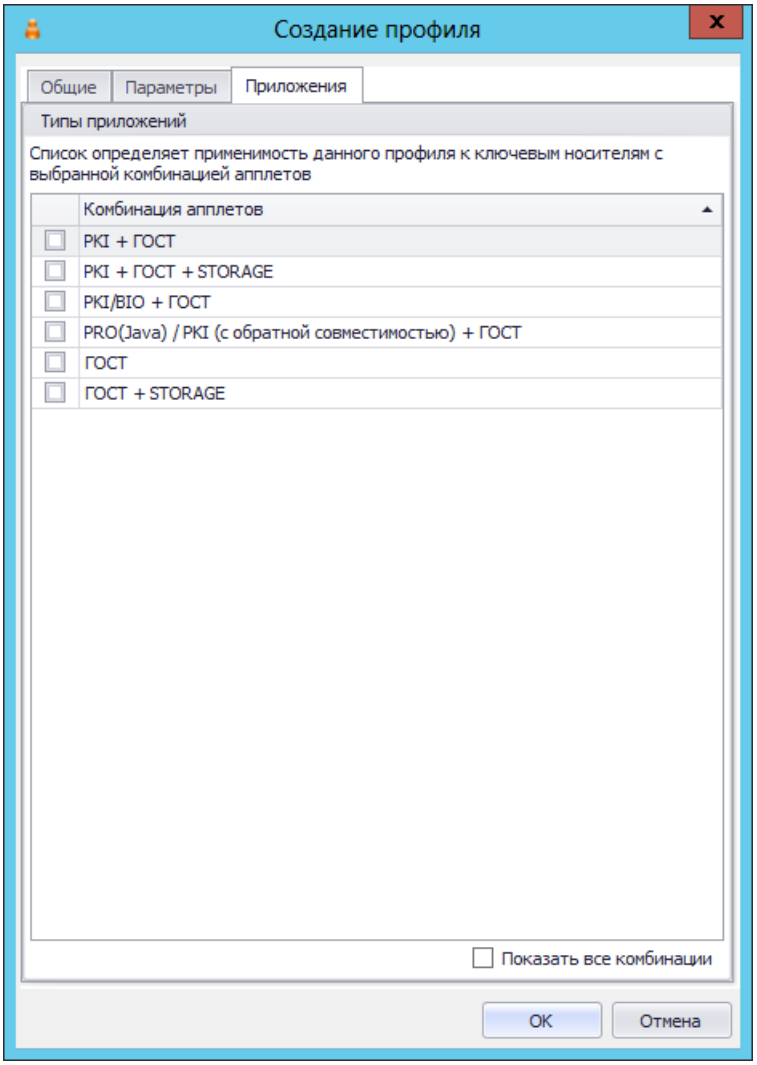


*Рис. 188 – Вкладка **Приложения***

6. Отметьте нужные комбинации приложений, после чего нажмите **OK**, чтобы завершить процедуру.

3.9.4.4 RuToken S/RuToken ЭЦП/ RuToken ЭЦП 2.0/ RuToken Lite

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

   – чтобы создать новый профиль, выберите нужный тип профиля (**Инициализация RuToken S**, **RuToken ЭЦП/ЭЦП 2.0** или **RuToken Lite**) и в верхней панели нажмите **Создать**.
   – чтобы изменить существующий профиль, отметьте этот профиль (например, **Инициализация RuToken S по умолчанию**, **RuToken ЭЦП/ЭЦП 2.0 по умолчанию** или **RuToken Lite по умолчанию**) в центральной части окна консоли управления JMS, после чего в верхней панели нажмите **Свойства**.

Отобразится следующее окно.

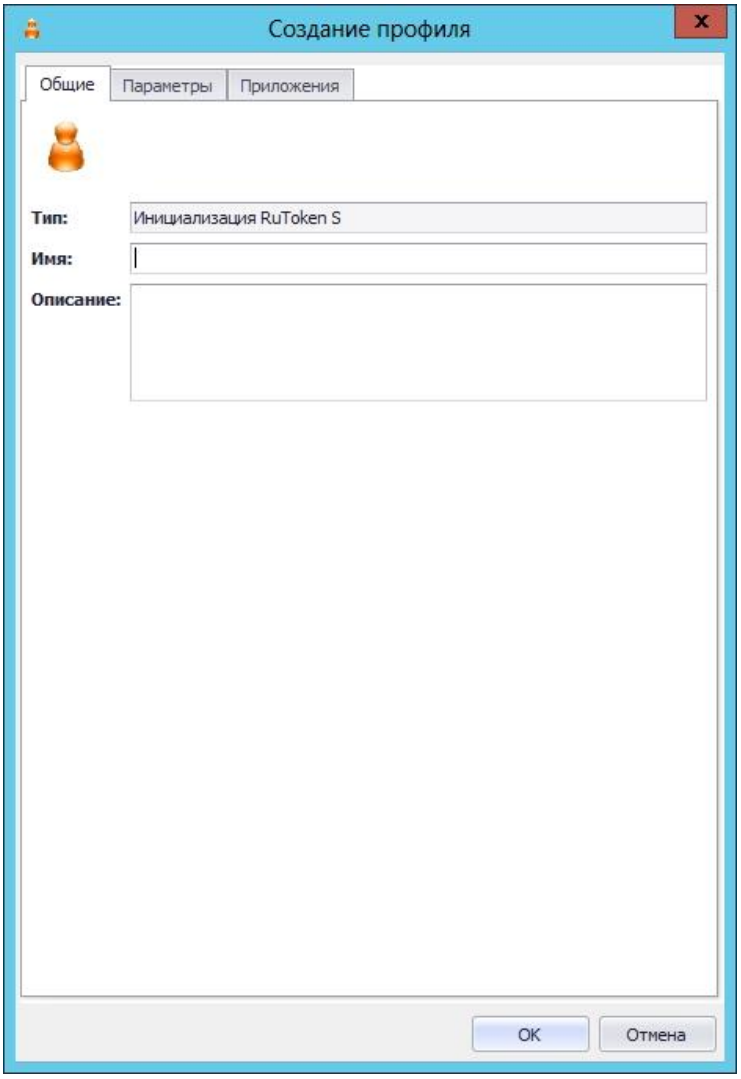


*Рис. 189 – Вкладка **Общие***

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

Окно примет следующий вид.

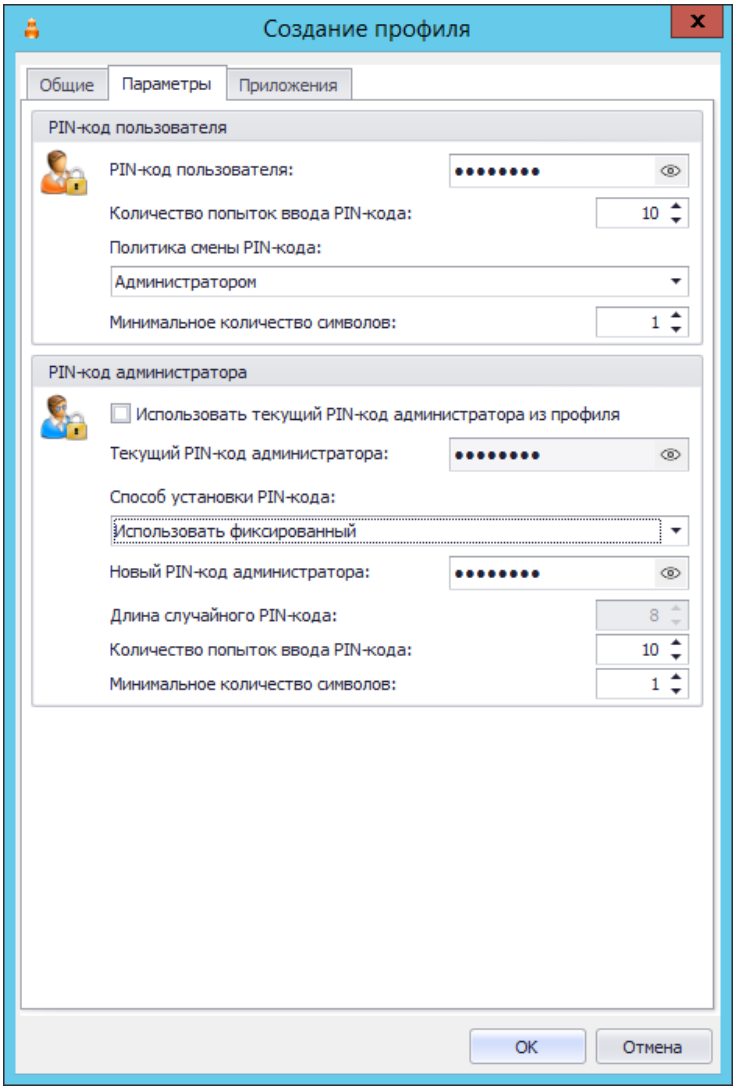


*Рис. 190 – Вкладка **Параметры***

4. Выполните настройку, руководствуясь табл. 29.

Табл. 29 – Настройка параметров инициализации

Секция	Настройка	Описание
PIN-код пользователя	**PIN-код пользователя**	Позволяет задать значение PIN-кода пользователя.
	Количество попыток ввода PIN-кода	Максимальное число попыток ввода неверного PIN-кода пользователя, по достижении которого PIN-код пользователя на электронном ключе блокируется.
	Политика смены PIN-кода	Определяет, какой PIN-код надо предъявить для смены текущего PIN-кода пользователя. Доступны следующие варианты: • **Администратором** – для смены PIN-кода пользователя необходимо предъявить PIN-код администратора; • **Пользователем** – для смены PIN-кода пользователя необходимо предъявить PIN-код пользователя;

Секция	Настройка	Описание
		• **Пользователем и Администратором** – для смены PIN-кода пользователя можно предъявить как PIN-код пользователя, так и PIN-код администратора. Если выбрана настройка **Пользователем**, удаленная разблокировка электронного ключа с использованием PIN-кода администратора будет невозможна.
	Минимальное количество символов	Позволяет задать минимальное число символов для 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. (см. также «Установка в БД PIN-кода администратора для приложения электронного ключа», с. 109)
	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-код администратора, если в списке **Способ установки PIN-кода** был выбран пункт **Генерировать случайный**.

Секция	Настройка	Описание
	Количество попыток ввода PIN-кода	Максимальное число попыток ввода неверного PIN-кода администратора, по достижении которого PIN-код администратора на электронном ключе блокируется.
	Минимальное количество символов	Позволяет задать минимальное количество символов для PIN-кода администратора.

5. Перейдите на вкладку **Приложения**.
   Окно примет следующий вид.

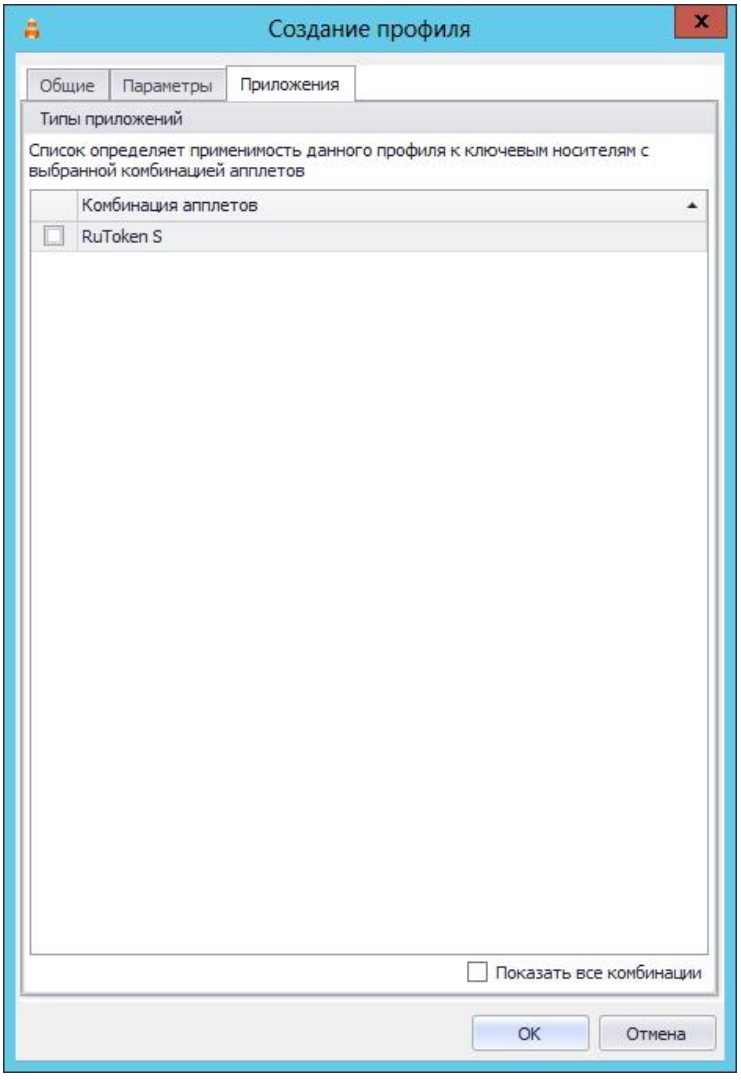


*Рис. 191 – Вкладка **Приложения***

6. Отметьте пункт нужного приложения и нажмите **OK**, чтобы сохранить изменения.

3.9.4.5 Datastore

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

   – чтобы создать новый профиль, выберите нужный тип профиля (**Инициализация Datastore**) и в верхней панели нажмите **Создать**.

– чтобы изменить существующий профиль, отметьте этот профиль (например, **Инициализация Datastore по умолчанию**) в центральной части окна консоли управления JMS, после чего в верхней панели нажмите **Свойства**.

Отобразится следующее окно.

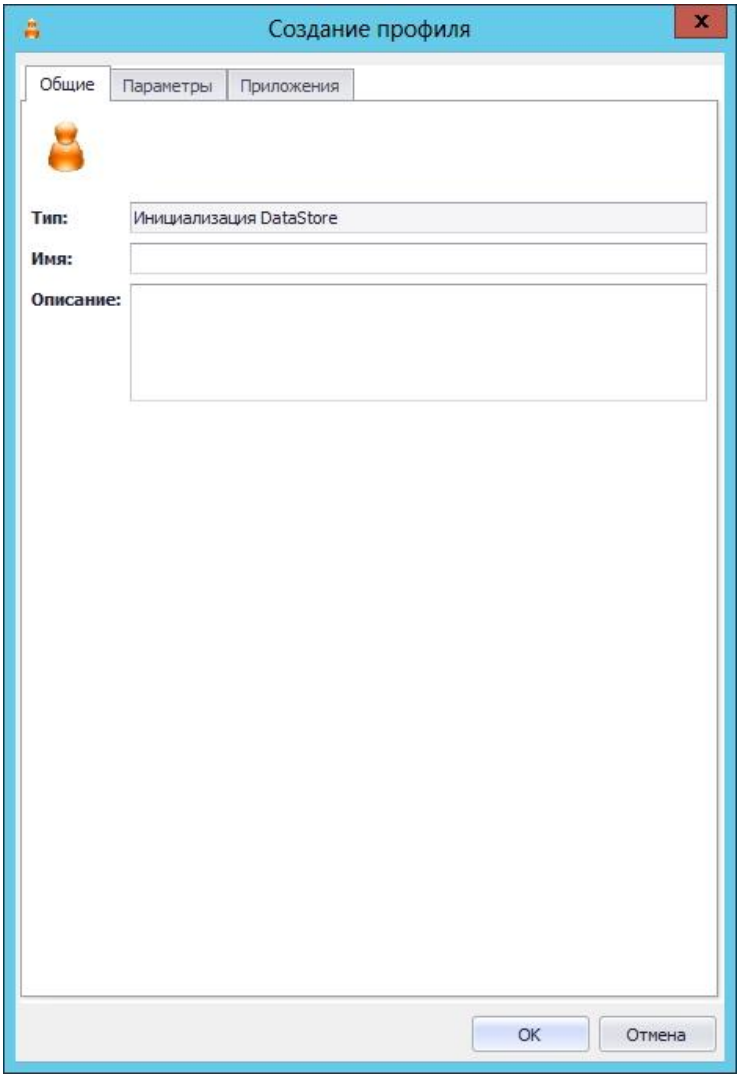


*Рис. 192 – Вкладка **Общие***

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

Окно примет следующий вид.

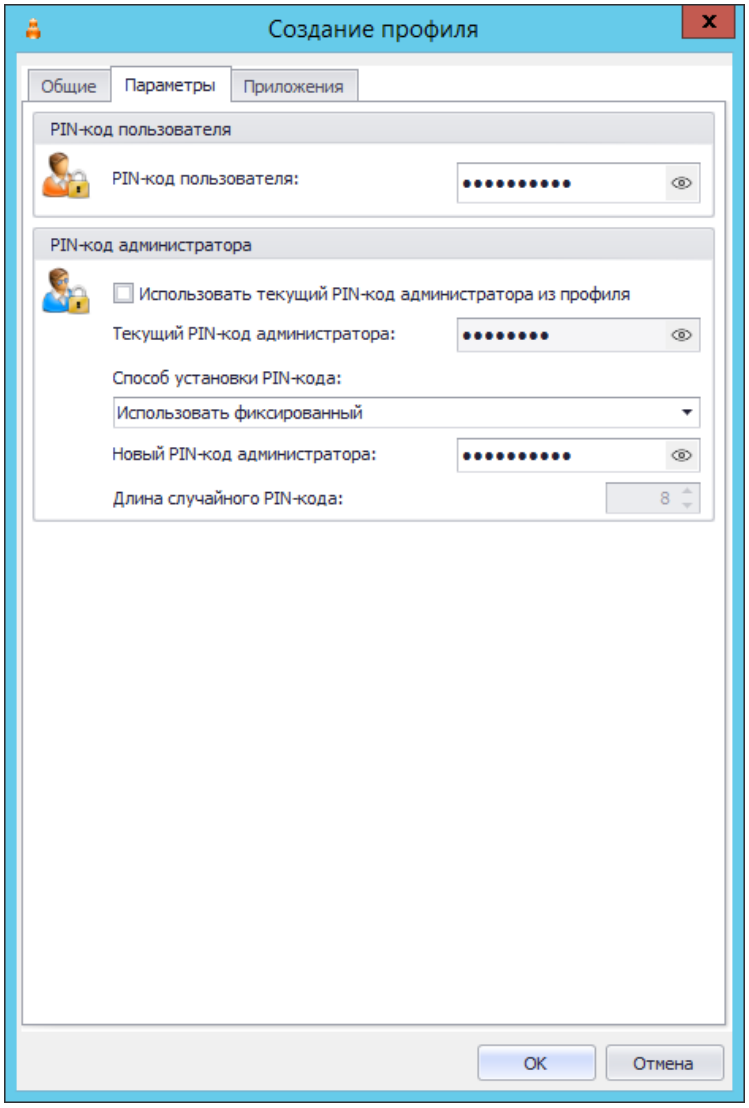


*Рис. 193 – Вкладка **Параметры***

4. Выполните настройку, руководствуясь табл. 30.

Табл. 30 – 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).

Секция	Настройка	Описание
		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. (см. также «Установка в БД PIN-кода администратора для приложения электронного ключа», с. 109)
	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-код администратора, если в списке **Способ установки PIN-кода** был выбран пункт **Генерировать случайный**.

5. Переходите на вкладку **Приложения**.

Окно примет следующий вид.

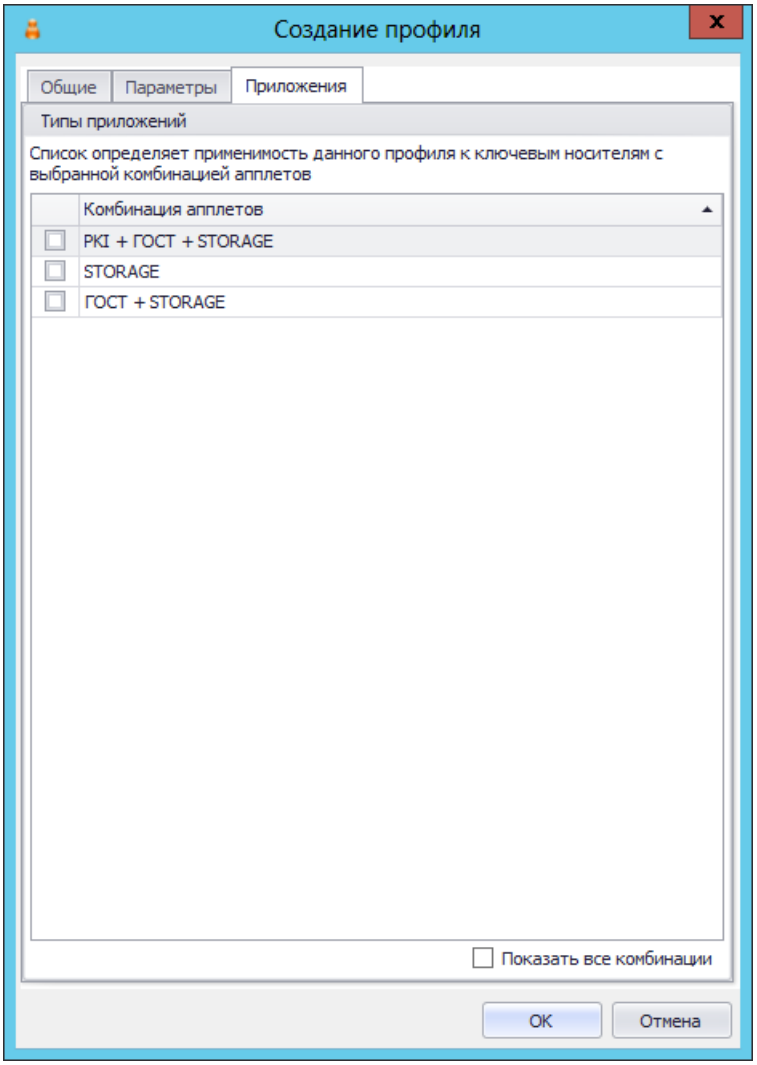


*Рис. 194 – Вкладка **Приложения***

6. Отметьте нужную комбинацию приложений, после чего нажмите **OK**, чтобы сохранить изменения.

3.9.4.6 JaCarta Cryptopro

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

   – чтобы создать новый профиль, выберите нужный тип профиля (**Инициализация ФКН**) и в верхней панели нажмите **Создать**.
   – чтобы изменить существующий профиль, отметьте этот профиль (например, **Инициализация ФКН по умолчанию**) в центральной части окна консоли управления JMS, после чего в верхней панели нажмите **Свойства**.

Отобразится следующее окно.

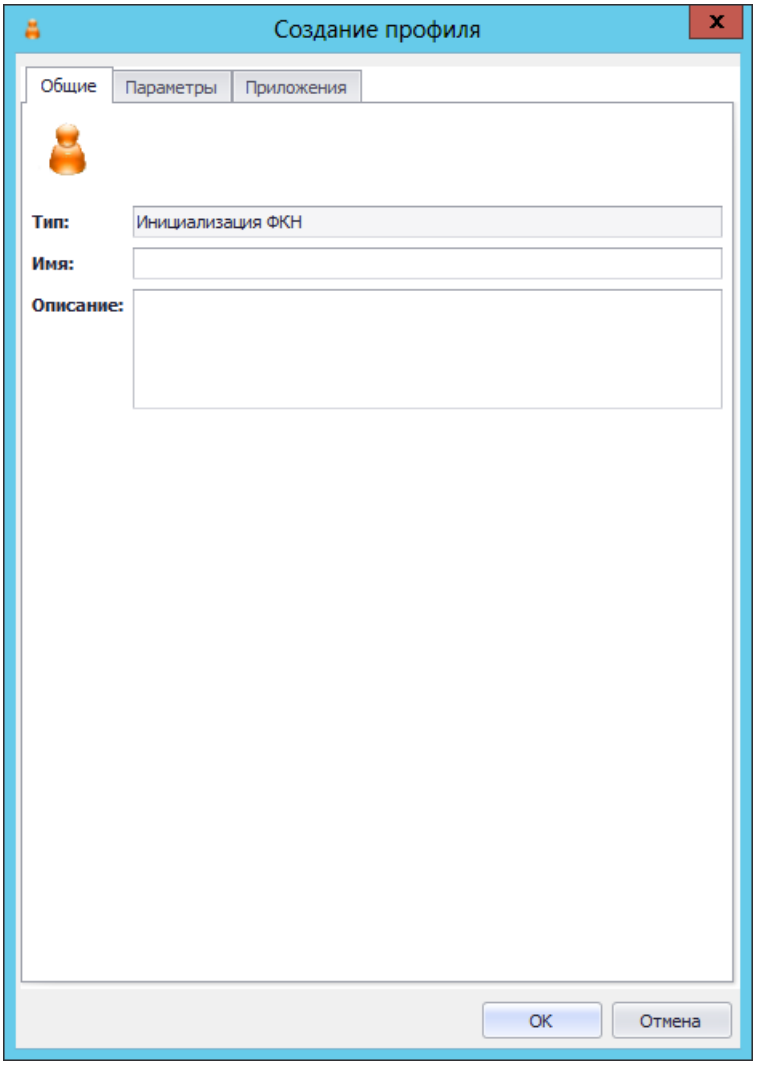


*Рис. 195 – Вкладка **Общие***

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

Окно примет следующий вид.

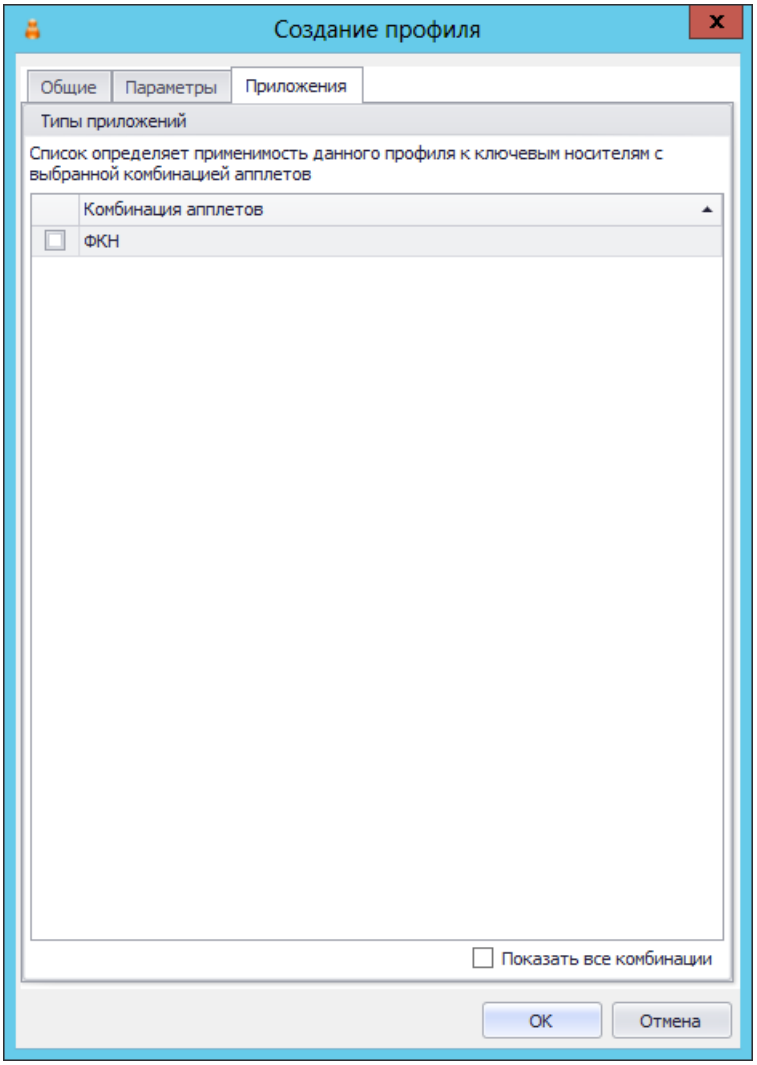


*Рис. 196 – Вкладка **Приложения***

4. Отметьте приложение **ФКН** и нажмите **ОК**, чтобы сохранить изменения и закрыть окно.

3.9.4.7 JaCarta-2 ГОСТ

Текущая версия JMS не позволяет выполнять инициализацию электронных ключей JaCarta-2 ГОСТ (см. «Особенности работы с электронными ключами JaCarta-2 ГОСТ», с. 104).

3.9.4.8 ESMART / ESMART ГОСТ

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

   – чтобы создать новый профиль, выберите нужный тип профиля (**Инициализация ESMART** или **Инициализация ESMART**) и в верхней панели нажмите **Создать**.
   – чтобы изменить существующий профиль, отметьте этот профиль (например, **Инициализация ESMART по умолчанию**) в центральной части окна консоли управления JMS, после чего в верхней панели нажмите **Свойства**.

Отобразится следующее окно.

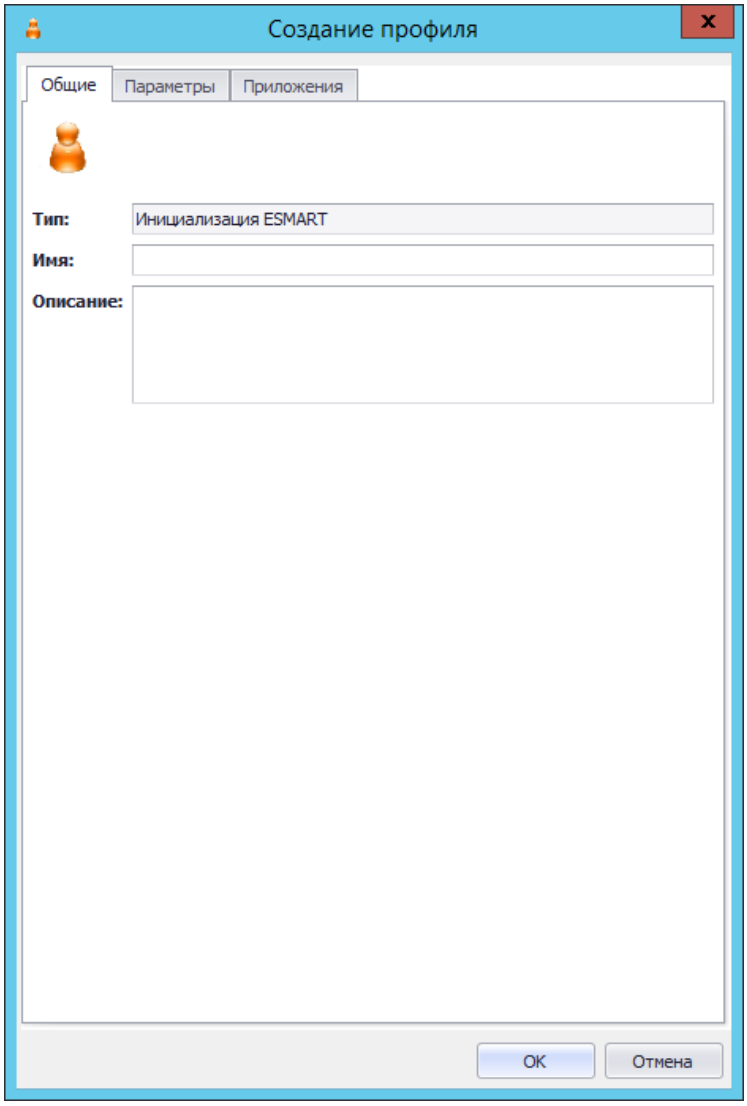


*Рис. 197 – Вкладка **Общие***

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

Окно примет следующий вид.

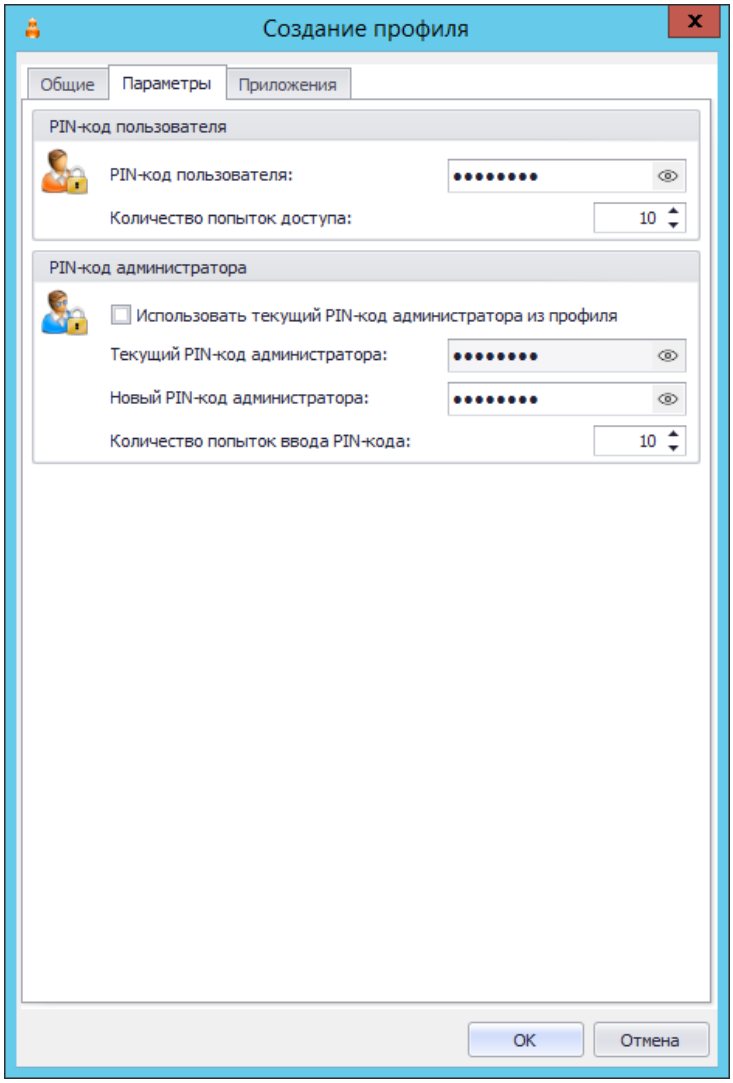


*Рис. 198 – Вкладка **Параметры***

4. Выполните настройку, руководствуясь Табл. 31.

Табл. 31 – Настройка параметров инициализации

Секция	Настройка	Описание
PIN-код пользователя	**PIN-код пользователя**	Поле служит для задания PIN-кода пользователя в *приложении* (электронном ключе).
	Количество попыток ввода PIN-кода	Максимальное число попыток ввода неверного PIN-кода пользователя, по достижении которого PIN-код пользователя на электронном ключе блокируется.
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*

Секция	Настройка	Описание
		(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. (см. также «Установка в БД PIN-кода администратора для приложения электронного ключа», с. 109)
	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**
	Новый PIN-код администратора	Поле содержит PIN-код, который будет установлен в приложении (в электронном ключе) после инициализации.
	Количество попыток ввода PIN-кода (поле недоступно в приложении ESMART ГОСТ)	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. **Примечание.** В приложении ESMART ГОСТ максимальное число попыток ввода PIN-кода администрирования задается при производстве электронных ключей и не может быть установлено при инициализации)

5. Перейдите на вкладку **Приложения**.

Окно примет следующий вид.

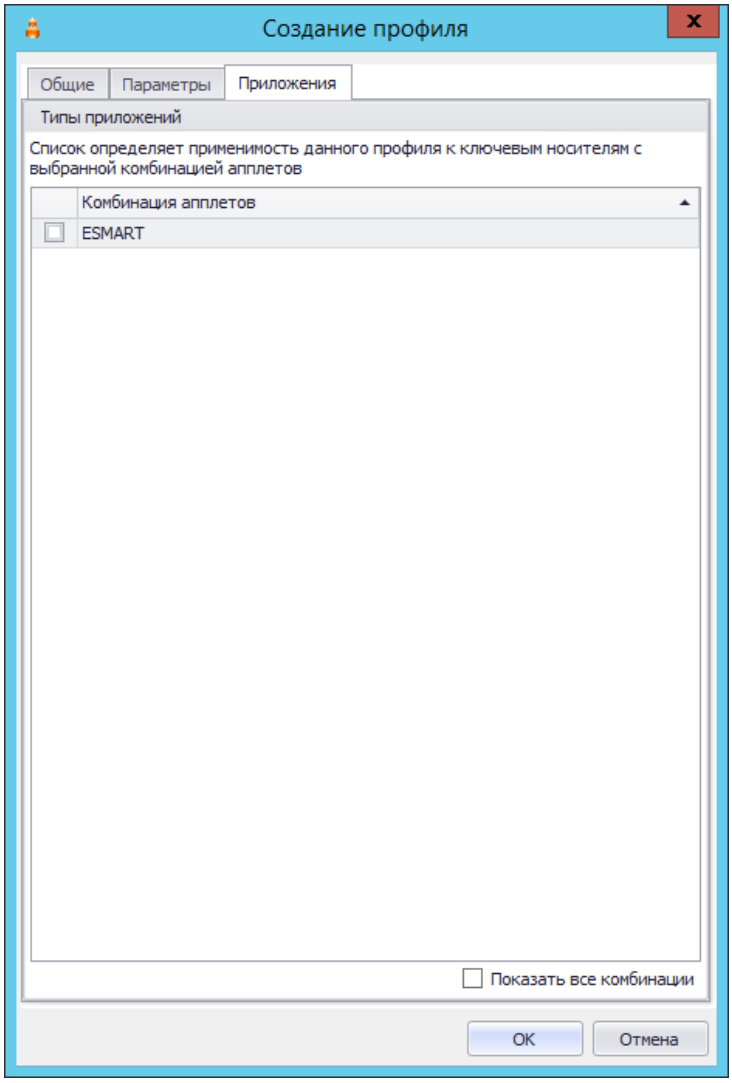


*Рис. 199 – Вкладка **Приложения***

6. Отметьте приложение ESMART, после чего нажмите **OK**, чтобы сохранить изменения.

3.9.5 Настройки профиля выпуска сертификатов в центре сертификации Microsoft

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

- если вы хотите создать новый профиль, в центральной части окна отметьте пункт **Выпуск сертификатов - УЦ Microsoft CA**, после чего в верхней панели нажмите **Создать**, отобразится следующее окно (см. рис. 200);
- если вы хотите отредактировать существующий профиль, в центральной части окна отметьте профиль, относящийся к типу **Выпуск сертификатов - УЦ Microsoft CA**, после чего в верхней панели нажмите **Свойства**.

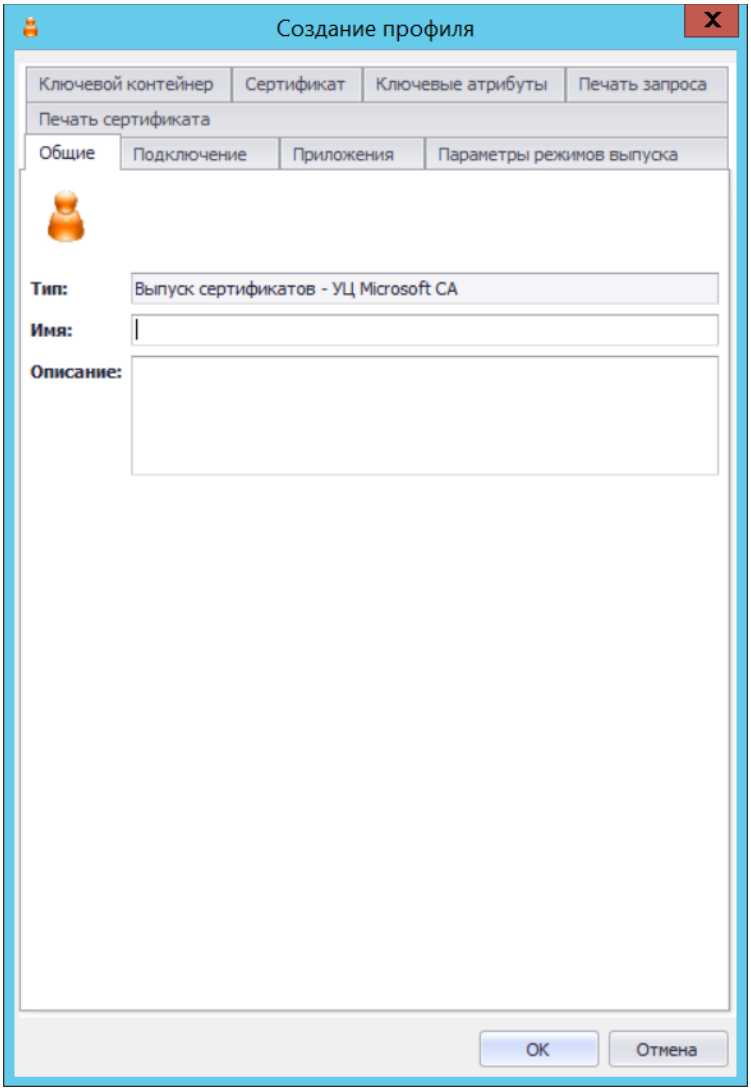


*Рис. 200 – Вкладка **Общие** профиля выпуска сертификатов*

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

3.9.5.1 Настройка параметров подключения

10. Перейдите на вкладку **Подключение**.

Окно примет следующий вид.

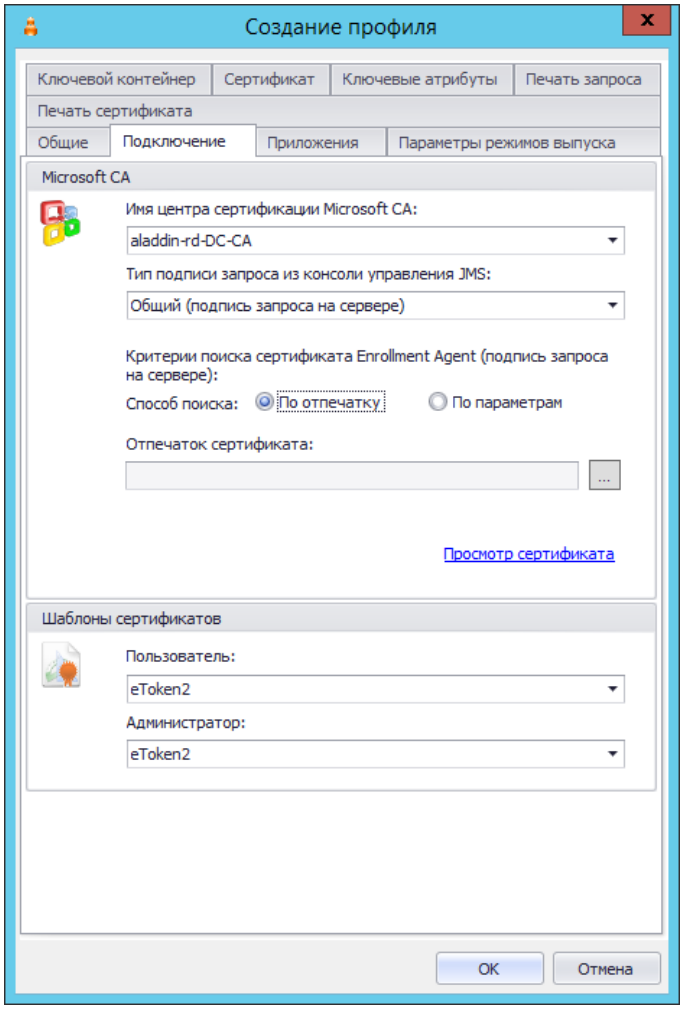


*Рис. 201 – Вкладка **Подключение** профиля выпуска сертификатов*

11. Выполните необходимые настройки, руководствуясь табл. 32.

Табл. 32 – Настройка параметров подключения к удостоверяющему центру

Секция	Настройка	Описание
Microsoft CA	**Имя центра сертификации Microsoft CA**	Выберите из списка нужный центр сертификации.
	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 пользоватля, то сертификат агента регистрации должен выпускаться на имя учетной записи данного пользователя и устанавливается в хранилище пользователя на сервере JMS.

Секция	Настройка	Описание
		• **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. Подробнее о сертификатах см. «Руководство администратора. Часть 1» [2], раздел «Сертификаты для работы с JMS».
	Критерии поиска сертификата Enrollment Agent (подпись запроса на сервере)	Настройка позволяет выбрать сертификат агента регистрации, выпущенный в хранилище компьютера сервера JMS (подробнее «Руководство администратора. Часть 1» [2], раздел «Сертификаты для работы с 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 **OK**. **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 будет 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. 213. Порядок развертывания кластерной конфигурации приведен в соответствующем руководстве [5].
Шаблоны сертификатов	**Пользователь**	Выберите из списка опубликованный шаблон сертификата, который будет использоваться при самостоятельном (т.е. из клиента JMS) выпуске пользователями электронных ключей (см. «Руководство администратора. Часть 1» [2], раздел «Шаблон сертификата для пользователей JMS»). 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 (см. «Руководство администратора. Часть 1» [2], раздел «Шаблон сертификата для пользователей JMS»). **Примечания:**

Секция	Настройка	Описание
		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. 2. В случае если сертификат выпускается в хранилище пользователя на рабочей станции (см. «Выпуск сертификата в хранилище пользователя», с. 308) поле **Администратор** не используется, поскольку в данном режиме сертификат может быть выпущен только пользователем из клиента JMS.

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

Режим **По параметрам** (Рис. 202) 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).

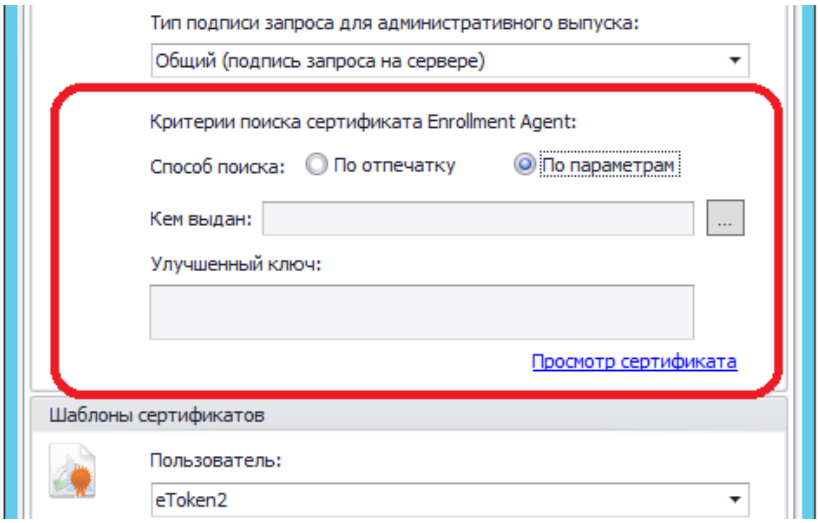


*Рис. 202 – Механизм поиска **По параметрам** на примере профиля выпуска сертификата MSCA*

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.

3.9.5.3 Настройки на вкладке Приложения

12. Перейдите на вкладку **Приложения**.

Окно примет следующий вид.

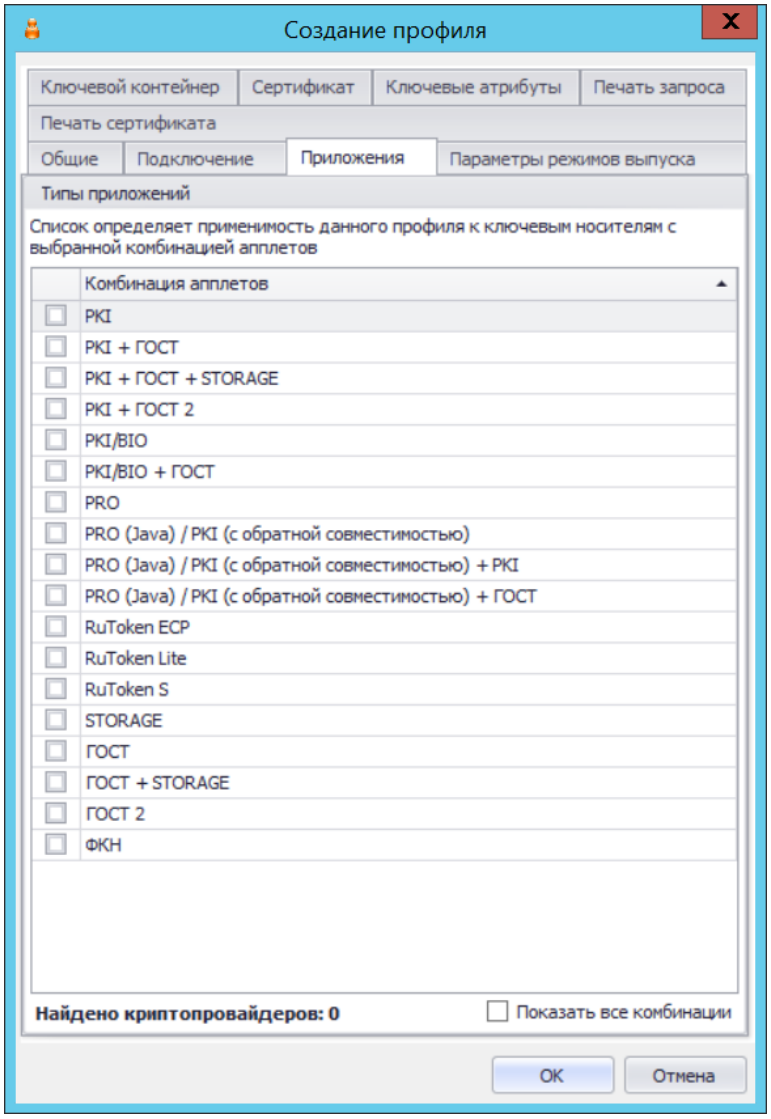


*Рис. 203 – Вкладка **Приложения***

13. Отметьте нужные комбинации приложений.

3.9.5.4 Настройка параметров режимов выпуска сертификатов

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

Окно будет выглядеть следующим образом.

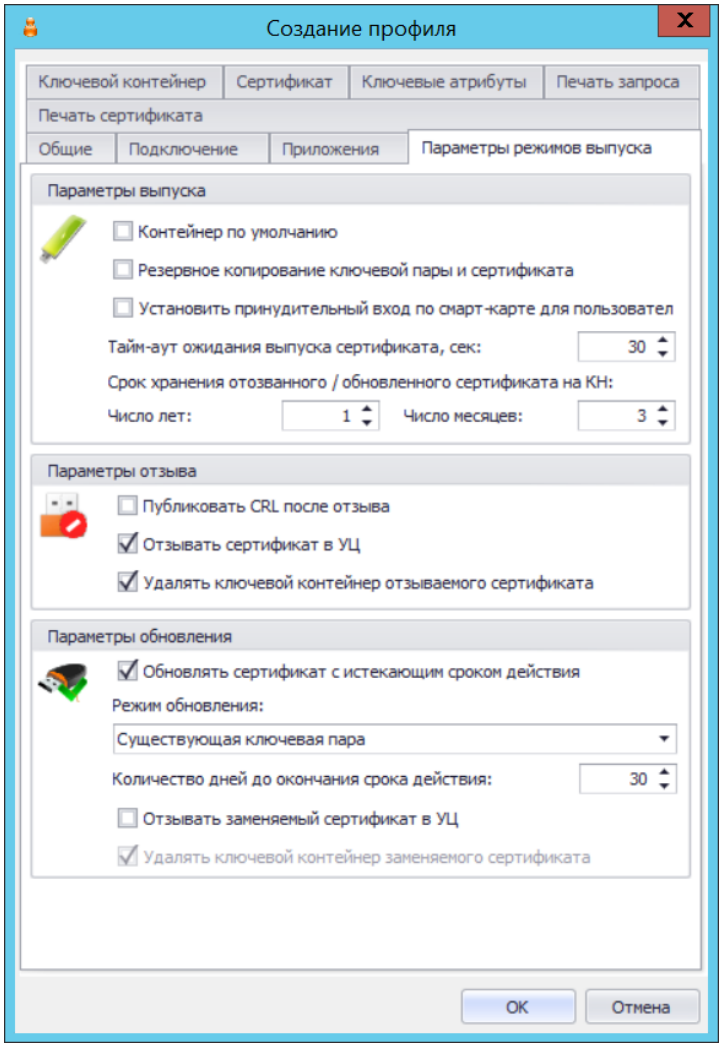


*Рис. 204 – Вкладка **Параметры режимов выпуска** профиля выпуска сертификатов*

15. Выполните необходимые настройки, руководствуясь табл. 33.

Табл. 33 – 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

Секция	Настройка	Описание
		восстановлены на электронном ключе с помощью резервной копии на сервере. **Примечание.** Доступность опции зависит от выбранного криптопровадера (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 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. (Для этого серверу JMS необходимы особые разрешения – подробнее см. «Руководство администратора. Часть 1» [2], раздел «Разрешения для принудительного входа по смарт-карте и открытия входа по паролю AD»)
	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
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 электронного ключа», с. 88); • при отмене привязки *профиля выпуска сертификата*, применявшегося к данному электронному ключу (см. «Привязка профилей», с. 296), в том числе и при удалении профиля; • при удалении сертификата средствами JMS (см. раздел «Операции с сертификатами», с. 50); • 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).

Секция	Настройка	Описание
	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: • **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**).

3.9.5.5 Настройка параметров ключевого контейнера

16. Перейдите на вкладку **Ключевой контейнер**.
    Окно примет следующий вид.

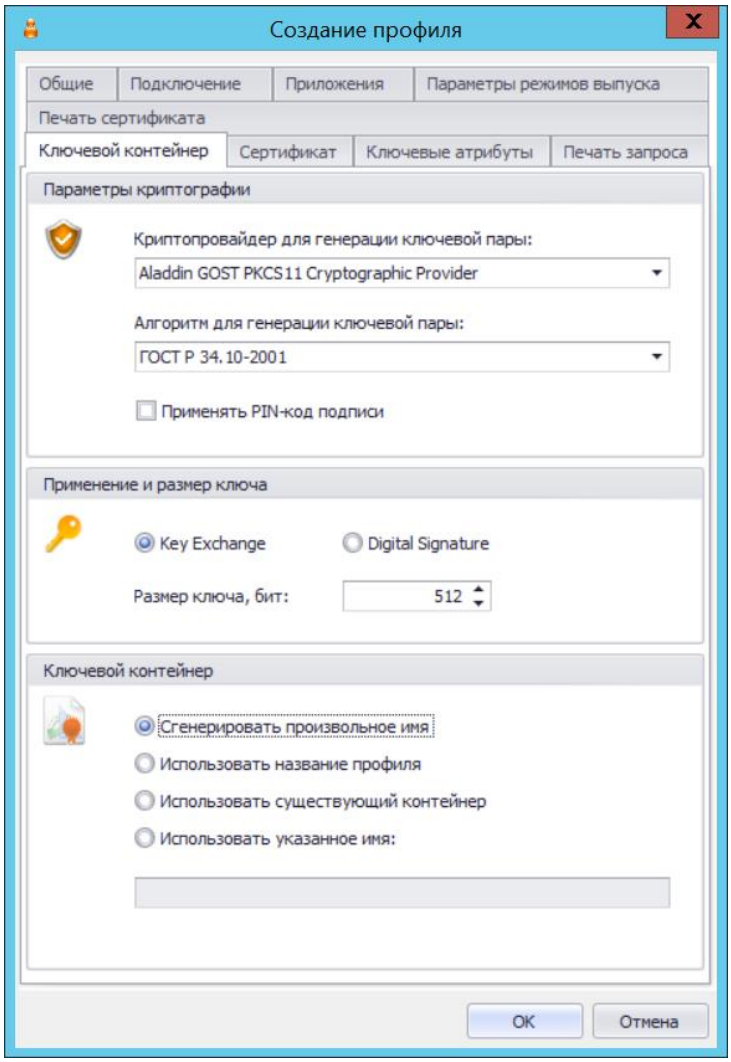


*Рис. 205 – Вкладка **Ключевой контейнер***

17. Выполните необходимые настройки, руководствуясь табл. 34.

Табл. 34 – 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	**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.
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

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

3.9.5.6 Настройка шаблонов полей сертификата

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

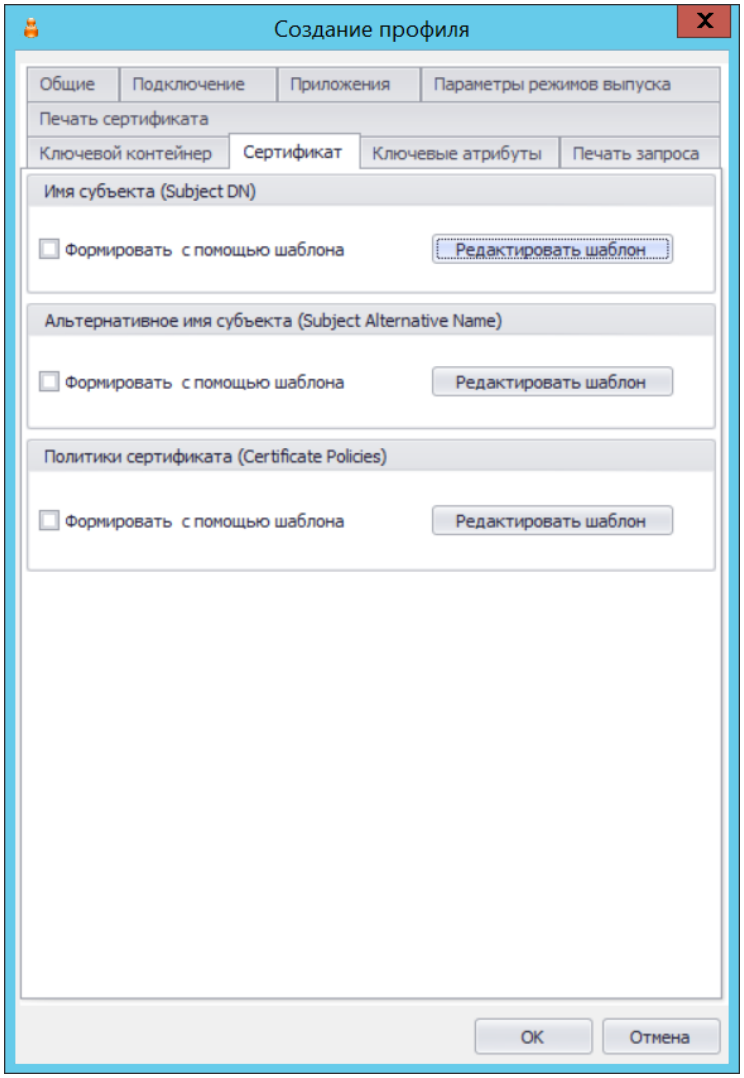


*Рис. 206 – Вкладка **Сертификат***

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

19.1. В секции с названием нужного поля нажмите **Редактировать шаблон**;
19.2. Отредактируйте шаблон, руководствуясь сведениями, представленными в Табл. 35.
19.3. В окне редактирования шаблона нажмите **OK**, чтобы сохранить изменения.
19.4. В секции с названием нужного поля установите флаг **Формировать с помощью шаблона**.
19.5. При необходимости повторите действия для других полей.

Табл. 35 – 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 атрибутов зарегистрированных в JMS ресурсных систем (каталогов учетных записей), выбранные в столбцах **OID** и **Значение**; **Примечание.** При выборе атрибута необходимов 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** – 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 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** – 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 ввести названия политик сертификата. Вы также можете установить флаг **Критическое расширение**, чтобы сделать данное поле критическим расширением.

3.9.5.7 Настройки на вкладке Ключевые атрибуты

20. Перейдите на вкладку **Ключевые атрибуты**.
Отобразится следующее окно.

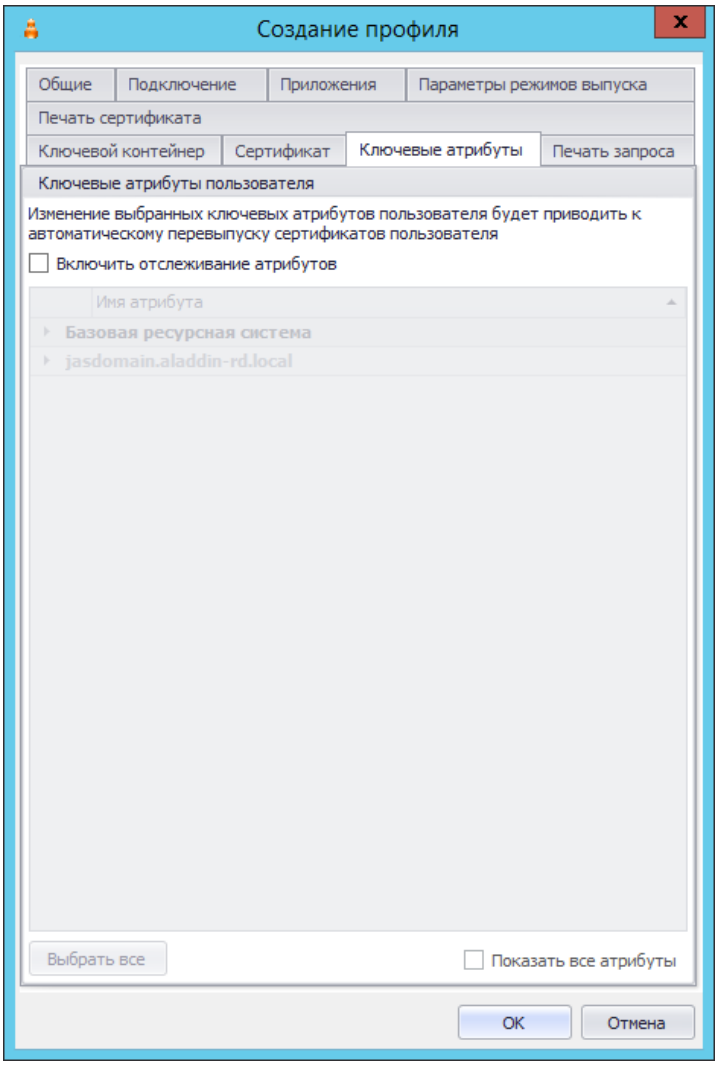


*Рис. 207 – Вкладка **Ключевые атрибуты***

21. 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:

21.1. Установите флаг **Включить отслеживание атрибутов**.
21.2. Выберите ресурсную систему, чтобы раскрылся соответствующий список атрибутов.
21.3. Если все необходимые для отслеживания атрибуты располагаются в окне в отображаемой части списка, отметитьте их.
21.4. 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. Отметье 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. 413. 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 электронного ключа», с. 85).
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. 36, 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 (см. «Руководство администратора. Часть 1» [2], раздел «Настройка каталога учетных записей») 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 (см. «Руководство администратора. Часть 1» [2], раздел «Привязки каталогов учетных записей»). В случае изменения атрибута, выбранного в такой «привязанной» ресурсной системе, также будет производиться перевыпуск сертификата.

Табл. 36 – Схема отображения атрибутов внешних ресурсных систем на базовый список атрибутов JMS

Наименование поля в *Базовой ресурсной системе*	Имя поля в Active Directory	Имя поля в КриптоПро УЦ 1.5	Имя поля в КриптоПро УЦ 2.0	Имя поля в JDS
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
Учетная запись	sAMAccountName	2.5.4.3 (CommonName)	DisplayName	AccountName
ФИО	displayName	2.5.4.3 (CommonName)	2.5.4.3 (CommonName)	FullName

3.9.5.8 Прочие настройки профиля выпуска сертификатов

22. 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. 304.
23. Нажмите **OK**, чтобы сохранить изменения.

3.9.6 Настройки профиля выпуска сертификатов на КриптоПро DSS

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

2. Выполните одно из следующих действий:

   – если вы хотите создать новый профиль, в центральной части окна отметьте пункт **Выпуск сертификатов на КриптоПро DSS**, после чего в верхней панели нажмите **Создать**, отобразится следующее окно (см. Рис. 208);
   – если вы хотите отредактировать существующий профиль, в центральной части окна отметьте профиль, относящийся к типу **Выпуск сертификатов на КриптоПро DSS**, после чего в верхней панели нажмите **Свойства**.

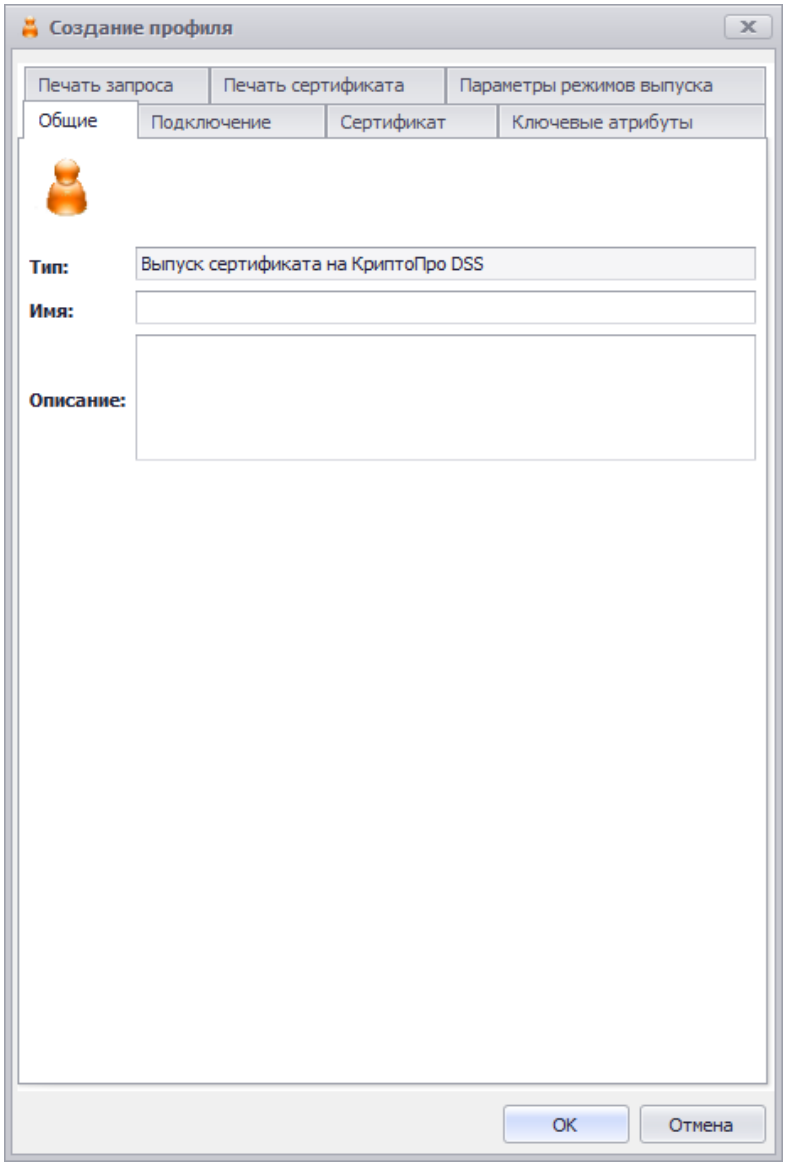


*Рис. 208 – Вкладка **Общие** профиля выпуска сертификатов на КриптоПро DSS*

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

3.9.6.1 Настройка параметров подключения

4. Перейдите на вкладку **Подключение**.

Окно примет следующий вид.

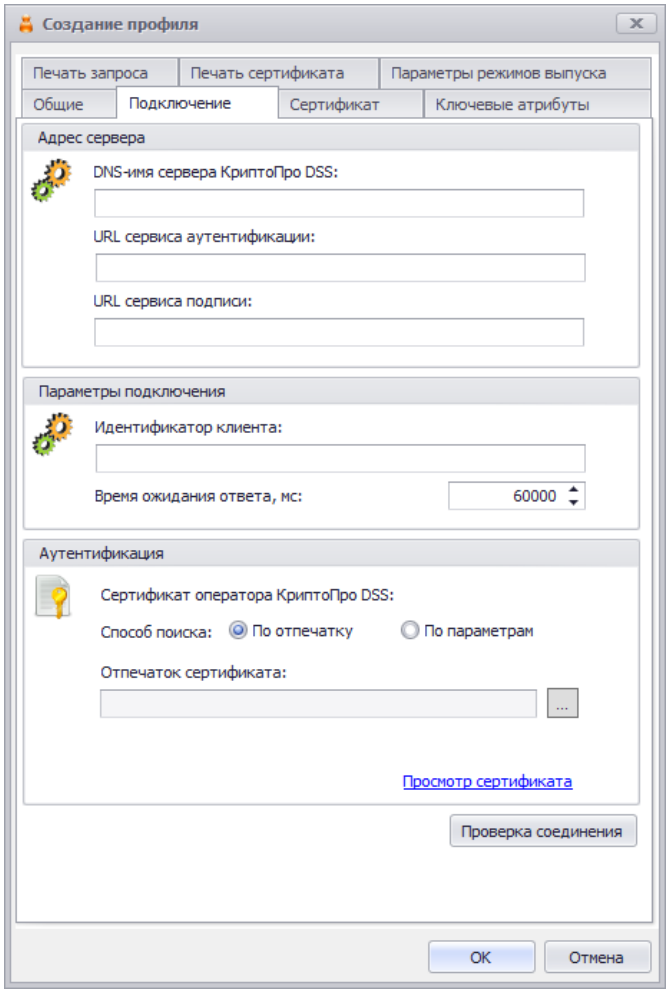


*Рис. 209 – Вкладка **Подключение** профиля выпуска сертификатов на КриптоПро DSS*

5. Выполните настройки подключения к серверу КрипоПро DSS, руководствуясь Табл. 56, с. 283 (раздел «Настройка профиля пользователя КриптоПро DSS»).

3.9.6.2 Настройка шаблонов сертификата

6. Перейдите на вкладку **Сертификат**.

Отобразится следующее окно.

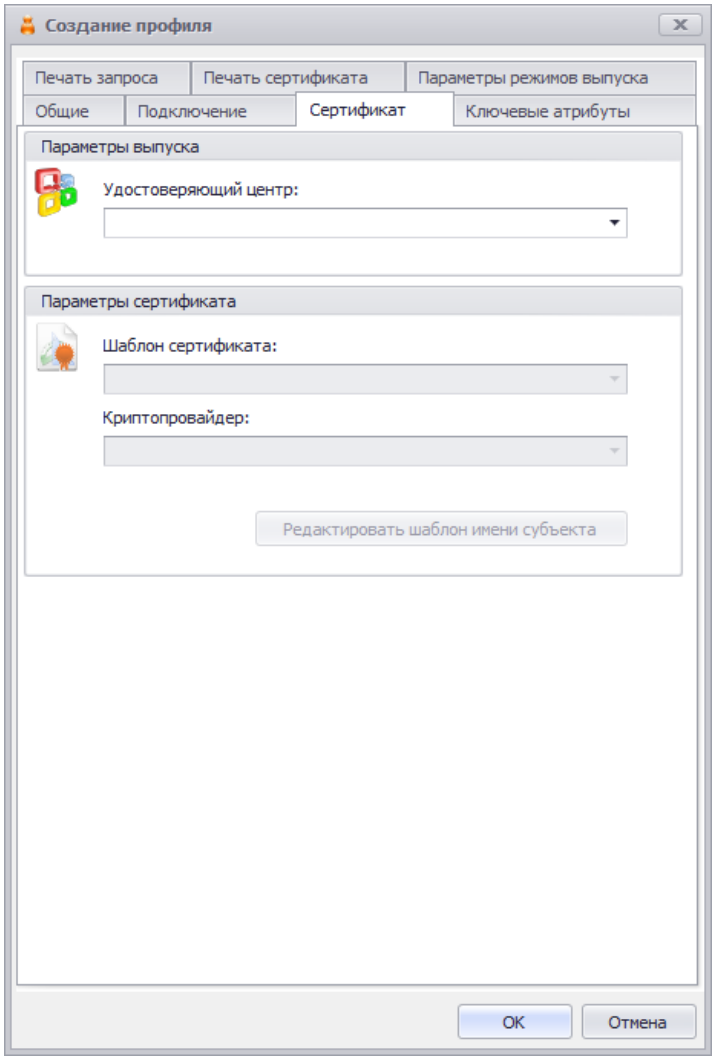


*Рис. 210 – Вкладка **Сертификат***

7. Выполните настройки параметров сертификата руководствуясь Табл. 37.

Табл. 37 – Настройка параметров выпуска сертификата в КриптоПро DSS

Настройка	Описание
Удостоверяющий центр	Выберите один из удостоверяющих центров, доступных в подключенном сервере КриптоПро DSS **Примечание.** Настройка становится доступной после выполнения подключения к серверу КриптоПро DSS на вкладке **Подключение**.
Шаблон сертификата	Выберите один из шаблонов сертификатов, доступный в удостоверяющем центре, выбранном в поле **Удостоверяющий центр**

Настройка	Описание
Криптопровайдер	Выберите один из криптопровайдеров для генерации ключевой пары, доступных в удостоверяющем центре, выбранном в поле **Удостоверяющий центр** **Важно!** После установки криптопровайдера следует отредактировать шаблон имени субъекта. При этом на форме отображается предупреждение *Требуется корректировка шаблона имени субъекта* (см. Рис. 211, ниже) Для обеспечения корректности настройки выпуска сертификата нажмите кнопку **Редактировать шаблон имени субъекта** и для поля *Общее имя* шаблона сертификата в УЦ на стороне КриптоПро DSS подберите соответствующий атрибут пользователя ресурсной системы на стороне JMS (например, атрибут пользователя *canonicalName (CN)* в службе каталога Active Directory).

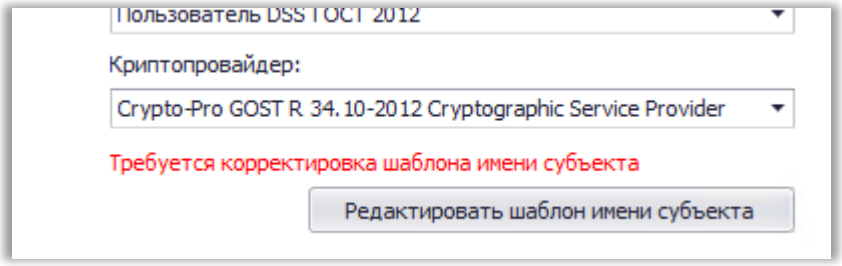


Рис. 211 – Предупреждение о необходимости корректировки шаблона имени субъекта

3.9.6.3 Настройки на вкладке Ключевые атрибуты

8. Перейдите на вкладку **Ключевые атрибуты**.

Отобразится следующее окно.

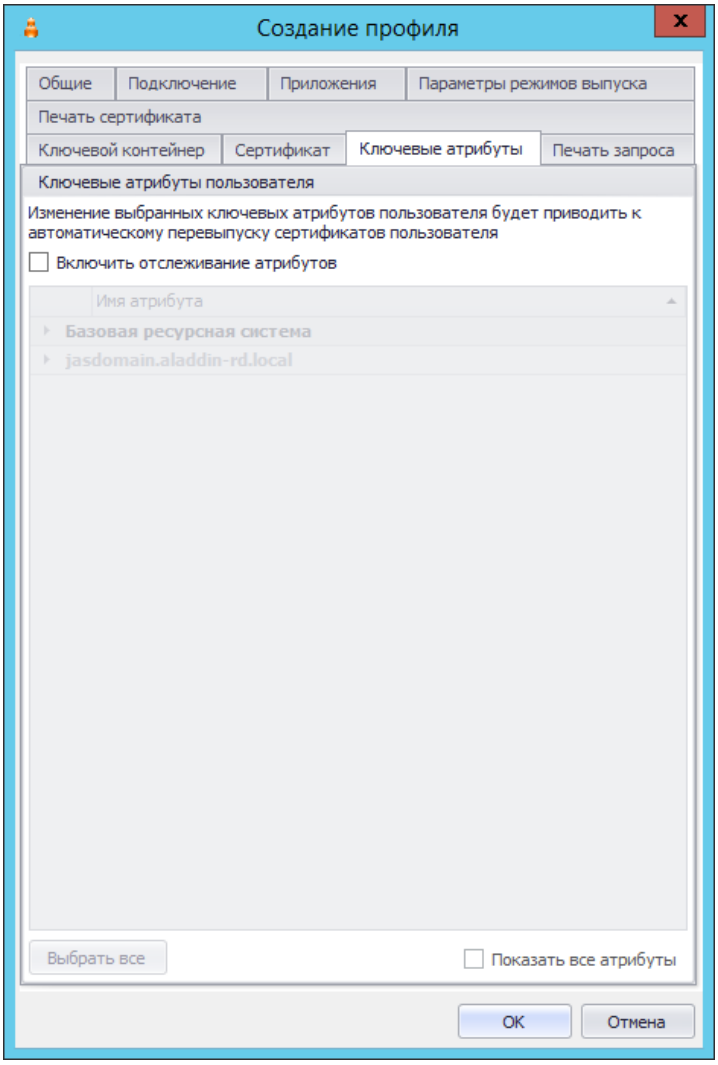


*Рис. 212 – Вкладка **Ключевые атрибуты***

9. Выполните настройки по аналогии с настройками Ключевых атрибутов профиля выпуска сертификатов в УЦ Microsoft CA (см. раздел «Настройки на вкладке Ключевые атрибуты», с. 222

3.9.6.4 Настройка параметров режимов выпуска сертификатов

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

Окно будет выглядеть следующим образом.

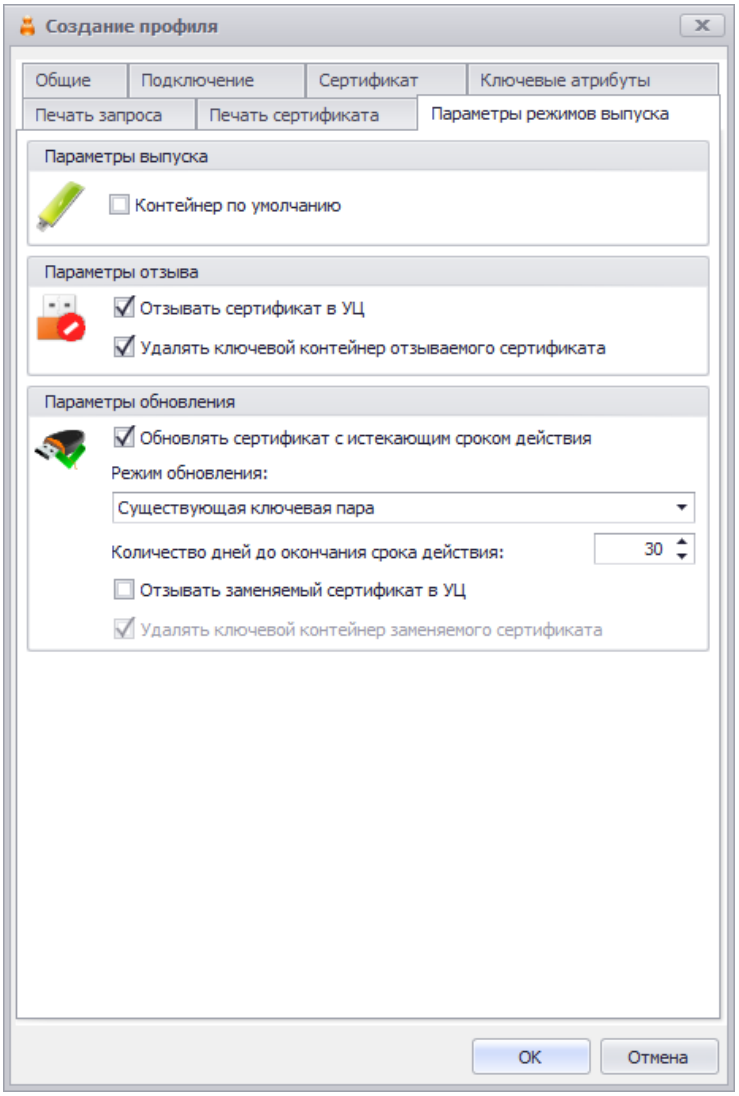


*Рис. 213 – Вкладка **Параметры режимов выпуска** профиля выпуска сертификатов*

11. Выполните необходимые настройки, руководствуясь Табл. 38.

Табл. 38 – 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.
Параметры отзыва		**Важно!** Под событием «отзыв» в настройках данной секции подразумевается отзыв сертификата в JMS, который выполняется в следующих случаях: • при отзыве виртуального токена (электронного ключа) типа *Хранилище сервера КриптоПро DSS* (см. «Отзыв электронного ключа», с. 88);

Секция	Настройка	Описание
		• при отмене привязки *профиля выпуска сертификата на КриптоПро DSS* (см. «Привязка профилей», с. 296), в том числе и при удалении профиля
	Отзывать сертификат в УЦ	Если флаг установлен, то выпущенный для пользователя КриптоПро DSS сертификат, который был впоследствии отозван в JMS, будет также отозван в соответствующем УЦ, привязанном к КриптоПро DSS (см. настройку Удостоверяющий центр на вкладке Сертификат (раздел «Настройка шаблонов сертификата», с. 225).
	Удалять ключевой контейнер отзываемого сертификата	Если флаг установлен, то при отзыве виртуального токена (электронного ключа) типа *Хранилище сервера КриптоПро DSS*, с сервера DSS будет удален ключевой контейнер, созданный при выпуске по данному профилю. Если флаг не установлен, то при отзыве сертификат из Хранилища сервера КриптоПро DSS 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: • **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 хранилища сервера КриптоПро DSS будет удален ключевой контейнер заменяемого сертификата. Если флаг не установлен, то из хранилища 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

Секция	Настройка	Описание
		ключевого контейнера (см. описание вкладки **Ключевой контейнер**).

3.9.6.5 Прочие настройки профиля выпуска сертификатов

12. При необходимости, выполните настройку печати соответствующих документов (вкладки **Печать запроса** и **Печать сертификата**). Подробнее о настройке **Шаблона печатной формы** см. в разделе «Настройка параметров печати при выпуске объектов JMS», с. 304.
13. Нажмите **OK**, чтобы сохранить изменения.

3.9.7 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 выполнять выпуск сертификатов пользователей в аккредитованных удостоверяющих центрах, не имеющих сетевого подключения к телекоммуникационным сетям общего пользования. Подробнее см. «Руководство администратора. Часть 1» [2], раздел «Коннектор к Offline Certification Authority».

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

14. В консоли управления JMS перейдите в раздел **Профили -> Профили**.
15. Выполните одно из следующих действий:

- если вы хотите создать новый профиль, в центральной части окна отметьте пункт **Выпуск сертификатов (режим офлайн)**, после чего в верхней панели нажмите **Создать**, отобразится следующее окно (Рис. 214);
- если вы хотите отредактировать существующий профиль, в центральной части окна отметьте профиль, относящийся к типу **Выпуск сертификатов (режим офлайн)**, после чего в верхней панели нажмите **Свойства**.

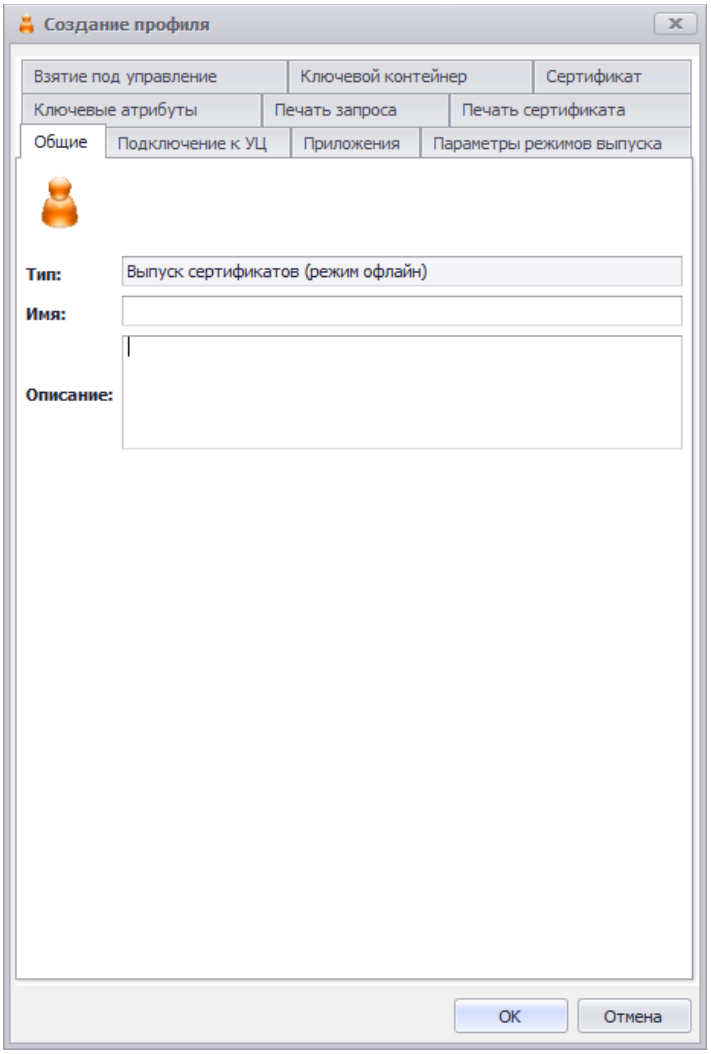


*Рис. 214 – Вкладка **Общие** профиля выпуска сертификатов*

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

3.9.7.1 Настройка параметров подключения к УЦ

17. Перейдите на вкладку **Подключение к УЦ**.

Окно примет следующий вид.

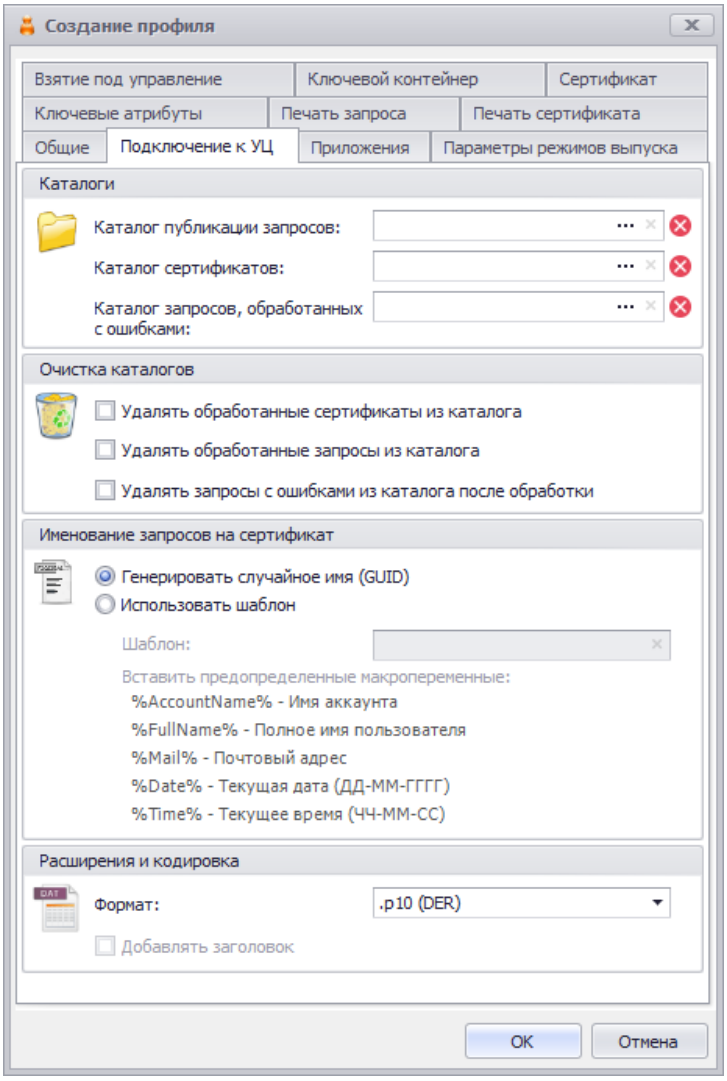


*Рис. 215 – Вкладка **Подключение к УЦ** профиля выпуска сертификатов*

18. Выполните необходимые настройки, руководствуясь Табл. 39.

Табл. 39 – Настройка параметров подключения к удостоверяющему центру

Настройка	Описание
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.
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)
<Секция **Именование запросов на сертификат**> **Использовать шаблон**	Выберите данную опцию, если для идентификации запроса необходимо сформировать его имя с помощью шаблона, формируемого в поле **Шаблон**. Для создания шаблона последовательно нажмите на приведенные ниже гиперссылки переменный: • %AccountName% — Имя аккаунта; • %FullName% — Полное имя пользователя; • %Mail% — Почтовый адрес; • %Date% — Текущая дата (ДД-ММ-ГГГГ); • %Time% — Текущее время (ЧЧ-ММ-СС). Переменные, указанные нажатием мыши, будут подставлены в шаблон.
<Секция **Расширение и кодировка**> **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)
<Секция **Расширение и кодировка**> **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

3.9.7.2 Настройки на вкладке Приложения

19. Перейдите на вкладку **Приложения** (Рис. 203, с. 214), выполните настройки по аналогии с настройкой вкладки **Приложения** профиля выпуска сертификатов в центре сертификации Microsoft (см. раздел «Настройки на вкладке Приложения», с. 213).

3.9.7.3 Настройка параметров режимов выпуска сертификатов

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

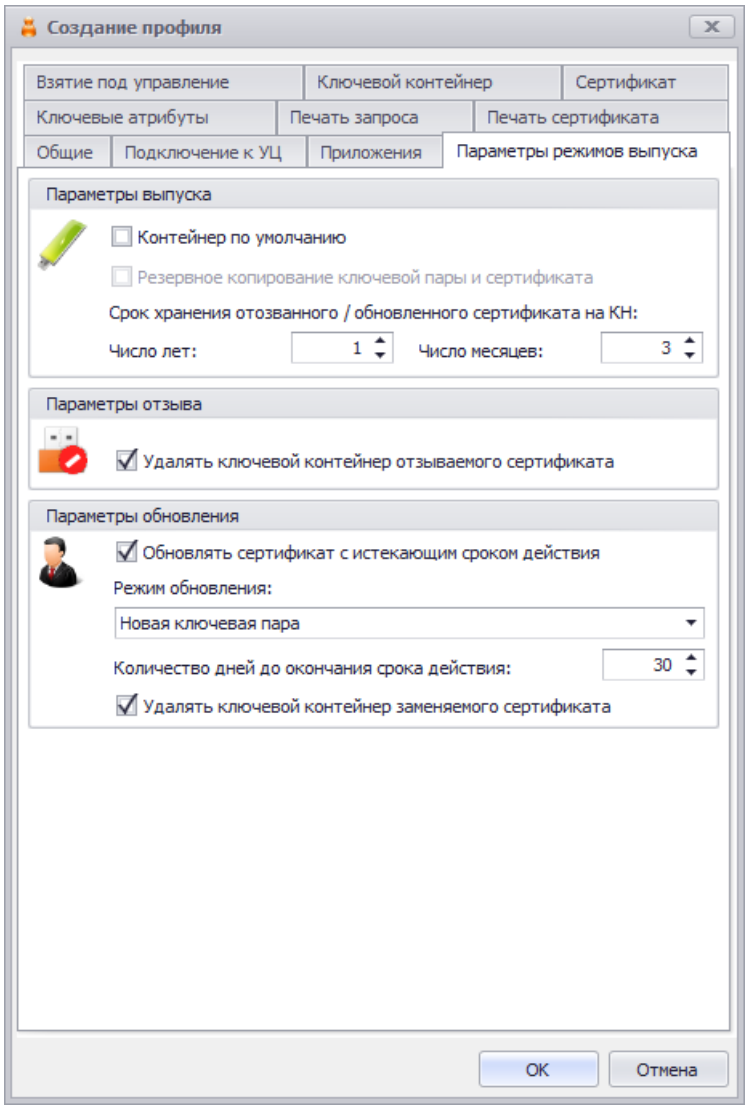


*Рис. 216 – Вкладка **Параметры режимов выпуска** профиля выпуска сертификатов*

21. Выполните необходимые настройки, руководствуясь Табл. 40.

Табл. 40 – 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.

Секция	Настройка	Описание
		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)
	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 электронного ключа», с. 88); • при отмене привязки *профиля выпуска сертификата*, применявшегося к данному электронному ключу (см. «Привязка профилей», с. 296), 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:

Секция	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**.

3.9.7.4 Настройка параметров ключевого контейнера

22. Перейдите на вкладку **Ключевой контейнер** (Рис. 205, с. 218)выполните настройки по аналогии с настройкой параметров на вкладке **Ключевой контейнер** профиля выпуска сертификатов в центре сертификации Microsoft (см. раздел «Настройка параметров ключевого контейнера», с. 218).

3.9.7.5 Настройка шаблонов полей сертификата

23. Перейдите на вкладку **Сертификат**.

Отобразится следующее окно.

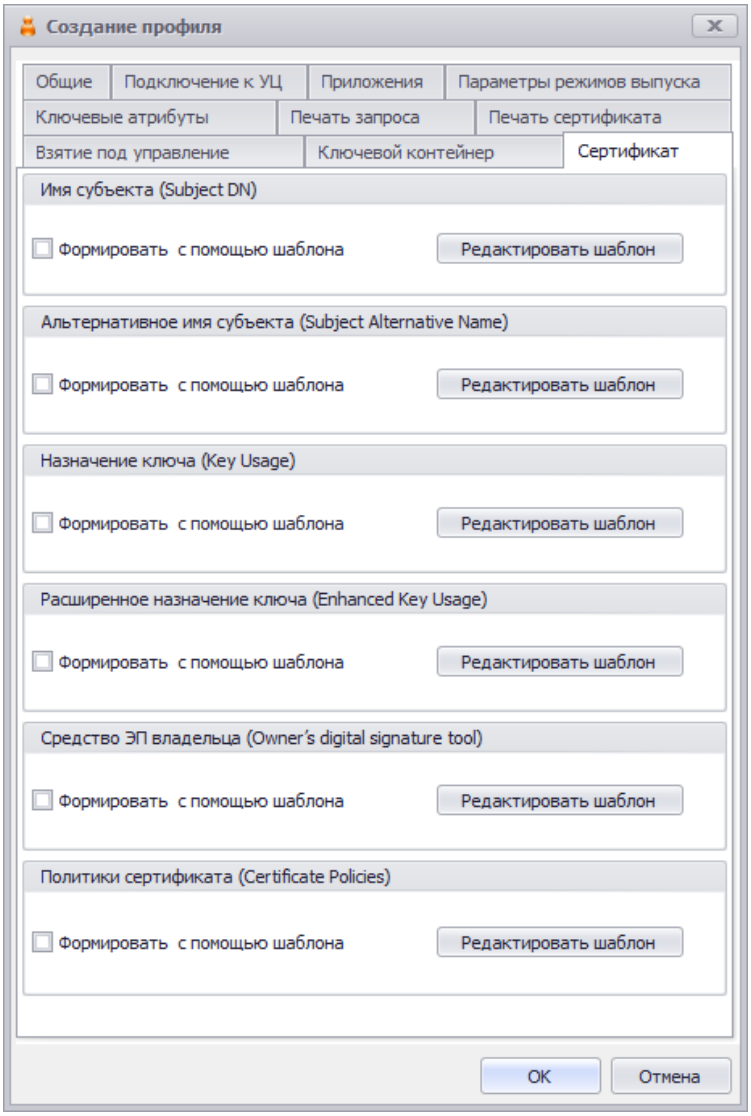


*Рис. 217 – Вкладка **Сертификат***

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

24.1. В секции с названием нужного поля нажмите **Редактировать шаблон**;
24.2. Отредактируйте шаблон, руководствуясь сведениями, представленными в Табл. 134, с. 627.
24.3. В окне редактирования шаблона нажмите **ОК**, чтобы сохранить изменения.
24.4. В секции с названием нужного поля установите флаг **Формировать с помощью шаблона**.
24.5. При необходимости повторите действия для других полей.

3.9.7.6 Настройки на вкладке Ключевые атрибуты

25. Перейдите на вкладку **Ключевые атрибуты** (Рис. 207, с. 222), 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. 222).

3.9.7.7 Прочие настройки профиля выпуска сертификатов

26. 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. 304.
27. Нажмите **ОК**, чтобы сохранить изменения.

3.9.8 Создание и настройка профиля Внешние объекты

Нажмите **Профили** -> **Внешние объекты** -> **Создать**.

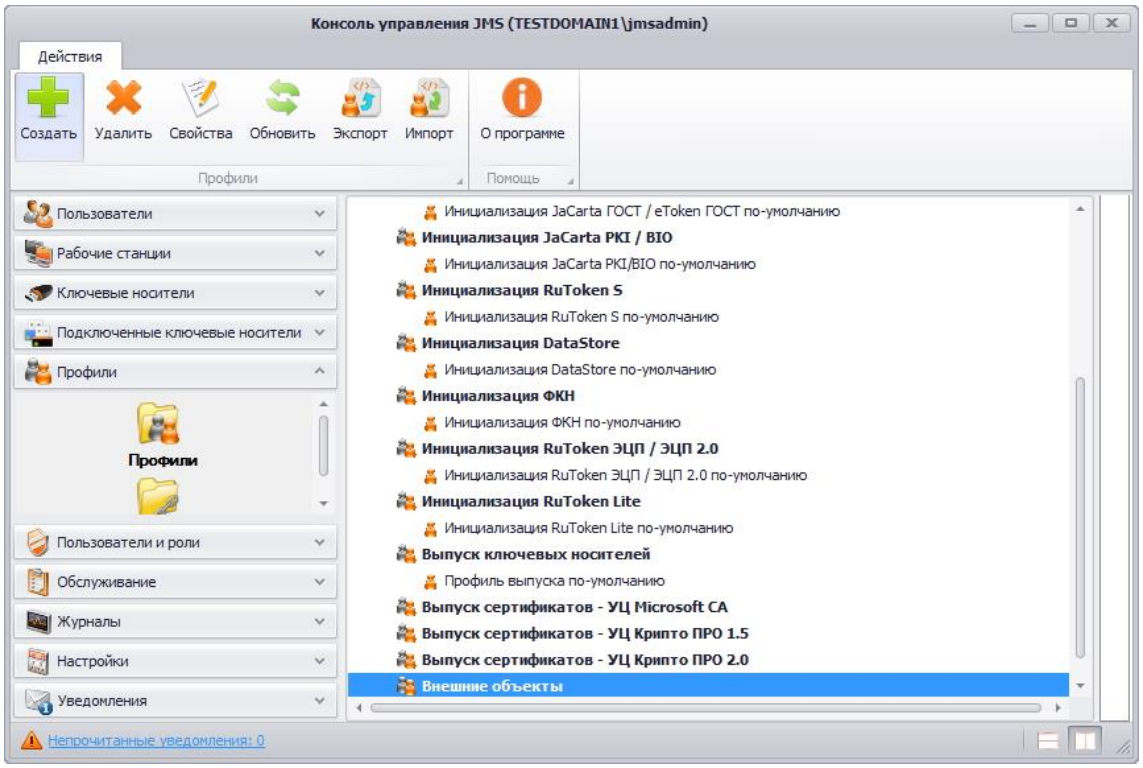


Рис. 218 – Создание профиля внешнего объекта

В появившемся окне (см. рис. 219) перейдите на вкладку **Общие** и заполните поле **Имя**.

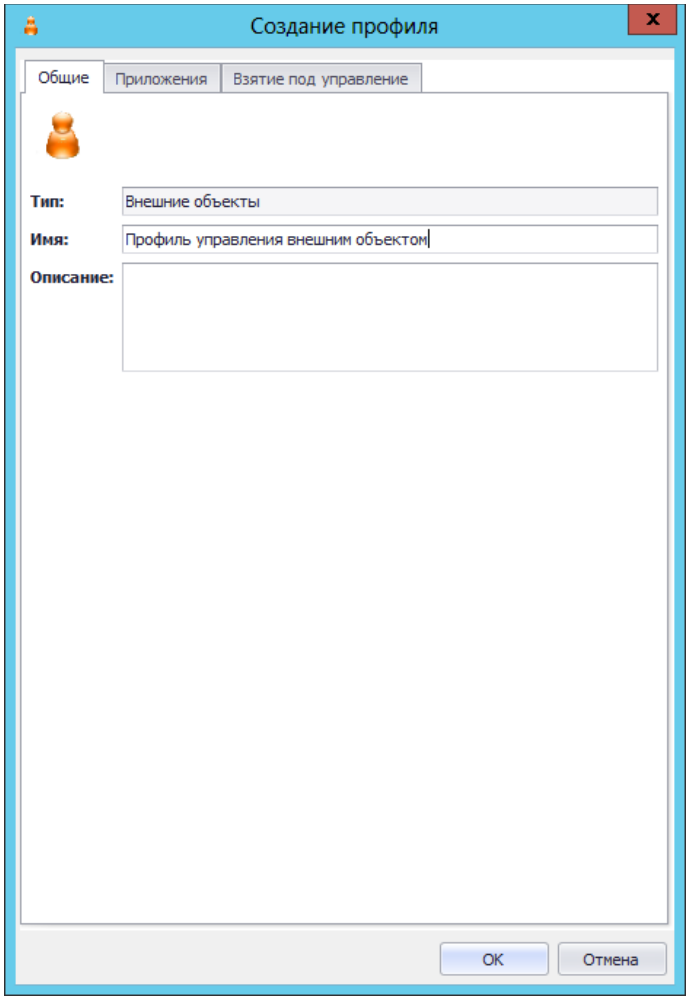


Рис. 219 – Вкладка Общие в окне Создание профиля

Перейдите на вкладку **Приложения** (см. рис. 220) и 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 на вкладке **Взятие под управление** таким образом, чтобы у всех выбранных приложений имелся хотя бы один общий поставщик криптографии (секция **Криптопровайдеры для внешних объектов**), поддерживаемый данными приложениями.

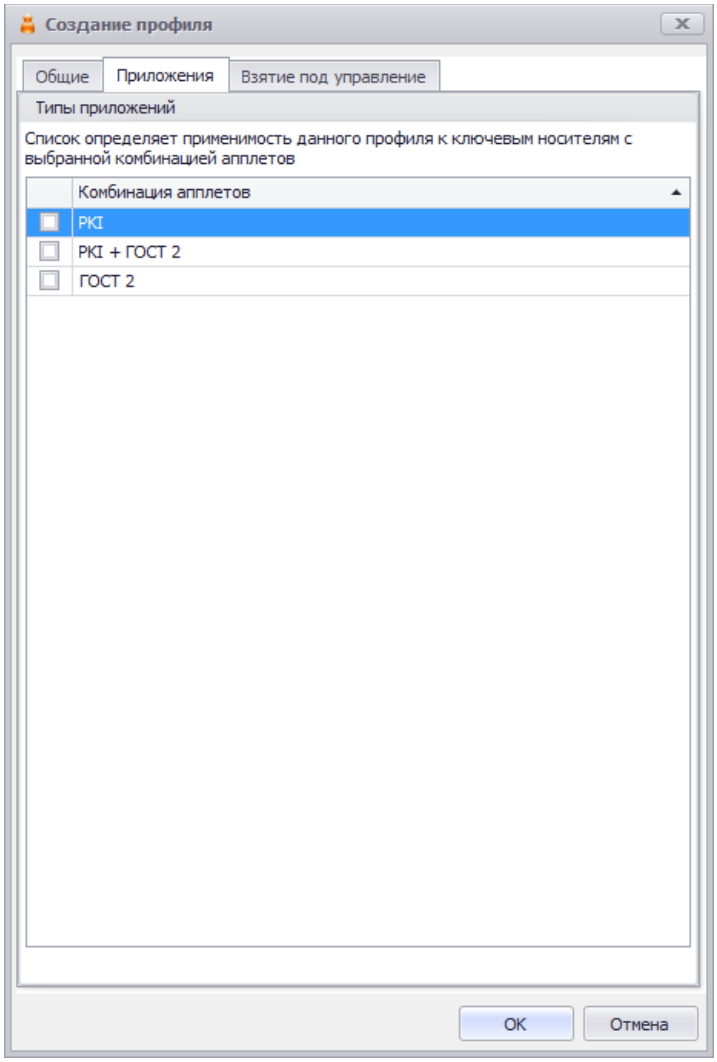


Рис. 220 – Вкладка Приложения в окне Создание профиля

Перейдите на вкладку **Взятие под управление** (см. рис. 221) и в секции **Параметры криптографии** выберите поставщик криптографии (**Криптопровайдер**), с помощью которого может быть распознан данный внешний объект (сертификат) или объекты. Возможен выбор одновременно нескольких поставщиков криптографии.

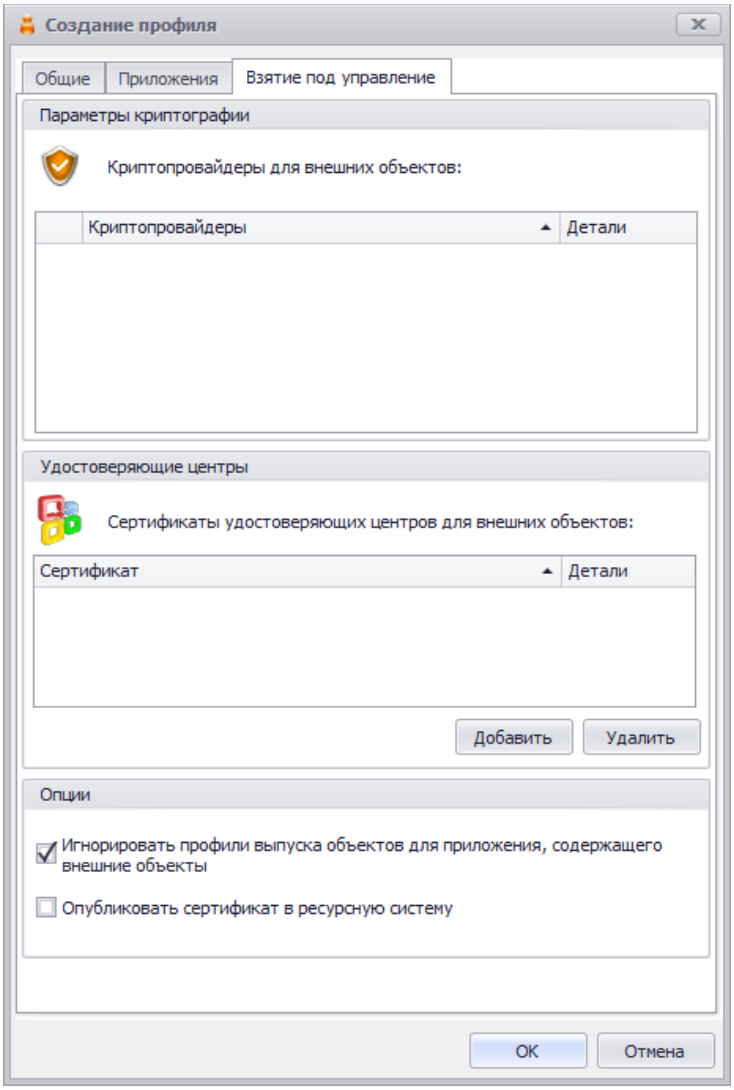


Рис. 221 – Вкладка Взятие под управление в окне Создание профиля

В секции **Удостоверяющие центры** нажмите **Добавить** и 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). 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, необходимо предварительно сохранить на сервер JMS сертификат корневого УЦ и цепочку сертификатов УЦ (см. раздел «Регистрация в JMS сертификатов сторонних УЦ (внешних объектов)», с. 460), один из которых впоследствии будет загружен из окна на Рис. 221.

Опция **Игнорировать профили выпуска объектов для приложения, содержащего внешние объекты** при ее выборе позволяет не выпускать сертификаты MSCA, КриптоПро, объекты SecurLogon и т.п. для записи в те приложения электронного ключа, которые содержат внешние объекты.

Опцию **Опубликовать сертификат в ресурсную систему** следует выбрать, если взятый под управление сертификат необходимо добавить в ресурсную систему (в привязке к пользователю, для которого он был выпущен в соответствующей ресурсной системе, например Active Directory).

После добавления сертификатов УЦ следует выполнить настройку отмеченных криптопровайдеров. Для этого в секции **Параметры криптографии** напротив соответствующего криптопровайдера нажмите **Настроить**. Откроется окно настройки работы с сертификатами УЦ, ассоциированными с данным криптопровайдером:

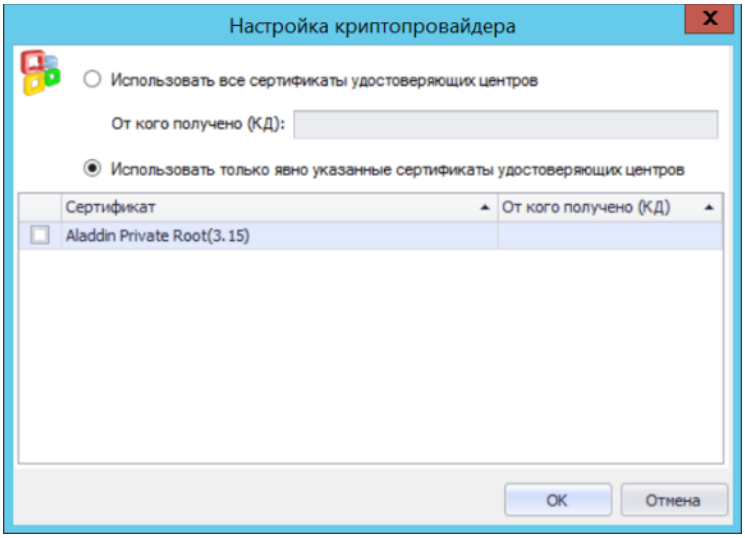


Рис. 222 – Окно Настройка криптопровайдера

Выполните необходимые настройки, руководствуясь Табл. 41.

Табл. 41 – 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,** Рис. 221
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 удостоверяющего центра	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 (Рис. 222). 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)

После настройки всех криптопровайдеров в окне настройки профиля нажмите **OK** и переходите к привязке профиля (подробнее см. раздел «Привязка профилей», с. 296).

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

3.9.8.1 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**, Рис. 221);
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.

3.9.9 Профиль настройки синхронизации рабочей станции

Внимание! Профиль настройки синхронизации рабочей станции не предусмотрен в версии *CA Edition* продукта JMS (см. «Руководство администратора. Часть 1» [2], раздел «Версии поставки продукта и лицензионные опции»).

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

   – если вы хотите создать новый профиль настройки синхронизации рабочей станции, в центральной части окна консоли управления JMS отметьте **Настройки синхронизации рабочей станции** и в верхней панели нажмите **Создать**;
   – если вы хотите отредактировать существующий профиль, в центральной части окна консоли управления JMS отметьте этот профиль и в верхней панели нажмите **Свойства**.

Отобразится следующее окно.

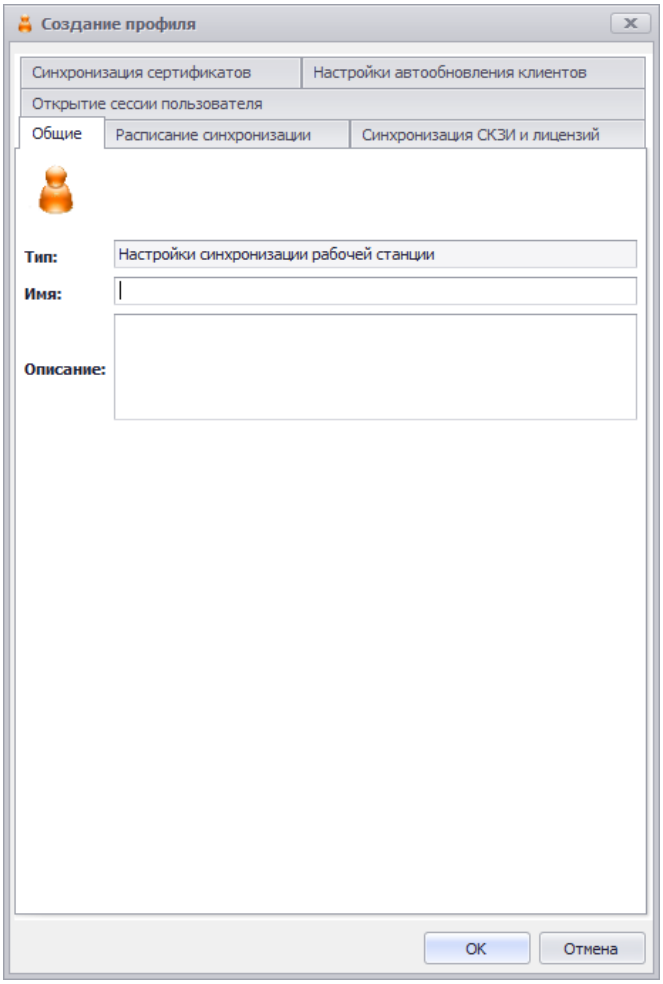


*Рис. 223 – Вкладка **Общие** свойств профиля **Настройки синхронизации рабочей станции***

3. В полях **Имя** и **Описание** введите название и описание профиля соответственно (либо отредактируйте существующие), после чего перейдите на вкладку **Синхронизация СКЗИ и лицензий**.

Окно примет следующий вид.

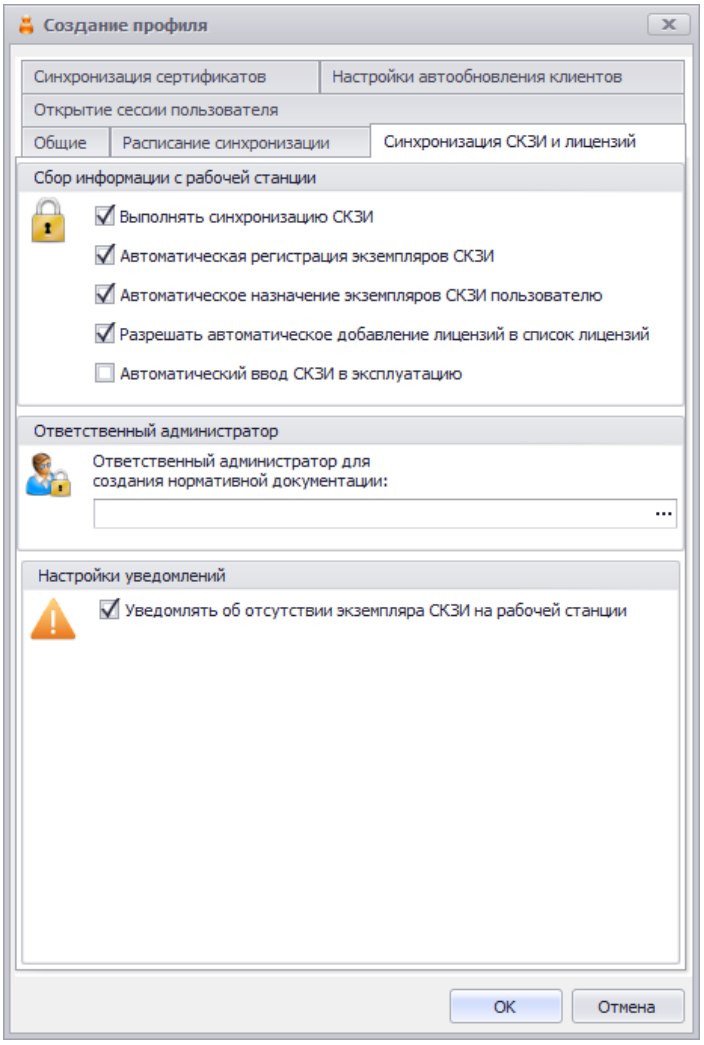


*Рис. 224 – Вкладка **Синхронизация СКЗИ и лицензий***

Примечание. Вкладка **Синхронизация СКЗИ и лицензий** доступна (отображается) только при условии добавления в JMS лицензии на поддержку СКЗИ (см. раздел «Руководство администратора. Часть 1» [2], раздел «Окно управления сервером JMS (серверный агент)» -> «Лицензии»).

4. Выполните настройку, руководствуясь Табл. 42.

Табл. 42 – Настройка параметров синхронизации СКЗИ и лицензий

Настройка	Описание
	Секция **Сбор информации с рабочей станции**
Выполнять синхронизацию СКЗИ	Включите данную настройку, если требуется синхронизация СКЗИ.
Автоматическая регистрация экземпляров СКЗИ	Если настройка включена, то при синхронизации рабочей станции данные об установленном на ней программном СКЗИ будут перенесены на сервер JMS (на сервере будет зарегистрирован экземпляр данного СКЗИ в привязке к рабочей станции).

Настройка	Описание
	Примечание. Автоматическая регистрация СКЗИ возможна только в случае, если для данного СКЗИ на рабочей станции установлена лицензия его производителя. Экземпляры СКЗИ КриптоПро CSP с *демонстрационной лицензией* производителя не могут быть зарегистрированы в JMS.
Автоматическое назначение экземпляров СКЗИ пользователю	Если настройка включена, то пользователь, открывший сеанс (сессию) связи с сервером JMS из клиентского агента JMS будет автоматически назначен ответственным лицом за программное СКЗИ, установленное на данной рабочей станции. Такое назначение выполняется лишь в первый раз после установки СКЗИ. В дальнейшем, назначение ответственного лица за данное СКЗИ может быть изменено администратором из административной консоли JMS (см. раздел «Экземпляры СКЗИ», с. 326) **Примечание.** Назначение пользователя ответственным лицом за данное СКЗИ выполняется в момент синхронизации рабочей станции с сервером. Периодичность синхронизации для данной станции определяется параметром **Выполнять синхронизацию каждые (минут)** данного профиля (вкладка **Расписание синхронизации**). Для того чтобы данный профиль вступил в действие на рабочей станции немедленно, следует перезагрузить данную рабочую станцию.
Разрешить автоматическое добавление лицензий в список лицензий	Если настройка включена, то лицензия установленного на данной рабочей станции программного СКЗИ будет автоматически добавлена в пул лицензий СКЗИ (см. раздел «Лицензии СКЗИ», с. 351). **Примечание.** В текущей реализации JMS для избежания ошибок регистрации СКЗИ данную настройку рекомендуется включать вместе с настройкой **Автоматическая регистрация экземпляров СКЗИ**
Автоматический ввод СКЗИ в эксплуатацию	Если настройка включена, то экземпляры программных СКЗИ с привязанными лицензиями, установленные на рабочих станциях и привязанные к пользователям (см. «Порядок назначения программного СКЗИ пользователю», с. 465) будут автоматически введены в эксплуатацию при выполнении плана обслуживания СКЗИ (см. раздел «План обслуживания СКЗИ», с. 421) и при условии включения соответствующей задачи. Настройка доступна только при включенных флагах **Выполнять синхронизацию СКЗИ** и **Автоматическое назначение экземпляров СКЗИ пользователям** (см. выше). По умолчанию настройка отключена
Секция **Ответственный администратор**	
Ответственный администратор для создания нормативной документации	Пользователь, который назначается ответственным за создание нормативной документации. Для выбора и назначения пользователя нажмите три точки «**...**»
Секция **Настройки уведомлений**	
Уведомлять об отсутствии экземпляра СКЗИ на рабочей станции	Если настройка включена, то в случае отсутствии на рабочей станции СКЗИ, ранее зарегистрированного в JMS в привязке к данной рабочей станции, в журнал будет добавлено уведомление об отсутствии данного СКЗИ.

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.

5. Перейдите на вкладку **Расписание синхронизации**.
   Окно примет следующий вид.

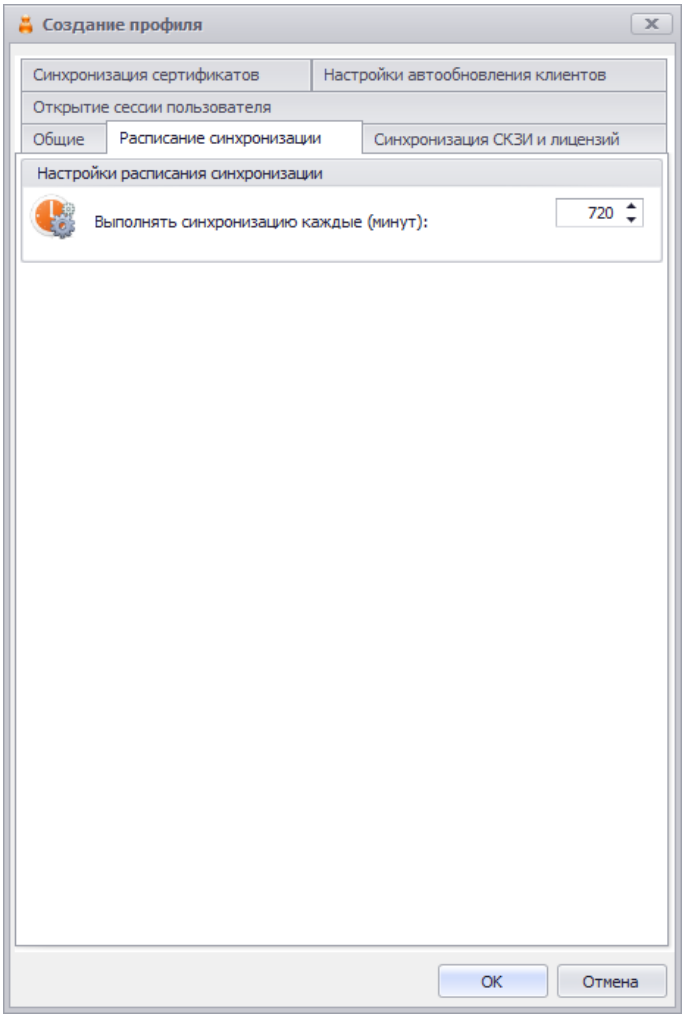


*Рис. 225 – Вкладка **Расписание синхронизации***

6. Выполните настройку, руководствуясь Табл. 43.

Табл. 43 – Настройка расписания синхронизации

Настройка	Описание
Выполнять синхронизацию каждые (минут)	Настройка определяет период выполнения проверки наличия на сервере JMS привязанного к данной рабочей станции профиля синхронизации с последующей установкой настроек профиля на клиенте JMS (либо с последующим обновлением ранее установленных настроек). Если привязанный профиль синхронизации найден, то производятся синхронизация рабочей станции в соответствии с установленными в нем настройками, а именно: 1. Передача на сервер JMS обновленной информации об установленных на рабочей станции СКЗИ (в соответствии с вкладкой **Синхронизация СКЗИ и лицензий**) и о сертификатах (в соответствии с вкладкой **Синхронизация сертификатов**).

Настройка	Описание
	2. Обновление ПО JMS Client в соответствии с вкладкой **Настройки автообновления клиентов**. Проверку наличия на сервере JMS привязанного к данной рабочей станции профиля синхронизации можно выполнить также принудительно путем перезагрузки компьютера. **Примечания:** 1. По умолчанию (в случае если профиль синхронизации для рабочей станции еще не создан) проверка его наличия и привязки будет осуществляться раз в 24 ч. 2. В случае удаления из JMS ранее загруженного на рабочую станцию профиля (или отмены его привязки) синхронизация СКЗИ и сертификатов прекращается до появления нового профиля, в то время как расписание обновления клиента будет продолжать выполняться до тек пор, пока не обновится ПО клиента (или пока не будут применены параметры нового профиля синхронизации). 3. Для выполнения всех задач синхронизации (например, считывания сертификатов из личного хранилища пользователя) помимо запуска JMS-клиента необходимо также выполнить открытие пользовательской сессии (сеанса) JMS. В противном случае будут выполнены только задачи, не требующие аутентификации пользователя. 4. Настоящая настройка не имеет отношения к синхронизации электронных ключей (ключевых носителей) в JMS-клиенте. Параметры синхронизации электронных ключей устанавливаются в профиле **Настройки клиентского агента.**

7. Перейдите на вкладку **Настройки автообновления клиентов**.

Окно примет следующий вид.

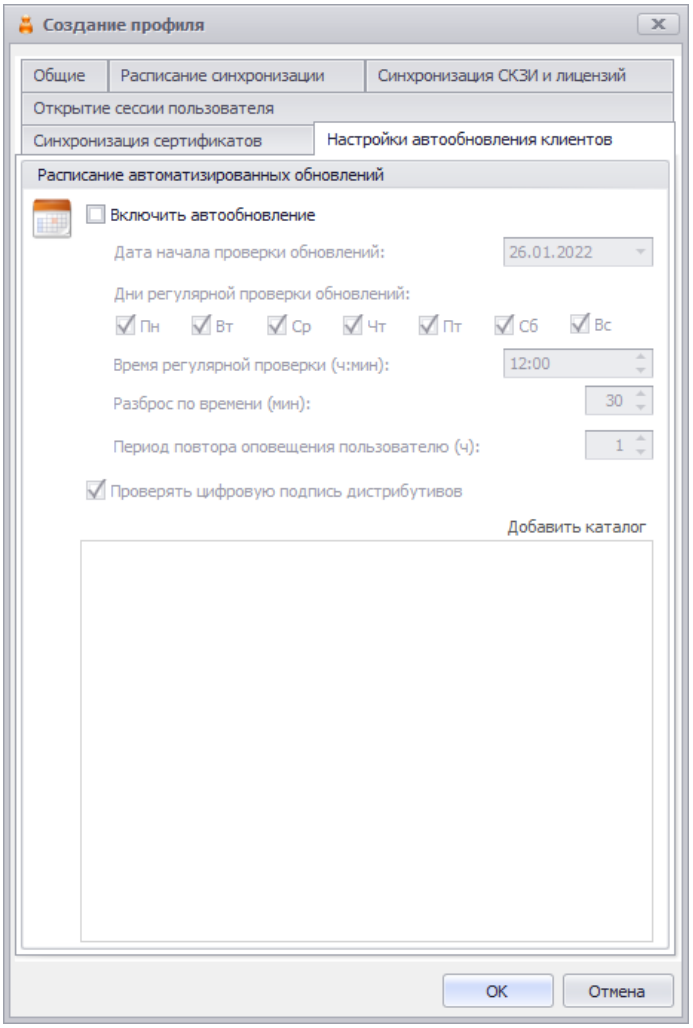


*Рис. 226 – Вкладка **Настройка автообновления клиентов***

8. Выполните настройку, руководствуясь Табл. 44.

Табл. 44 – Настройка автообновления клиентов

Настройка	Описание
Включить обновление	Включите настройку, если требуется обеспечить автоматизированное обновление программы JMS Client на рабочих станциях
Дата начала проверки обновлений	Установите дату, с которой начинается выполнение расписания автоматизированного обновления ПО JMS Client на рабочих станциях.
Дни регулярной проверки обновлений	Настройте расписание проверки наличия обновлений ПО JMS Client по дням недели
Время регулярной проверки (ч:мин)	Настройте время, с которого должна начаться проверка наличия обновлений ПО JMS Client (проверка будет выполняться начиная с указанного момента времени в ближайший день недели, указанный в параметре **Дни регулярной проверки обновлений**, см. выше)

Настройка	Описание
Разброс по времени (мин)	Установите временной диапазон для вычисления случайного отклонения (в минутах) от параметра **Время регулярной проверки** (требуется, чтобы избежать одновременного массового обращения со стороны рабочих станций к файлу дистрибутива из папки общего доступа). Значение по умолчанию: 30 (минут)
Период повтора оповещения (ч)	Временной интервал (в часах), через который выполняется проверка наличия обновления ПО с последующим оповещением пользователя о необходимости обновить ПО JMS Client (в случае если обновление найдено). В случае отказа пользователя от обновления оповещение повторяется через указанный в настоящей настройке период до тех пор, пока обновление ПО не будет произведено. Повтор оповещений отсчитывается от момента, установленного вышеописанными настройками (днем недели и временем) с учетом случайной величины, задаваемой в настройке **Разброс по времени**. Значение по умолчанию: 1 (час)
Проверять цифровую подпись дистрибутивов	Установите флаг, если при настройке ссылки на дистрибутив в JMS следует проверить его электронную подпись. (Проверка дистрибутива при его загрузке на рабочую станцию осуществляется по контрольной сумме, вычисляемой в момент его предварительной загрузки на сервер JMS)
Добавить каталог	Нажмите ссылку для добавления каталога с дистрибутивами JMS Client. (Подробнее см. ниже)

При нажатии на ссылку **Добавить каталог** в поле редактора профиля (Рис. 227) появляются поля для ввода каталога – доступной JMS-серверу сетевой папки с файлами дистрибутивов JMS Client – и имен самих файлов (доступны поля для ввода 32- и 64-битных версий дистрибутива).

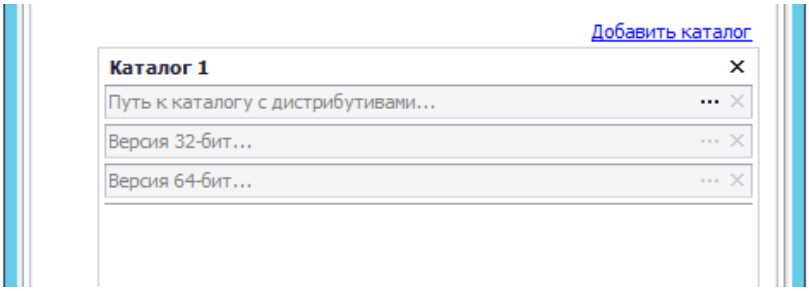


Рис. 227 – Редактор добавления каталога с дистрибутивами JMS Client

Для ввода дистрибутивов выберите сначала **Путь к каталогу с дистрибутивами**, нажав на три точки «...». Затем в полях **Версия 32-бит** и **Версия 64-бит** выберите соответствующий файл дистрибутива (дистрибутивы должны быть одной версии). При загрузке дистрибутива может быть проверена его подпись (см. параметр **Проверить цифровую подпись дистрибутива**).

При необходимости можно добавить дополнительные каталоги дистрибутивов (в целях резервирования). Все указанные дистрибутивы должны быть одной версии.

При принятии решения об обновлении клиентом будет выбран первый файл дистрибутива, отвечающий критериям обновления JMS Client на рабочей станции, а именно: более поздняя версия, чем текущая, и разрядность, соответствующая разрядности установленного клиента.

При добавлении дистрибутива JMS вычисляет и запоминает контрольную сумму файла, которая используется в дальнейшем при его загрузке на рабочую станцию.

Важно! При указании пути к каталогу с дистрибутивами необходимо предоставить разрешение на чтение данного каталога всем доменным компьютерам с установленным JMS-клиентом (т.е. рабочим станциям JMS), а также предоставить разрешение на запись в данный каталог учетной записи, от имени которой запускается серверная служба JMS (на единичном сервере JMS или на узлах кластера JMS).

9. Перейдите на вкладку **Синхронизация сертификатов**.
Окно примет следующий вид.

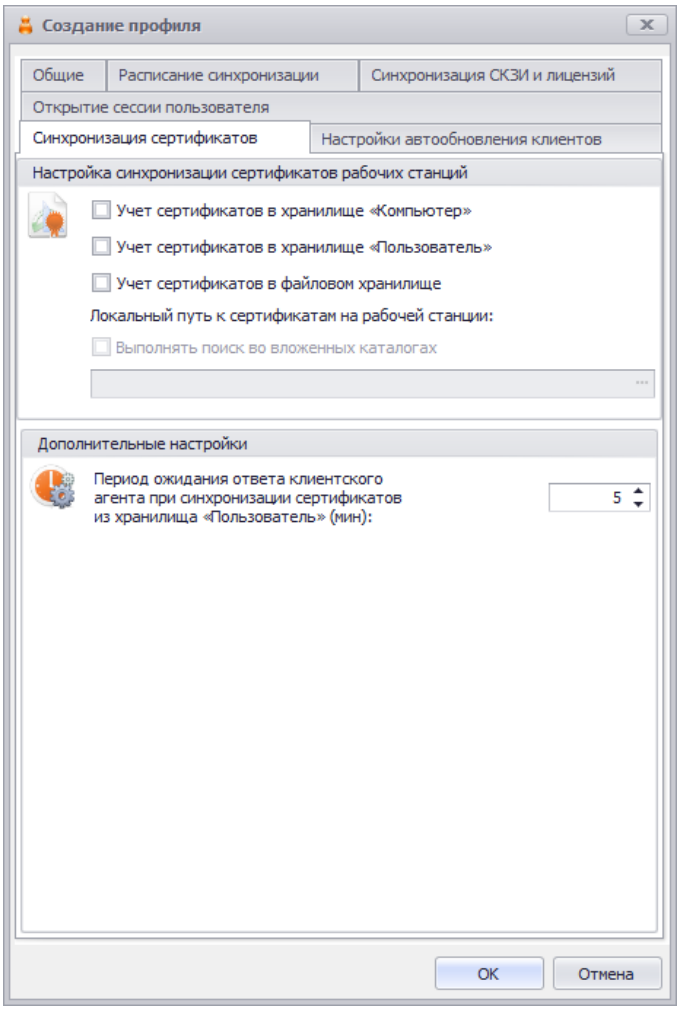


*Рис. 228 – Вкладка **Синхронизации сертификатов***

10. Выполните настройку, руководствуясь Табл. 45.

Табл. 45 – Настройка синхронизации сертификатов

Настройка	Описание
Учет сертификатов в хранилище «Компьютер»	В случае выбора настройки при синхронизации рабочей станции в JMS будет вести учет сертификатов из хранилища «Компьютер» на рабочей станции. После синхронизации сертификаты будут зарегистрированы в JMS и отображаться в разделе **Сертификаты** со статусом **Унаследован.**

Настройка	Описание
	Примечание. Учет (контроль) сертификатов включает в себя также возможность их удаления из хранилища на рабочей стации в том случае, если данные сертификаты были удалены (запланированы к удалению) из консоли управления JMS. Удаление сертификатов с рабочей станции производится в момент синхронизации рабочей станции в соответствии с профилем синхронизации. Синхронизация сертификатов по данному профилю не предусматривает их восстановления на рабочей станции.
Учет сертификатов в хранилище «Пользователь»	В случае выбора настройки при синхронизации рабочей станции в JMS будет вместить учет сертификатов из личного хранилища пользователя на рабочей станции. После синхронизации сертификаты будут зарегистрированы в JMS и отображаться в разделе **Сертификаты** со статусом **Унаследован.** **Примечания:** 1. Синхронизация сертификатов из личного хранилища выполняется только для того пользователя, который открыл пользовательский сеанс (сессию) в клиенте JMS. 2. Учет (контроль) сертификатов включает в себя также возможность их удаления из хранилища на рабочей стации в том случае, если данные сертификаты были удалены (запланированы к удалению) из консоли управления JMS. Удаление сертификатов с рабочей станции производится в момент синхронизации рабочей станции в соответствии с профилем синхронизации. Синхронизация сертификатов по данному профилю не предусматривает их восстановления на рабочей станции.
Учет сертификатов в файловом хранилище	При выборе настройки выполняется учет сертификатов в локальной файловой системе рабочей станции. Поддерживаются следующие типы сертификатов: *.P7B, *.P7C, *.DER, *.PEM, *.CER, *.CRT (размер файла не должен превышать 10 Кбайт). После выбора данной настройки в поле **Локальный путь к сертификатам на рабочей станции** следует указать каталог с сертификатами. Для выбора каталога нажмите три точки «**...**». Допускается указание нескольких каталогов, разделенных символом «;». После синхронизации сертификаты будут зарегистрированы в JMS и отображаться в разделе **Сертификаты** со статусом **Унаследован.** **Примечание.** Учет (контроль) сертификатов включает в себя также возможность их удаления из хранилища на рабочей стации в том случае, если данные сертификаты были удалены (запланированы к удалению) из консоли управления JMS. Удаление сертификатов с рабочей станции производится в момент синхронизации рабочей станции в соответствии с профилем синхронизации. Синхронизация сертификатов по данному профилю не предусматривает их восстановления на рабочей станции.
Выполнять поиск во вложенных каталогах	Настройка доступна при выборе учета сертификатов в файловом хранилище
Период ожидания ответа клиентского агента при синхронизации сертификатов из хранилища «Пользователь» (мин)	Таймаут указанного ожидания в минутах. Настройка используется только при учете сертификатов из личного хранилища пользователя на рабочей станции. Значение по умолчанию: 5 (мин)

11. Перейдите на вкладку **Открытие сессии пользователя**.

Окно примет следующий вид.

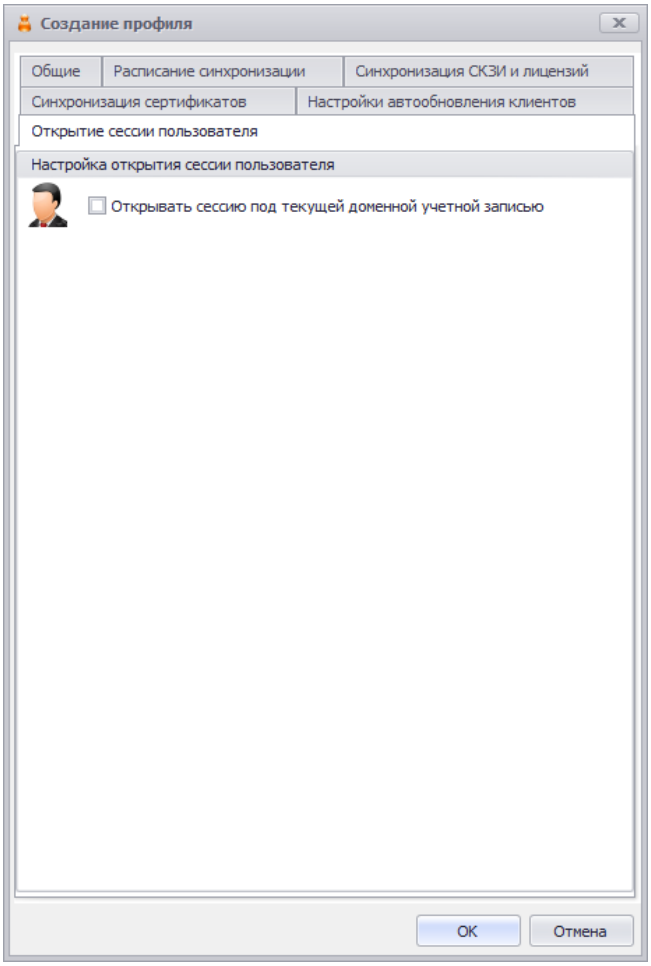


*Рис. 229 – Вкладка **Открытие сессии пользователя***

12. Установите флаг **Открывать сессию под текущей доменной учетной записью**, если необходимо, чтобы сеанс работы зарегистрированного в AD пользователя с JMS открывался автоматически при открытии приложения *Клиент JMS*.

> **Примечание.** Настройка не будет применена к конкретной рабочей станции, если на ней в реестре выполнены настройки для параметра **HKEY_CURRENT_USER\SOFTWARE\Aladdin\Enterprise Application Platform Client\SessionManager\OpenSessionOnAppStart**, подробнее см. в руководстве по установке и настройке JMS [2] в разделе «Настройка параметров автоматического открытия/закрытия клиентского сеанса».
> Любые локальные настройки (настройки в реестре рабочей станции) откткытия пользовательского сеанса в приложения Клиент JMS будут иметь приоритет перед данной настройкой профиля.

13. Для сохраннения настроек профиля нажимите **OK**.

3.9.10 Настройка профиля выпуска аппаратных OTP-токенов

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

- если вы хотите создать новый профиль выпуска токенов, в центральной части окна консоли управления JMS отметьте профиль **Выпуск аппаратных OTP-токенов** и в верхней панели нажмите **Создать**, отобразится окно следующего вида (см. Рис. 230);

– если вы хотите отредактировать существующий профиль, в центральной части окна консоли управления JMS отметьте этот профиль и в верхней панели нажмите **Свойства**.

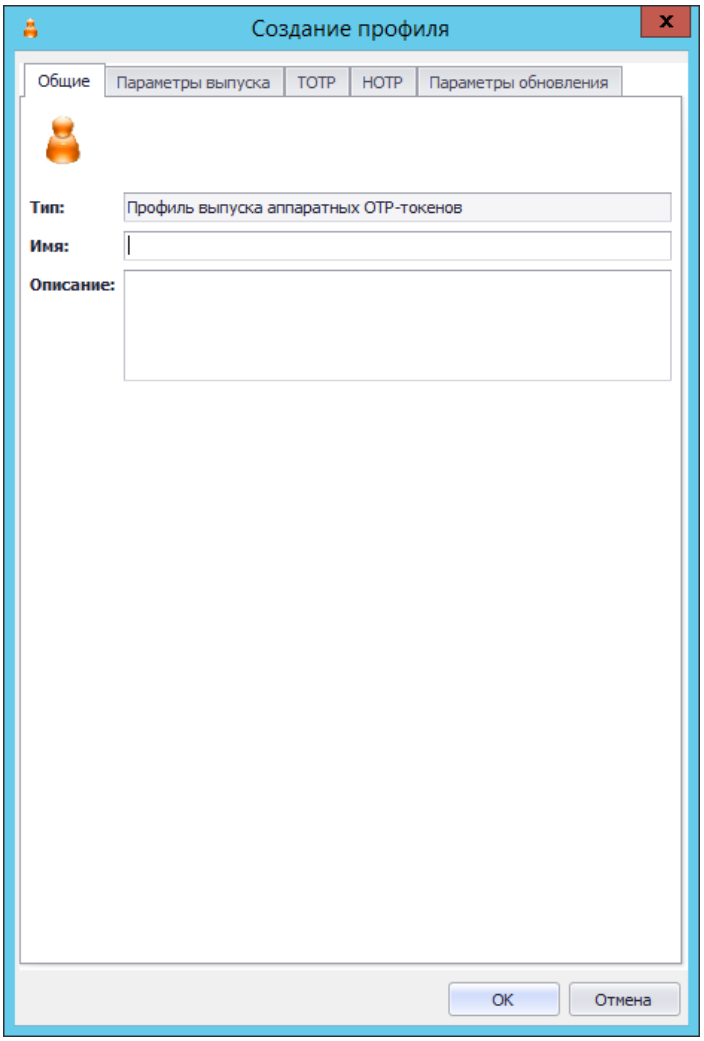


*Рис. 230 – Вкладка **Общие** свойств профиля выпуска аппаратных OTP-токенов*

3. Введите необходимые данные (или измените существующие), после чего перейдите на вкладку **Параметры выпуска**.

Окно примет следующий вид.

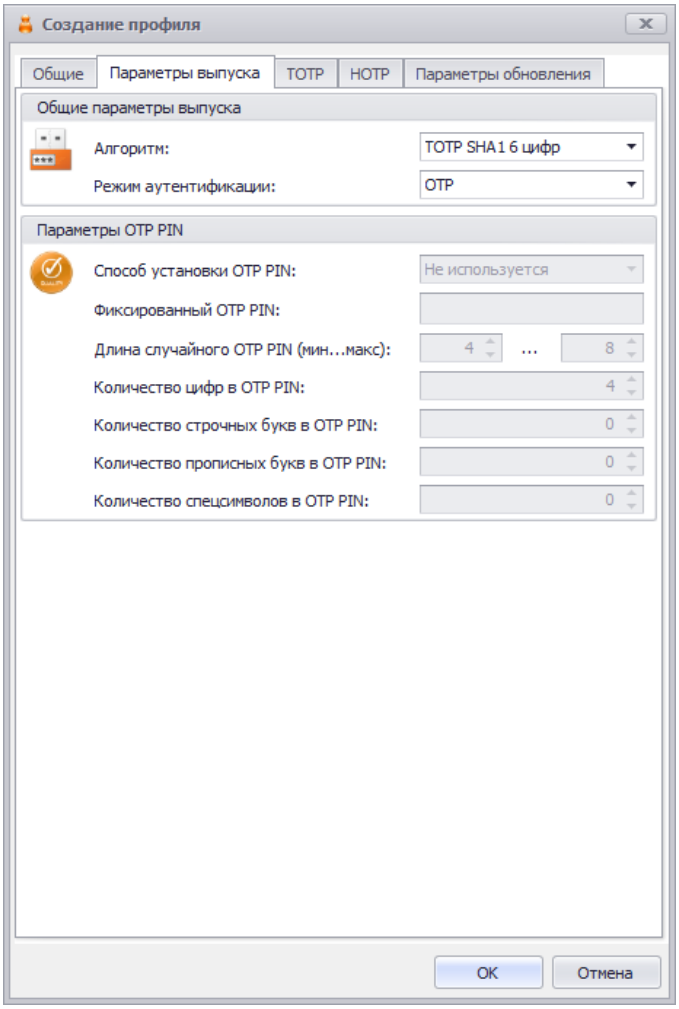


*Рис. 231 – Вкладка **Параметры выпуска***

4. Выполните настройки, руководствуясь Табл. 46.

Табл. 46 – 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;

Настройка	Описание
	– **TOTP SHA1 7 цифр** –пароль длиной 7 цифр; – **TOTP SHA1 8 цифр** –пароль длиной 8 цифр. **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**, раздел «Настройка вкладки Вход по OTP», Табл. 115, с. 508). 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

Настройка	Описание
	разослав по доступным каналам связи: e-mail, SMS и др.) довести до пользователей, для которых выпущены данные аппаратные OTP-токены. 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 … макс)	В случае если в поле **Способ установки OTP PIN** был выбрано **Случайное значение**, установите минимальную (**мин**) и максимальную (**макс**) длину PIN-кода, генерируемого автоматически
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 значение **TOTP_SHA_1_6**, выберите вкладку **TOTP**, в противном случае перейдите к шагу 7, с. 259 (настройки на вкладке **HOTP**).
Окно примет следующий вид.

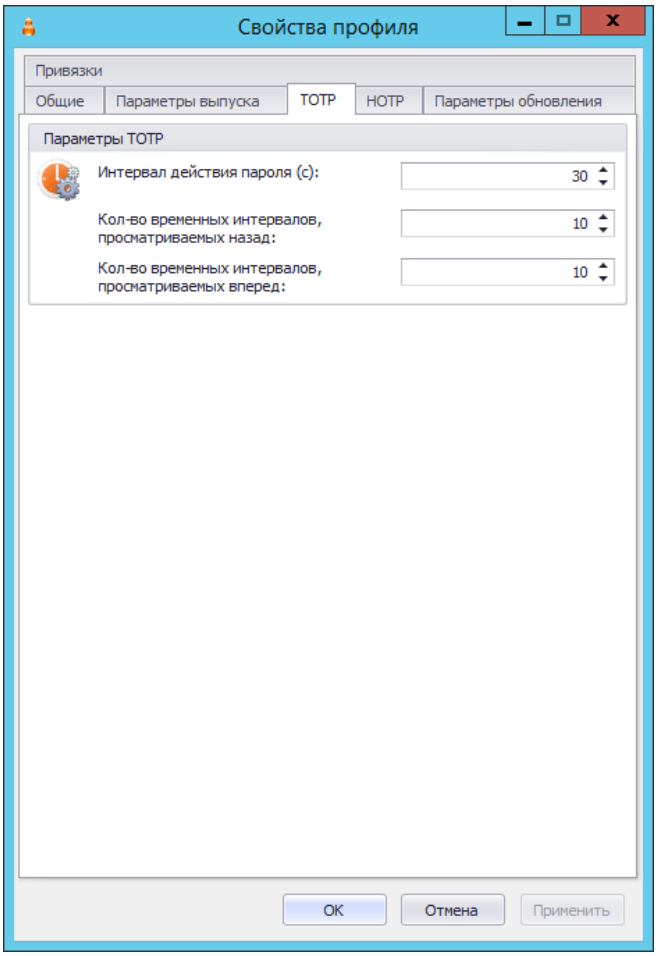


*Рис. 232 – Вкладка **TOTP***

6. Выполните настройки, руководствуясь Табл. 47.

Табл. 47 – Параметры выпуска TOTP-токенов

Настройка	Описание
Интервал действия пароля (с)	Интервал времени (в секундах), в течение которого действителен одноразовый пароль 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.

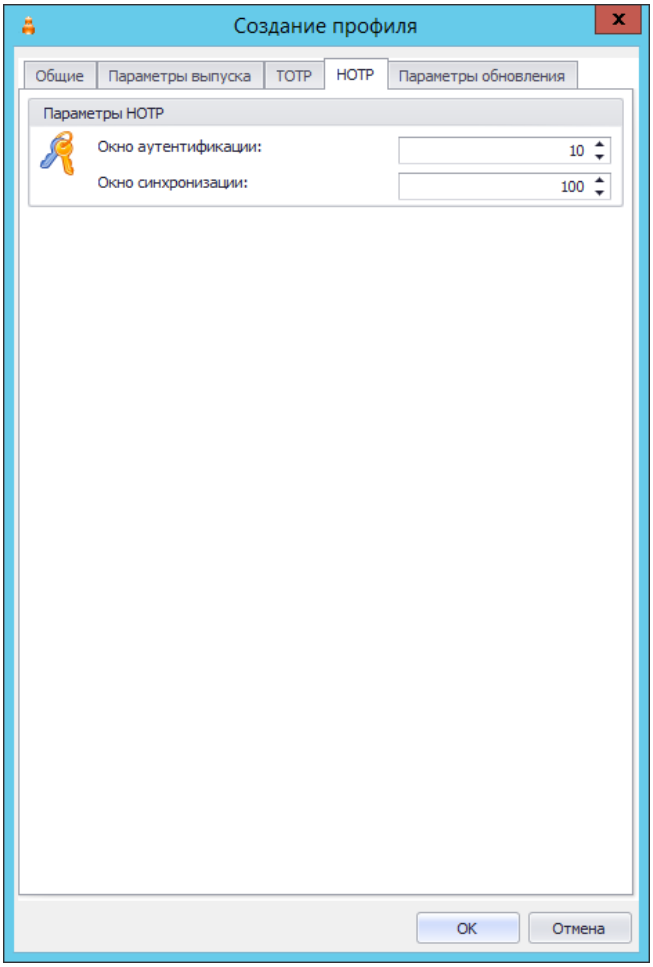


*Рис. 233 – Вкладка **HOTP***

8. Выполните настройки, руководствуясь Табл. 48.

Табл. 48 – 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. 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.

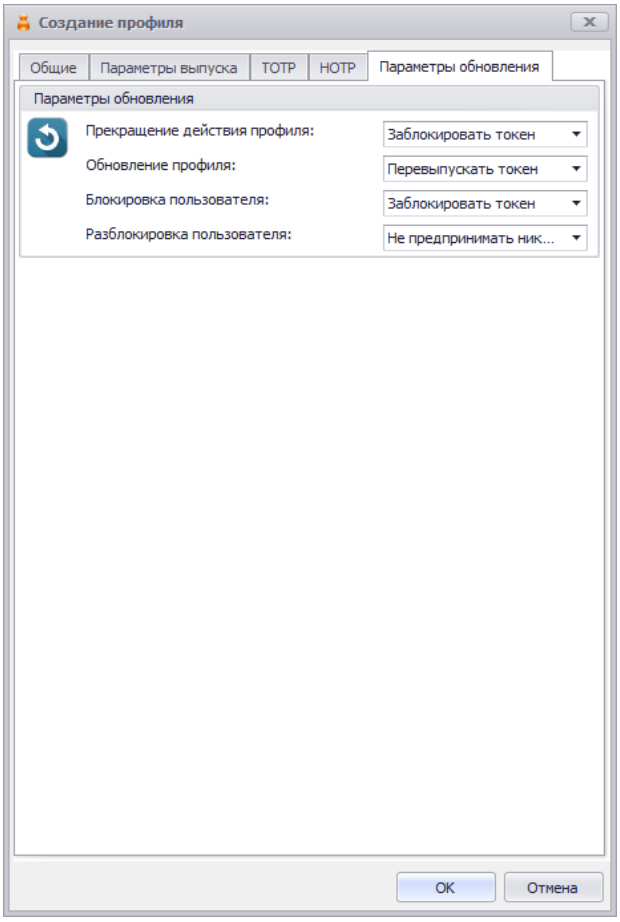


*Рис. 234 – Вкладка **Параметры обновления***

10. Выполните настройки, руководствуясь Табл. 49.

Табл. 49 – 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**
Обновление профиля	Параметр определяет действия, которые необходимо предпринять с OTP-токенами, выпускавшимися по данному профилю, в случае изменения параметров профиля.

Настройка	Описание
	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 завершении настройки профиля нажмите **Ок** для сохранения профиля (сохранения изменений).

3.9.11 Настройка профиля выпуска программных OTP-токенов

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

   – если вы хотите создать новый профиль выпуска токенов, в центральной части окна консоли управления JMS отметьте профиль **Выпуск программных OTP-токенов** и в верхней панели нажмите **Создать**, отобразится окно следующего вида (см. Рис. 235);
   – если вы хотите отредактировать существующий профиль, в центральной части окна консоли управления JMS отметьте этот профиль и в верхней нажмите **Свойства**.

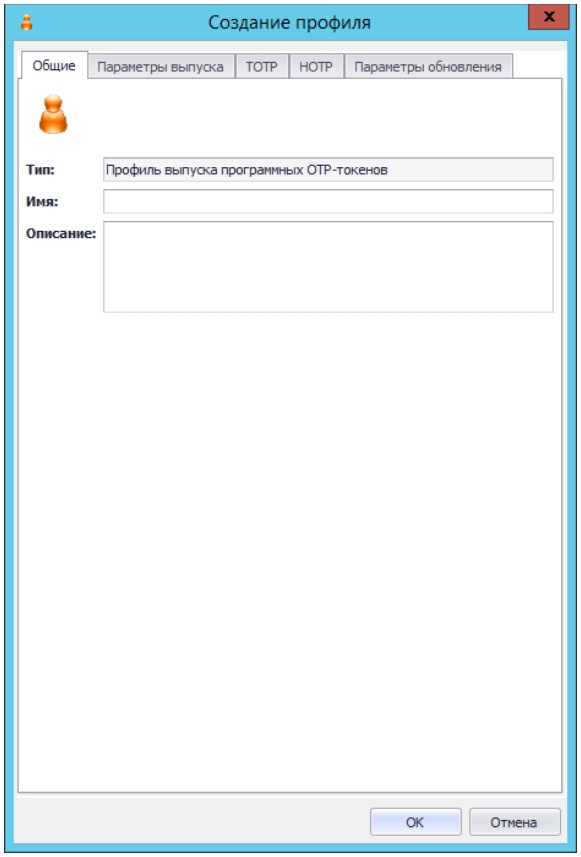


*Рис. 235 – Вкладка **Общие** свойств профиля выпуска программных OTP-токенов*

3. Введите необходимые данные (или измените существующие), после чего перейдите на вкладку **Параметры выпуска**.

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.

Окно примет следующий вид.

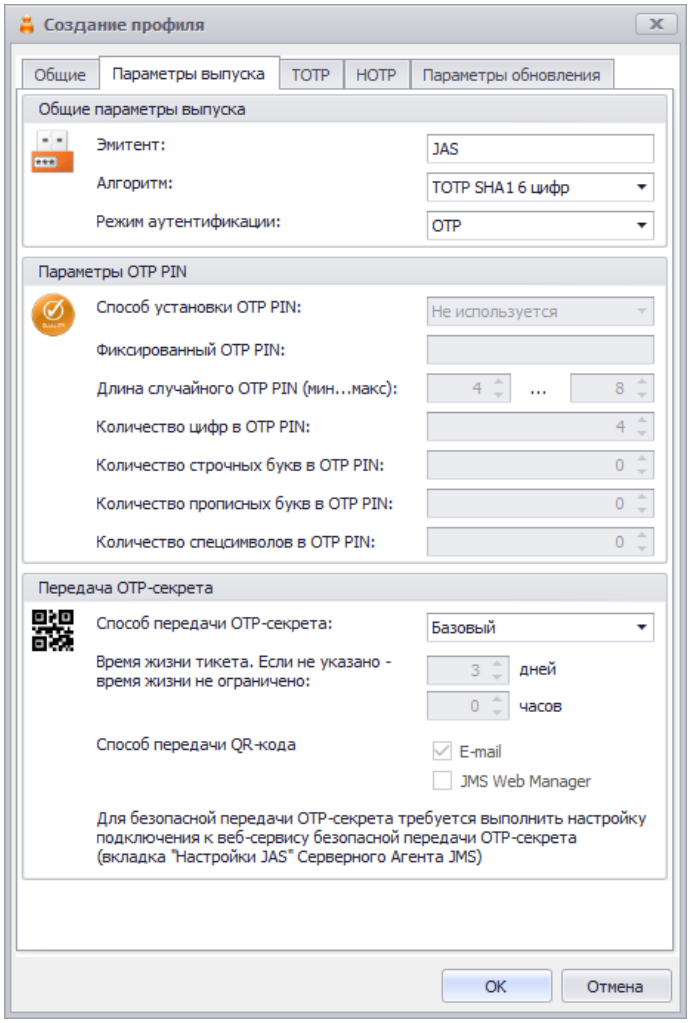


*Рис. 236 – Вкладка **Параметры выпуска***

4. Выполните настройки, руководствуясь Табл. 50.

Табл. 50 – 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:

Настройка	Описание
	– **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. **Примечание.** Обратите внимание, что создаваемый экземпляр профиля может быть предназначен для выпуска только одного типа программных токенов: либо TOTP, либо HOTP.
<секция> **Параметры OTP PIN**	
Режим аутентификации **Способ установки OTP PIN** **Фиксированный OTP PIN** **Длина случайного OTP PIN** **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. 46, с. 256)
<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	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 буде передан пользователю: • **E-mail** – в почтовый ящик пользователя; • **JMS Web Manager** – непосредственно в интерфейсе личного кабинета пользователя (посредством сервера JWM)

5. В случае, если в поле **Алгоритм** было выбран алгоритм по спецификации *TOTP*, выберите вкладку **TOTP** (в противном случае перейдите к шагу 7, с. 267 – настройки на вкладке **HOTP**). Окно примет следующий вид.

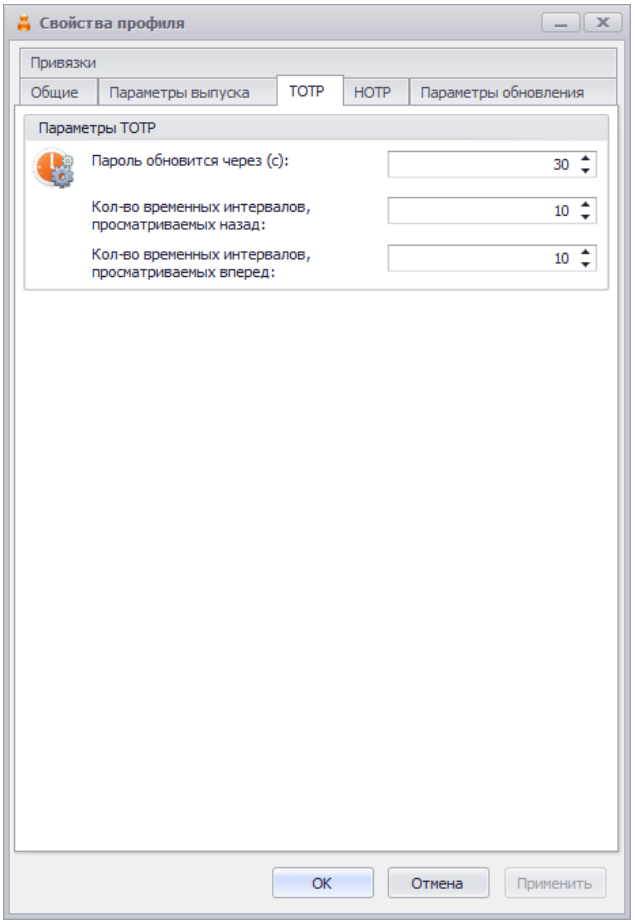


*Рис. 237 – Вкладка **TOTP***

6. Выполните настройки, руководствуясь Табл. 51.

Табл. 51 – 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**
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**

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

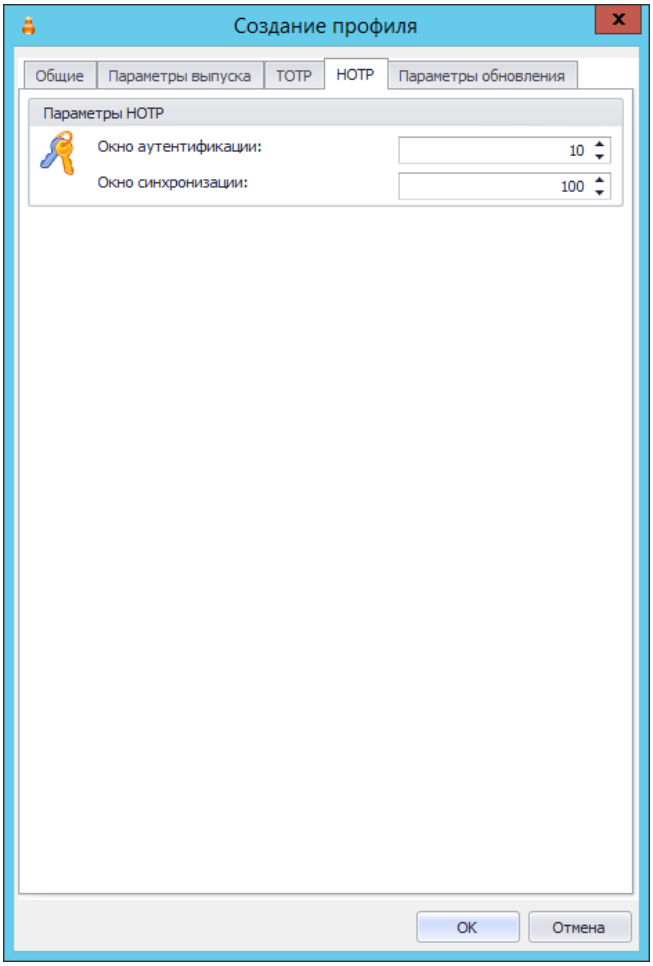


*Рис. 238 – Вкладка **HOTP***

8. Выполните настройки, руководствуясь Табл. 48, с. 260.
9. Выберите вкладку **Параметры обновления**.

Окно примет следующий вид.

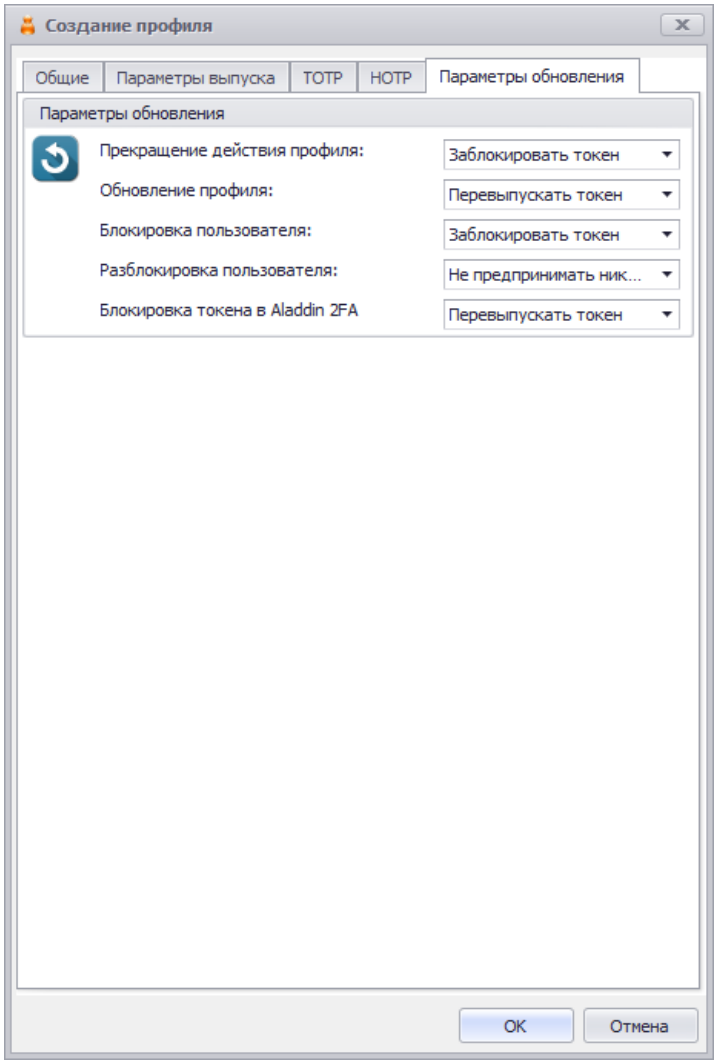


*Рис. 239 – Вкладка **Параметры обновления***

10. Выполните настройки, руководствуясь Табл. 52.

Табл. 52 – Параметры обновления профиля

Настройка	Описание
Прекращение действия профиля **Обновление профиля** **Блокировка пользователя** **Разблокировка пользователя**	Для данных параметров выполните настройки, руководствуясь Табл. 49, с. 261.
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

Настройка	Описание
	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**

11. По завершении настройки профиля нажмите **Ок** для сохранения профиля (сохранения изменений).

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. 240) выполните соответствующую настройку в серверном агенте JMS (приложение *Сервер JMS*), (вкладка **Настройка -> Настройка транспорта -> Настройка SMTP**). Подробнее см. руководство по установке и настройке JMS [2].

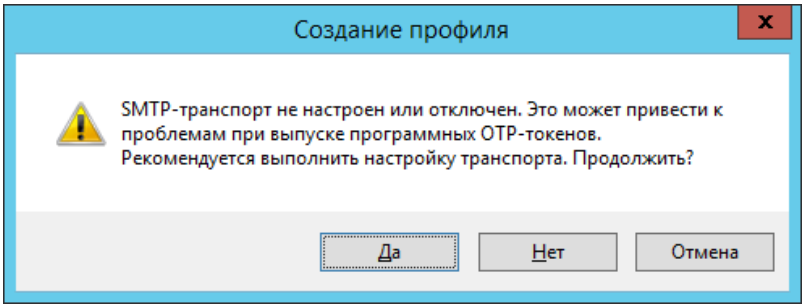


Рис. 240 – Предупреждение о необходимости включить и настроить SMTP-транспорт

3.9.12 Настройка профиля выпуска Messaging-токенов

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

   – если вы хотите создать новый профиль выпуска messaging-аутентификаторов, в центральной части окна консоли управления JMS отметьте профиль **Выпуск Messaging-токенов** и в верхней панели нажмите **Создать**, отобразится окно следующего вида (см. Рис. 241);
   – если вы хотите отредактировать существующий профиль, в центральной части окна консоли управления JMS отметьте этот профиль и в верхней панели нажмите **Свойства**.

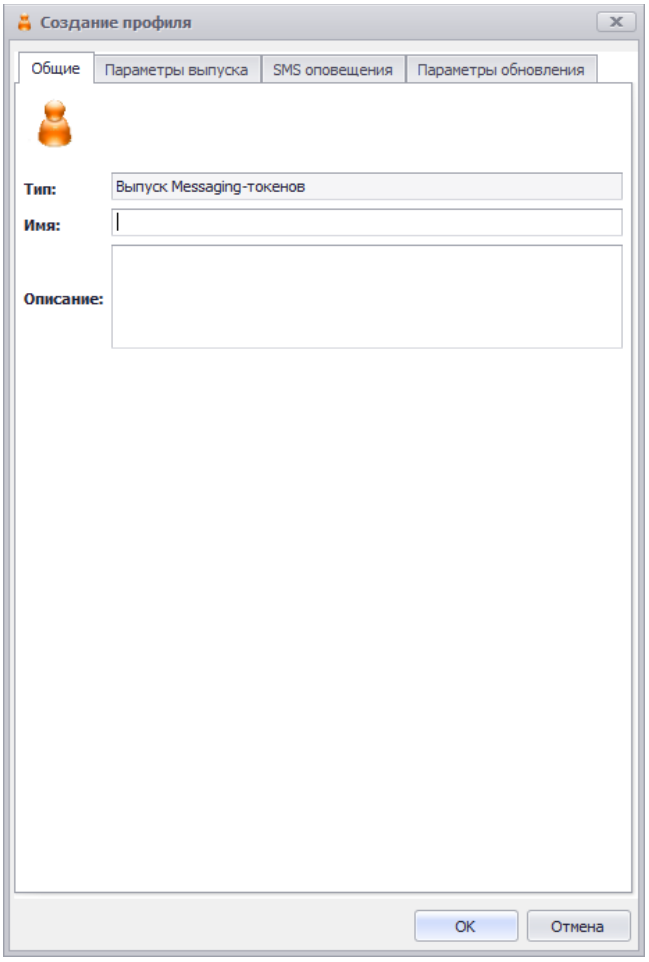


*Рис. 241 – Вкладка **Общие** свойств профиля выпуска Messaging-токенов*

3. Введите необходимые данные (или измените существующие), после чего перейдите на вкладку **Параметры выпуска**.

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.

Окно примет следующий вид.

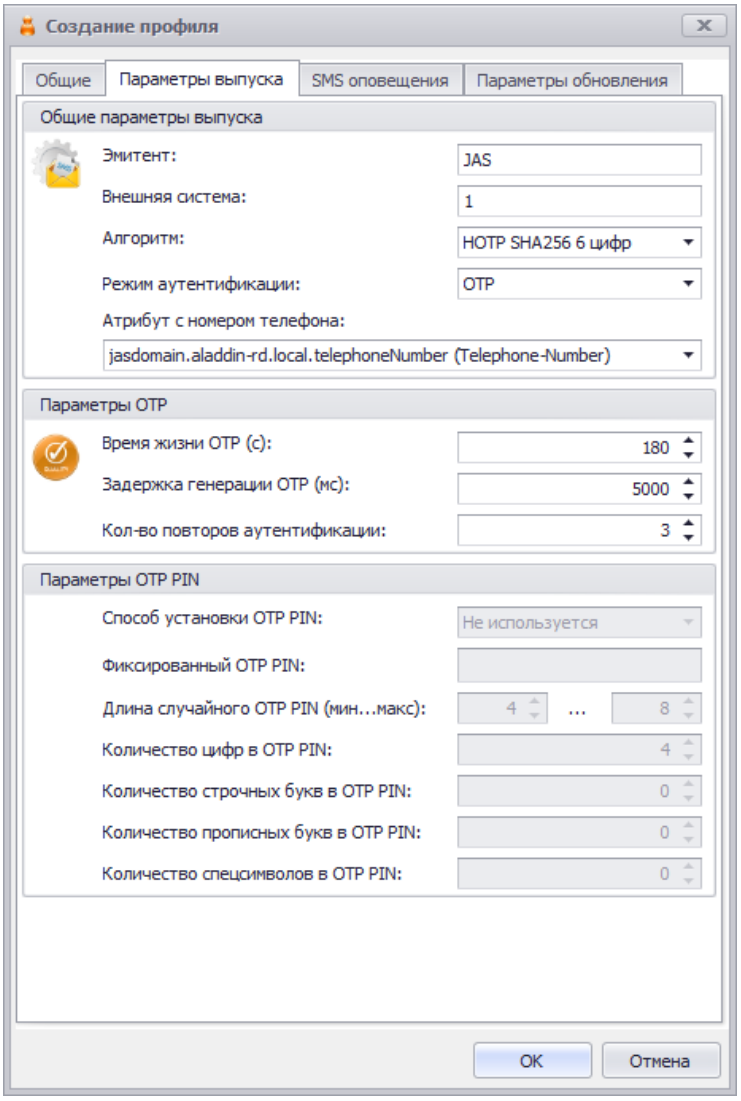


*Рис. 242 – Вкладка **Параметры выпуска***

4. Выполните настройки, руководствуясь Табл. 53.

Табл. 53 – Параметры выпуска Messaging-токенов

Настройка	Описание
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).

Настройка	Описание
	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** (см. , раздел «Настройка вкладки Вход по Messaging», Табл. 117, с. 512). 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 данные настройки согласованы с настройками модуля JWM (см. параметры **Запрашивать OTP-PIN**-код и **Запрашивать доменный пароль** в секции **Настройки OTP**, раздел «Настройка вкладки Вход по Messaging», Табл. 117, с. 512). 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 (Рис. 12, с. 40), пролистав поле **Атрибуты учетной записи**.

Настройка	Описание
	2. Атрибут может содержать одновременно несколько номеров телефонов (данная возможность реализуется средствами самой ресурсной системы).
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** • **Способ установки OTP PIN** • **Фиксированный OTP PIN** • **Длина случайного OTP PIN (мин … макс)** • **Количество цифр в OTP PIN** • **Количество строчных букв в OPT PIN** • **Количество прописных букв в OPT PIN** • **Количество спецсимволов в OPT PIN**	Выполните настройки по аналогии настройками **Параметров выпуска** в профиле выпуска аппаратных OTP-токенов (см. Табл. 46, с. 256).

5. Выберите вкладку **SMS-оповещения**.

Окно примет следующий вид.

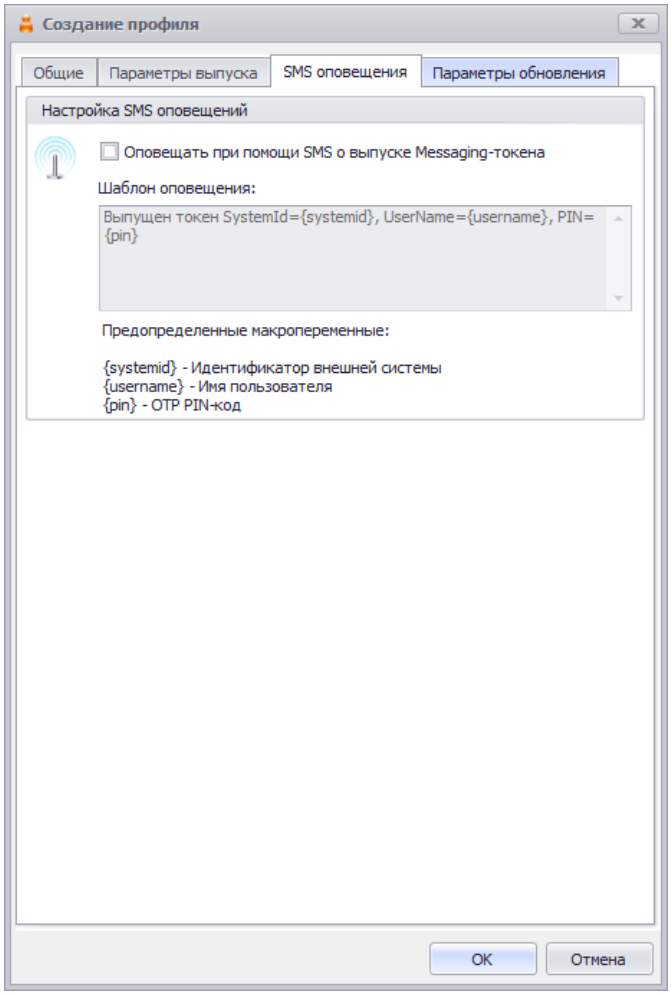


*Рис. 243 – Вкладка **SMS оповещения***

6. Выполните настройки, руководствуясь Табл. 54.

Табл. 54 – 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 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.

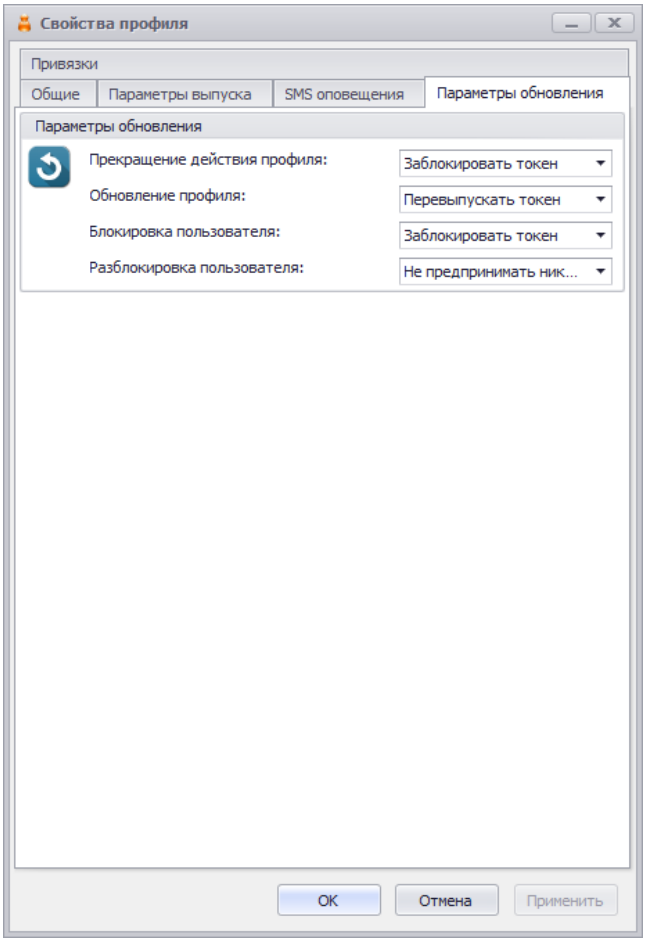


*Рис. 244 – Вкладка **Параметры обновления***

8. Выполните настройки по аналогии с настройками **Параметров обновления** в профиле выпуска OTP-токенов (см. Табл. 49, с. 261).
9. По завершении настройки профиля нажмите **Ок** для сохранения профиля (сохранения изменений).

3.9.13 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 -> Профили**.
2. Выполните одно из следующих действий:

- если вы хотите создать новый профиль выпуска токенов, в центральной части окна консоли управления JMS отметьте профиль **Выпуск Push OTP-токенов** и в верхней панели нажмите **Создать**, отобразится окно следующего вида (см. Рис. 235);
- если вы хотите отредактировать существующий профиль, в центральной части окна консоли управления JMS отметьте этот профиль и в верхней нажмите **Свойства**.

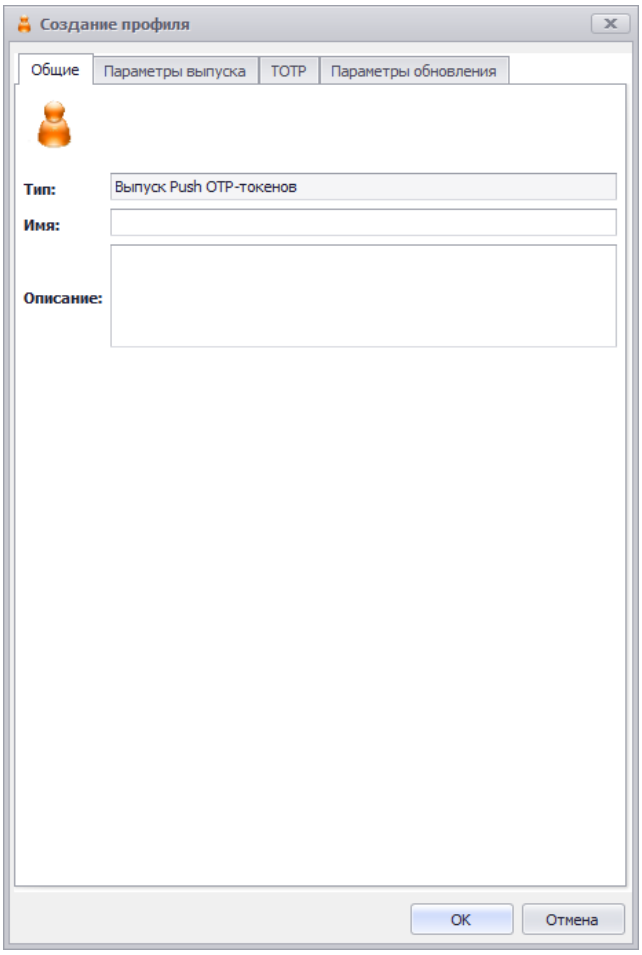


*Рис. 245 – Вкладка **Общие** свойств профиля выпуска Push OTP-токенов*

3. Введите необходимые данные (или измените существующие), после чего перейдите на вкладку **Параметры выпуска**.

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.

Окно примет следующий вид.

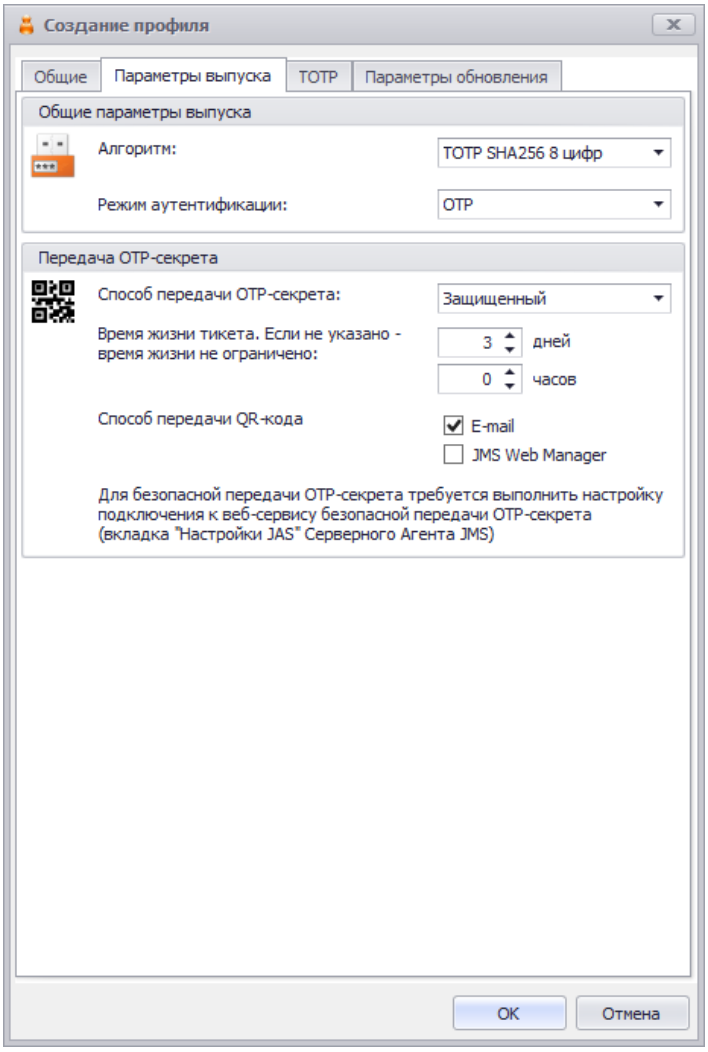
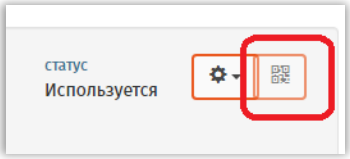


*Рис. 246 – Вкладка **Параметры выпуска***

4. Выполните настройки, руководствуясь Табл. 55.

Табл. 55 – 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*

Настройка	Описание
Время жизни тикета	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 серверном агенте JMS (приложение *Сервер JMS*) должен настроен транспортный почтовый сервис (вкладка **Настройка -> Настройка транспорта -> Настройка SMTP**). Подробнее см. руководство по установке и настройке JMS [2].

5. Выберите вкладку **TOTP**.

Окно примет следующий вид.

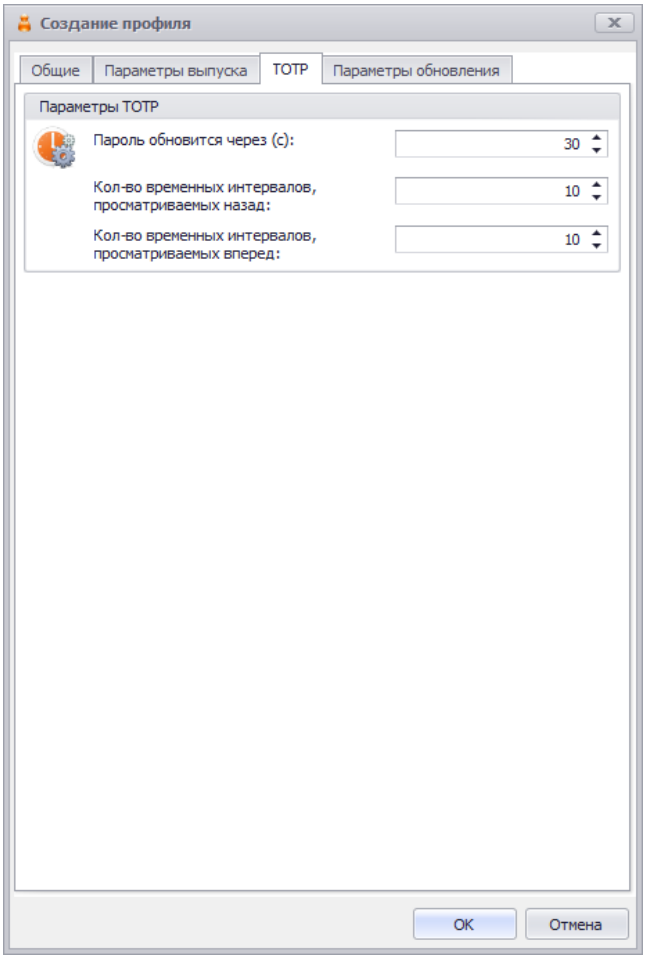


*Рис. 247 – Вкладка **TOTP***

6. Выполните настройки, руководствуясь Табл. 51, с. 267.
7. Выберите вкладку **Параметры обновления**.

Окно примет следующий вид.

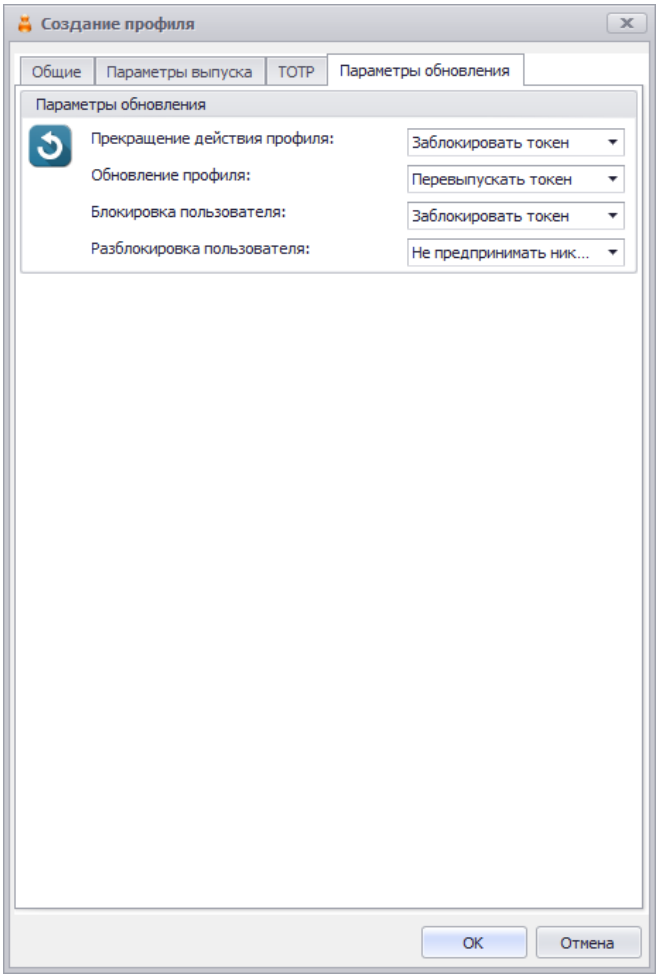


*Рис. 248 – Вкладка **Параметры обновления***

8. Выполните настройки, руководствуясь Табл. 49, с. 261.
9. По завершении настройки профиля нажмите **Ок** для сохранения профиля (сохранения изменений).

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. 249) выполните дополнительные настройки в серверном агенте JMS (приложение *Сервер 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].
2. При появлении предупреждения об отсутствии настройки SMTP-транспорта (Рис. 250) выполните соответствующую настройку в серверном агенте JMS, (вкладка **Настройка -> Настройка транспорта -> Настройка SMTP**). Подробнее см. руководство по установке и настройке JMS [2].

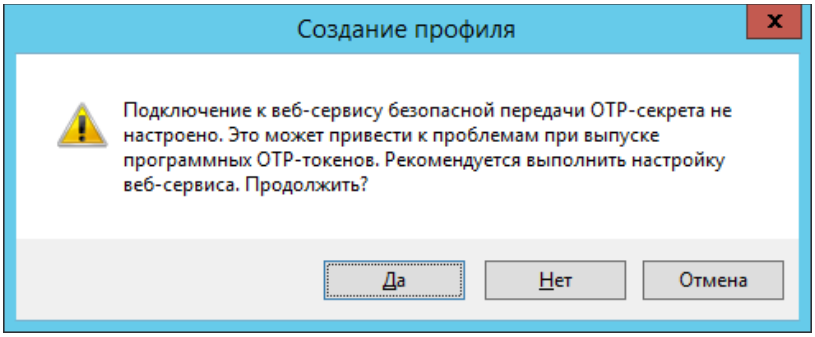


Рис. 249 – Предупреждение о необходимости настроить веб-сервис безопасной передачи OTP-секрета

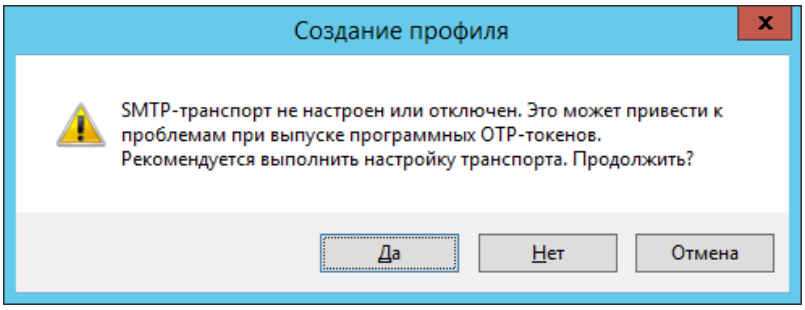


Рис. 250 – Предупреждение о необходимости включить и настроить SMTP-транспорт

3.9.14 Настройка профиля пользователя КриптоПро DSS

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

   - если вы хотите создать новый профиль пользователя КриптоПро DSS, в центральной части окна консоли управления JMS отметьте **Пользователь КриптоПро DSS** и в верхней панели нажмите **Создать**, отобразится окно следующего вида (см. Рис. 251);
   - если вы хотите отредактировать существующий профиль, в центральной части окна консоли управления JMS отметьте этот профиль и в верхней панели нажмите **Свойства**.

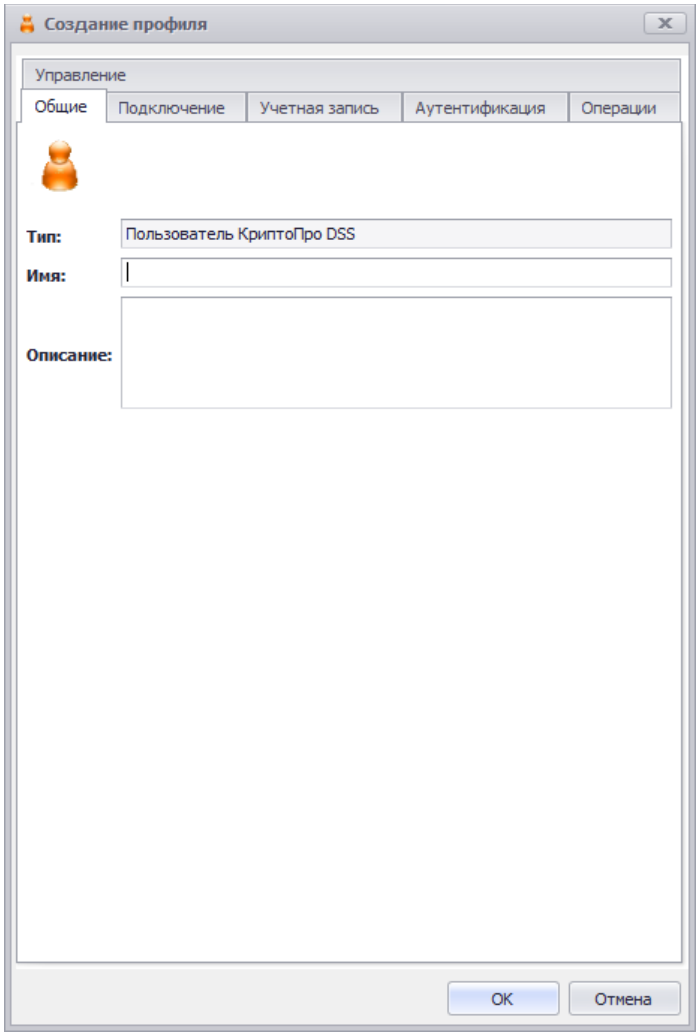


*Рис. 251 – Вкладка **Общие** свойств профиля пользователя КриптоПро DSS*

3. Введите необходимые данные (или измените существующие), после чего перейдите на вкладку **Подключение**.

Окно примет следующий вид.

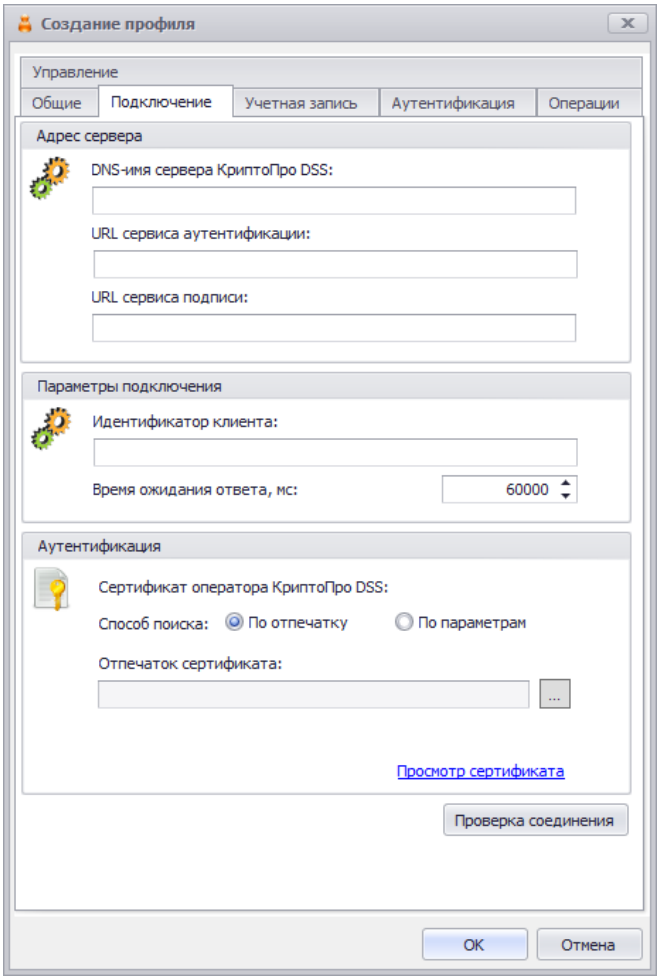


*Рис. 252 – Вкладка **Подключение***

4. Выполните настройки, руководствуясь Табл. 56.

Табл. 56 – Параметры подключения к серверу КриптоПро DSS

Настройка	Описание
DNS-имя сервера КриптоПро DSS	Введите DNS-имя хоста, на котором установлен сервер КриптоПро DSS
URL сервера аутентификации	Введите абсолютный URL-адрес *Центра Идентификации КриптоПро DSS* в формате: `https://<hostname>:<port >/<ApplicationName>`, где • **hostname** – DNS-имя хоста, на котором развёрнут экземпляр Центра Идентификации DSS; • **port** – TLS порт. По умолчанию «4430». • **ApplicationName** – имя веб-приложения *Центр Идентификации КриптоПро DSS*. По умолчанию «STS». **Примечания.** 1. Значение по умолчанию заполняется автоматически при заполнении поля **DNS-имя сервера КриптоПро DSS** 2. Подробную информацию о формате адреса Центра идентификации DSS см. в комплекте документации производителя [6]

Настройка	Описание
URL сервера подписи	Введите абсолютный URL-адрес *Сервиса подписи КриптоПро DSS* в формате: `https://<hostname>:<port >/<ApplicationName>`, где • **hostname** – DNS-имя хоста, на котором развёрнут экземпляр *Сервис Подписи КриптоПро DSS*; • **port** – TLS порт. По умолчанию «4430». • **ApplicationName** – имя веб-приложения *Сервиса Подписи КриптоПро DSS*. По умолчанию «SignServer». **Примечания.** 1. Значение по умолчанию заполняется автоматически при заполнении поля **DNS-имя сервера КриптоПро DSS** 2. Подробную информацию о формате адреса *Сервиса Подписи КриптоПро DSS* см. в комплекте документации производителя [6]
Идентификатор клиента	Идентификатор клиентского приложения КриптоПро DSS, формируемый при добавлении нового OAuth-клиента (подробнее см. документацию производителя [6]). Значение параметра следует получить у владельца сервиса КриптоПро DSS.
Время ожидания ответа, мс	Время ожидания ответа (таймаута) от OAuth-клиента на сервере КриптоПро DSS в миллисекундах. Значение по умолчанию: **60000**
Сертификат оператора КриптоПро DSS	Сертификат оператора – должностного лица, выполняющего функции администрирования пользователей и сертификатов в рамках OAuth-клиента на сервере КриптоПро DSS. (Сервер JMS взаимодействует с сервером КриптоПро DSS от имени оператора КриптоПро DSS). Данный сертификат следует получить у владельца сервиса КриптоПро DSS. Выберите сертификат и нажмите **Проверка соединения** для проверки корректности настроек подключения к серверу КриптоПро DSS, сделанных на вкладке **Подключение** **Примечание.** Сертификат оператора должен быть предварительно установлен в хранилище «Личное» той учетной записи, от которой запущена служба JMS; сертификат корневого УЦ (сертификата оператора) – в хранилище «Доверенные корневые центры сертификации», а промежуточных – в хранилище «Промежуточные центры сертификации» той же учетной записи. **Важно!** Для успешного подключения к серверу КриптоПро DSS убедитесь что в настройках хоста (сервера JMS) и установленных на нем библиотек .Net доступен протокол TLS 1.2. Подробнее см. раздел «Подготовка к использованию протоколов SSL/TLS» руководства по установке и настройке JMS [2].

5. Выберите вкладку **Учетная запись**.

Окно примет следующий вид.

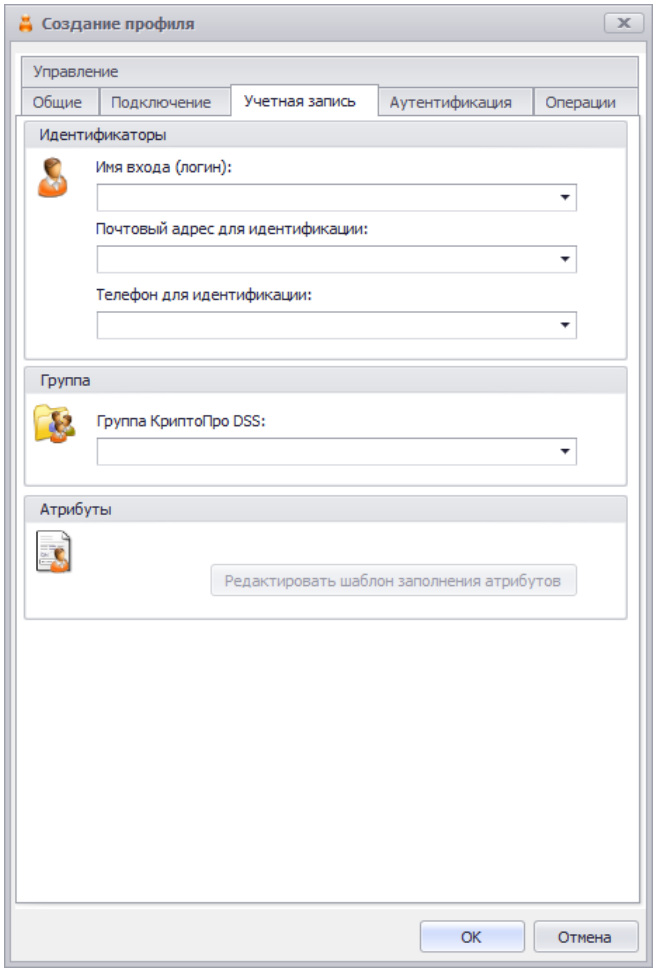


*Рис. 253 – Вкладка **Учетная запись***

6. Выполните настройки, руководствуясь Табл. 57.

Табл. 57 – Параметры учетной записи пользователя создаваемого/администрируемого в КриптоПро DSS

Настройка	Описание
Идентификаторы (секция)	В секции **Идентификаторы** перечислены атрибуты пользователя, которые могут быть использованы при аутентификации/аутентификации пользователя в КриптоПро DSS: • **Имя входа (Логин)** – выберите атрибут пользователя в JMS, который должен соответствовать полю **Логин** в web-интерфейсе КриптоПро DSS • **Почтовый адрес для идентификации** – следует установить, если в КриптоПро DSS установлена возможность идентификации/аутентификации по адресу электронной почты • **Телефон для идентификации** – следует установить, если в КриптоПро DSS установлена возможность идентификации/аутентификации по номеру телефона **Примечание.** Атрибуты пользователя, выбираемые для их идентификации/аутентификации (например e-mail) могут отличаться от соответствующих атрибутов (e-mail), используемых при выпуске сертификата пользователя в КриптоПро DSS.
Группа КриптоПро DSS	Выберите группу КриптоПро DSS, определенную на сервере DSS для вашей организации

Настройка	Описание
Атрибуты	Нажмите **Редактировать шаблон заполнения атрибутов**, чтобы настроить соответствие атрибутов пользователя в КриптоПро DSS атрибутам пользователя в ресурсной системе (или системах) JMS. Редактирование шаблона производится по аналогии с редактированием шаблона в профиле выпуска сертификата КриптоПро УЦ 2.0, см. Рис. 646, с. 658 и Табл. 138, с. 658. Указанные в строках таблицы атрибуты могут в дальнейшем использоваться в полях сертификата (определяется *профилем выпуска сертификата на КриптоПро DSS* с помощью шаблона сертификата, заданного в DSS). Если в DSS какие-либо из атрибутов пользователя помечены как обязательные, на необходимость настройки их отображения на атрибут в JMS указывает предупреждение «Требуется корректировка шаблона атрибутов пользователя» (предупреждение отображается в секции **Атрибуты** красным цветом). Если при создании профиля в столбце **Profile OID** таблицы редактирования атрибутов какие-либо атрибуты уже определены (например атрибут **Общее имя**), это значит, что в КриптоПро DSS данные атрибуты для группы, указанной в **Группа КриптоПро DSS**, помечены как обязательные, и настройка соответствия для них в JMS также является обязательной (в противном случае профиль не сможет быть сохранен).

7. Выберите вкладку **Аутентификация**.

Окно примет следующий вид.

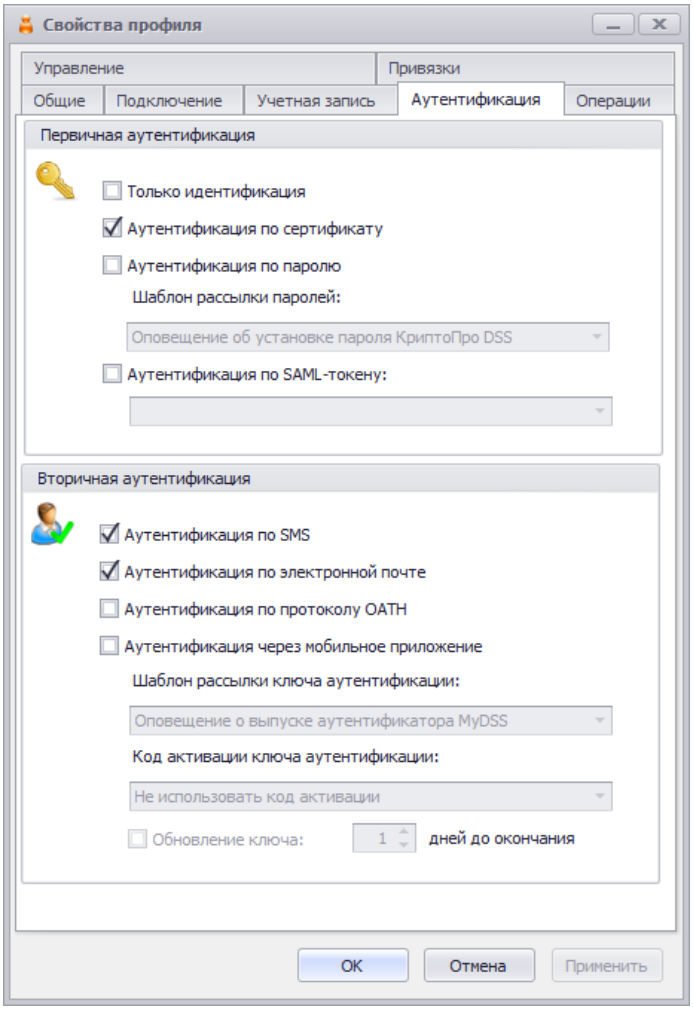


*Рис. 254 – Вкладка **Аутентификация***

8. Выполните настройки, руководствуясь Табл. 58.

Табл. 58 – Параметры аутентификации пользователя в КриптоПро DSS

Настройка	Описание
Только идентификация	Флаг, соответствует одноименному флагу[1] в разделе настроек параметров пользователя *Методы первичной аутентификации* в интерфейсе КриптоПро DSS
Аутентификация по паролю	Флаг, соответствует одноименному флагу[1] в разделе настроек параметров пользователя *Методы первичной аутентификации* в интерфейсе КриптоПро DSS
Шаблон рассылки паролей	Выберите шаблон для оповещения пользователей о назначении пароля. По умолчанию в JMS предусмотрен шаблон **Оповещение об установке пароля КриптоПро DSS.** Оповещение передается на стандартный email-адрес пользователя (определяется в ресурсной системе Active Directory, используемой JMS).

Настройка	Описание
	Примечания: 3. При необходимости использовать собственный шаблон, следует его разработать и импортировать в JMS (см. раздел «Шаблоны уведомлений», с. 433) 4. Для получения оповещений у пользователей, привязанных к настоящему профилю, в ресурсной системе Active Directory должен быть настроен адрес электронной почты. 5. В серверном агенте JMS (приложение *Сервер JMS*) должен быть настроен транспортный почтовый сервис (вкладка **Настройка -> Настройка транспорта -> Настройка SMTP**). Подробнее см. руководство по установке и настройке JMS [2].
Аутентификация по SAML-токену	Флаг, соответствует одноименному флагу[1] в разделе настроек параметров пользователя *Методы первичной аутентификации* в интерфейсе КриптоПро DSS При установке флага в поле раскрывающегося списка следует выбрать имя *стороннего центра идентификации* (список сторонних центров идентификации настраивается на стороне КриптоПро DSS)
Аутентификация по SMS	Флаг, соответствует одноименному флагу[1] в разделе настроек параметров пользователя *Методы вторичной аутентификации* в интерфейсе КриптоПро DSS
Аутентификация по электронной почте	То же
Аутентификация по протоколу OATH	То же
Аутентификация через мобильное приложение	Флаг, соответствует флагу **Аутентификация с помощью мобильного прилжоения**[1] в разделе настроек параметров пользователя *Методы вторичной аутентификации* в интерфейсе КриптоПро DSS При установке флага **Аутентификация через мобильное приложение следует**
Шаблон рассылки ключа аутентификации	При установке флага **Аутентификация через мобильное приложение** выберите шаблон сообщения с ключом аутентификации. По умолчанию в JMS предусмотрен шаблон **Оповещение об установке пароля КриптоПро DSS.** Оповещение передается на стандартный email- адрес пользователя (определяется в ресурсной системе Active Directory, используемой JMS). **Примечание.** Порядок создания собственного шаблона и условия рассылки те же, что и для поля **Шаблон рассылки паролей** (выше).
Код активации ключа аутентификации	При установке флага **Аутентификация через мобильное приложение выберите** действия, которое необходимо произвести по отношению к коду активации ключа аутентификации: • **Не использовать код активации**

Настройка	Описание
	• **Высылать код активации по email** — отправка кода активации осуществляется средствами КриптоПро DSS по стандартному email-адресу пользователя (определяется в ресурсной системе Active Directory, используемой JMS). • **Высылать код активации по SMS –** — отправка кода активации осуществляется средствами КриптоПро DSS через SMS по номеру телефона пользователя, указанному в БД КриптоПро DSS
Обновление ключа	При установке флага **Аутентификация через мобильное приложение** при необходимости установите флаг **Обновление ключа** и выберите, за какой период времени в днях до окончания действия ключа аутентификации должно быть выполнено автоматическое обновление данного ключа. **Примечание.** Срок действия ключа аутентификации (определяется настройками КриптоПро DSS) следует узнать у администратора данного сервиса.

[1]Подробное описание параметров аутентификации пользователя в КриптоПро DSS см. в документации производителя [6]

9. Выберите вкладку **Операции**.
Окно примет следующий вид.

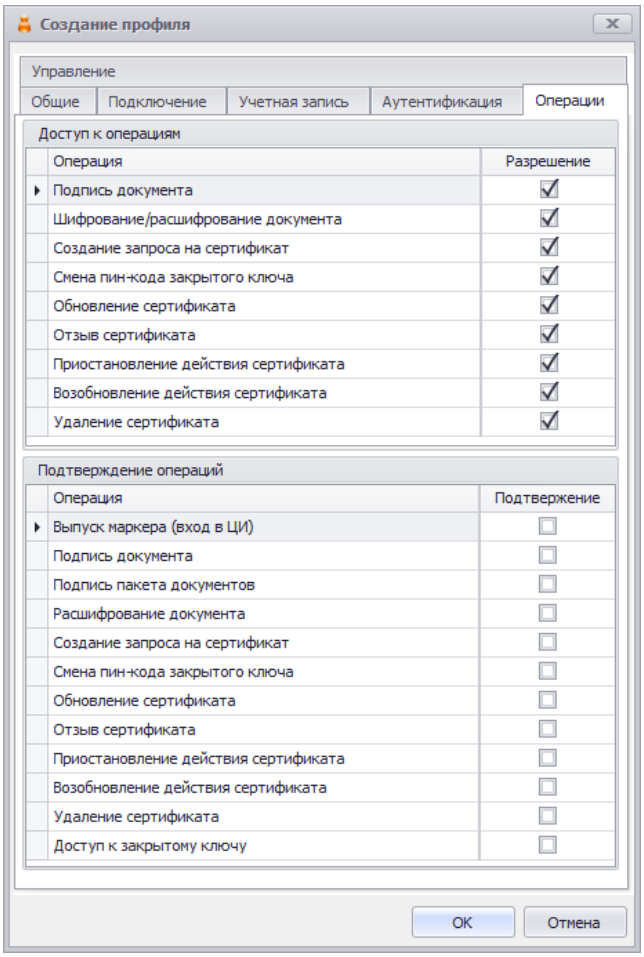


*Рис. 255 – Вкладка **Операции***

10. Выполните настройки, руководствуясь Табл. 59.

Табл. 59 – Параметры обновления профиля

Настройка	Описание
(параметры секции **Доступ к операциям**) • **Подпись документа** • **Шифрование/расшифрование документа** • **Создание запроса на сертификат** • **Смена пин-кода закрытого ключа** • **Удаление сертификата** • **Обновление сертификата** • **Отзыв сертификата** • **Приостановление действия сертификата** • **Возобновление действия сертификата**	Параметры секции соответствуют одноименным параметрам[1] секции **Доступ к операциям** настроек аутентификации пользователя в web-интерфейсе оператора КриптоПро DSS
(параметры секции **Подтверждение операций**) • **Выпуск маркера (вход в ЦИ)** • **Подпись документа** • **Подпись пакета документов** • **Расшифрование документа** • **Создание запроса на сертификат** • **Смена пин-кода закрытого ключа** • **Обновление сертификата** • **Отзыв сертификата** • **Приостановление действия сертификата** • **Возобновление действия сертификата** • **Удаление сертификата** • **Доступ к закрытому ключу**	Параметры секции соответствуют одноименным параметрам[1] секции **Подтверждение операций** настроек аутентификации пользователя в web-интерфейсе оператора КриптоПро DSS

[1]Подробное описание параметров аутентификации пользователя в КриптоПро DSS см. в документации производителя [6]

11. Выберите вкладку **Управление**.

Окно примет следующий вид.

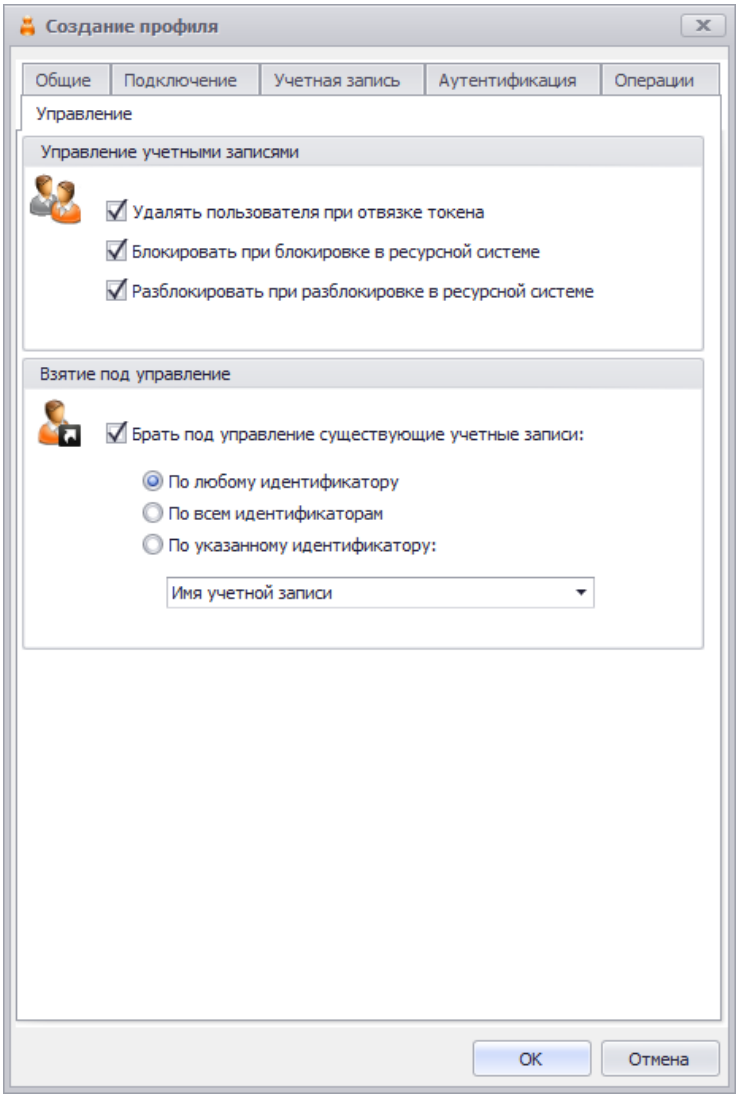


*Рис. 256 – Вкладка **Управление***

12. Выполните настройки, руководствуясь Табл. 60.

Табл. 60 – Параметры управление объектом пользователя в КриптоПро DSS

Настройка	Описание
Удалять пользователя при отвязке токена	При установленном флаге автоматически выполняются следующие действия. При удалении или отключении (см. операции **Отключить**, раздел «Отключение/включение возможности использования электронного ключа», с. 81 и **Удалить**, раздел «Удаление электронного ключа», с. 100) виртуального токена (электронного ключа) типа *Хранилище сервера КриптоПро DSS*: • если настоящий профиль все еще привязан к пользователю (контейнеру с пользователем), то после выполнения плана обслуживания **Синхронизация КриптоПро DSS** пользователь будет удален из КритпоПро DSS; • если привязка настоящего профиля к пользователю (контейнеру с пользователем) была прекращена, то после выполнения плана обслуживания **Синхронизация КриптоПро DSS** пользователь будет сначала удален из

Настройка	Описание
	КритпоПро DSS (вместе со всеми аутентификаторами), и заново создан в соотетствии с параметрами настоящего профиля.
Блокировать при блокировке в ресурсной системе	При установленном флаге пользователь будет автоматически заблокирован к КритпоПро DSS, если произойдет его блокировка в JMS (см. раздел «Блокировка/разблокировка пользователей», с. 46). **Примечание.** Для вступления в силу такой блокировки должен быть выполнен план обслуживания **Синхронизация КриптоПро DSS** (см. раздел «План обслуживания «Синхронизация КриптоПро DSS»», с. 418).
Разблокировать при разблокировке в ресурсной системе	При установленном флаге пользователь будет автоматически разблокирован к КритпоПро DSS, если будет выполнена его разблокировка в JMS. **Примечание.** Для вступления в силу такой блокировки должен быть выполнен план обслуживания **Синхронизация КриптоПро DSS** (см. раздел «План обслуживания «Синхронизация КриптоПро DSS»», с. 418).
Брать под управление существующие учетные записи	При установленном флаге, в случае если в КриптоПро DSS существует пользователь с указанным идентификатором (или идентификаторами, определяется настройками, см. ниже), для такого пользователя должен быть создан виртуальный токен типа *Хранилище сервера КриптоПро DSS*, и в дальнейшем управление таким пользователем будет осуществляться средствами JMS (см. раздел «Взятие под управление пользователей КриптоПро DSS», с. 459). В качестве критерия выбора учетных записей в КриптоПро DSS для взятия под управления используются идентификаторы пользователя, установленные на вкладке **Учетная запись** (Рис. 253, с. 285), комбинация которых устанавливается следующими параметрами: • **По любому идентификатору** – для отбора учетной записи достаточно совпадения хотя бы по одному определенному идентификатору); • **По всем идентификаторам** – для отбора учетной записи необходимо совпадение по всем определенным идентификаторам; • **По указанному идентификатору** – выберите идентификатор из списка: – **Имя учетной записи** – для поиска совпадений должен использоваться атрубут, указанный в поле **Имя входа (логин)** на вкладке **Учетная запись**; – **Адрес электронной почты** – для поиска совпадений должен использоваться атрубут, указанный в поле **Почтовый адрес для идентификации** на вкладке **Учетная запись**; – **Основной телефон** – для поиска совпадений должен использоваться атрубут, указанный в поле **Телефон для идентификации** на вкладке **Учетная запись.** При выборе комбинации нужно обеспечить условие, что выбранные идентификаторы определены на вкладке **Учетная запись**. (см. Табл. 57, с. 285).

13. По завершении настройки нажмите **Ок** для сохранения профиля (сохранения изменений).

3.9.15 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. 412).

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 -> Профили**.
2. Выполните одно из следующих действий:

   – если вы хотите создать новый профиль доступа пользователей в личный кабинет, в центральной части окна консоли управления JMS отметьте **Доступ в личный кабинет** и в верхней панели нажмите **Создать**, отобразится окно следующего вида (см. Рис. 257);
   – если вы хотите отредактировать существующий профиль, в центральной части окна консоли управления JMS отметьте этот профиль и в верхней панели нажмите **Свойства**.

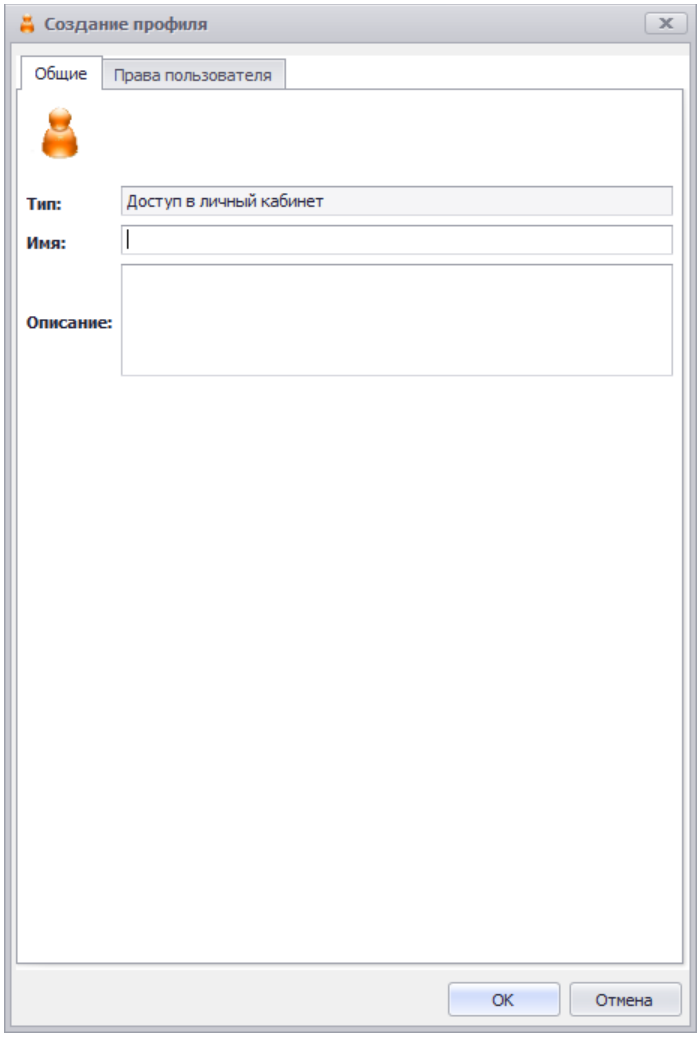


*Рис. 257 – Вкладка **Общие** свойств профиля Доступ в личный кабинет*

3. Введите необходимые данные (или измените существующие), после чего перейдите на вкладку **Права пользователя**.

Окно примет следующий вид.

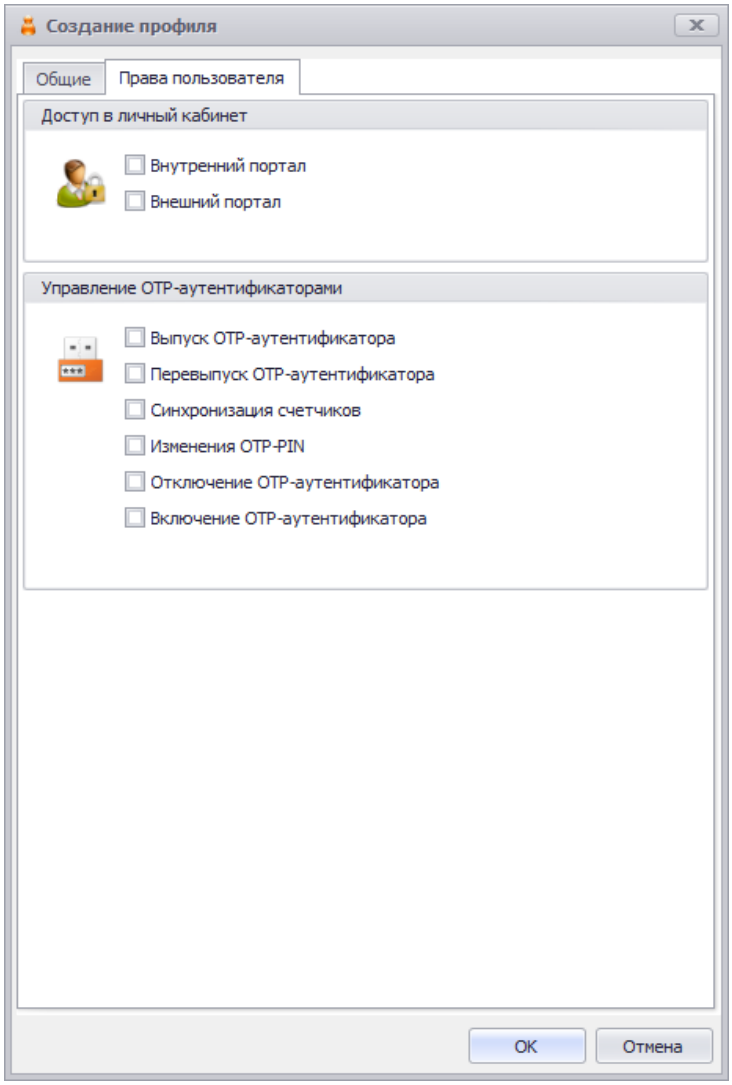


*Рис. 258 – Вкладка **Права пользователя***

4. Выполните настройки, руководствуясь Табл. 61.

Табл. 61 – 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)	

Настройка	Описание
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 счётчиков	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

5. По завершении настройки нажмите **Ок** для сохранения профиля (сохранения изменений).

3.9.16 Привязка профилей

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

Важно! Профили синхронизации рабочих станций (см. «Профиль настройки синхронизации рабочей станции», с. 244) должны быть привязаны к рабочим станциям (контейнерам рабочих станций), а не к пользователям.

Чтобы привязать созданные профили к пользователям, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Профили -> Привязка профилей**. Окно консоли будет иметь следующий вид.

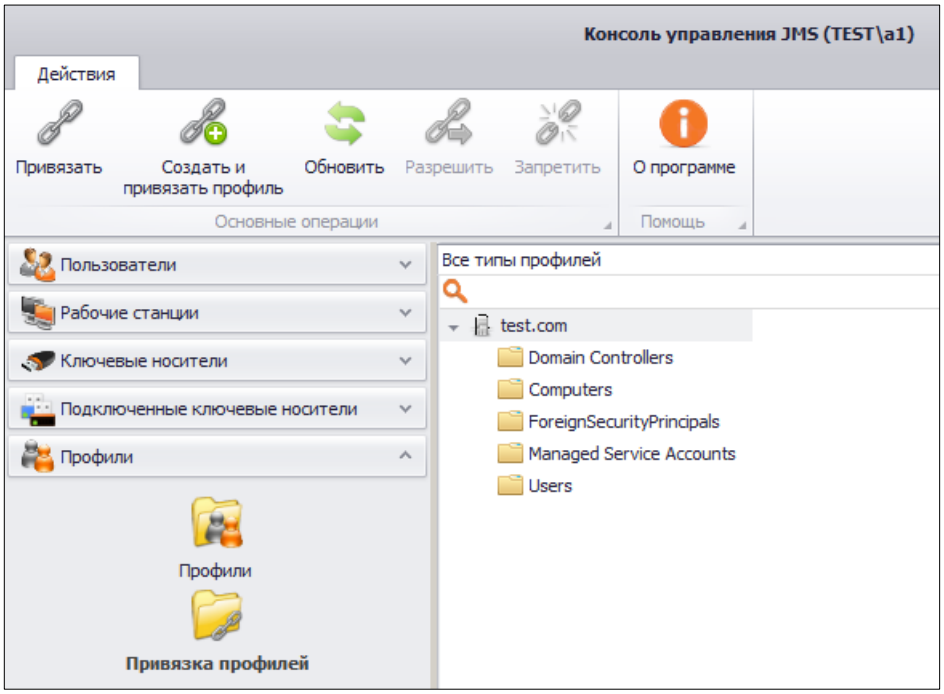


Рис. 259 – Привязка профилей

2. В центральной части окна отметьте каталог, содержащий пользователей, к которым вы хотите привязать настроенные профили (например, каталог **Users**), после чего в верхней панели нажмите **Привязать**.
   Отобразится следующее окно.

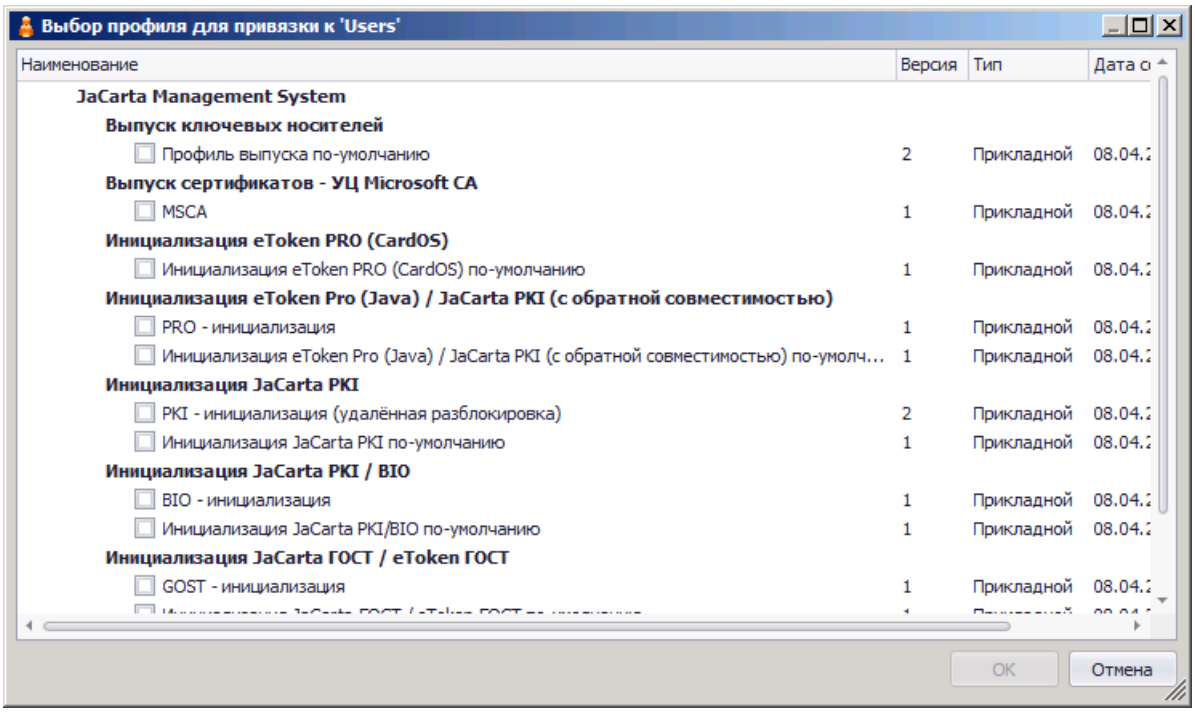


Рис. 260 – Список доступных профилей

3. Отметьте профили, которые вы хотите привязать к выбранному каталогу, и нажмите **OK**.
   Список привязок отобразится в основном окне консоли управления JMS (см. рис. 261).

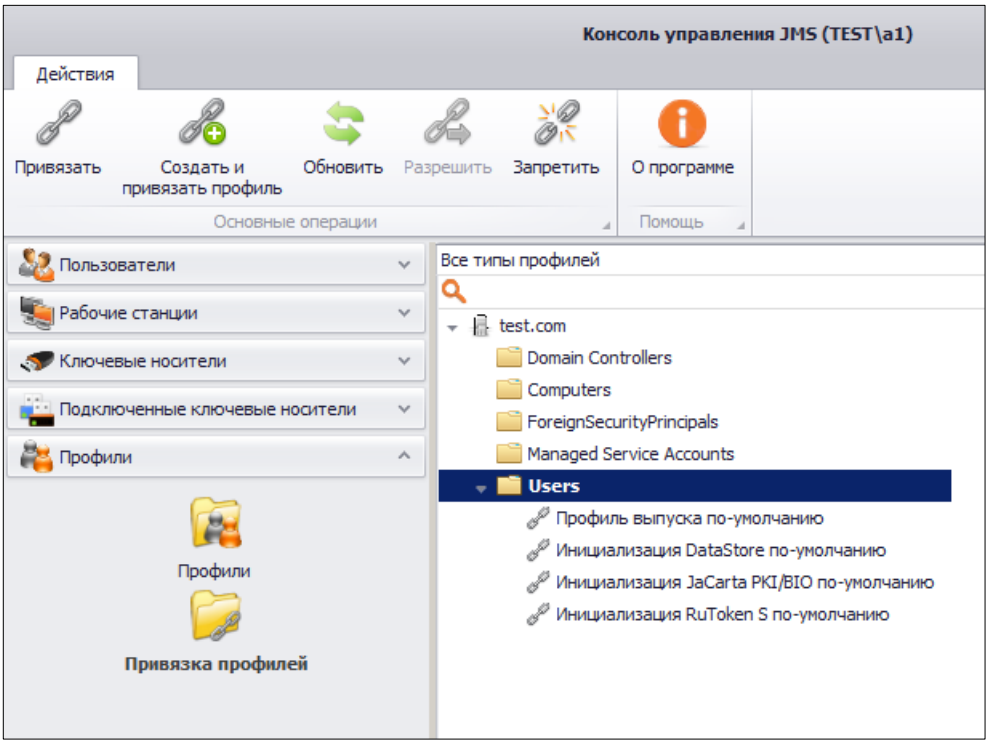


Рис. 261 – Список привязок профилей

Также вы можете распространить действие привязки профиля только на определенных пользователей выбранного каталога, используя глобальные группы Active Directory или создав глобальные группы JMS (см. «Ограничение действия профилей через группы домена/глобальные группы JMS» below).

Для отмены привязки профиля к контейнеру выполните следующие действия.

1. Выберите необходимую привязку профиля в центральной части окна (Рис. 262).
2. В верхней панели нажиме **Отменить**.

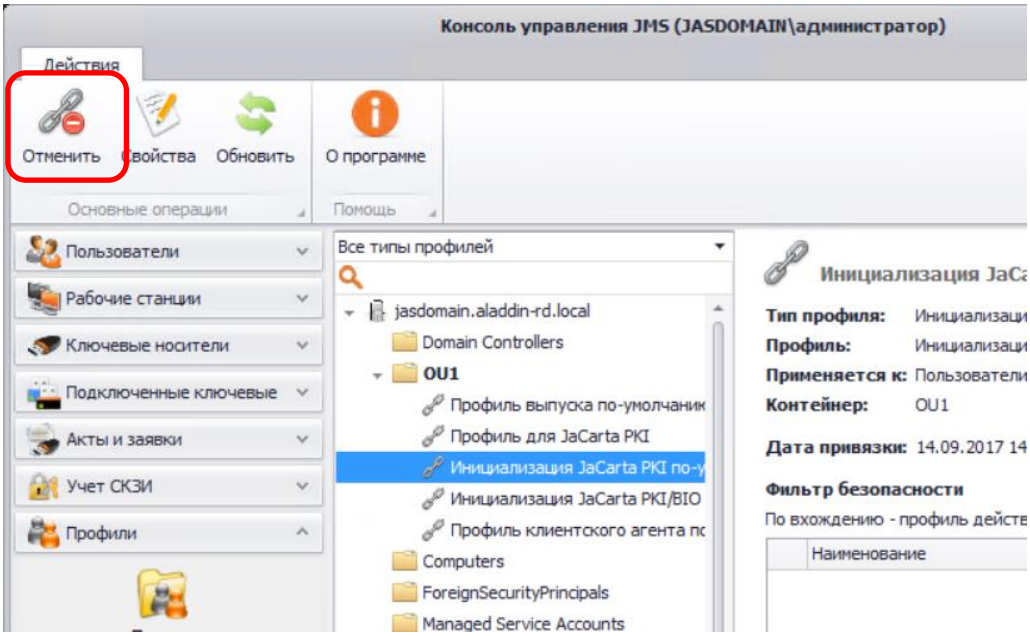


Рис. 262 – Отмена привязки профиля

С примерами порядка настройки и привязки профилей можно ознакомиться в разделе «Примеры настроек профилей», с. 306.

3.9.17 Наследование профилей

В JMS контейнеры (например, организационные единицы – OU) ресурсных систем (напр., Active Directory) 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** -> **Привязка профилей**.
2. В центральной части окна выберите необходимый контейнер и в верхней панели (Рис. 261, выше) нажмите **Запретить** (в случае запрета наследования) или **Разрешить** (в случае разрешения наследования)
3. В окне подтверждения действия нажмите **ОК**.

После запрета/разрешения наследования профилей изменения отразятся в полях **Наследование** и **Унаследованные профили** свойств контейнера в правой части окна (Рис. 263).

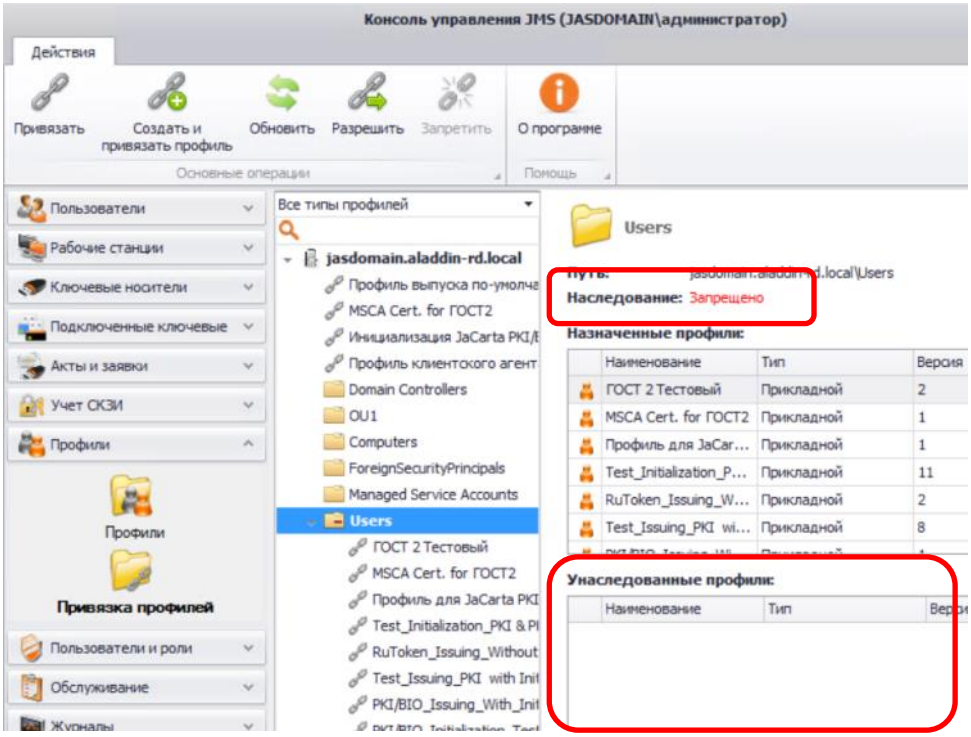


Рис. 263 – Отражение наследования профилей контейнера Users

3.9.18 Ограничение действия профилей через группы домена/глобальные группы JMS

Чтобы распространить действие привязки профиля только на определенных пользователей выбранного каталога (а также на определенные рабочие станции), используя группы Active Directory (группы домена) 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. 386).

1. В консоли управления JMS перейдите в раздел **Профили -> Привязка профилей**.

Окно консоли будет выглядеть следующим образом.

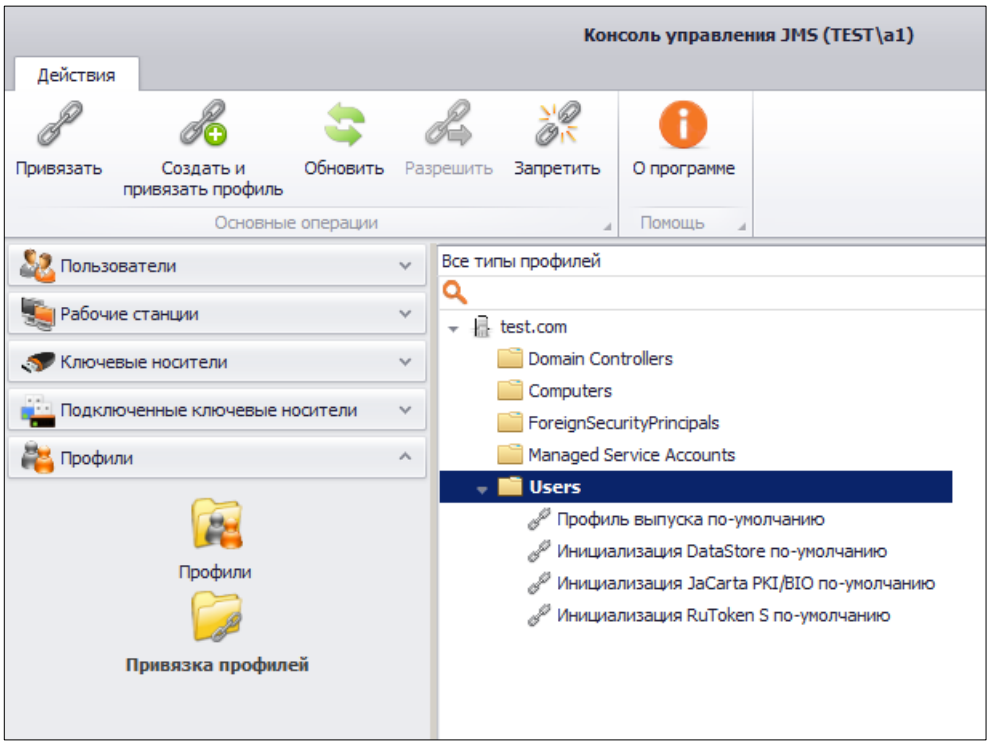


Рис. 264 – Привязки профилей

2. В центральной части окна отметьте привязку, действие которой необходимо ограничить глобальной группой, и в верхней панели нажмите **Свойства**.
3. В отобразившемся окне перейдите на вкладку **Фильтр**.

Окно примет следующий вид.

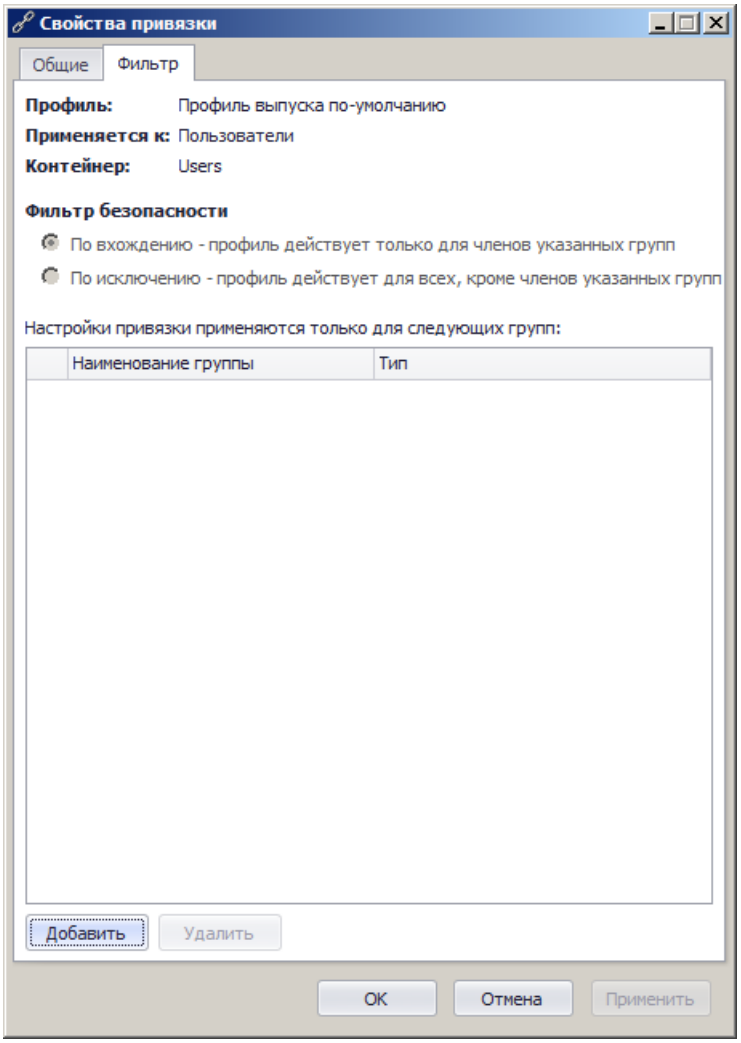


Рис. 265 – Вкладка Фильтр окна свойств привязки профиля

4. Чтобы выбрать глобальную группу, нажмите **Добавить**.

Отобразится следующее окно.

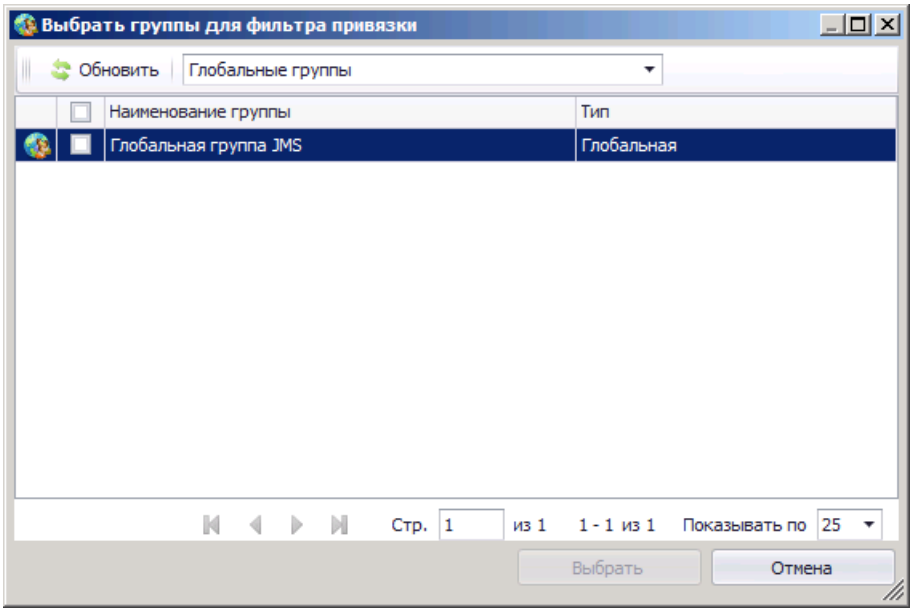


Рис. 266 – Выбор глобальной группы

5. Выполните одно из следующих действий:

   – чтобы добавить глобальную группу Active Directory, в раскрывающемся списке в верхней части окна выберите нужный домен – в этом случае в окне отобразится список групп выбранного домена;
   – чтобы добавить глобальную группу JMS, оставьте в раскрывающемся списке в верхней части окна выбранным пункт **Глобальные группы** – в этом случае в окне будет отображен список глобальных групп JMS.

В настоящем документе процедура рассмотрена на примере глобальных групп JMS.

6. Отметьте доменную группу (группы) или глобальную группу (группы) JMS, которой вы хотите ограничить область действия привязки профиля, после чего нажмите **Выбрать**.

Выбранные группы отобразятся в списке **Фильтр безопасности**.

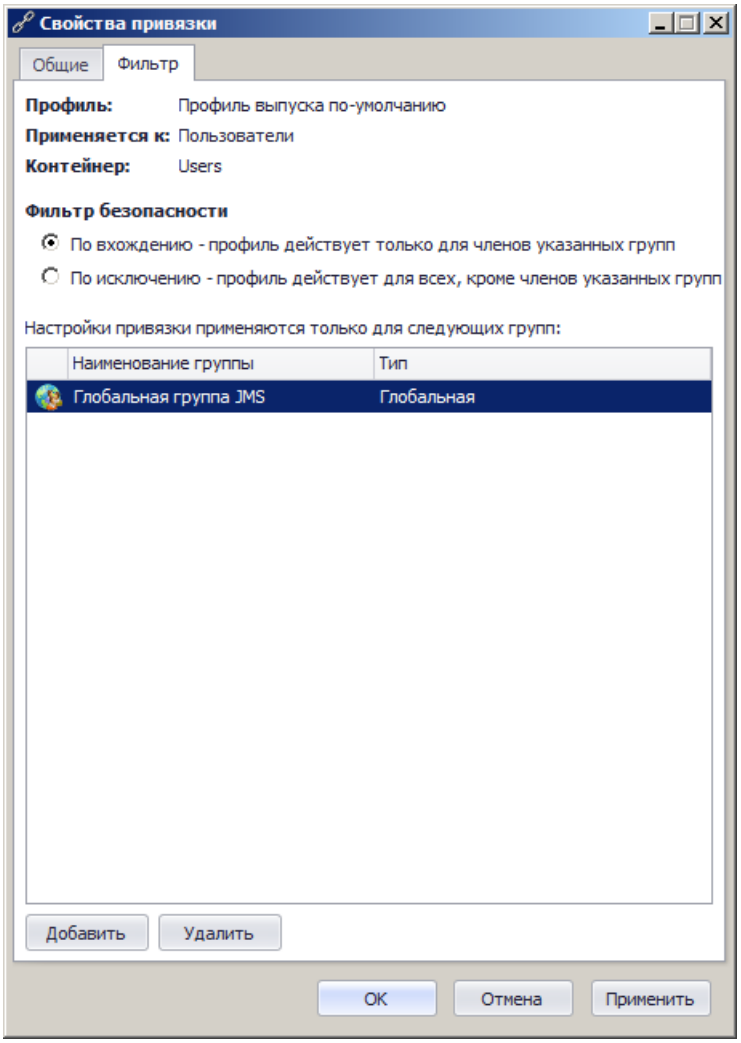


Рис. 267 – Выбранная глобальная группа JMS отображена в списке

7. В секции **Фильтр безопасности** выберите один из двух пунктов:
   - **По вхождению – профиль действует только для членов указанной группы**;
   - **По исключению – профиль действует для всех, кроме членов указанной группы**.
8. Повторите необходимые действия, если необходимо создать фильтр с использованием других групп JMS.
9. Нажмите **OK**, чтобы сохранить изменения и закрыть окно.

3.9.19 Экспорт/импорт профилей

Чтобы экспортировать/импортировать профиль JMS, выполните следующие действия.

Экспорт профилей

1. В консоли управления JMS перейдите в раздел **Профили -> Профили**.
2. В центральной части интерфейса выберите профиль, который нужно экспортировать.
3. В верхней панели нажмите **Экспорт**.
4. В отобразившемся окне предупреждения нажмите **Да**, чтобы подтвердить действие.
5. В отобразившемся окне укажите путь сохранения файла экспортированного профиля и нажмите **Сохранить**.

Импорт профилей

1. В консоли управления JMS перейдите в раздел **Профили -> Профили**.
2. В верхней панели нажмите **Импорт**.
3. В отобразившемся окне укажите путь к файлу профиля и нажмите **Открыть**.
4. В отобразившемся окне предупреждения нажмите **Да**, чтобы подтвердить действие.
5. В окне сообщения об успешном импорте нажмите **ОК**.

3.9.20 Настройка параметров печати при выпуске объектов JMS

JMS позволяет настроить параметры печати документов, которые формируются при выпуске различных объектов в JMS (электронных ключей 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. раздел «Акты и заявки», с. 312).

В зависимости от профиля, в котором происходит настройка печати, возможна настройка параметров печати для следующих типов документов (см. табл. 62).

Табл. 62 – Параметры печати

Профиль	Тип документа
См. «Настройка профиля выпуска электронных ключей», с. 158.	• Заявка на выпуск КН; • Акт выдачи КН.
См. «Настройки профиля выпуска сертификатов в центре сертификации Microsoft», с. 209.	• Запрос на сертификат; • Сертификат.
См. «Настройка профиля для выпуска сертификатов в КриптоПро УЦ 1.5», с. 620.	
См. «Настройка профиля для выпуска сертификатов в КриптоПро УЦ 2.0», с. 648.	

Настройка параметров печати документов рассмотрена ниже на примере вкладки **Печать запроса** на сертификат. Настройка параметров печати на вкладках **Печать заявки на выпуск КН**, **Печать акта выдачи КН** и **Печать сертификата** аналогична приведенному примеру.

3.9.20.1 Настройка печати на примере вкладки Печать запроса на сертификат

В настоящем разделе приводится типовой пример настроек печати на соответствующей вкладке профилей выпуска ключевых носителей и сертификатов.

Вкладка **Печать запроса** на сертификат выглядит следующим образом:

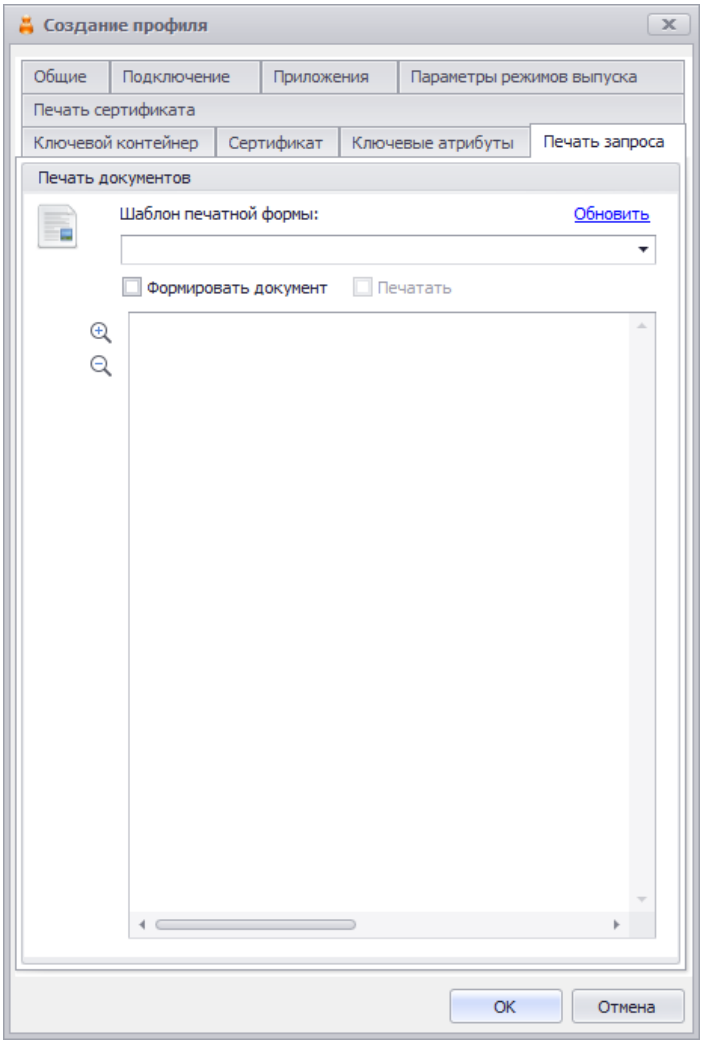


*Рис. 268 – Вкладка **Печать запроса** на сертификат*

Чтобы настроить печать документов, связанных с выпуском электронных ключей, выполните следующие действия:

1. В поле **Шаблон печатной формы** из раскрывающегося списка выберите шаблон печатной формы, по которому будет создан и распечатан документ.

О создании и настройке **Шаблона печатной формы** подробнее см. в разделе «Подсистема печати», с. 369.

2. После выбора **Шаблона печатной формы** его можно просмотреть, используя при этом кнопки увеличения и уменьшения "**+**" и "**-**" (рис. 269).
   Чтобы в процессе выпуска ключевого носителя/сертификата происходило формирование соответствующего документа следует установить флаг **Формировать документ**. 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. 312)

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.

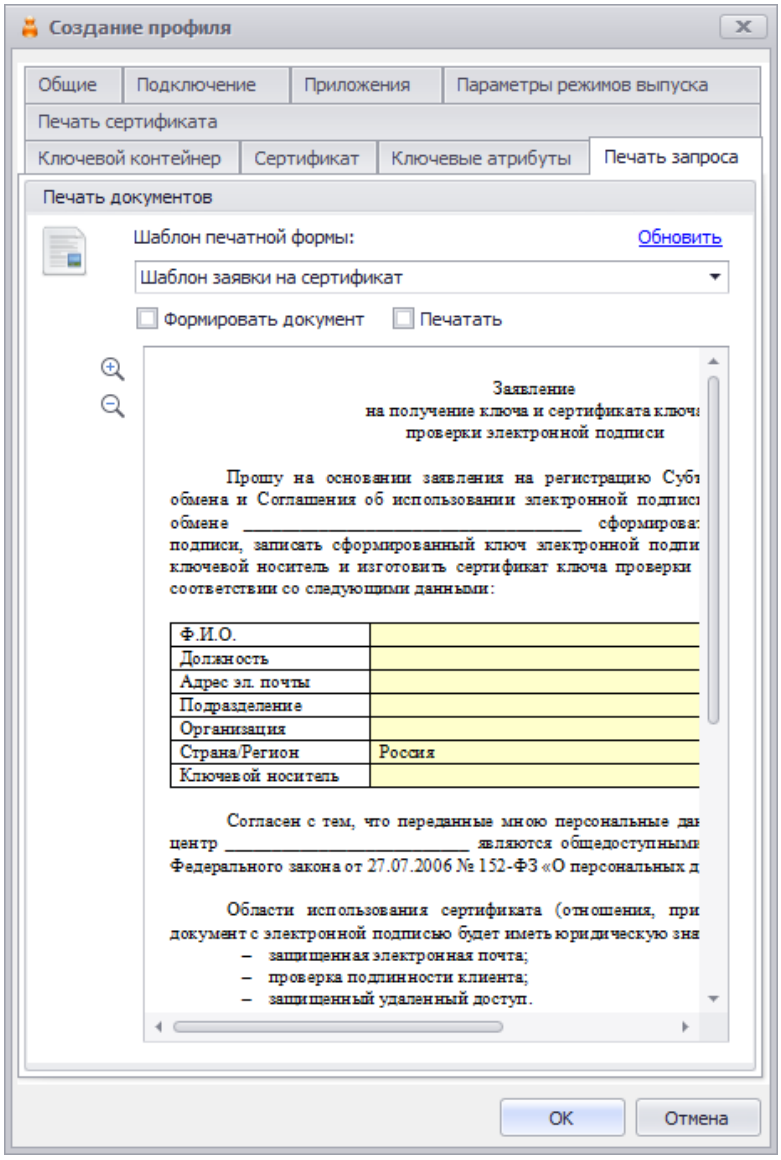


*Рис. 269 – Вкладка **Печать запроса** на сертификат. Просмотр шаблона печатной формы*

3.9.21 Примеры настроек профилей

Комплекс профилей, привязываемых в JMS к контейнеру (см. «Привязка профилей», с. 296) или конкретному пользователю (см. «Ограничение действия профилей через группы домена/глобальные группы JMS», с. 299), полностью определяет набор возможных действий в отношении электронного ключа 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.

3.9.21.1 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) следующего набора профилей:

- *профиль выпуска ключевого носителя* (см. «Настройка профиля выпуска электронных ключей», с. 158);

  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 центре сертификации Microsoft», с. 209).

  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, биометрической информации аутентификации, парольной политики и др.), следует также:

- создать (если отсутствует) и привязать соответствующий *профиль инициализации ключевого носителя* (см. «Настройки параметров инициализации», с. 174)
- в *профиле выпуска ключевого носителя* в настройках параметров выпуска нужно разрешить инициализацию в соответствующем приложении (параметр **Способ выпуска для консоли администратора**).

3.9.21.2 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.

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. 164).

3.9.21.3 Профили для отключения и замены пользователем электронного ключа

Для того чтобы в клиенте JMS пользователю стало доступно *отключение* (временная блокировка в JMS) и замена электронного ключа следует настроить и привязать к пользователю профили, указанные в разделах «Профили для выпуска администратором электронного ключа с сертификатом» и «Профили для выпуска пользователем электронного ключа с сертификатом», выше.

Кроме того, в настройках профиля клиентского агента следует установить признаки **Разрешить отключение** и **Разрешить замену** на вкладке **Работа с ключевыми носителями** (см. «Настройка профиля клиентского агента», с. 164).

3.9.21.4 Выпуск сертификата в хранилище пользователя

JMS позволяет выпускать сертификат пользователя с закрытым ключом в личное хранилище пользователя на рабочей станции с установленным JMS-клиентом. В JMS для выпуска такого сертификата используется абстрактная модель электронного ключа: сертификат выпускается на виртуальный «ключевой носитель», в качестве которого выступает личное хранилище сертификатов пользователя на рабочей станции (см. «Виртуальный электронный ключ «Хранилище пользователя», с. 118).

Для подготовки выпуска такого сертификата выполните следующие действия.

1. Создайте профиль выпуска сертификата, как это описано в соответствующем разделе:

   - раздел «Настройки профиля выпуска сертификатов в центре сертификации Microsoft», с. 209, — для выпуска сертификата в MSCA;
   - раздел «Настройка профиля для выпуска сертификатов в КриптоПро УЦ 2.0», с. 648, — для выпуска сертификата в КриптоПро УЦ;
   - раздел «Настройка профиля для выпуска сертификатов в ViPNet УЦ», с. 585, — для выпуска сертификата в ViPNet УЦ;

   при этом на вкладке **Приложение** выберите «апплет» **UserStore**.

Примечание. При выборе «апплета» **UserStore** остальные апплеты становится недоступны (если какие-то апплеты уже были выбраны, их выбор будет отменен).

2. Создайте профиль выпуска ключевых носителей в соответствии с разделом «Настройка профиля выпуска электронных ключей», с. 158, при этом на вкладке **Базовые параметры выпуска** выберите пункт **Выпускать только указанные типы ключевых носителей с индивидуальными настройками**, после чего выберите «апплет» **UserStore**.

Примечание. При выборе «апплета» UserStore остальные апплеты становится недоступны.

3. Создайте профиль **Настройки клиентского агента** в соответствии с разделом «Настройка профиля клиентского агента», с. 164.
4. Выполните привязку профилей, настроенных на шагах 1—3 к контейнерам, содержащим обслуживаемых пользователей (см. «Привязка профилей», с. 296), и/или к отдельным пользователям (см. «Ограничение действия профилей через группы домена/глобальные группы JMS», с. 299), для которых следует выпускать сертификат в хранилище пользователя на рабочей станции средствами JMS.

Сертификат вместе с закрытым ключом будет выпускаться в хранилище пользователя на рабочей станции только при условии, что сеанс (сессия) JMS открыта тем же пользователем, от имени которого был открыт текущий сеанс Windows

Выпуск/синхронизация сертификата (при соблюдении всех указанных выше условий) выполняется в следующих случаях:

- в момент открытия пользовательского сеанса (сессии) в клиенте JMS;
- при нажатии кнопки **Обновить** в окне приложения **Клиент JMS**;
- при обработке одного из событий, перечисленных на вкладке **Синхронизация** привязанного профиля настройки клиентского агента (см. «Настройка профиля клиентского агента», с. 164).

Примечания:

1. Запуск синхронизации, выполняемой в момент открытия пользовательского сеанса и при нажатии кнопки **Обновить**, производится независимо от факта привязки профиля настройки клиентского агента.
2. Процедура синхронизации для случаев, указанных в предыдущем пункте, включает в себя помимо проверки актуальности текущего сертификата синхронизацию остальных сертификтаов, выпущенных посредством JMS для данного пользователя в хранилище сертификатов на рабочей станции.

Выпущенный в хранилище пользователя сертификат в консоли управления JMS отображается:

- в разделе **Сертификаты**;
- в свойствах соответствующей рабочей станции на вкладке **Сертификаты**;
- в свойствах пользователя на вкладке **Объекты пользователя**.

После выпуска сертификат имеет статус **Выпущен на КН** и не отличается от сертификатов, выпущенных на электронных ключах.

Объект «виртуального электронного ключа» (для которого выпускается сертификат) после выпуска сертификата отображается в разделе **Ключевые носители** консоли управления JMS как электронный ключ модели **Хранилище пользователя**. Сертификат можно посмотреть также на вкладке **Содержимое** свойств этого «виртуального электронного ключа».

3.9.21.5 Выпуск сертификата в хранилище сервера КриптоПро DSS

JMS позволяет выпускать сертификат пользователя с закрытым ключом в хранилище КриптоПро DSS.

Примечание. Для выпуска такого сертификата в системе JMS должен быть установлен коннектор КриптоПро DSS, подробнее см. в документе «Руководство администратора. Часть 1» [2], раздел «Коннектор КриптоПро DSS».

В JMS для выпуска такого сертификата используется абстрактная модель электронного ключа: сертификат выпускается на виртуальный «ключевой носитель», в качестве которого выступает хранилище сервера КриптоПро DSS (см. «Виртуальный электронный ключ «Хранилище сервера КриптоПро DSS», с. 119).

Для подготовки выпуска такого сертификата выполните следующие действия.

1. Создайте профиль создания/синхронизации пользователей КриптоПро DSS (см. «Настройка профиля пользователя КриптоПро DSS», с. 281).
2. Создайте профиль выпуска сертификата на КриптоПро DSS (см. «Настройки профиля выпуска сертификатов на КриптоПро DSS», с. 223).
3. Создайте профиль выпуска ключевых носителей в соответствии с разделом «Настройка профиля выпуска электронных ключей», с. 158.

Примечание. Вместо профиля выпуска сертификата на КриптоПро DSS можно также использовать один из профилей выпуска сертификатов для сторонних УЦ (например, КриптоПро УЦ 1.5 / 2 или ViPNet УЦ). В этом случае на вкладке **Приложения** нужно выбрать соответствующий «апплет» (приложение).

4. Выполните привязку профилей, настроенных на шагах 1—3 к контейнерам, содержащим обслуживаемых пользователей (см. «Привязка профилей», с. 296), и/или к отдельным пользователям (см. «Ограничение действия профилей через группы домена/глобальные группы JMS», с. 299), для которых следует выпускать сертификат в хранилище сервера КриптоПро DSS средствами JMS.
5. Настройте план обслуживания «Синхронизация КриптоПро DSS» (см. раздел «План обслуживания «Синхронизация КриптоПро DSS»», с. 418) и запустите его на выполнение (см. раздел «Запуск и просмотр результатов планов обслуживания из Консоли управления JMS», с. 405). Результатом работы плана обслуживания будет выпуск/синхронизация сертификатов для пользователей, привязанных к определённым выше профилям.

Выпущенный в хранилище сервера КриптоПро DSS сертификат в консоли управления JMS отображается:

- в разделе **Сертификаты**;
- в свойствах пользователя на вкладке **Объекты пользователя**.

После выпуска сертификат имеет статус **Выпущен на КН** и не отличается от сертификатов, выпущенных на электронных ключах.

Объект «виртуального электронного ключа» (для которого выпускается сертификат) после выпуска сертификата отображается в разделе **Ключевые носители** консоли управления JMS как электронный ключ модели **Хранилище сервера КриптоПро DSS** (Рис. 122, с. 119). Сертификат можно посмотреть также на вкладке **Содержимое** свойств этого «виртуального электронного ключа».

3.9.21.6 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. 262);
   - профиль выпуска Messaging-токена (см. «Настройка профиля выпуска Messaging-токенов», с. 269);
   - профиль выпуска Push OTP-токена (см. «Настройка профиля выпуска Push OTP-токенов», с. 275).
2. Создайте глобальную группу для пользователей, которым необходимо предоставить право на самостоятельный выпуск OTP (см. «Глобальные группы JMS», с. 386, группу можно оставить пустой, не добавляя в нее пользователей, подробнее см. далее)
3. Выполните привязку профиля (см. «Привязка профилей», с. 296).
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. 299). 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. 293)
6. Выполните привязку профиля (см. «Привязка профилей», с. 296) 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. 412) и запустите его на выполнение

(см. раздел «Запуск и просмотр результатов планов обслуживания из Консоли управления JMS», с. 405). 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. 270, ниже. (При необходимости права на самостоятельный выпуск OTP-токена можно также предоставить вручную в свойствах конкретного пользователя на вкладке **Личный кабинет**)

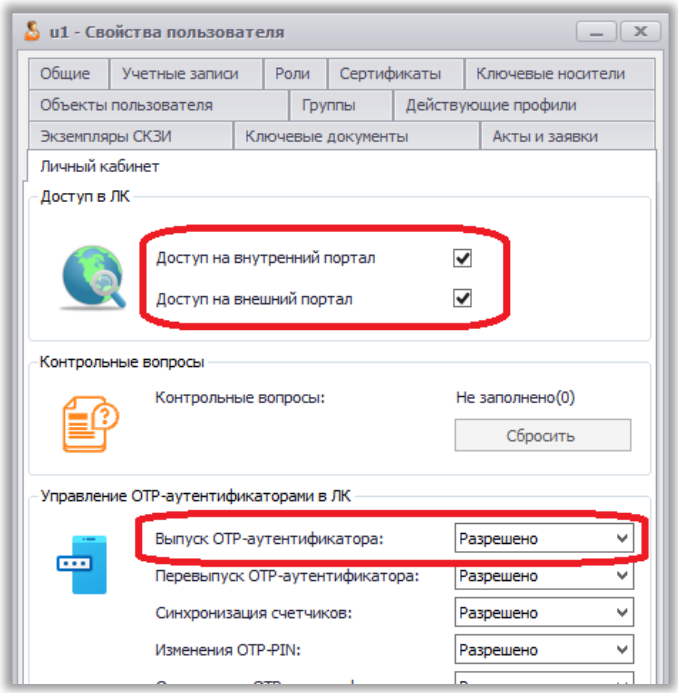


Рис. 270 – Пример разрешений пользователя в ЛК для самостоятельного выпуска OTP-аутентификатора

8. В настройках личного кабинета (раздел **Настройки личного кабинета** –> **Выпуск OTP-аутентификаторов**) у соответствующего профиля установите флаг **Разрешить выпуск через личный кабинет** (см. раздел «Раздел Выпуск OTP-аутентификаторов», Рис. 462 с. 520).
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), подронее см. «Раздел Аутентификация», с. 488.

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».

3.9.21.7 Настройка автоматического перевыпуска сертификата на электронном ключе

Для того чтобы обеспечить заблаговременный автоматический перевыпуск сертификата на пользовательском электронном ключе (т.е. до истечения срока действия сертификата), например, из JMS-клиента, выполните следующие действия.

1. Убедитесь, что выполнены настройки профилей, как это указано в разделе «Профили для выпуска пользователем электронного ключа с сертификатом», с. 307.
2. В профиле выпуска сертификата (например в профиле **Выпуск сертификата в УЦ Microsoft CA**) на вкладке **Параметры режимов выпуска** (например, Рис. 204, с. 215) установите опцию **Обновлять сертификат с истекающим сроком действия** и выполните дополнительные необходимые настройки (включая срок в днях до окончания действия сертификата).

После привязки такого сертификата к пользователю (его контейнеру) и выпуска на его основе электронного ключа, автоматический перевыпуск сертификата (по наступлению указанного срока) произойдет в момент синхронизации ЭК (настройка синхронизации выполняется в профиле клиентского агента, Рис. 173, с. 169).

3.10 Акты и заявки

В JMS существует возможность распечатать указанные в настройках профиля документы, формируемые при выпуске электронного ключа, не только в момент выпуска электронного ключа, но и по прошествии времени после выпуска электронного ключа.

Примечание. При печати документа возможен выбор другого шаблона для печати (если, например, были внесены правки в шаблон и требуется перепечатать документ о выпуске электронного ключа по новому шаблону).

Для того чтобы распечатать документы после выпуска электронного ключа выполните следующие действия:

1. Перейдите на вкладку **Акты и заявки**, выберите нужный каталог (например, Users) и нажмите **Отображать вложенные** (см. рис. 271).
2. Выделите требуемый документ в списке и нажмите **Печать**. Для просмотра документа – нажмите **Просмотр**.

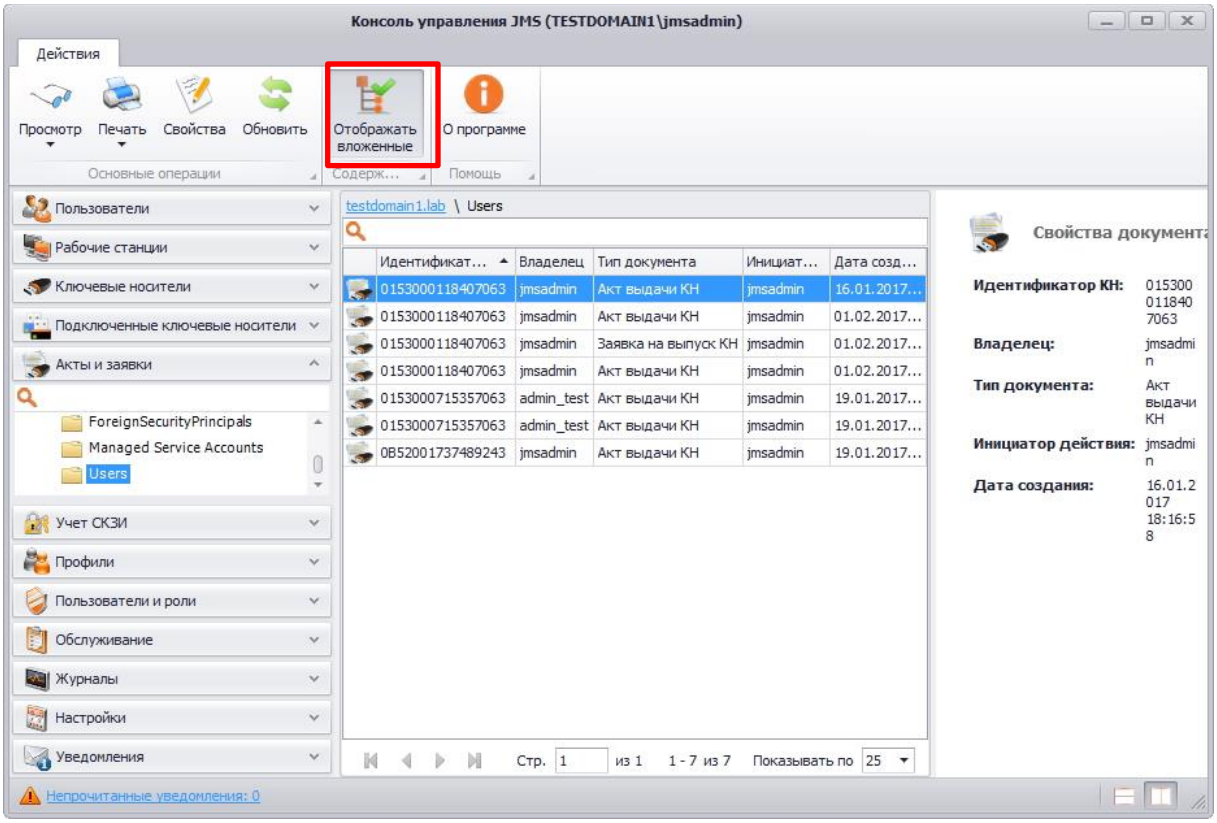


*Рис. 271 – Вкладка **Акты и заявки.** Выбор опции **Отображать вложенные***

Кнопки **Просмотр** и **Печать** имеют раскрывающийся список, состоящий из двух опций (см. рис. 272):

- **Шаблон <***[имя шаблона]***>** – печать (просмотр) документа по указанному в настройках шаблону печати;
- **Выбрать шаблон** – выбор другого шаблона для печати (просмотра).

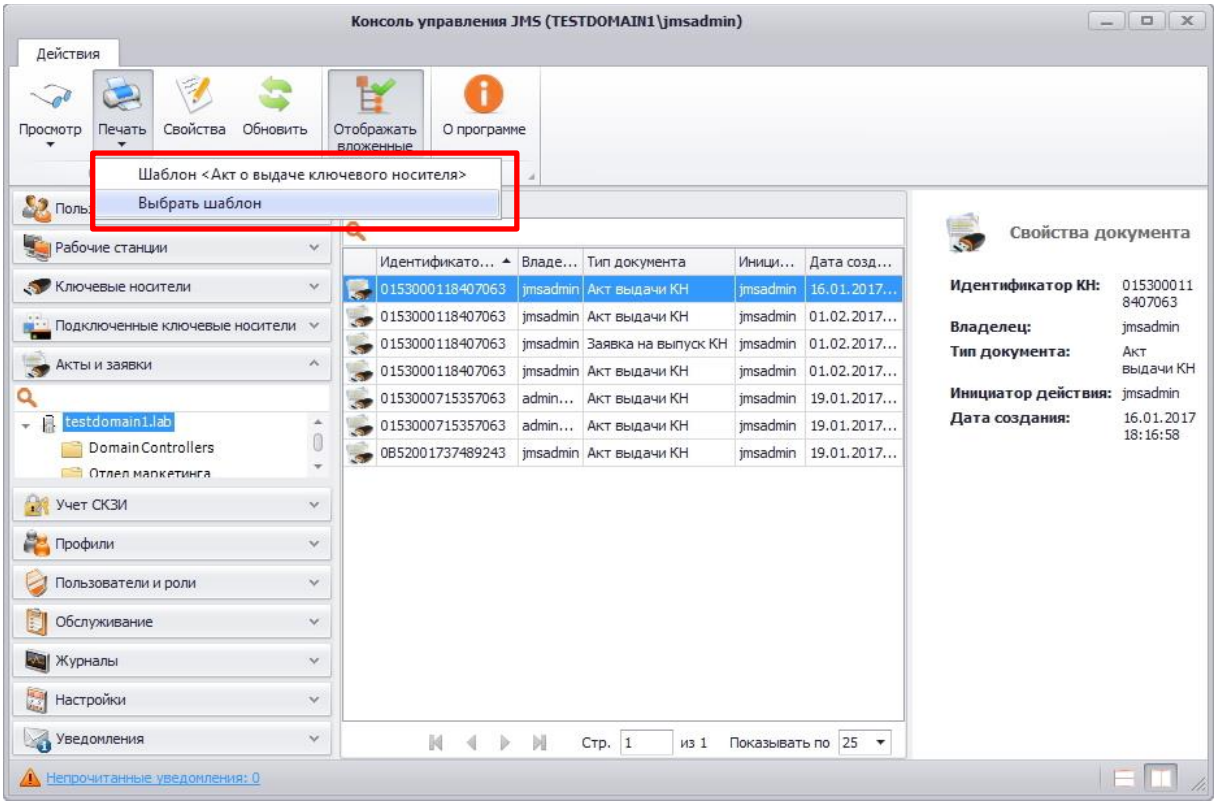


*Рис. 272 – Вкладка **Акты и заявки.** Выбор опции **Печать –> Выбрать шаблон***

При выборе другого шаблона для печати в появившемся окне (см. рис. 273) следует в поле **Шаблон печати** выбрать из раскрывающегося списка требуемый шаблон и нажать **OK**.

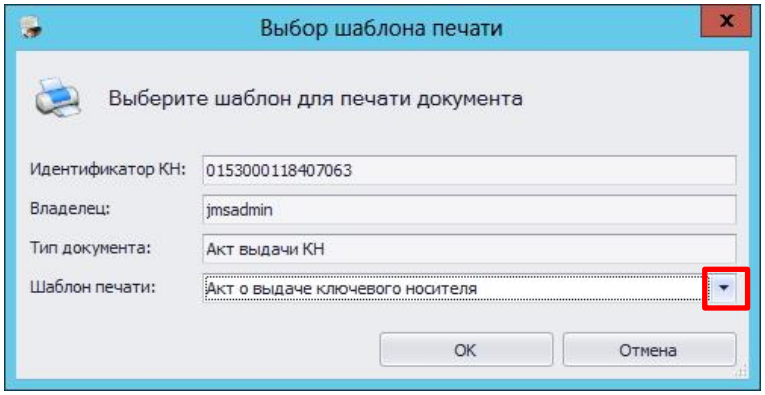


*Рис. 273 – Вкладка **Акты и заявки.** Выбор опции **Печать –> Выбрать шаблон***

О создании и настройке Шаблона печатной формы подробнее см. раздел «Подсистема печати», с. 369.

3.11 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. 274) 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.

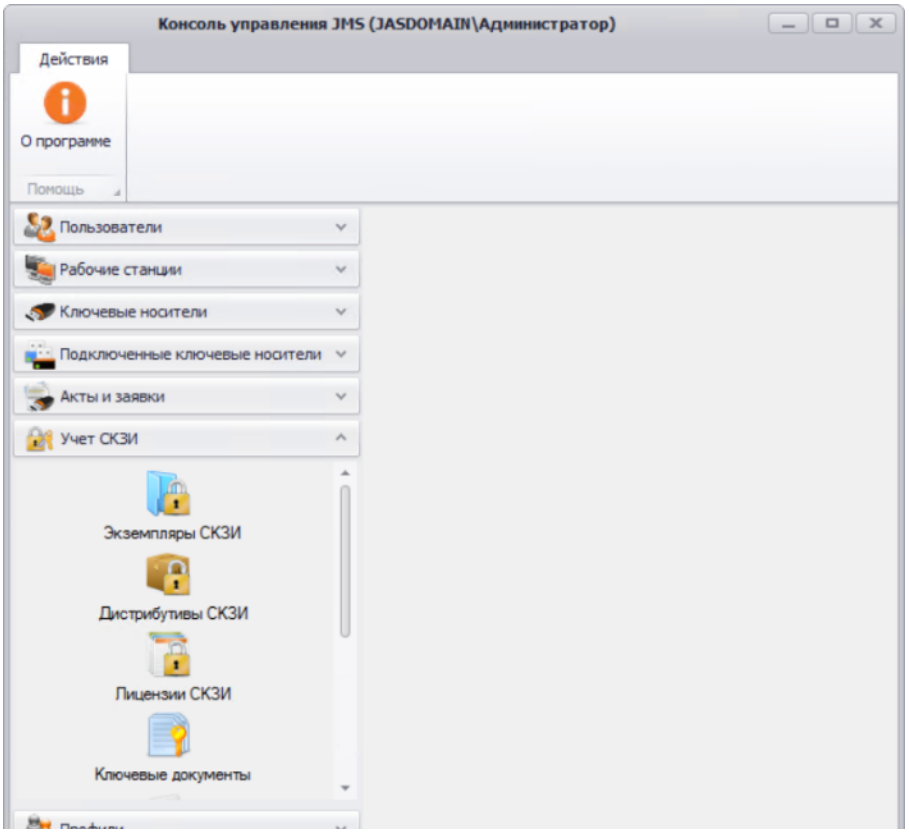


Рис. 274 – Раздел Учет СКЗИ консоли управления JMS

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. 463, «Порядок управления ключевым носителем как аппаратным СКЗИ», с. 461)

Учет СКЗИ, являющихся ключевыми носителями, ведется автоматически при их регистрации или выпуске (см. раздел «Порядок управления ключевым носителем как аппаратным СКЗИ», с. 461).

3.11.1 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 63.

Табл. 63 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 (прекратитьучет/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; • импорт 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.

Наименование	Назначение
Лицензии СКЗИ	Для выполнения следующих действий с лицензиями СКЗИ: • просмотра списка и свойств зарегистрированных лицензий; • регистрации лицензий (включая пакетную); • 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).
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.

Наименование	Назначение
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 встроенные 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.
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**.

3.11.2 Типы СКЗИ

Действия, выполнение которых возможно в разделе **Учет СКЗИ** -> **Типы СКЗИ**, перечислены в Табл. 63.

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).
- Рутокен ЭЦП (ключи Рутокен ЭЦП и Рутокен ЭЦП 2.0).
- ФКН (JaCarta CryptoPro).

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 списка зарегистрированных типов СКЗИ отображаются свойства, описание которых представлено в таблице 64.

Табл. 64 – Параметры типов СКЗИ

Наименование свойства	Описание
Наименование	Наименование типа СКЗИ
Подтип	Допустимые значения: • **Пользовательский** – создается пользователем; • **Встроенный**
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
Номер сертификата ФСБ	Номер сертификата ФСБ
Дата выдачи сертификата ФСБ	Дата выдачи сертификата ФСБ
Срок действия сертификата ФСБ	Срок действия сертификата ФСБ
Номер сертификата технической поддержки	Номер сертификата технической поддержки

Наименование свойства	Описание
Дата выдачи сертификата технической поддержки	Дата выдачи сертификата технической поддержки
Срок действия сертификата технической поддержки	Срок действия сертификата технической поддержки

3.11.2.1 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** (см. рис. 275).

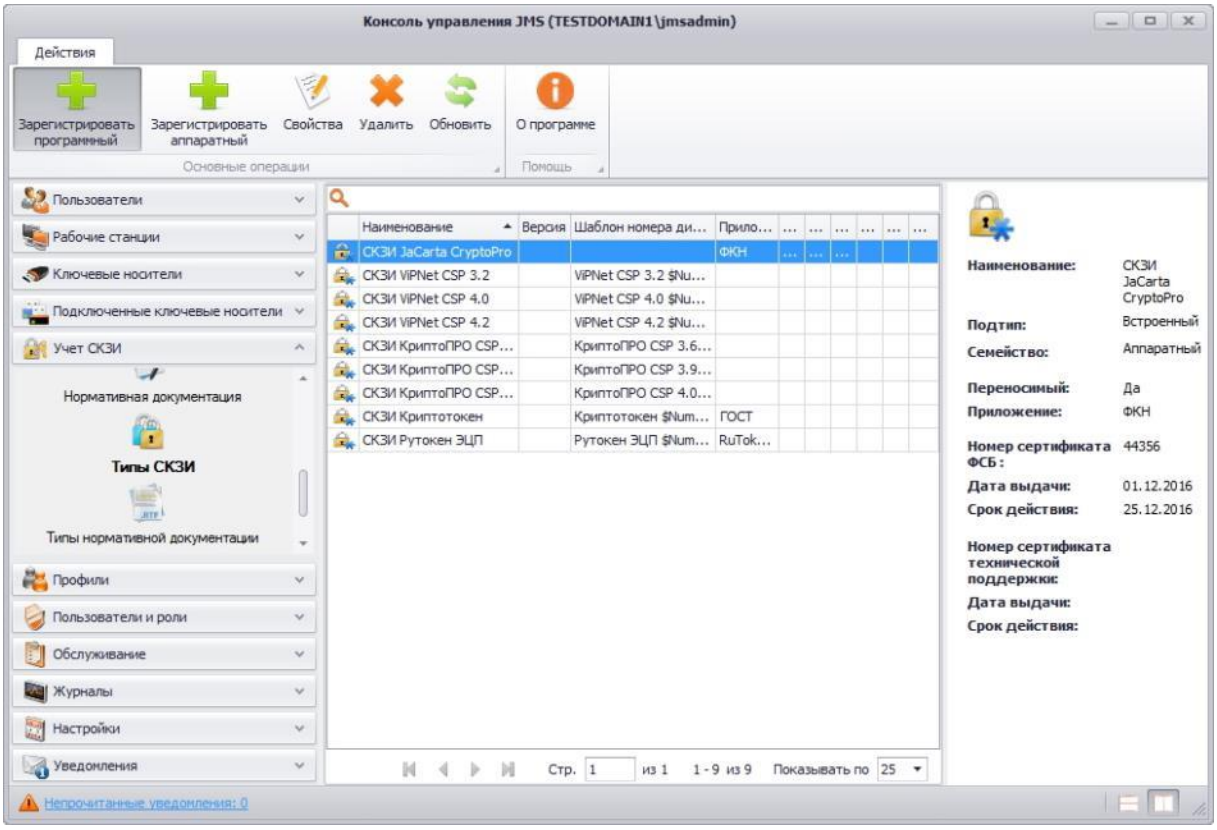


Рис. 275 – Вызов окна регистрации программного типа СКЗИ

2. В появившемся окне (см. рис. 276) 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);

3. Введите **шаблон формирования идентификатора** (Это шаблон, при использовании которого будет формироваться номер копии дистрибутива. Опция применима только для программных 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**.

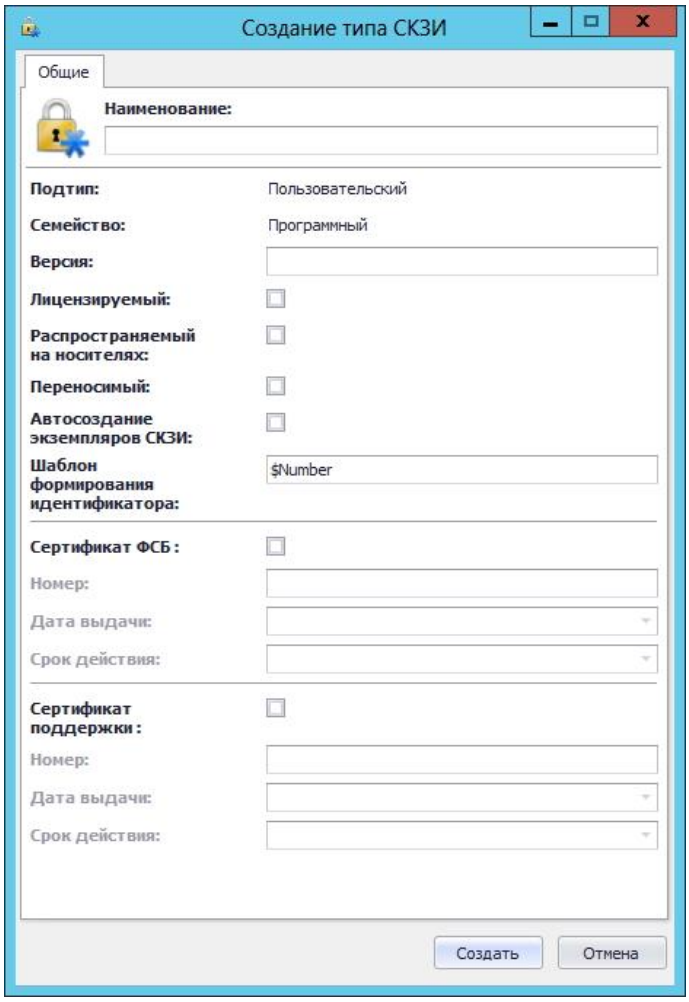


Рис. 276 – Окно создания программного типа СКЗИ

Зарегистрированный тип СКЗИ отобразится в окне консоли управления JMS в разделе **Учет СКЗИ** -> **Тип СКЗИ**.

3.11.2.2 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** (см. рис. 277).

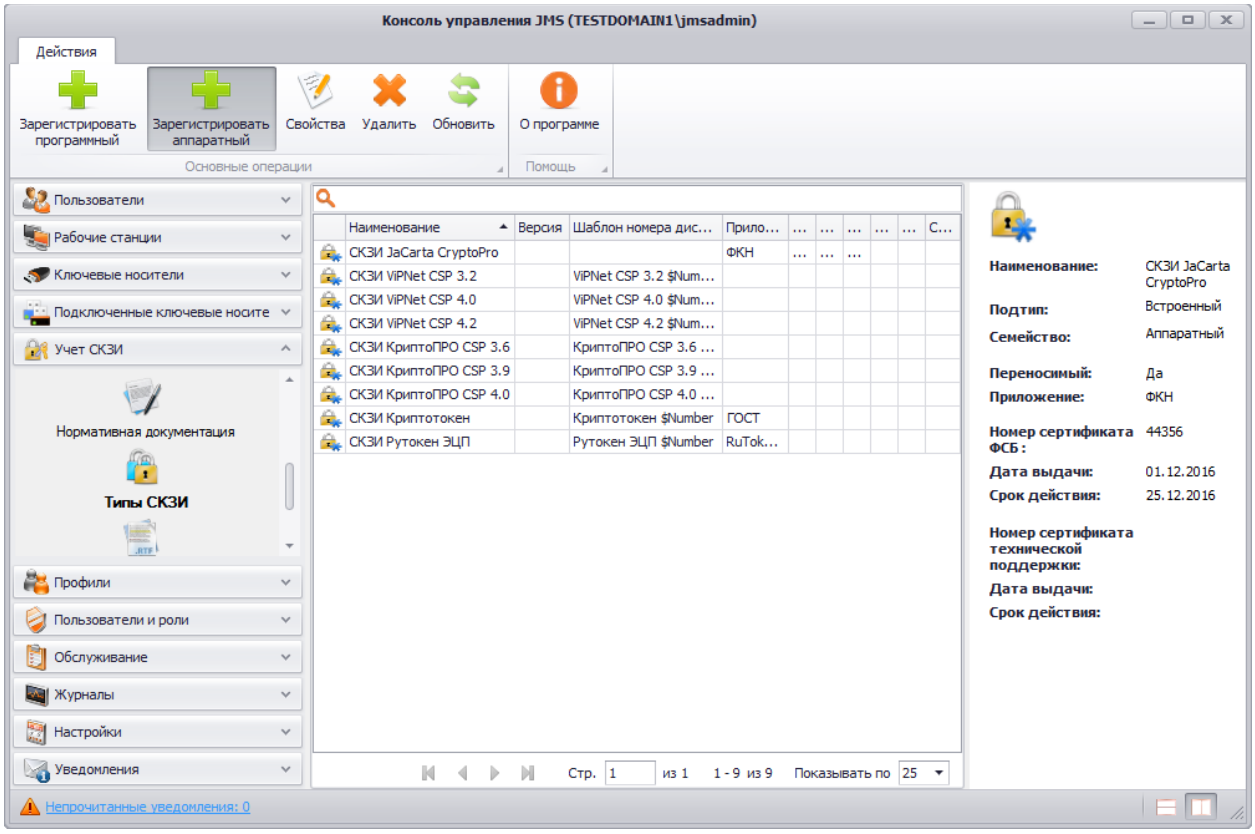


Рис. 277 – Вызов окна регистрации аппаратного типа СКЗИ

2. В появившемся окне (рис. 278) введите **Наименование** типа СКЗИ. Если необходимо выберите опцию **Переносимый**, из раскрывающегося списка в поле **Приложение:** выберите Приложение, используемое СКЗИ.
3. Если необходимо, выберите опцию **Сертификат ФСБ** и введите **Номер**, **Дату выдачи** и **Срок действия** сертификата ФСБ.
4. Если необходимо, выберите опцию **Сертификат поддержки** и введите **Номер**, **Дату выдачи** и **Срок действия** сертификата поддержки.
5. Нажмите **Создать**.

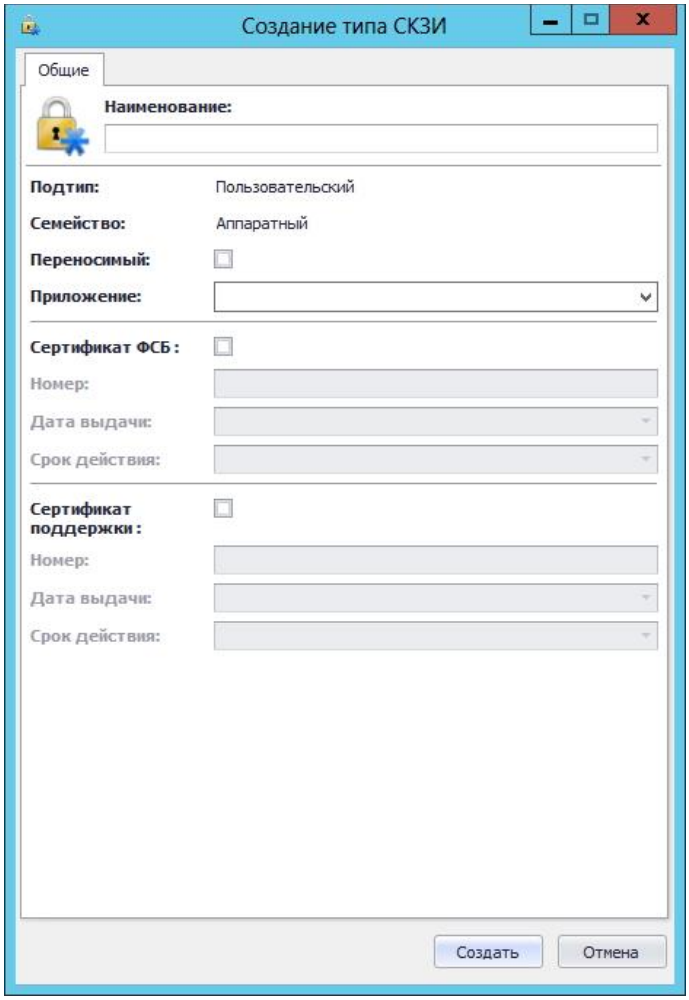


Рис. 278 – Окно создания типа СКЗИ

Зарегистрированный тип СКЗИ отобразится в окне консоли управления JMS в разделе **Учет СКЗИ** -> **Тип СКЗИ**.

3.11.3 Типы нормативной документации

В JMS зарегистрировано определенное количество 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 списка типов нормативной документации отображаются свойства, описание которых представлено в таблице 65.

Табл. 65

Наименование свойства	Описание
Наименование	Наименование нормативного документа
Тип сущности	Предмет, фигурирующий в нормативном документе:

Наименование свойства	Описание
	– 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. 369.

Для того чтобы просмотреть список нормативных документов, перейдите в раздел **Учет СКЗИ** -> **Типы нормативной документации** (см. рис. 279).

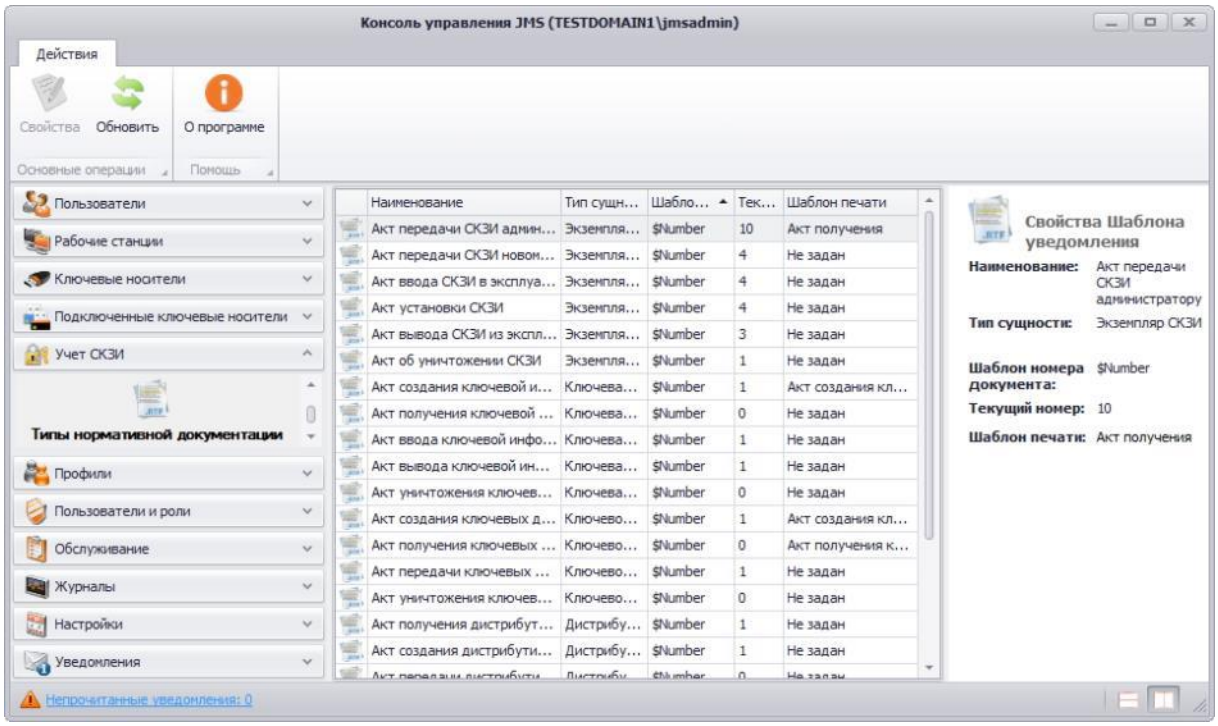


Рис. 279 – Окно типов нормативной документации

3.11.3.1 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 и на верхней панели консоли управления JMS нажмите **Свойства** (см. рис. 280).

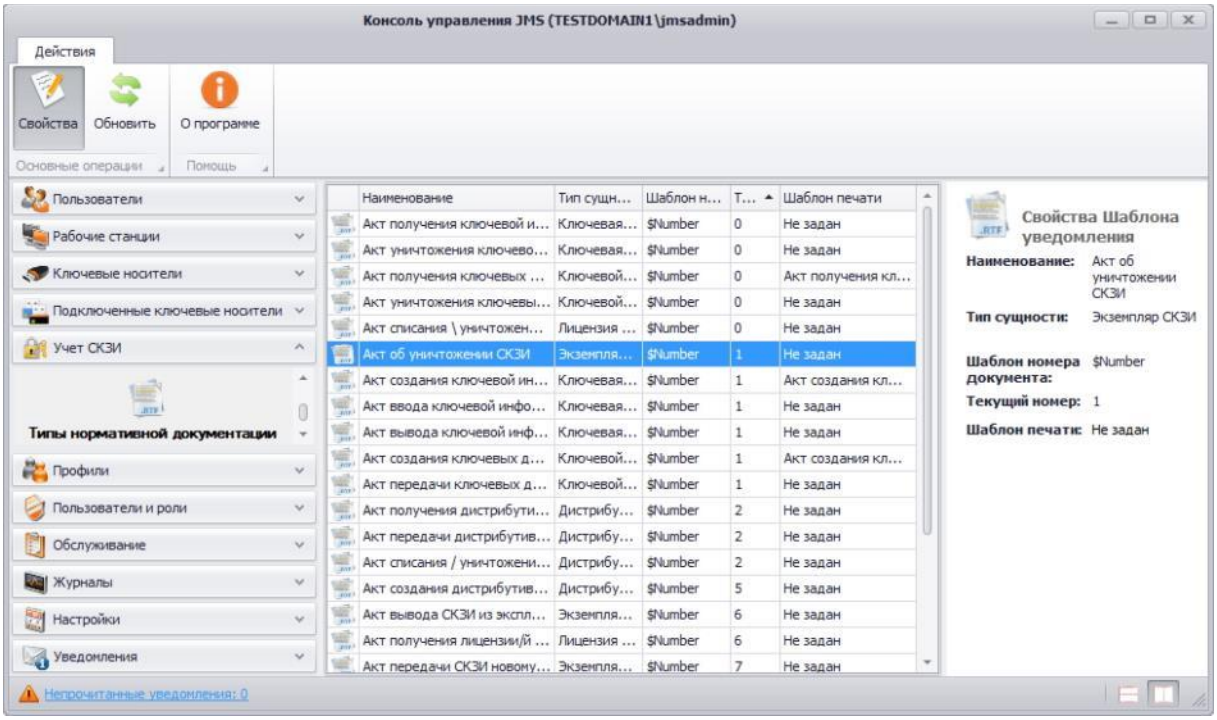


*Рис. 280 – Вызов окна просмотра свойств **Типа нормативного документа***

2. В появившемся окне перейдите на вкладку **Шаблон печатной формы** (см. рис. 281) и выберите из раскрывающегося списка в поле **[нет данных]** 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. 369).

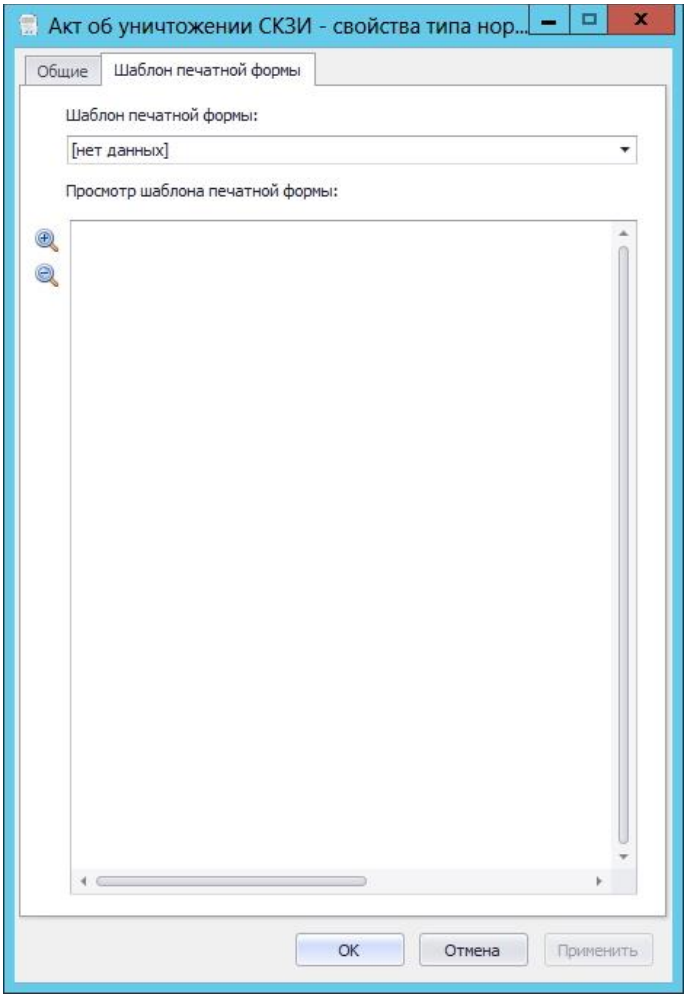


Рис. 281 – Окно просмотра шаблона печатной формы нормативного документа

3.11.4 Экземпляры СКЗИ

Действия, выполнение которых возможно в разделе **Учет СКЗИ** -> **Экземпляры СКЗИ** перечислены в таблице 63.

При просмотре списка зарегистрированных программных СКЗИ отображаются свойства, описание которых представлено в таблице 66.

Табл. 66

Наименование свойства	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

Наименование свойства	Описание
Место установки	Текстовое описание места установки
От кого получено	Текстовое описанием лица, от которого СКЗИ получено
Ответственное лицо	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. 330)
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 67.

Табл. 67

Наименование опции	Описание
Содержимое -> **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
Содержимое -> **Показывать неучитываемые**	При выборе этой опции в списке отображаются СКЗИ, учет которых прекращен
Содержимое -> **Показывать уничтоженные**	При выборе этой опции в списке отображаются СКЗИ, которые были уничтожены

3.11.4.1 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, Users /**Пользователи**) и в верхней панели и нажмите **Зарегистрировать** (см. рис. 282).

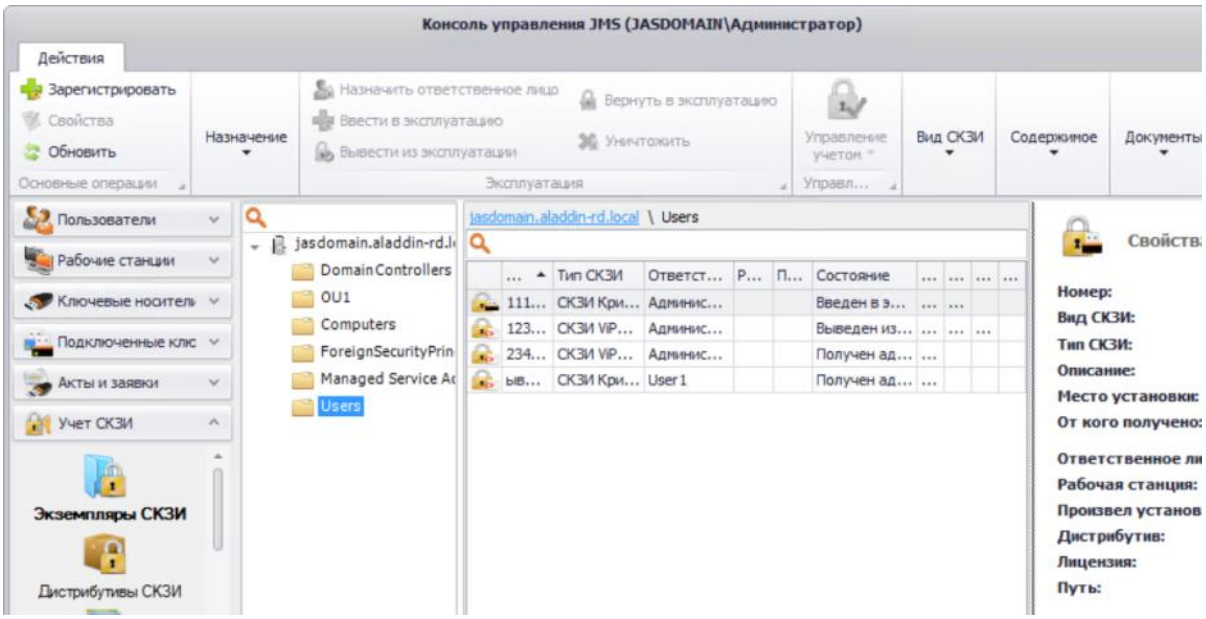


Рис. 282 – Вызов окна регистрации программного СКЗИ

2. В появившемся окне (см. рис. 283) введите **Номер** экземпляра СКЗИ, из раскрывающегося списка выберите **Тип СКЗИ**, при необходимости заполните поле **Описание**, **Место установки** и поле **От кого получено**. Нажмите **Создать**.

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 автомитически зарегистрированы при добавлении их лицензии (см. толкование свойства **Автосоздание экземпляров СКЗИ** в разделе «Типы СКЗИ», с. 318).
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.

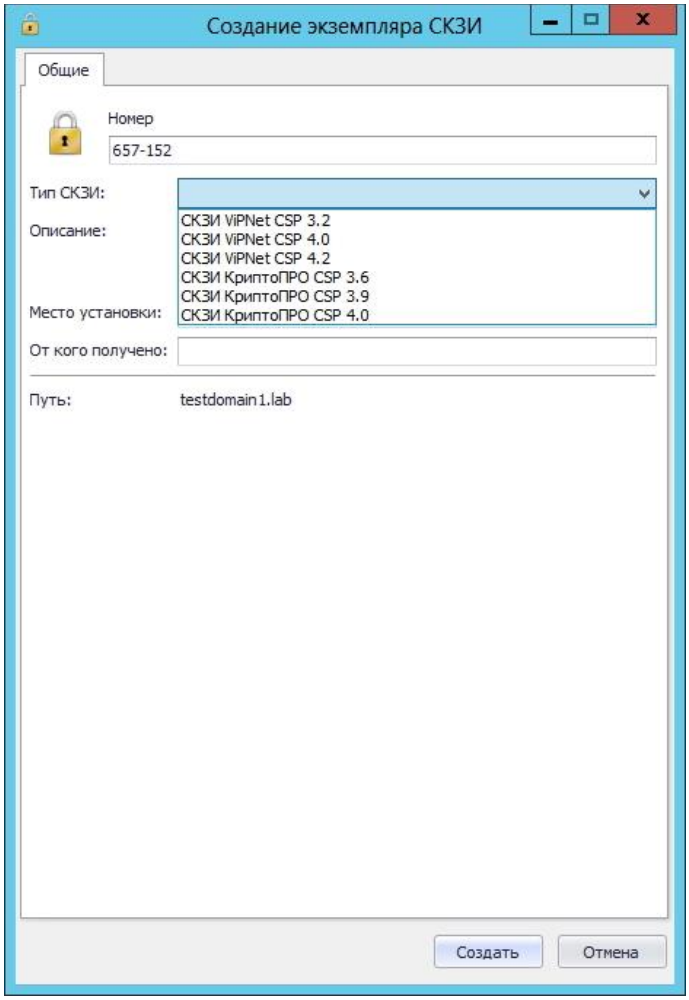


Рис. 283 – Создание экземпляра СКЗИ

4. Отобразится следующее окно (см. рис. 284). При необходимости просмотреть сформированный нормативный документ нажмите **Да**, в противном случае – нажмите **Нет.**

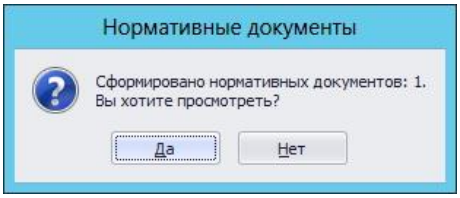


Рис. 284 – Окно сообщения о формировании нормативных документов

5. В случае нажатия **Да** – в появившемся окне (см. рис. 285) отобразится название сформированного документа, который при необходимости можно просмотреть или распечатать. Нажмите **Закрыть**.

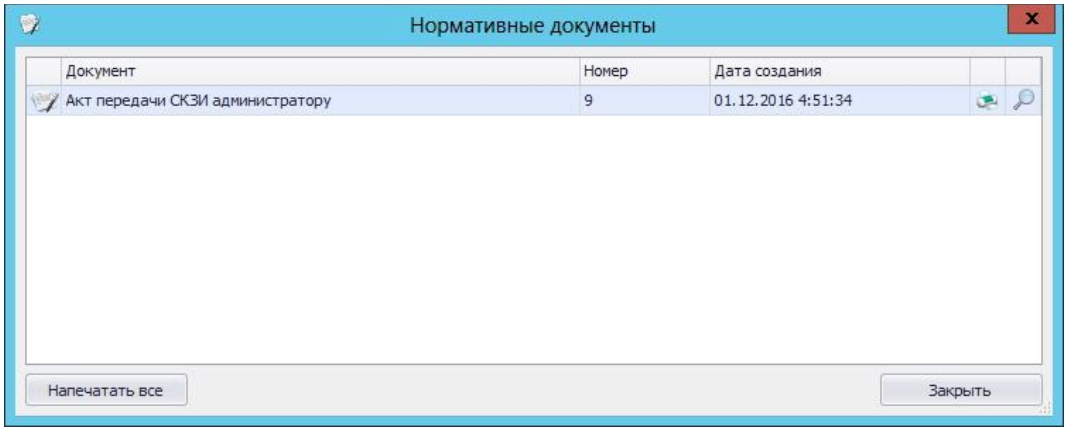


Рис. 285 – Окно нормативных документов

Зарегистрированное программное СКЗИ отобразится в окне консоли управления JMS в разделе **Учет СКЗИ** -> **Экземпляры СКЗИ**.

3.11.4.2 Управление назначением экземплряра СКЗИ

3.11.4.2.1 Установившее лицо

Для того чтобы назначить зарегистрированному экземпляру программного СКЗИ **Установившее лицо,** выполните следующие действия:

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр и на верхней панели консоли управления JMS нажмите **Установившее лицо** –> **Назначить** (см. рис. 286).

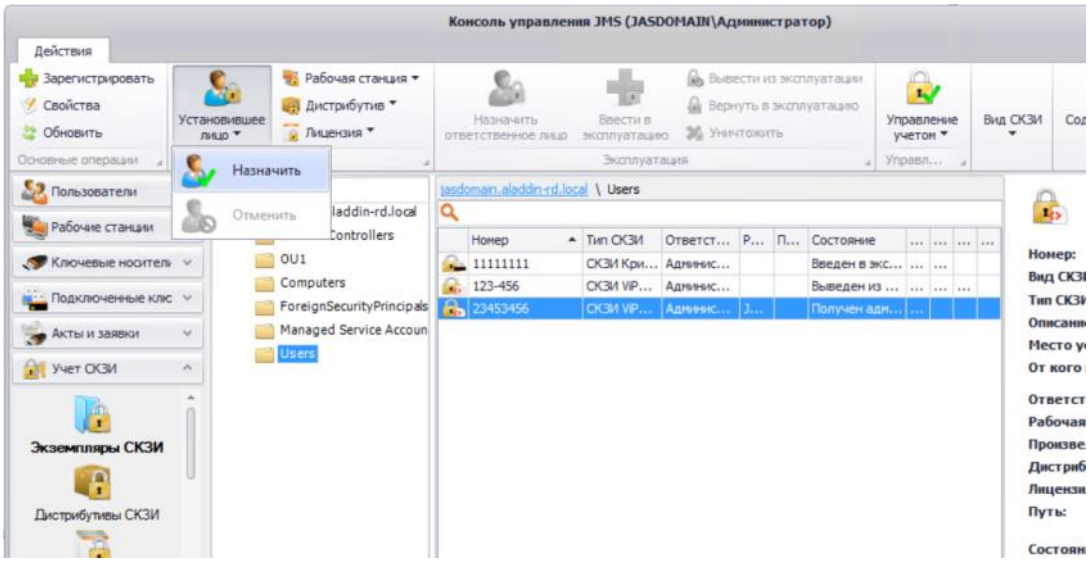


Рис. 286 – Окно назначения программному СКЗИ установившего лица

2. Далее появится окно со списком пользователей, в котором необходимо выделить пользователя для назначения и нажать кнопку **Выбрать**.

Чтобы отменить назначение нажмите **Установившее лицо** –> **Отменить**.

3.11.4.2.2 Рабочая станция

Для того чтобы зарегистрировать в JMS рабочую станцию, на которой установлен экземпляр программного СКЗИ, выполните следующие действия:

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр и на верхней панели консоли управления JMS нажмите **Рабочая станция** –> **Назначить** (см. рис. 287).

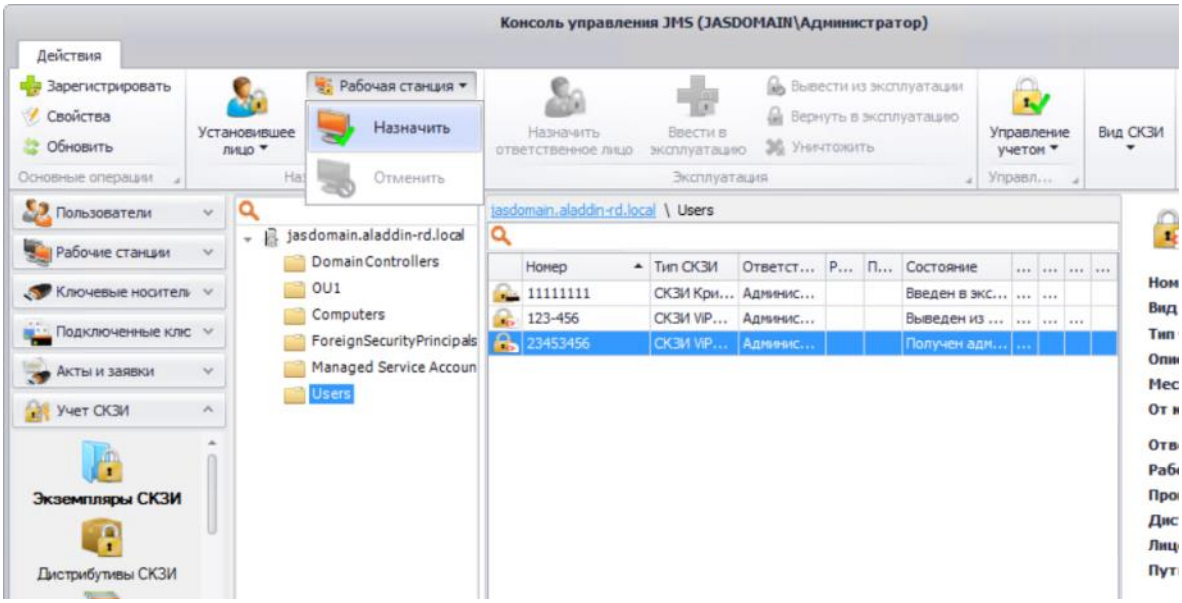


Рис. 287 – Окно назначения программному СКЗИ рабочей станции

2. Далее появится окно со списком рабочих станций, в котором необходимо выделить рабочую станцию для назначения и нажать кнопку **Выбрать**.

   Чтобы отменить назначение нажмите **Рабочая станция** –> **Отменить**.

3.11.4.2.3 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 и на верхней панели консоли управления JMS нажмите **Дистрибутив** –> **Назначить** (см. рис. 288).

Примечание. Операция назначения дистрибутива необязательна.

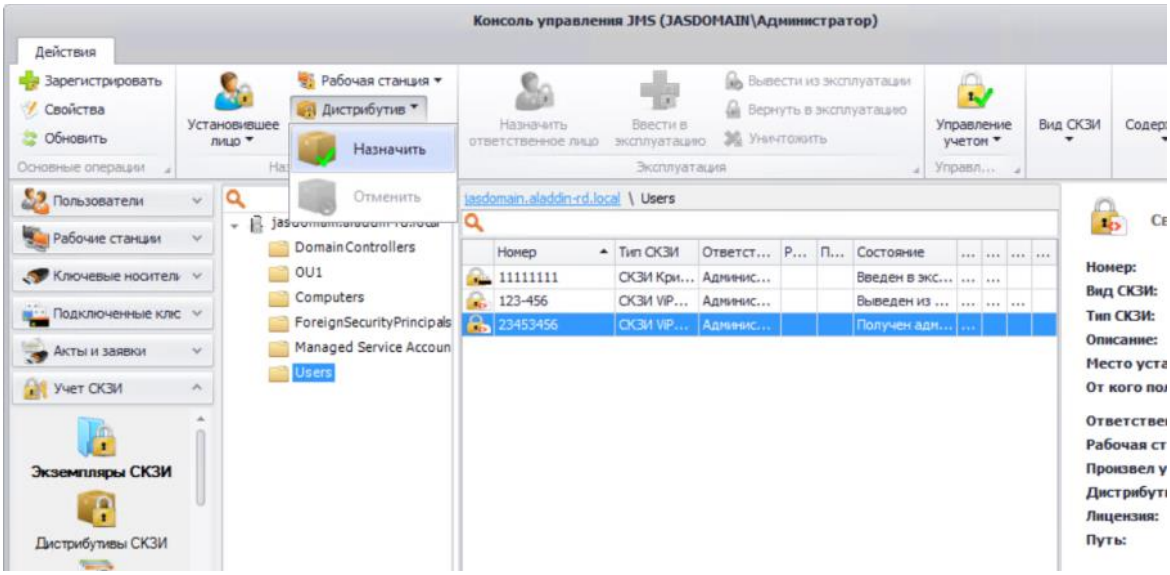


Рис. 288 – Окно назначения дистрибутива программному СКЗИ

2. Далее появится окно со списком дистрибутивов, в котором необходимо выделить дистрибутив для назначения и нажать кнопку **Выбрать**.

   Чтобы отменить назначение нажмите **Дистрибутив** –> **Отменить**.

3.11.4.2.4 Лицензия

Для того чтобы назначить зарегистрированному экземпляру программного СКЗИ **Лицензию,** выполните следующие действия:

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр и на верхней панели консоли управления JMS нажмите **Лицензия** –> **Назначить** (см. рис. 289).

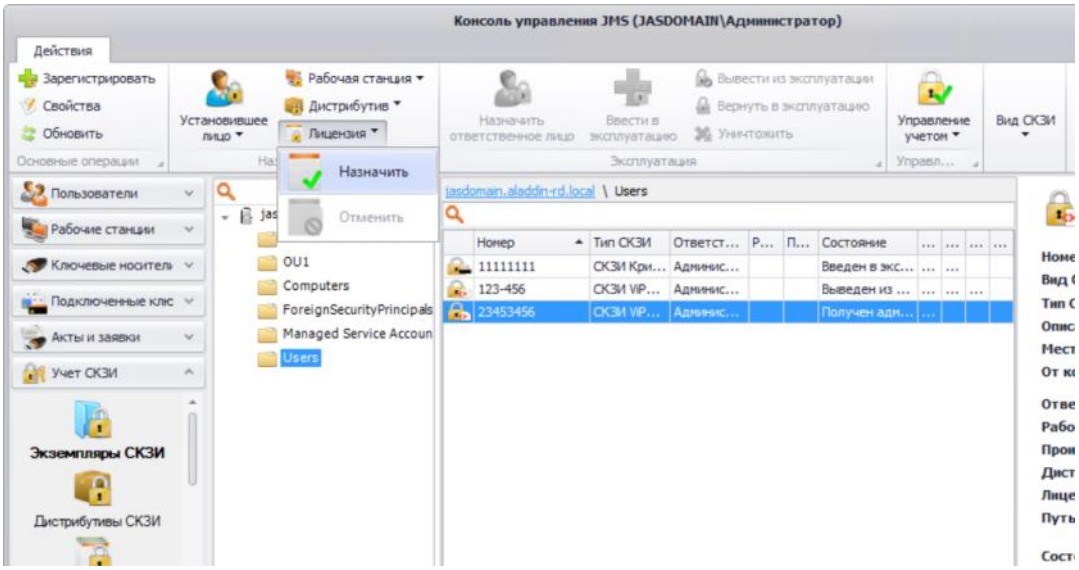


Рис. 289 – Окно назначения лицензии программному СКЗИ

2. Далее появится окно со списком лицензий, в котором необходимо выделить лицензию для назначения и нажать кнопку **Выбрать**.

Чтобы отменить назначение, нажмите **Лицензия** –> **Отменить**.

3.11.4.3 Управление эксплуатацией экземпляра СКЗИ

3.11.4.3.1 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 и на верхней панели консоли управления JMS нажмите **Назначить ответственное лицо** (см. рис. 290).

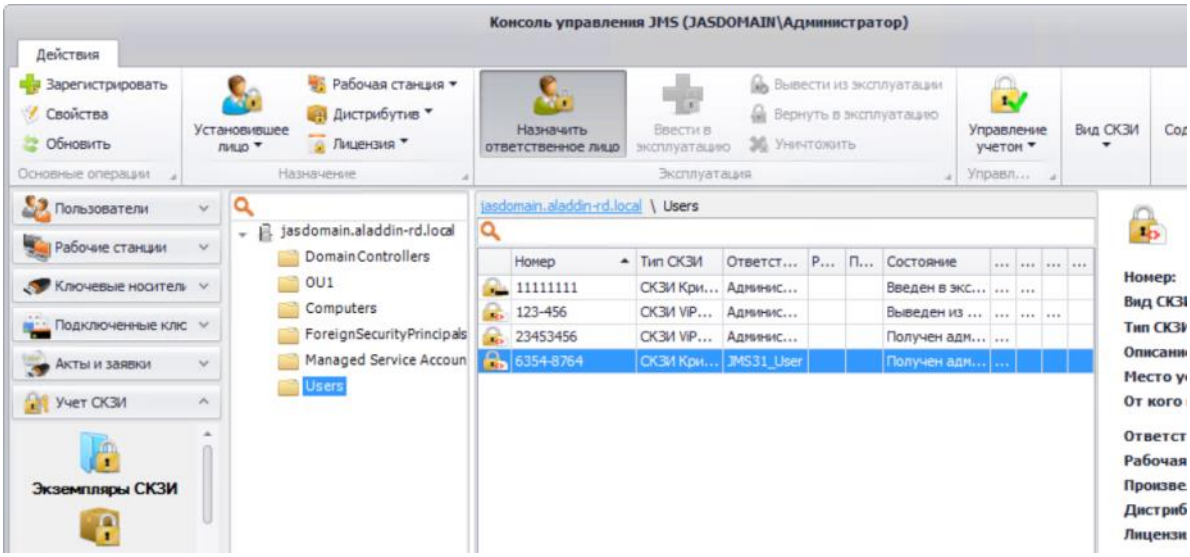


Рис. 290 – Окно назначения ответственного лица программному СКЗИ

2. Далее появится окно со списком пользователей, в котором необходимо выделить пользователя для назначения и нажать кнопку **Выбрать**.

3.11.4.3.2 Ввести в эксплуатацию

Примечание. Помимо приведённого ниже «ручного» способа, ввод программных СКЗИ в эксплуатацию может производиться также автоматически путем выполнения соответствующего плана обслуживания (см. «План обслуживания СКЗИ», с. 421). Для этого должны выполняться следующие условия:

- СКЗИ зарегистрировано;
- СКЗИ назначено пользователю;
- для СКЗИ назначена рабочая станция, на которой он установлен (см. «Рабочая станция», с. 330).

При автоматическом вводе в эксплуатацию формируются все соответствующие документы, которые можно распечатать при необходимости из раздела Акты и заявки.

Для того чтобы ввести в эксплуатацию зарегистрированный экземпляр программного СКЗИ, выполните следующие действия.

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр и на верхней панели консоли управления JMS нажмите **Ввести в эксплуатацию** (см. рис. 291).

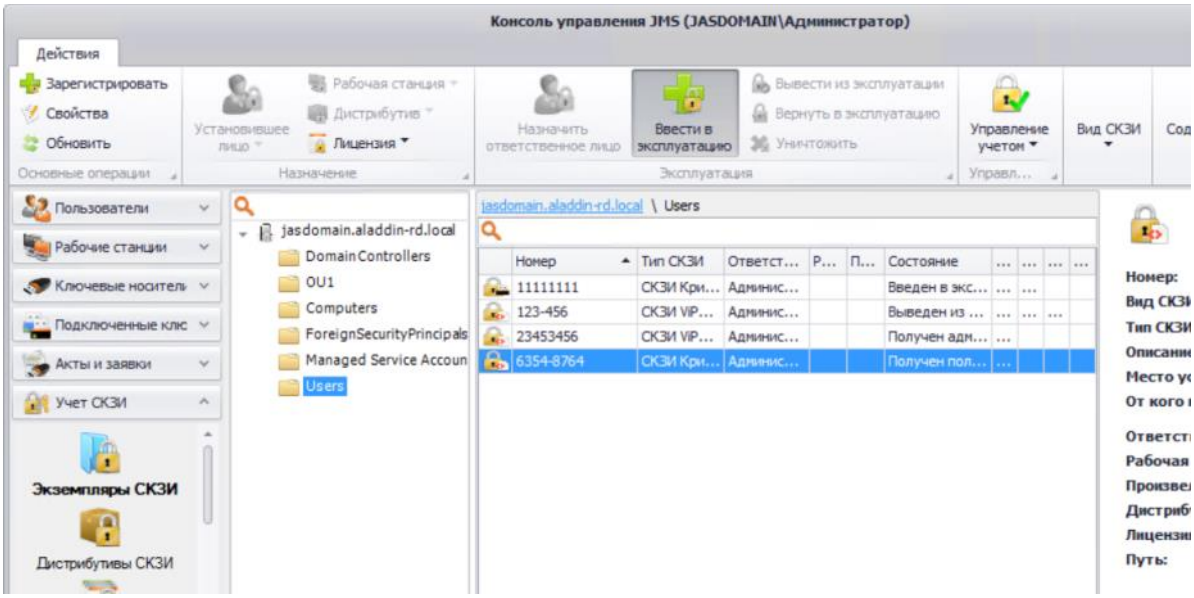


Рис. 291 – Окно ввести в эксплуатацию программный СКЗИ

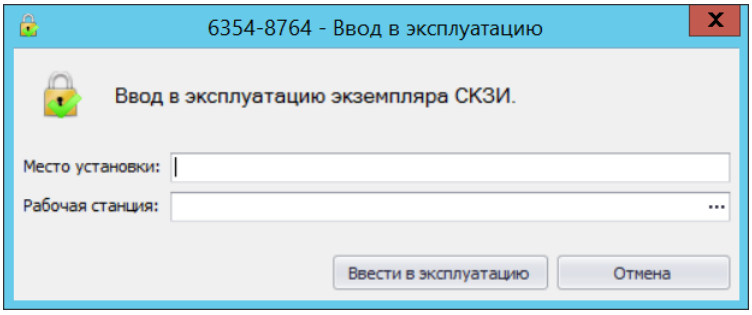


Рис. 292 – Окно ввода места установки и рабочей станции

2. В появившемся окне (см. рис. 292) введите данные в поле **Место установки** и в поле **Рабочая станция** выберите Рабочую станцию (для выбора рабочей станции воспользуйтесь кнопкой «...»). Затем нажмите на кнопку **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. Отобразится следующее окно (см. рис. 293). При необходимости просмотреть сформированные нормативные документы нажмите **Да**, в противном случае – нажмите **Нет.**

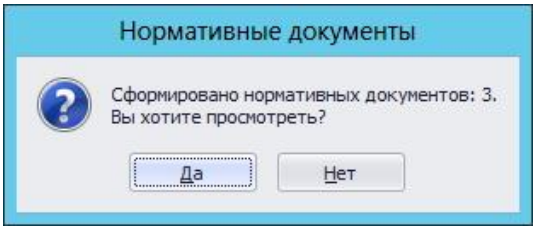


Рис. 293 – Окно сообщения о формировании нормативных документов

4. В случае нажатия **Да** – в следующем появившемся окне отобразятся названия сформированных документов, которые при необходимости можно просмотреть или распечатать.

3.11.4.3.3 Вывести из эксплуатации

Для того чтобы вывести из эксплуатации экземпляр программного СКЗИ, выполните следующие действия:

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр и на верхней панели консоли управления JMS нажмите **Вывести из эксплуатации** (см. рис. 294).

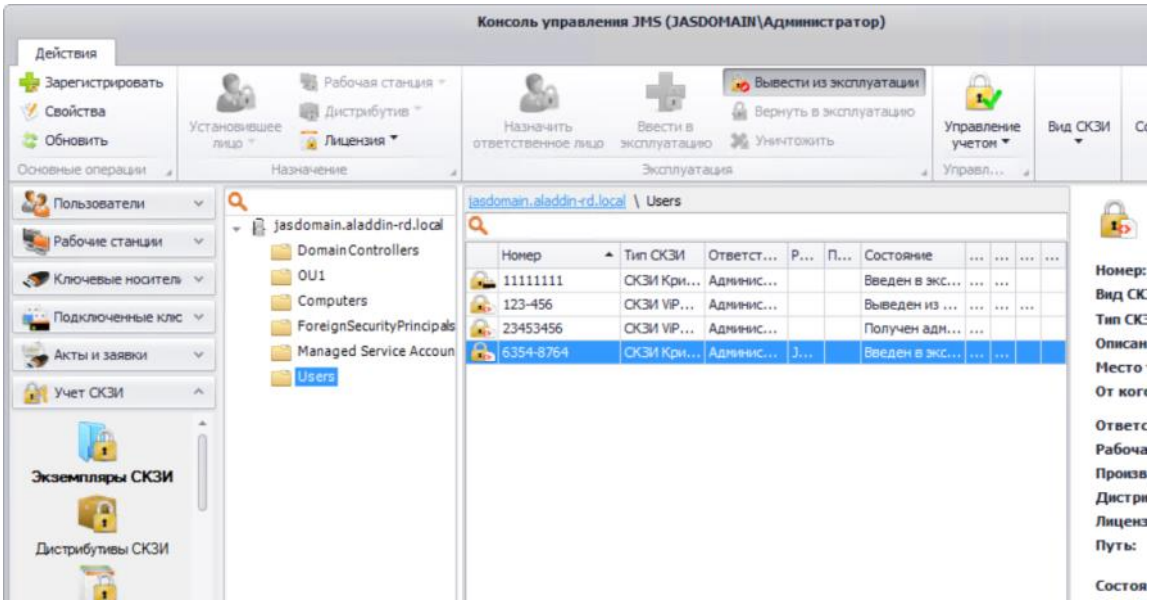


Рис. 294 – Окно вывода из эксплуатации программного СКЗИ

2. В появившемся окне (см. рис. 295) подтвердите свои действия нажатием **Да**.

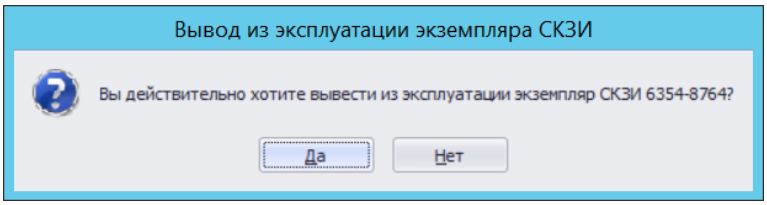


Рис. 295 – Окно подтверждения вывода из эксплуатации

3. Отобразится следующее окно (см. рис. 296). При необходимости просмотреть сформированные нормативные документы нажмите **Да**, в противном случае – нажмите **Нет.**

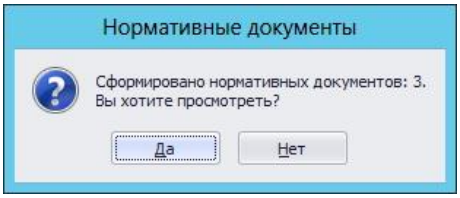


Рис. 296 – Окно сообщение о формировании нормативных документов

4. В случае нажатия **Да** – в следующем появившемся окне отобразятся названия сформированных документов, которые при необходимости можно просмотреть или распечатать.

3.11.4.3.4 Вернуть в эксплуатацию

Для того чтобы вернуть в эксплуатацию экземпляр программного СКЗИ, выполните следующие действия:

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр и на верхней панели консоли управления JMS нажмите **Вернуть в эксплуатацию** (см. рис. 297).

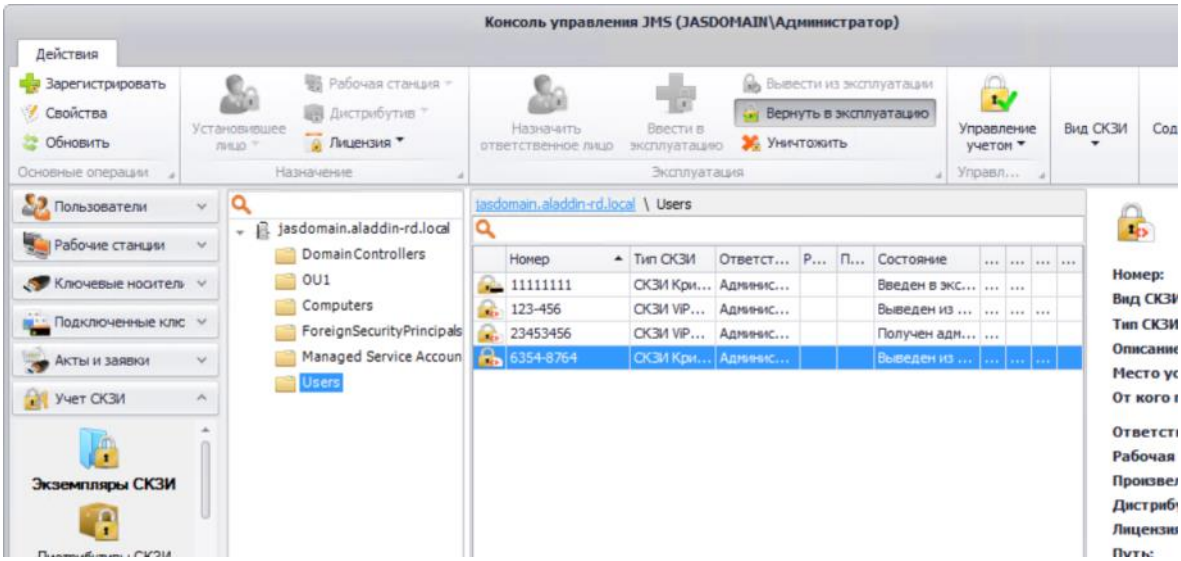


Рис. 297 – Окно вернуть в эксплуатацию программное СКЗИ

2. В появившемся окне (см. рис. 298) подтвердите свои действия нажатием **Да**.

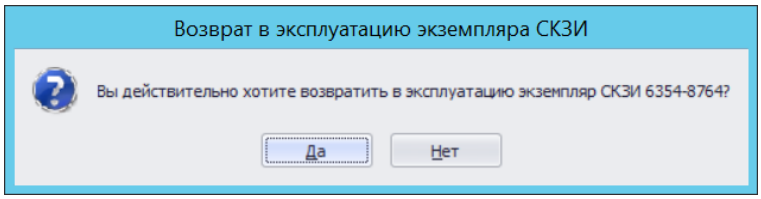


Рис. 298 – Окно подтверждения о возврате в эксплуатацию программного СКЗИ

3. Отобразится следующее окно (см. рис. 299). При необходимости просмотреть сформированные нормативные документы нажмите **Да**, в противном случае – нажмите **Нет.**

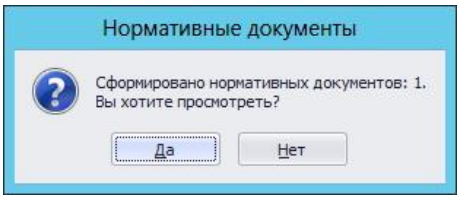


Рис. 299 – Окно сообщение о формировании нормативных документов

4. В случае нажатия **Да** – в следующем появившемся окне отобразятся названия сформированных документов, которые при необходимости можно просмотреть или распечатать.

3.11.4.3.5 Уничтожить

Для того чтобы уничтожить зарегистрированный экземпляр программного СКЗИ, выполните следующие действия:

1. Выделите в списке зарегистрированных программных СКЗИ требуемый экземпляр и на верхней панели консоли управления JMS нажмите **Уничтожить** (см. рис. 300).

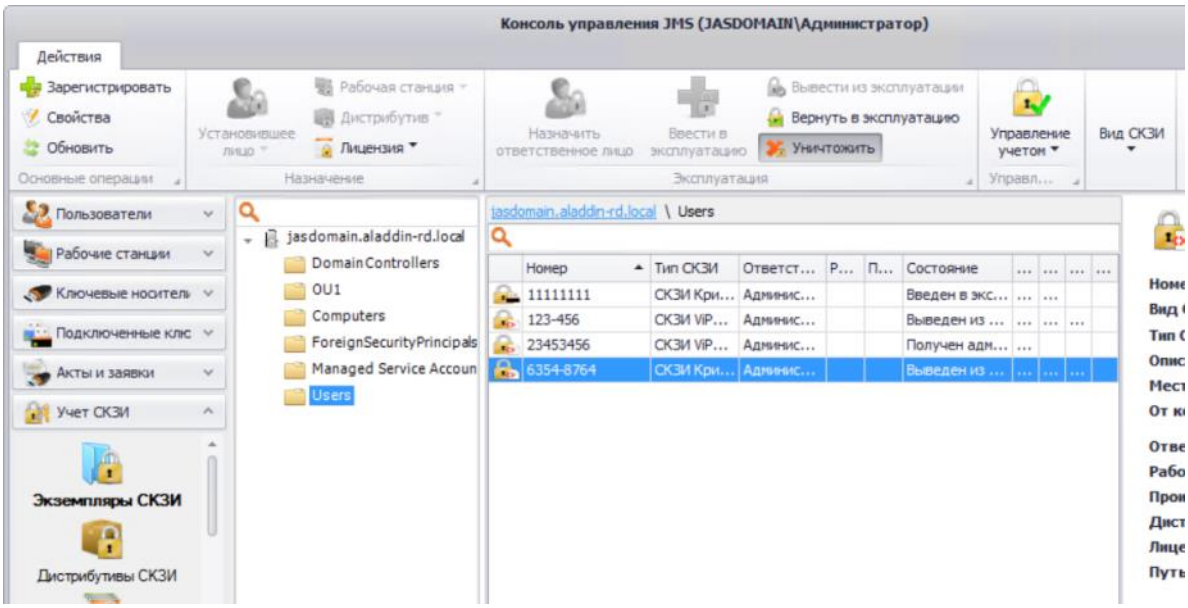


Рис. 300 – Окно уничтожения программного СКЗИ

2. В появившемся окне (см. рис. 301) подтвердите свои действия нажатием **Да**.

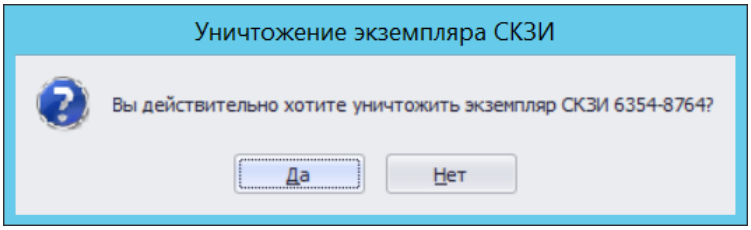


Рис. 301 – Окно подтверждения об уничтожении программного СКЗИ

3.11.5 Дистрибутивы СКЗИ

Действия, выполнение которых возможно в разделе **Учет СКЗИ** -> **Дистрибутивы СКЗИ** перечислены в таблице 63.

При просмотре списка зарегистрированных дистрибутивов СКЗИ отображаются свойства, описание которых представлено в таблице 68.

Табл. 68

Наименование свойства	Описание
Учетный номер дистрибутива	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

Наименование свойства	Описание
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
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

3.11.5.1 Регистрация дистрибутива СКЗИ

Для того чтобы зарегистрировать дистрибутив СКЗИ, выполните следующие действия:

1. Перейдите в раздел **Учет СКЗИ** –> **Дистрибутивы СКЗИ** и нажмите **Зарегистрировать** (см. рис. 302).

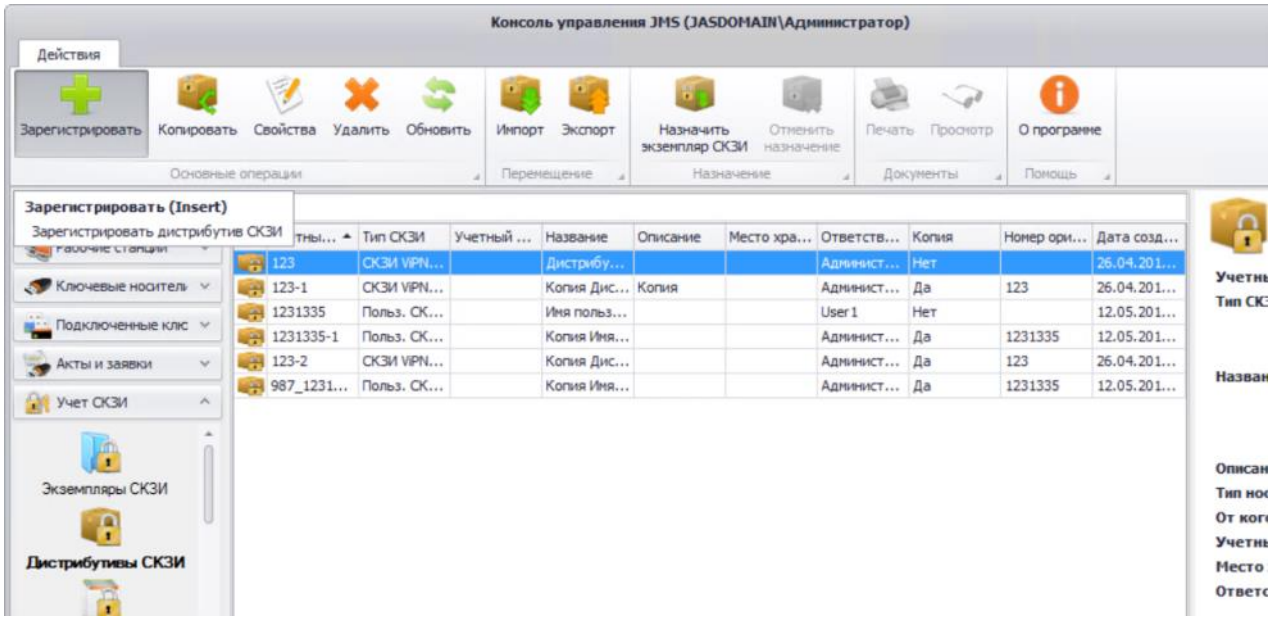


Рис. 302 – Начало регистрации дистрибутив СКЗИ

2. В появившемся окне (см. рис. 303) 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 **Создать**.

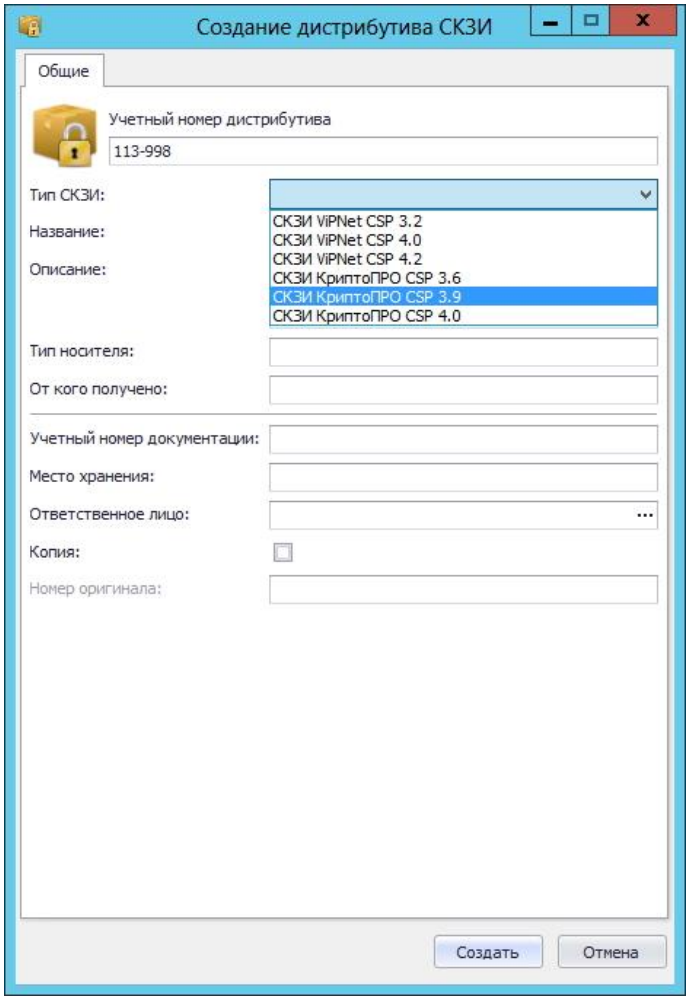


Рис. 303 – Окно создание дистрибутива СКЗИ

3. Отобразится следующее окно (см. рис. 304). При необходимости просмотреть сформированный нормативный документ нажмите **Да**, в противном случае – нажмите **Нет.**

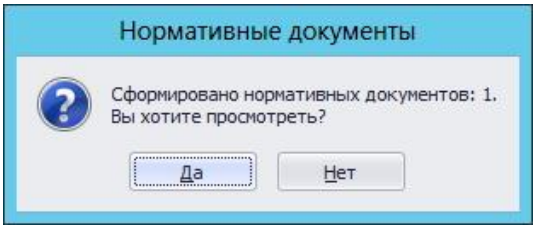


Рис. 304 – Окно сообщения о формировании нормативных документов

4. В случае нажатия **Да** – в появившемся окне (см. рис. 305) отобразится название сформированного документа, который при необходимости можно просмотреть или распечатать. Нажмите **Закрыть**.

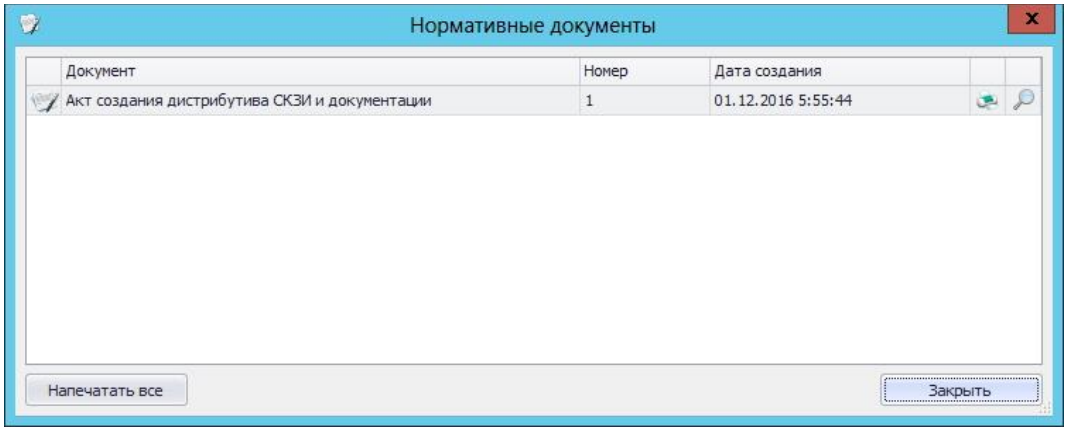


Рис. 305 – Окно нормативных документов

Зарегистрированный дистрибутив СКЗИ отобразится в окне консоли управления JMS в разделе **Учет СКЗИ** -> **Дистрибутивы СКЗИ**.

3.11.5.2 Тиражирование копий дистрибутива

При копировании дистрибутива необходимо учитывать следующие особенности:

- копии диска присваивается свой учетный номер, который формируется из эталонного, например, добавлением числа: эталонный – ДСД01, копия – 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 и на верхней панели консоли управления JMS нажмите **Копировать** (см. рис. 306).

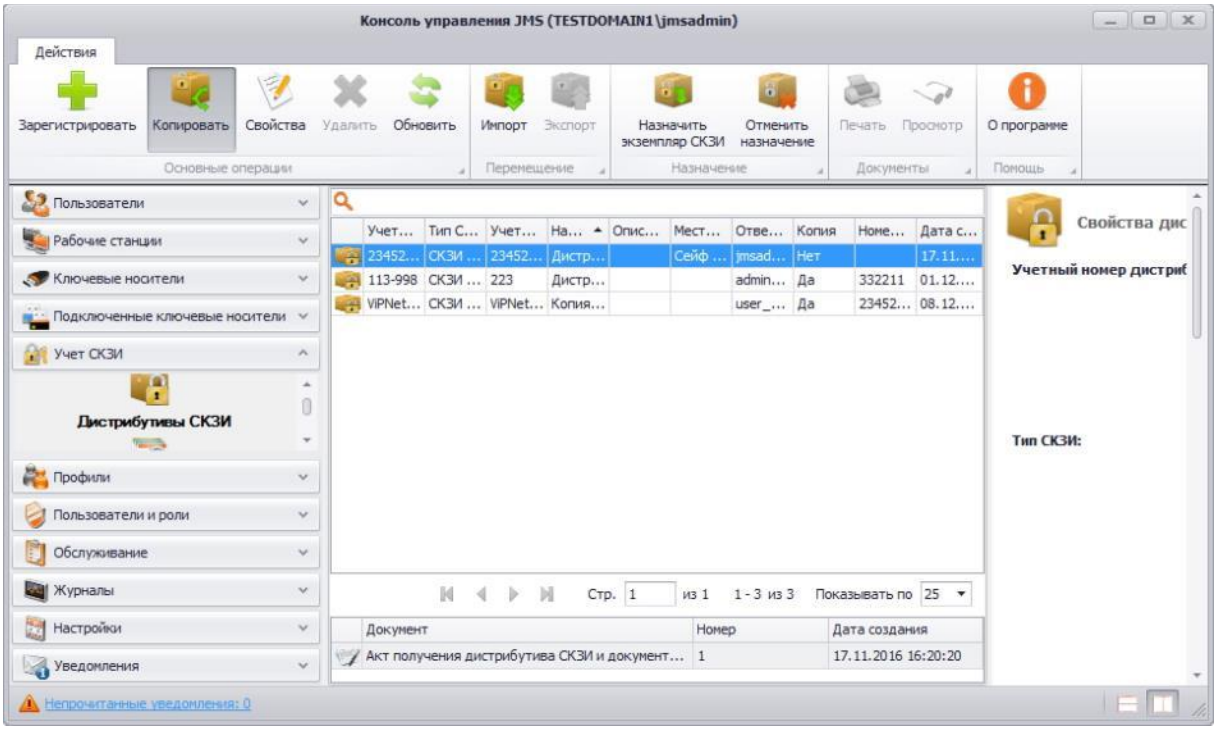


Рис. 306 – Окно копирования дистрибутива СКЗИ

2. В появившемся окне (см. рис. 307) укажите **Тип носителя** и **Количество копий оригинала**, затем нажмите **Копировать**.

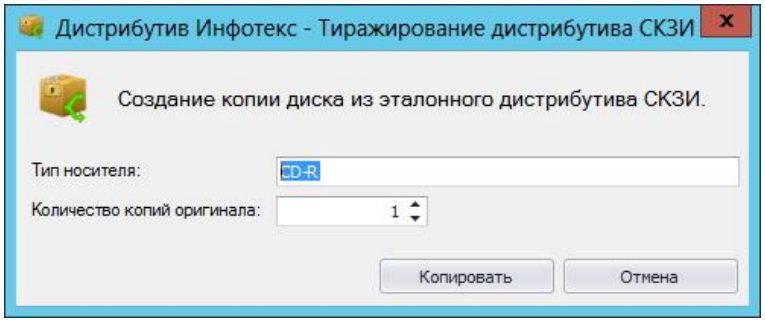


Рис. 307 – Окно создания копии эталонного дистрибутива СКЗИ

3. Отобразится следующее окно (см. рис. 308). При необходимости просмотреть сформированный нормативный документ нажмите **Да**, в противном случае – нажмите **Нет**.

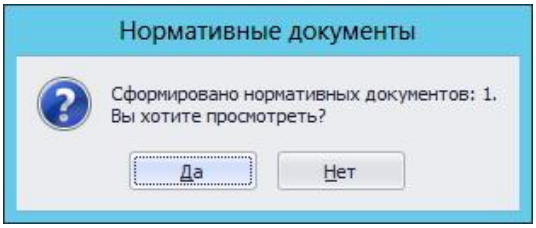


Рис. 308 – Окно сообщения о формировании нормативного документа

4. В случае нажатия **Да** – в следующем появившемся окне отобразится название сформированного документа, который при необходимости можно просмотреть или распечатать.

3.11.5.3 Импорт дистрибутивов (пакетная регистрация)

Для того чтобы произвести пакетную регистрацию дистрибутивов с помощью мастера импорта дистрибутивов выполните следующие действия:

1. На верхней панели консоли управления JMS нажмите **Импорт** (см. рис. 309).

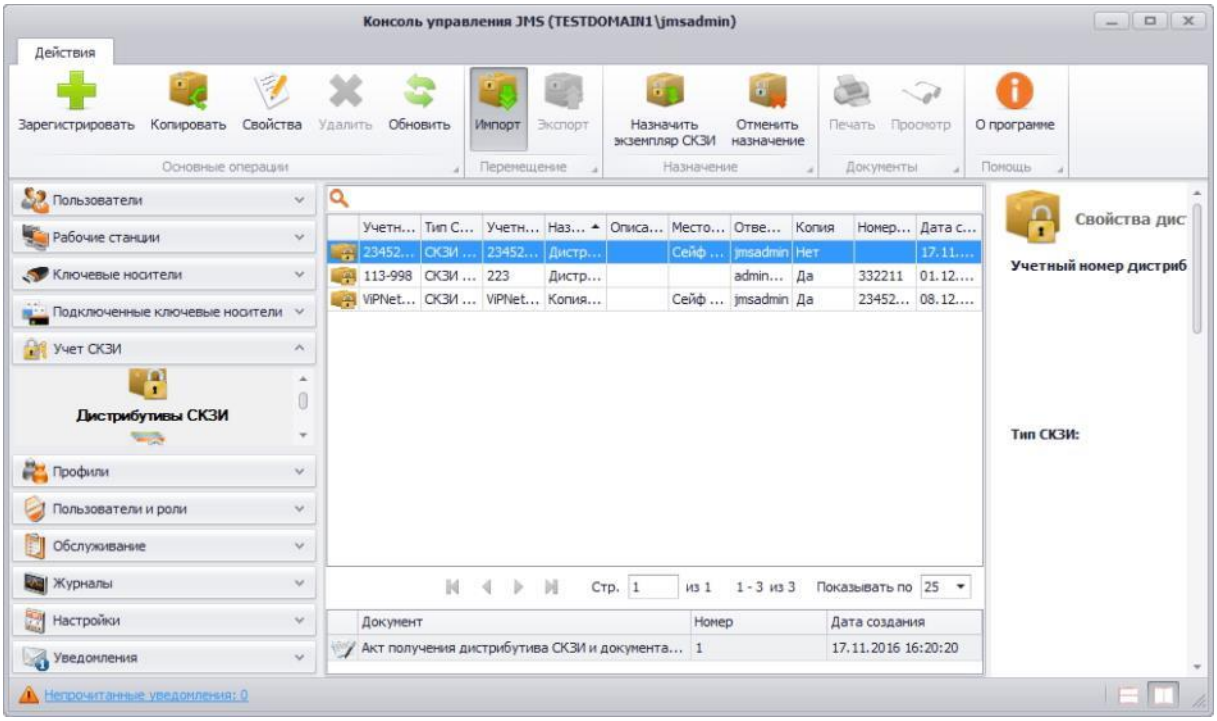


Рис. 309 – Окно импорта дистрибутива СКЗИ

2. В появившемся окне приветствия мастера импорта дистрибутивов СКЗИ (см. рис. 310) нажмите **Далее**.

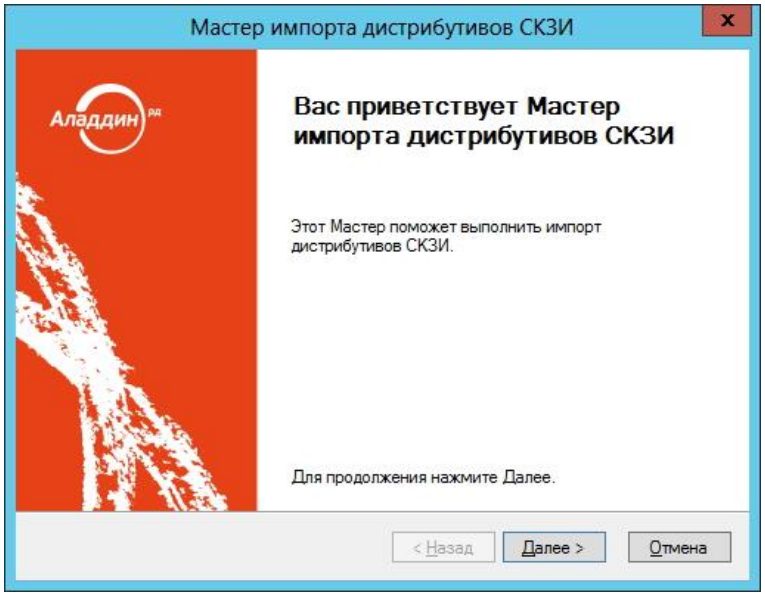


Рис. 310 – Окно приветствия мастера импорта дистрибутивов СКЗИ

3. В появившемся окне (см. рис. 311) выберите из раскрывающегося списка **Тип СКЗИ**, выберите **Ответственное лицо** и укажите **Файл импорта** и нажмите **Далее**.

Примечание. Файл импорта представляет собой файл в формате *.CSV. Подробнее о структуре файла см. Формат файлов импорта дистрибутива СКЗИ.

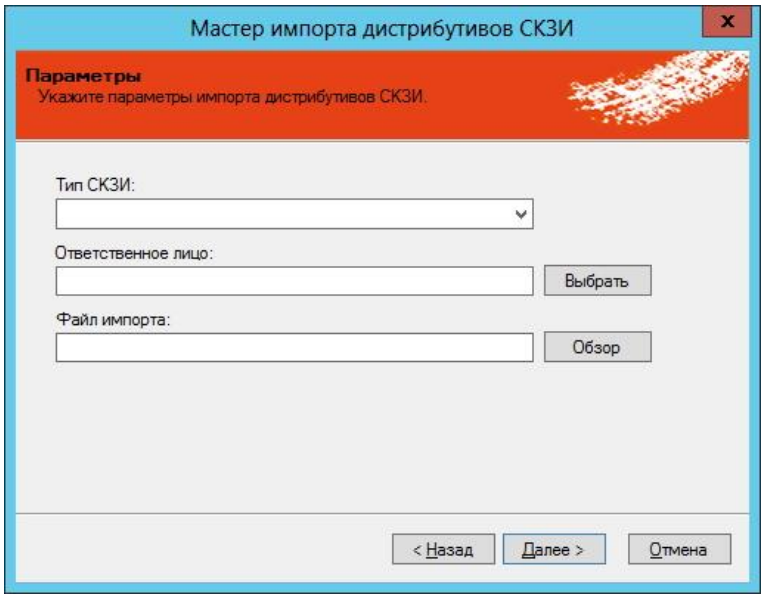


Рис. 311 – Окно ввода параметров импорта дистрибутива СКЗИ

4. В появившемся окне (см. рис. 312) нажмите **Далее**.

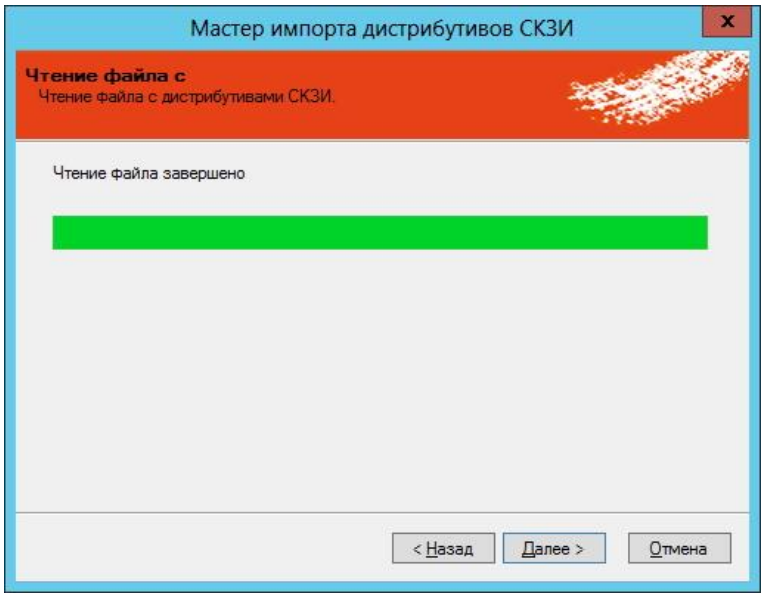


Рис. 312 – Окно чтения файла с дистрибутивами СКЗИ

5. В появившемся окне (см. рис. 313) нажмите **Далее**.

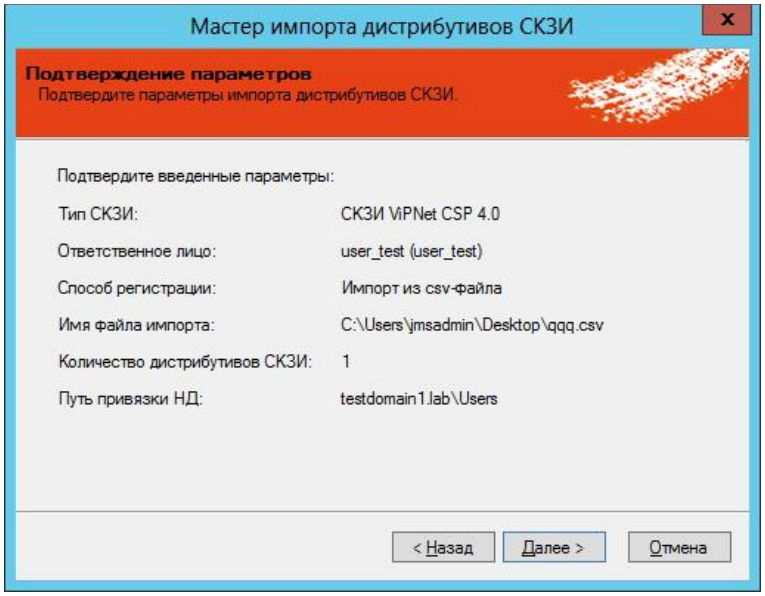


Рис. 313 – Окно подтверждения параметров импорта дистрибутива СКЗИ

6. В появившемся окне (см. рис. 314) нажмите **Далее**.

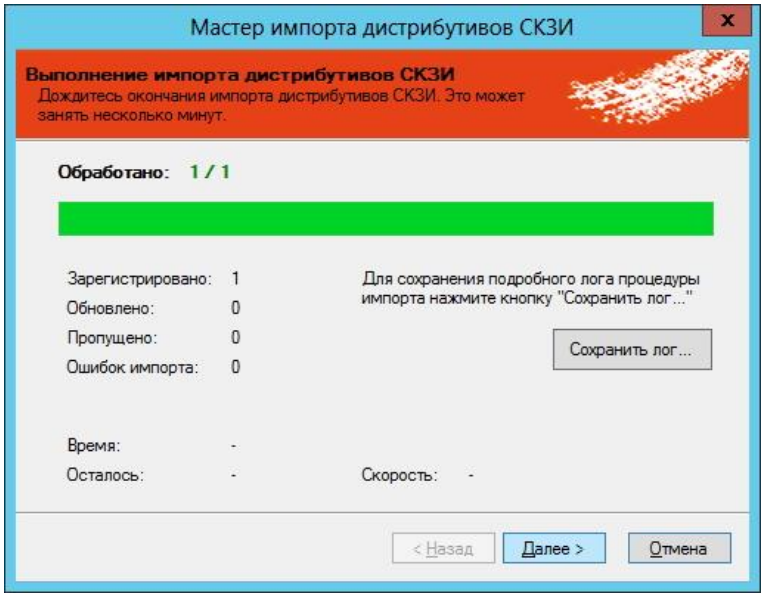


Рис. 314 – Окно выполнения импорта дистрибутива СКЗИ

7. В появившемся окне (см. рис. 315) нажмите **Завершить**.

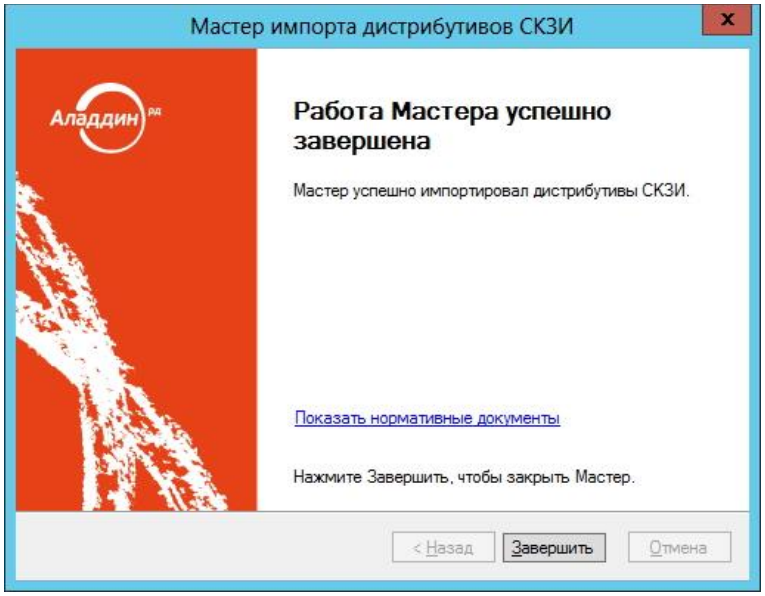


Рис. 315 – Окно завершения импорта дистрибутива СКЗИ

3.11.5.3.1 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}**».

Дальнейшие строки файла содержат значения полей из заголовка для дистрибутива СКЗИ. Порядок следования значений должен соответствовать порядку объявленных полей 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 69.

Табл. 69

№	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

№	Наименование поля в файле	Наименование свойства	Тип свойства	Обязательное поле	Обязательное значение
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:

NameDescriptionPackageNumberDocumentNumberIsCopyOriginalNumberReceivedFromMediaType

name1description11Falsereceived_from1media_type1

name2description22Falsereceived_from2media_type2

name3description331Falsereceived_from3media_type1

3.11.5.4 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. Выделите в списке зарегистрированных дистрибутивов СКЗИ требуемый экземпляр и на верхней панели консоли управления JMS нажмите **Экспорт** (см. рис. 316).

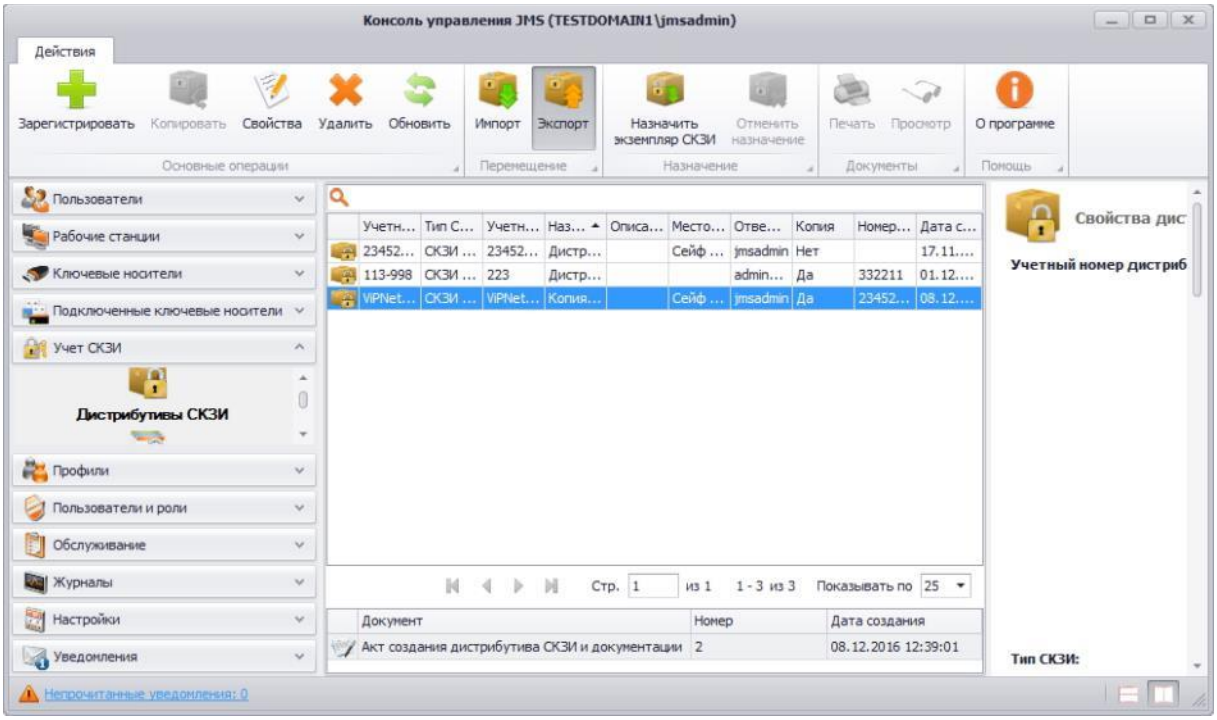


Рис. 316 – Окно экспорта дистрибутива СКЗИ

2. В появившемся окне приветствия мастера экспорта дистрибутивов СКЗИ (см. рис. 317) нажмите **Далее**.

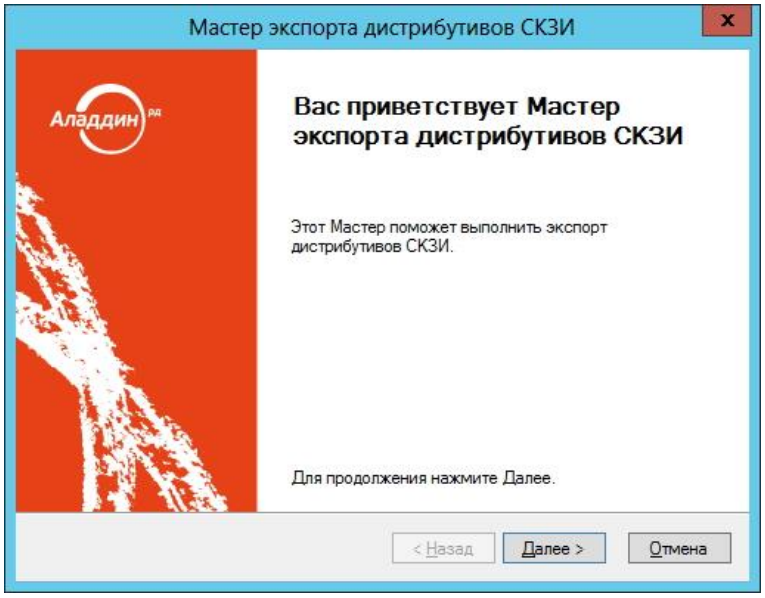


Рис. 317 – Окно приветствия мастера экспорта дистрибутива СКЗИ

3. В появившемся окне (см. рис. 318) выберите **Ответственное лицо**, укажите **Файл экспорта** и нажмите **Далее**.

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».

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.

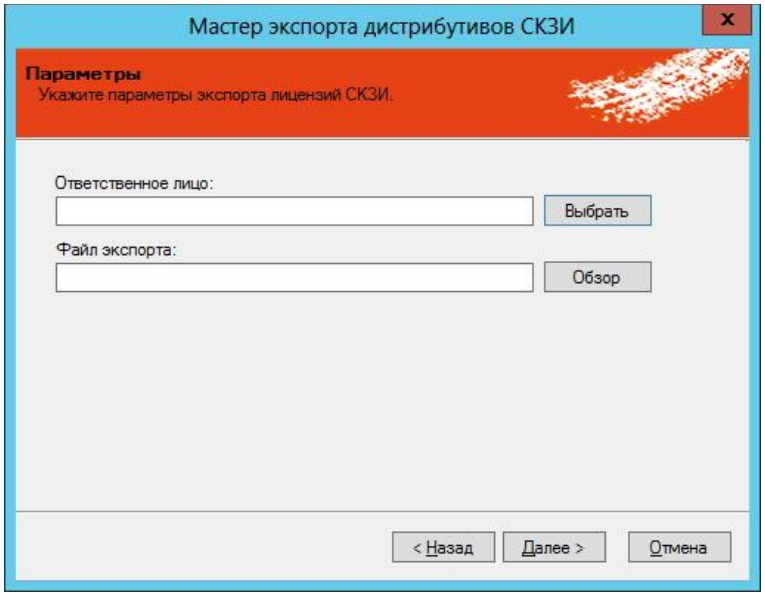


Рис. 318 – Окно ввода параметров экспорта дистрибутива СКЗИ

4. В появившемся окне (см. рис. 319) нажмите **Далее**.

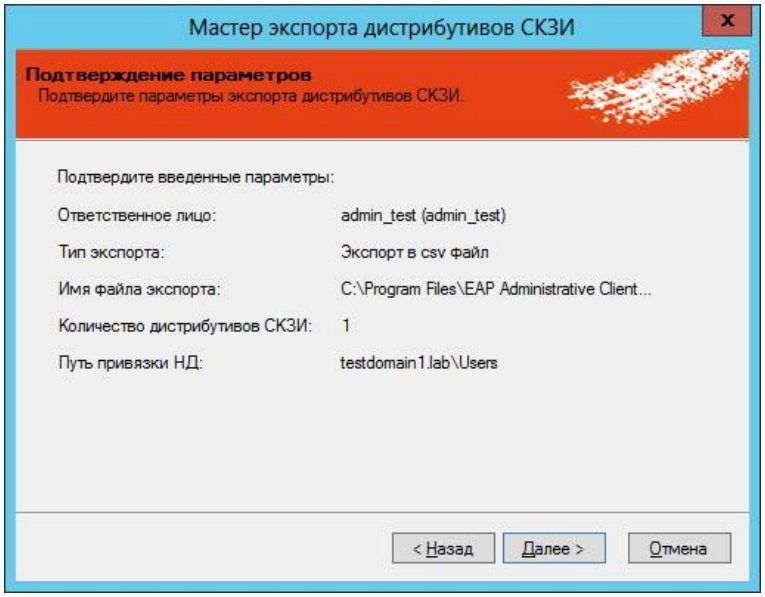


Рис. 319 – Окно подтверждения параметров экспорта дистрибутива СКЗИ

5. В появившемся окне (см. рис. 320) нажмите **Далее**.

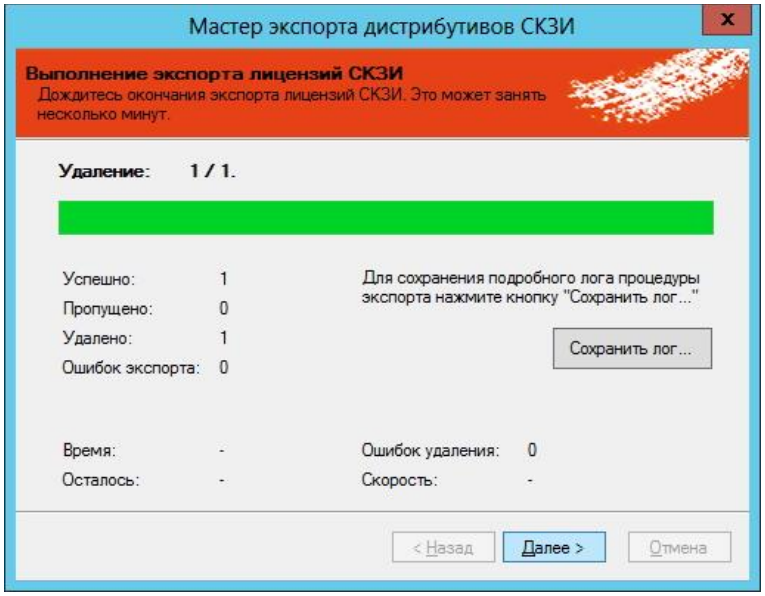


Рис. 320 – Окно выполнения экспорта лицензий СКЗИ

6. В появившемся окне (см. рис. 321) нажмите **Завершить**.

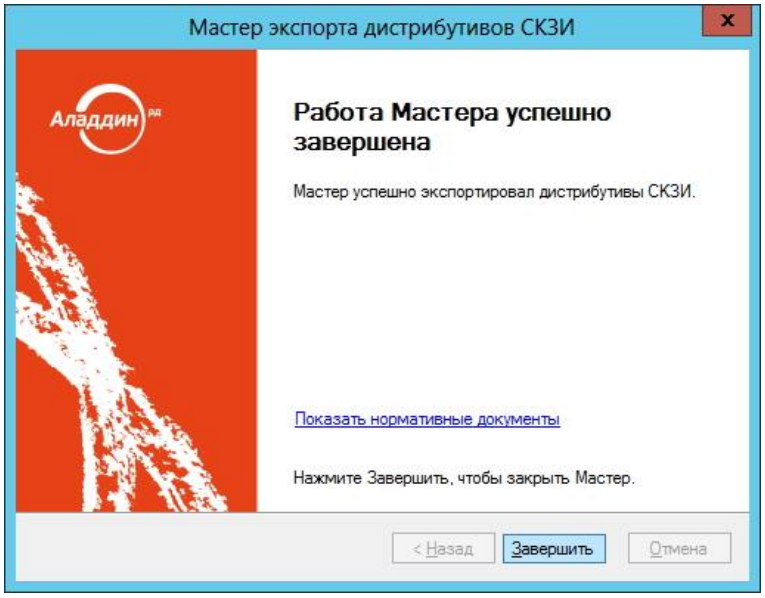


Рис. 321 – Окно завершения экспорта дистрибутива СКЗИ

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. 342).

3.11.5.5 Назначение дистрибутиву экземпляра СКЗИ

Для того чтобы назначить дистрибутиву экземпляр СКЗИ, выполните следующие действия:

1. Выберите Дистрибутивов СКЗИ из списка и на верхней панели консоли управления JMS нажмите **Назначить экземпляр СКЗИ** (см. рис. 322).

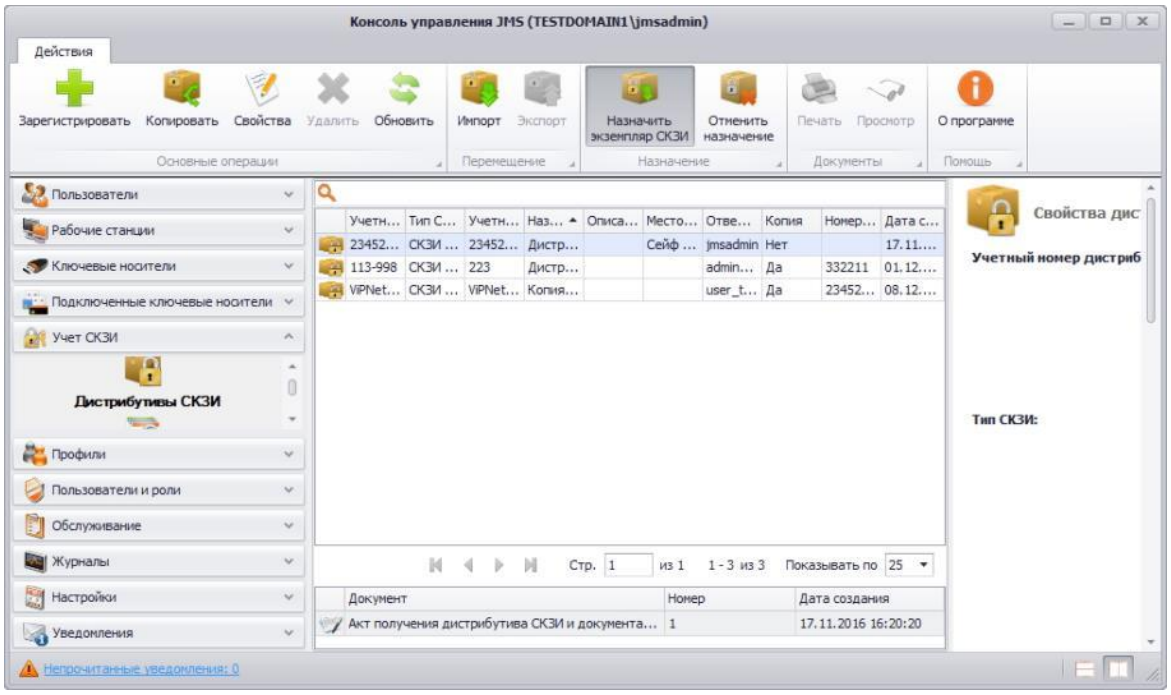


Рис. 322 – Окно назначения дистрибутиву СКЗИ экземпляра СКЗИ

2. В появившемся окне (см. рис. 323) выделите в списке зарегистрированных экземпляров СКЗИ требуемый экземпляр и нажмите **Выбрать**.

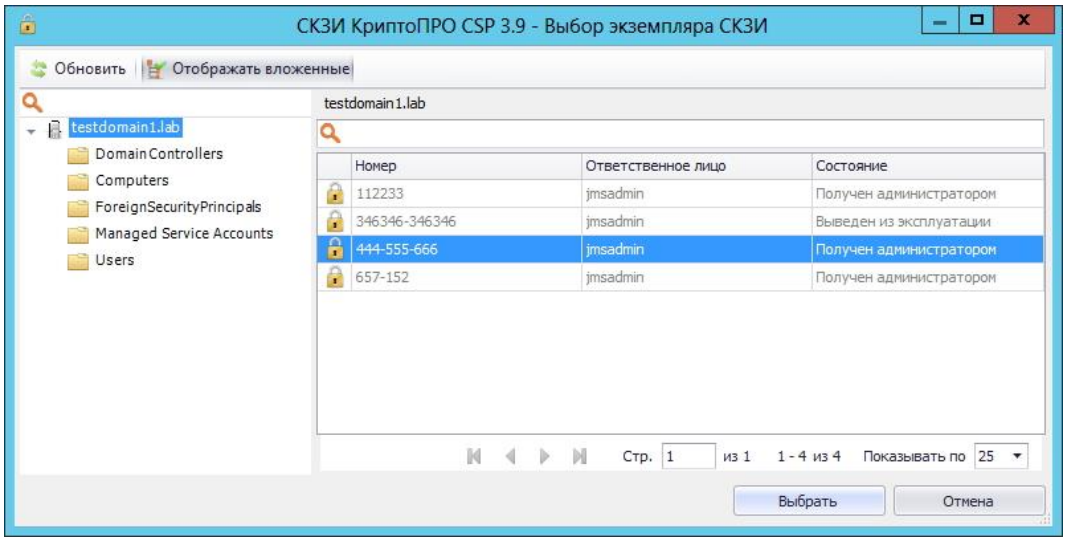


Рис. 323 – Окно выбора экземпляра СКЗИ

Для того чтобы отменить назначение, выберите дистрибутив из списка и нажмите **Отменить назначение** (см. рис. 324). После чего в появившемся окне подтвердите свой выбор, нажав **Да**.

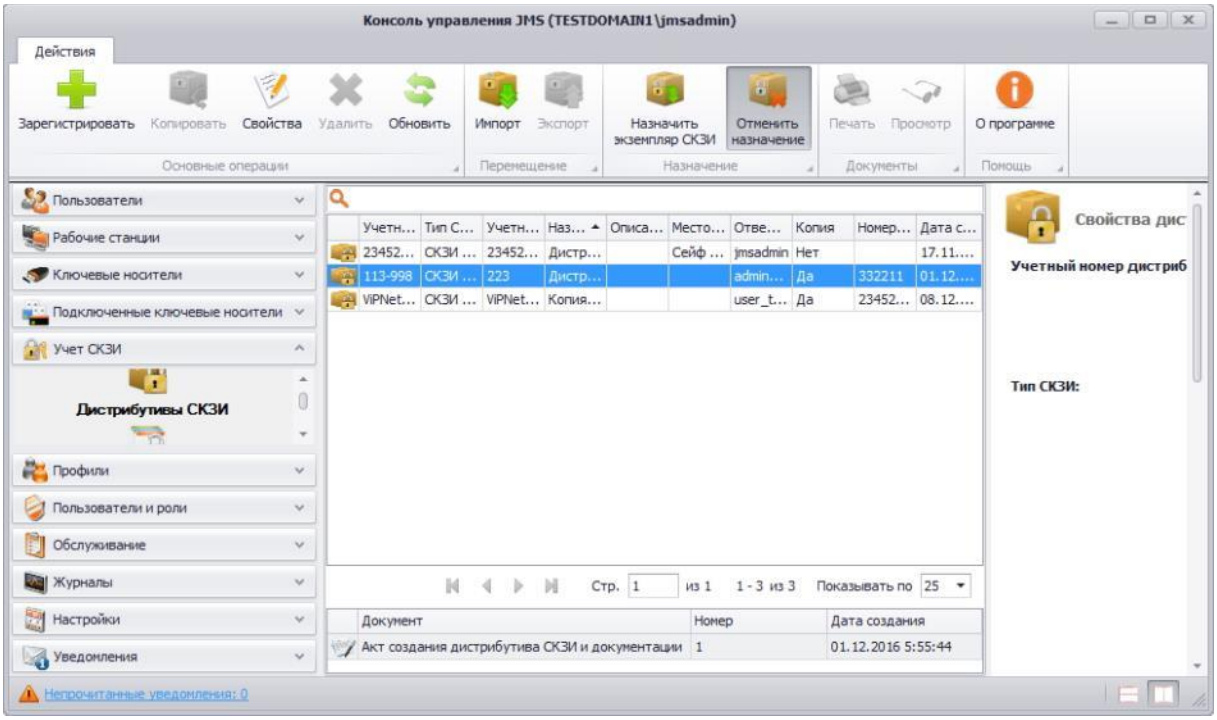


Рис. 324 – Окно отмены назначения дистрибутиву экземпляра СКЗИ

3.11.6 Лицензии СКЗИ

Действия, выполнение которых возможно в разделе **Учет СКЗИ** -> **Лицензии СКЗИ** перечислены в таблице 63.

При просмотре списка зарегистрированных лицензий СКЗИ отображаются свойства, описание которых представлено в таблице 70.

Табл. 70

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

Наименование свойства	Описание
Дата окончания действия	Дата окончания действия лицензии

3.11.6.1 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** и нажмите **Зарегистрировать** (см. рис. 325).

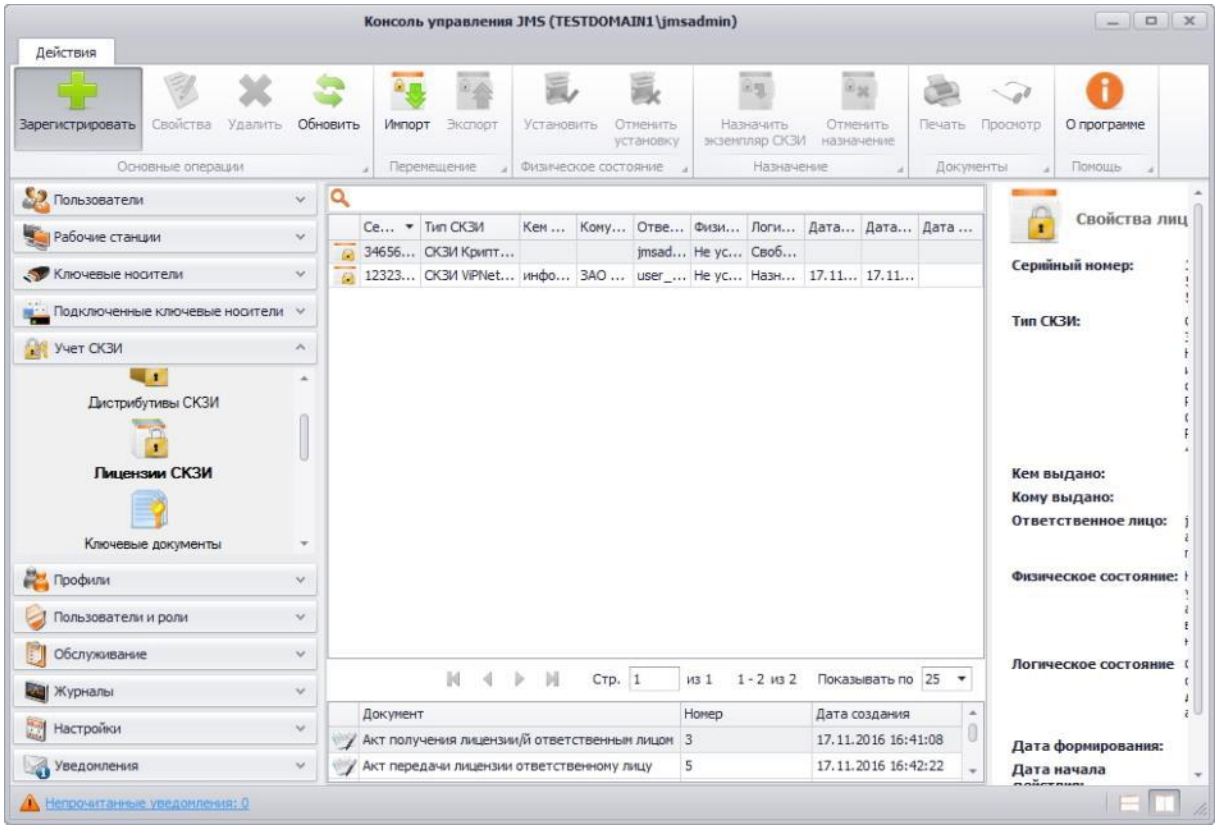


Рис. 325 – Окно регистрации лицензии СКЗИ

2. В появившемся окне (см. рис. 326) введите **Серийный номер*** лицензии СКЗИ, из раскрывающегося списка выберите **Тип СКЗИ**, заполните поля **Кем выдано** и **Кому выдано**. При необходимости введите **Ответственное лицо***, **Дату формирования**, **Дату начала действия** и **Дату окончания действия**. Нажмите **Создать**.

Примечание. Атрибуты, помеченные знаком * обязательны для заполнения, остальные атрибуты можно не указывать.

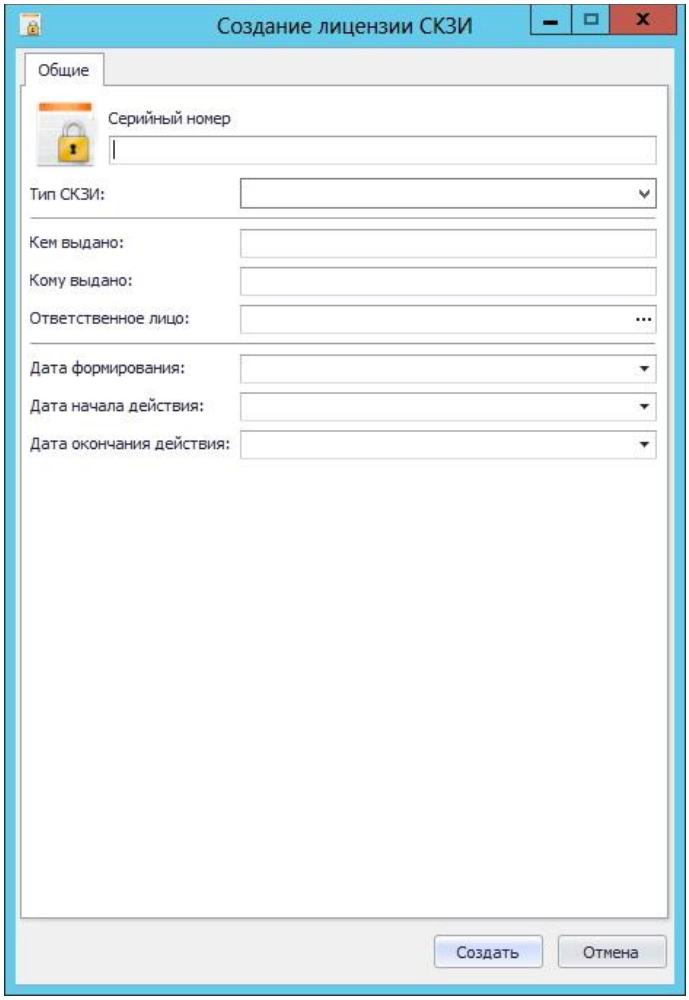


Рис. 326 – Окно создания лицензии СКЗИ

3. Отобразится следующее окно (см. рис. 327). При необходимости просмотреть сформированный нормативный документ нажмите **Да**, в противном случае – нажмите **Нет.**

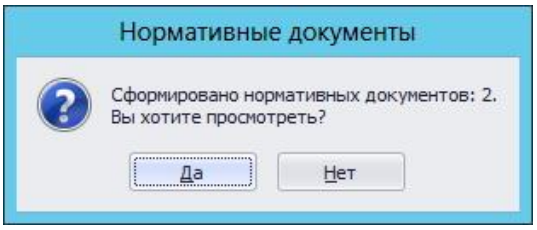


Рис. 327 – Окно сообщения о формировании нормативных документов

4. В случае нажатия **Да** – в появившемся окне (см. рис. 328) отобразятся названия сформированных документов, которые при необходимости можно просмотреть или распечатать. Нажмите **Закрыть**.

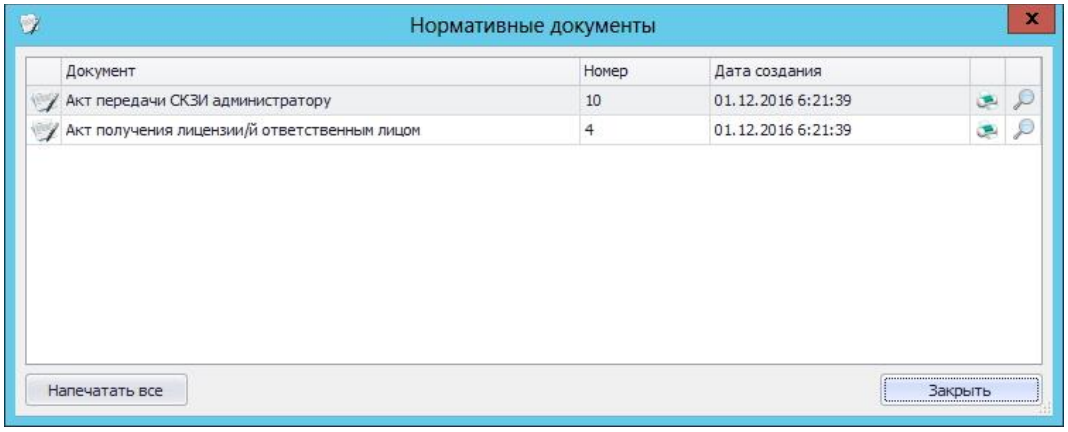


Рис. 328 – Окно нормативных документов

Зарегистрированная лицензия СКЗИ отобразится в окне консоли управления JMS в разделе **Учет СКЗИ** -> **Лицензии СКЗИ**.

3.11.6.2 Импорт лицензий (пакетная регистрация)

Для того чтобы выполнить пакетную регистрацию лицензий, выполните следующие действия:

1. На верхней панели консоли управления JMS нажмите **Импорт** (см. рис. 329).

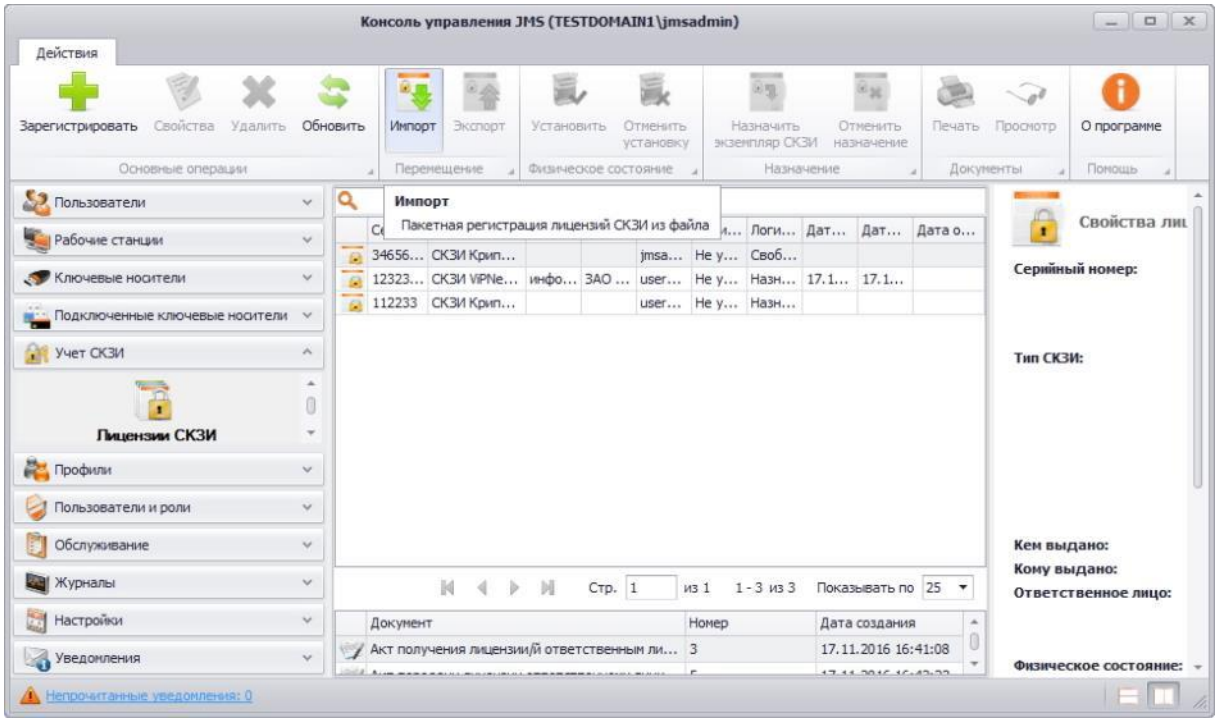


Рис. 329 – Окно импорта лицензии

2. В появившемся окне мастера импорта лицензий (см. рис. 330) нажмите **Далее**.

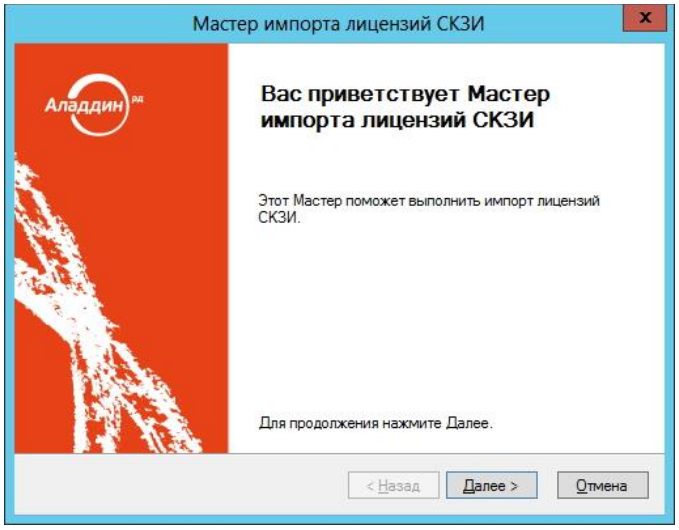


Рис. 330 – Окно приветствия мастера импорта лицензий

3. В появившемся окне (см. рис. 331) выберите **Тип СКЗИ**, **Ответственное лицо** и **Файл импорта**, после чего нажмите **Далее**.

Примечание. Файл импорта лицензий СКЗИ представляет собой файл в формате *.CSV. Подробнее о структуре файла см. Формат файлов импорта лицензий СКЗИ.

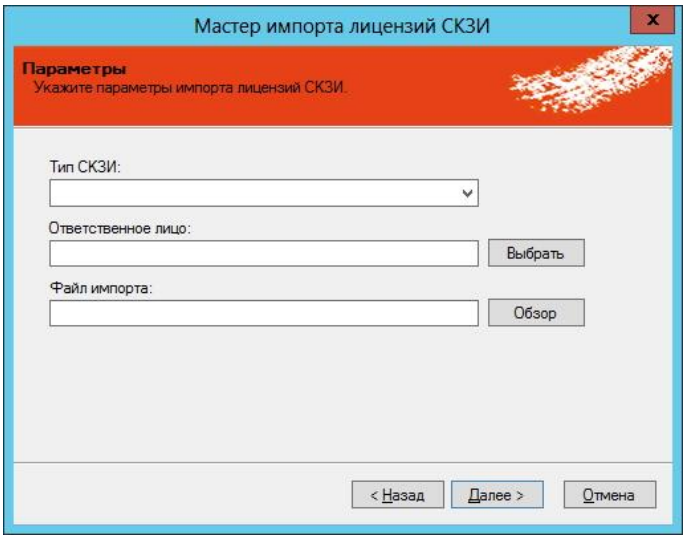


Рис. 331 – Окно ввода параметров импорта лицензий

4. В появившемся окне (см. рис. 332) нажмите **Далее**.

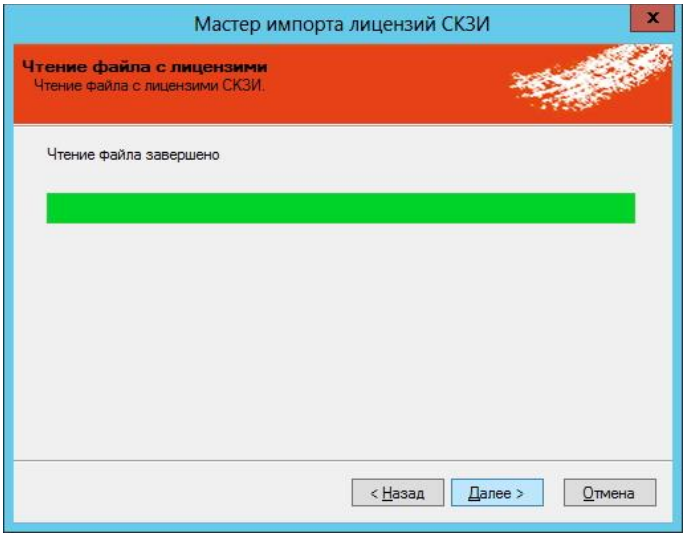


Рис. 332 – Окно чтения файла с лицензиями

5. В появившемся окне (см. рис. 333) нажмите **Далее**.

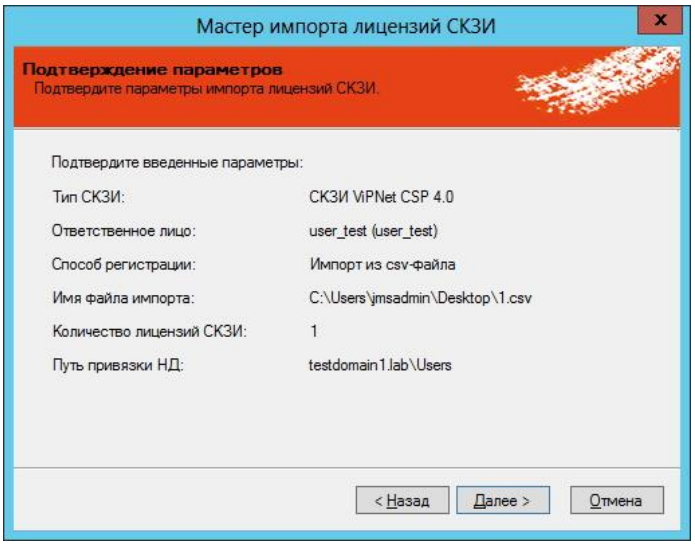


Рис. 333 – Окно подтверждения параметров импорта лицензий

6. В появившемся окне (см. рис. 334) нажмите **Далее**.

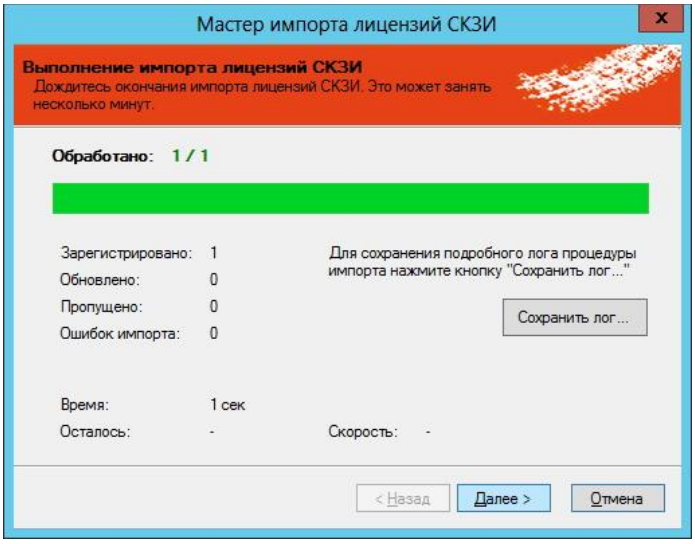


Рис. 334 – Окно выполнения импорта лицензий

7. В появившемся окне (см. рис. 335) нажмите **Завершить**.

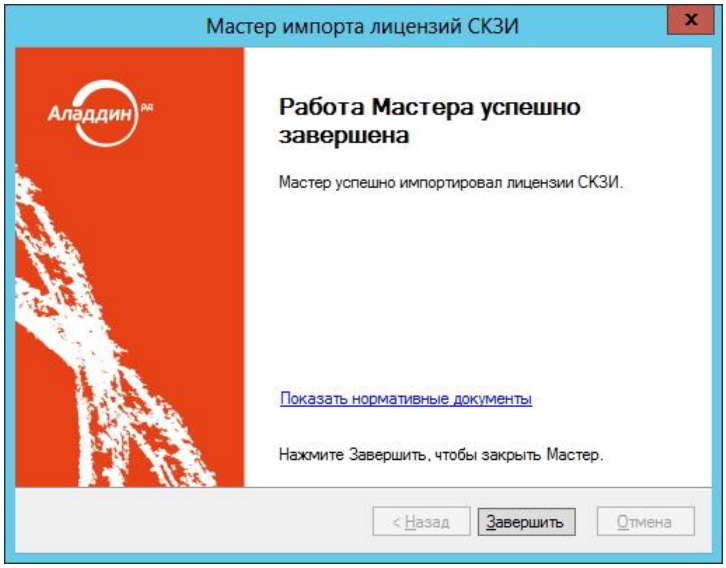


Рис. 335 – Окно завершения импорта лицензий

3.11.6.2.1 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}**».

Дальнейшие строки файла содержат значения полей из заголовка для лицензии СКЗИ. Порядок следования значений должен соответствовать порядку объявленных полей 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 дистрибутива СКЗИ приведен в таблице 71.

Табл. 71

№	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:

SerialNumberIssuedNameGrantedNameIssuedDateValidFromValidTo

1issued_name1granted_name116.12.201616.12.201616.01.2017

2issued_name2granted_name216.12.201616.12.201616.01.2017

3issued_name3granted_name316.12.201616.12.201616.01.2017

3.11.6.3 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 лицензий, выполните следующие действия:

1. Выделите в таблице лицензий СКЗИ те лицензии, которые подлежат экспорту из данного сервера JMS, и на верхней панели консоли управления JMS нажмите **Экспорт** (см. рис. 336).

Примечание. Выбираемые лицензии должны относиться к одному и тому же типу СКЗИ. Для удобства можно отсортировать записи в таблице по типу СКЗИ нажав **Тип СКЗИ** в заголовке таблице

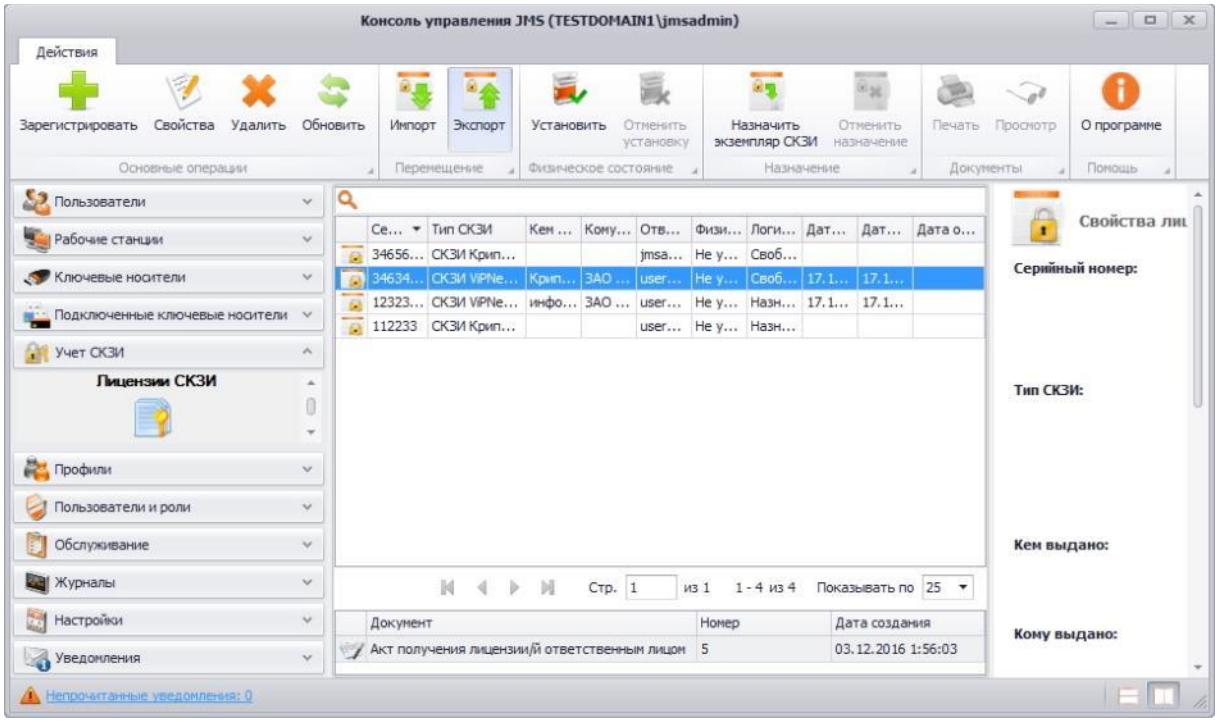


Рис. 336 – Окно экспорта лицензий СКЗИ

2. В появившемся окне приветствия мастера экспорта лицензий СКЗИ (см. рис. 337) нажмите **Далее**.

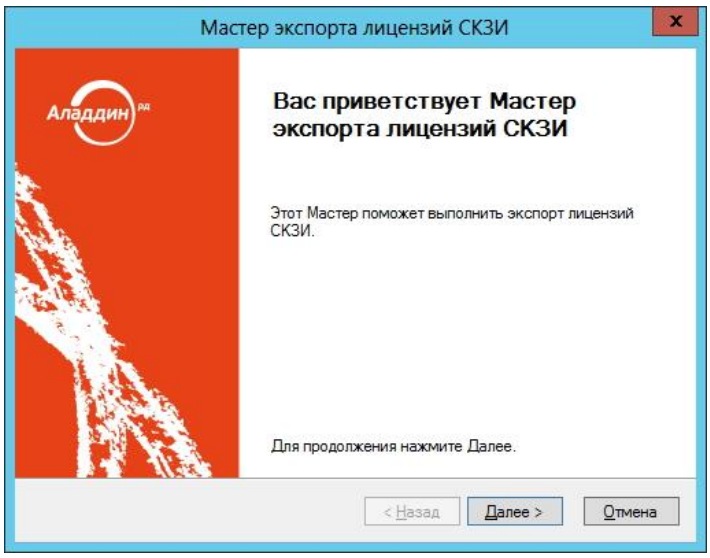


Рис. 337 – Окно приветствия мастера экспорта лицензий

3. В появившемся окне (см. рис. 338) выберите ответственное лицо и файл экспорта, после чего нажмите **Далее**.

Примечание. Файл экспорта формируется в формате *.CSV. Структура файлов экспорта аналогична структуре файлов импорта. Подробнее о структуре файла см. в разделе«Формат файлов импорта лицензий СКЗИ». При экспорте лицензии удаляются из БД и могут быть повторно импортированы из файла экспорта.

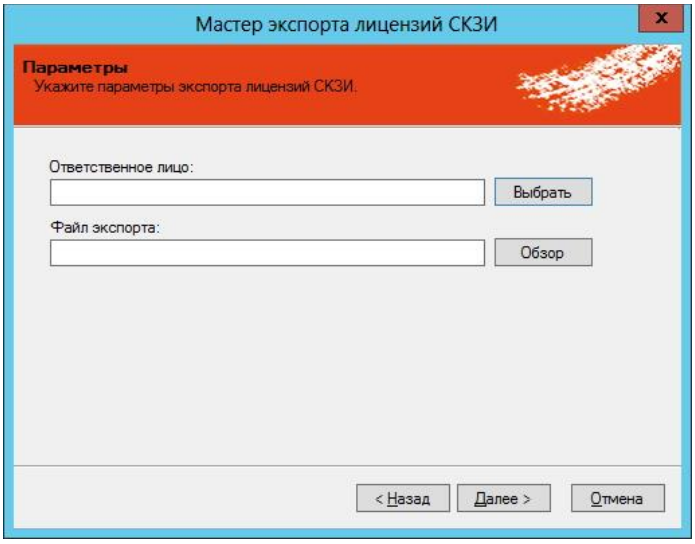


Рис. 338 – Окно ввода параметров экспорта лицензий

4. В появившемся окне (см. рис. 339) нажмите **Далее**.

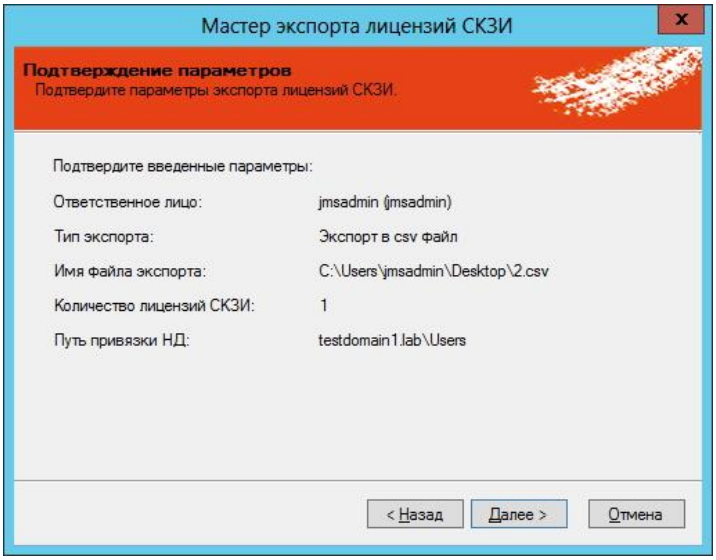


Рис. 339 – Окно подтверждения параметров экспорта лицензий

5. В появившемся окне (см. рис. 340) нажмите **Далее**.

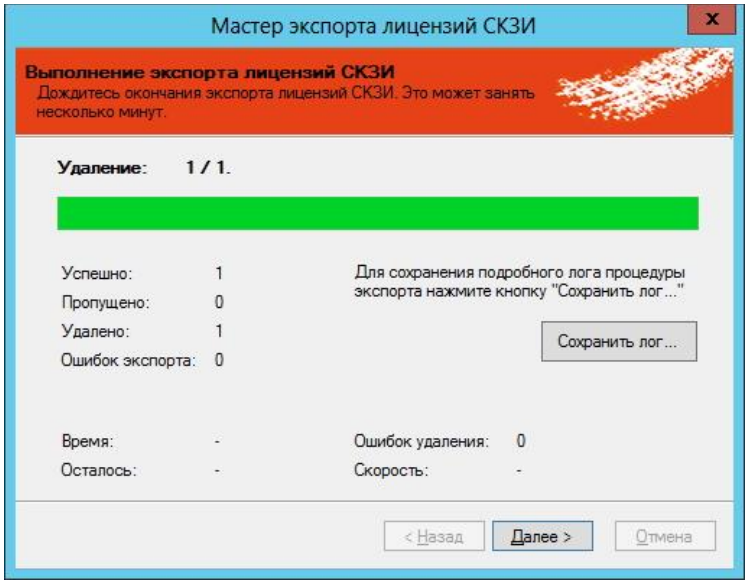


Рис. 340 – Окно выполнения экспорта лицензий

6. В появившемся окне (см. рис. 341) нажмите **Завершить**.

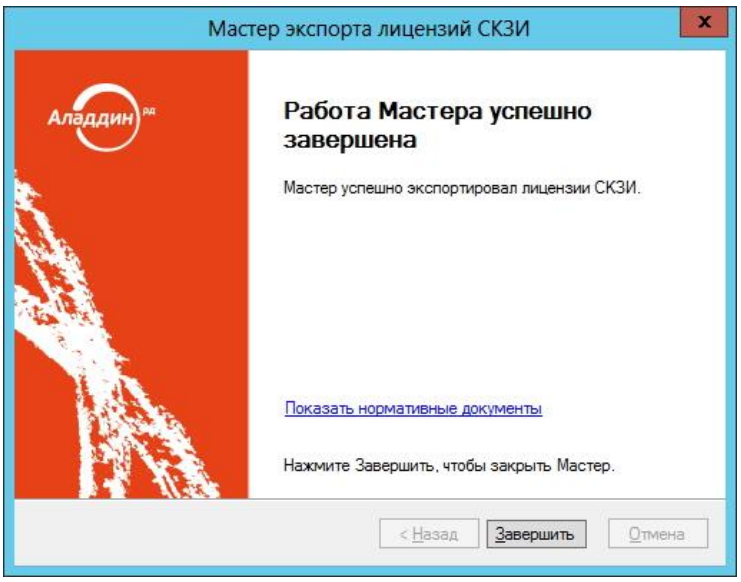


Рис. 341 – Окно завершения экспорта лицензий

По окончании экспорта информация об экспортированных лицензиях будет удалена с данного экземпляра сервера JMS. Полученный файл может быть использован для последующего импорта на другом экземпляре сервера JMS (см. раздел «Импорт дистрибутивов (пакетная регистрация)», с. 342).

3.11.6.4 Установка лицензии

Для того чтобы установить лицензию, выполните следующие действия:

1. Выделите в списке зарегистрированных Лицензий СКЗИ требуемый экземпляр и на верхней панели консоли управления JMS нажмите **Установить** (см. рис. 342).

Примечание. Для установки лицензии необходимо, чтобы значение свойства **Физическое состояние** требуемого экземпляра лицензии было «**Не установлена»**, в противном случае – установка невозможна.

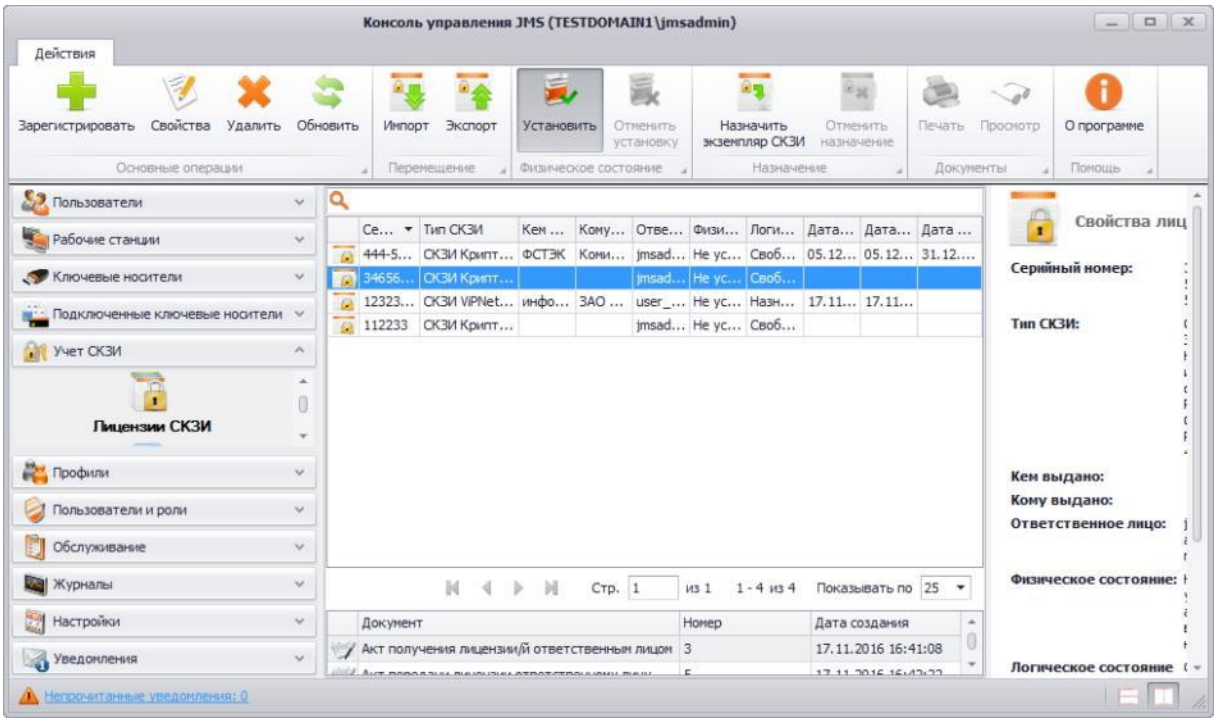


Рис. 342 – Окно установки лицензии

2. В появившемся окне (см. рис. 343) подтвердите свои действия, нажав **Да**.

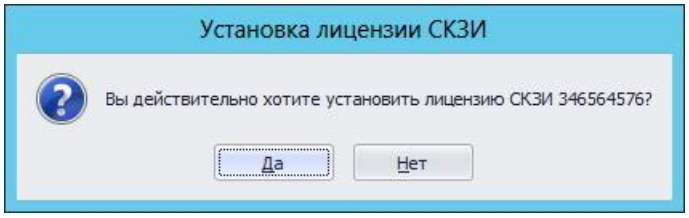


Рис. 343 – Окно подтверждения установки лицензии

Для того чтобы отменить установку лицензии, нажмите **Отменить установку** (см. рис. 344).

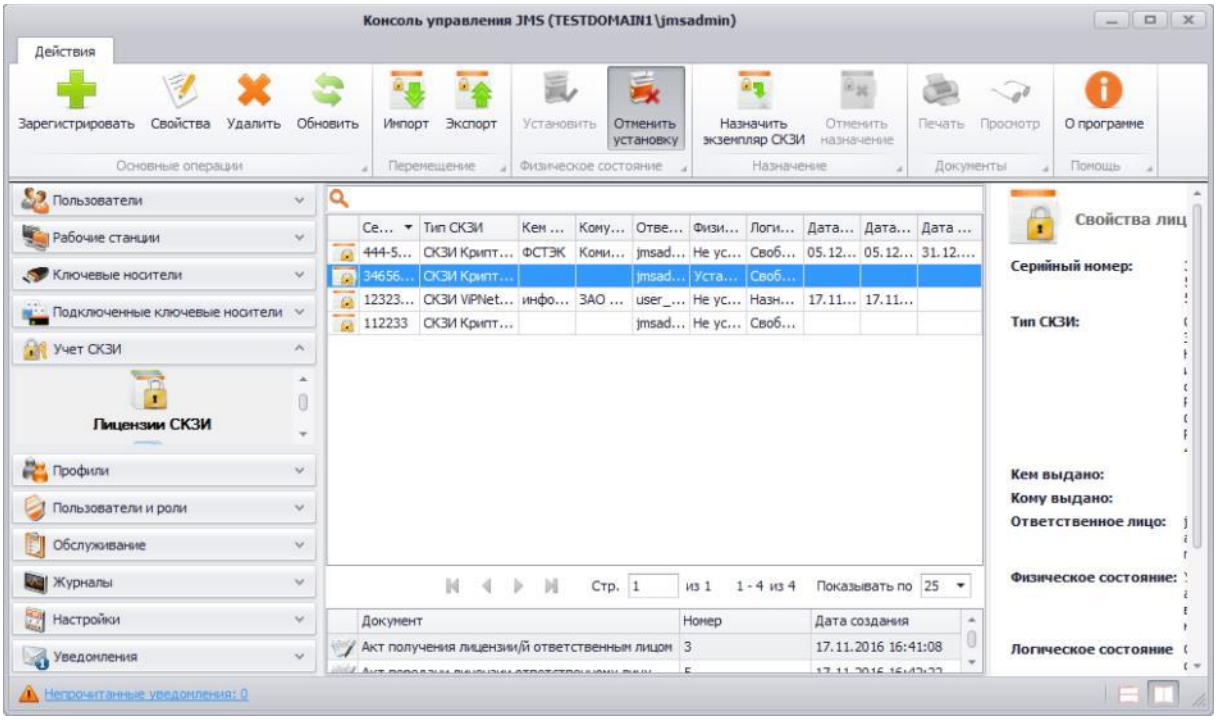


Рис. 344 – Окно отмены установки лицензии

3.11.6.5 Назначение лицензии экземпляра СКЗИ

Для того чтобы назначить лицензии экземпляр СКЗИ, выполните следующие действия:

1. Выберите в списке лицензию и на верхней панели консоли управления JMS нажмите **Назначить экземпляр СКЗИ** (см. рис. 345).

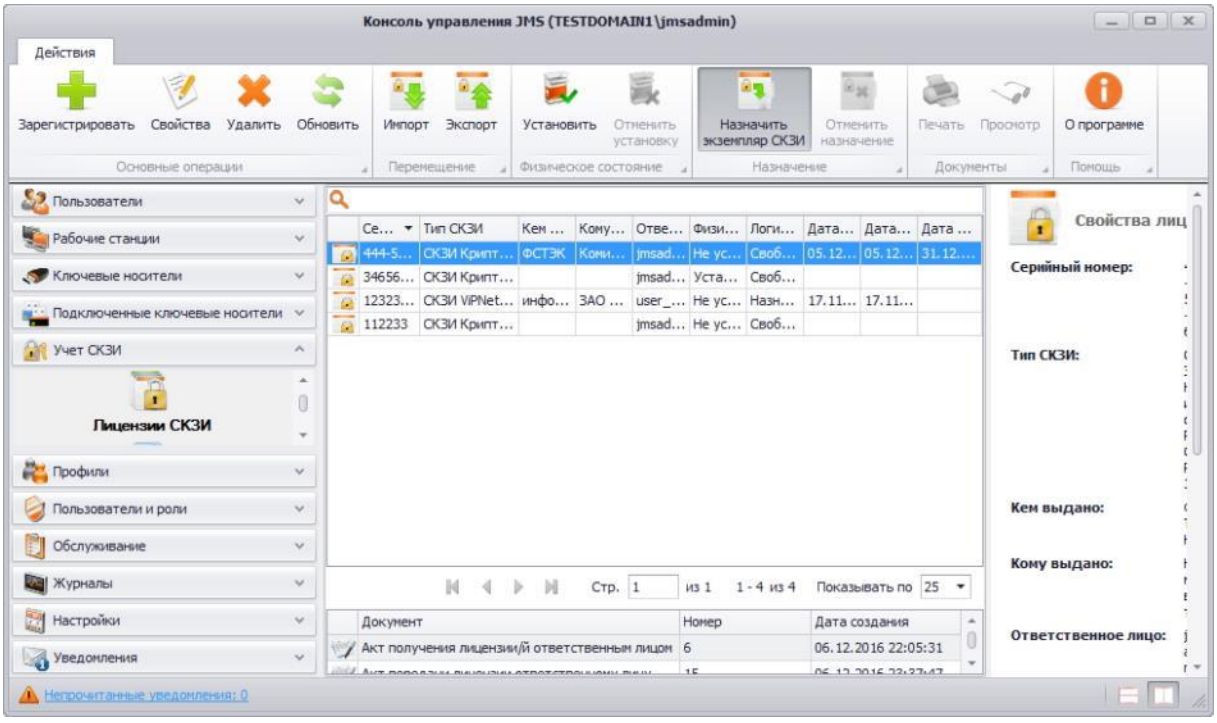


Рис. 345 – Окно назначения лицензии экземпляру СКЗИ

2. В появившемся окне (см. рис. 346) выберите экземпляр СКЗИ и нажмите **Выбрать**.

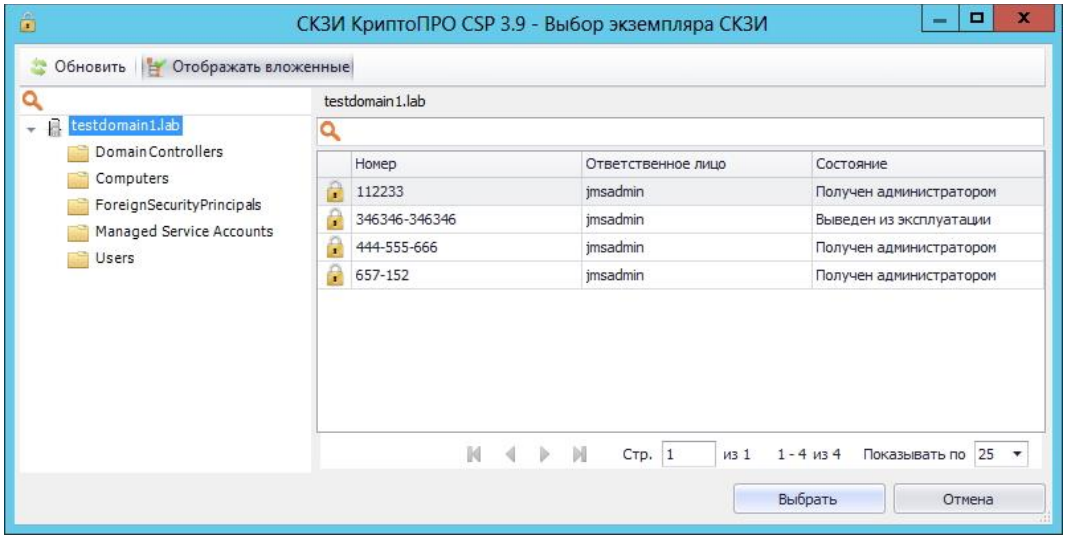


Рис. 346 – Окно выбора экземпляра СКЗИ

Чтобы отменить назначение выберите в списке лицензию и нажмите **Отменить назначение** (см. рис. 347).

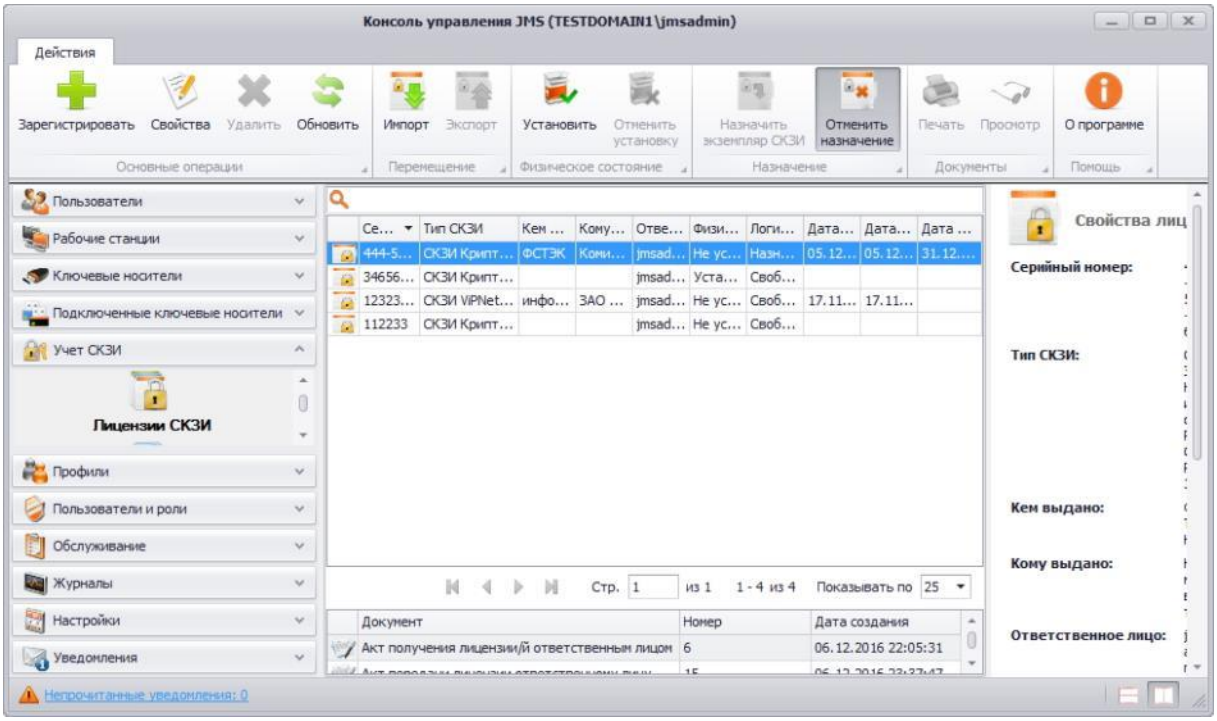


Рис. 347 – Окно отмены назначения лицензии экземпляру СКЗИ

3.11.6.6 Удаление лицензии

Для того чтобы удалить лицензию из списка зарегистрированных лицензий СКЗИ, выберите в списке лицензию и нажмите **Удалить** (см. рис. 348).

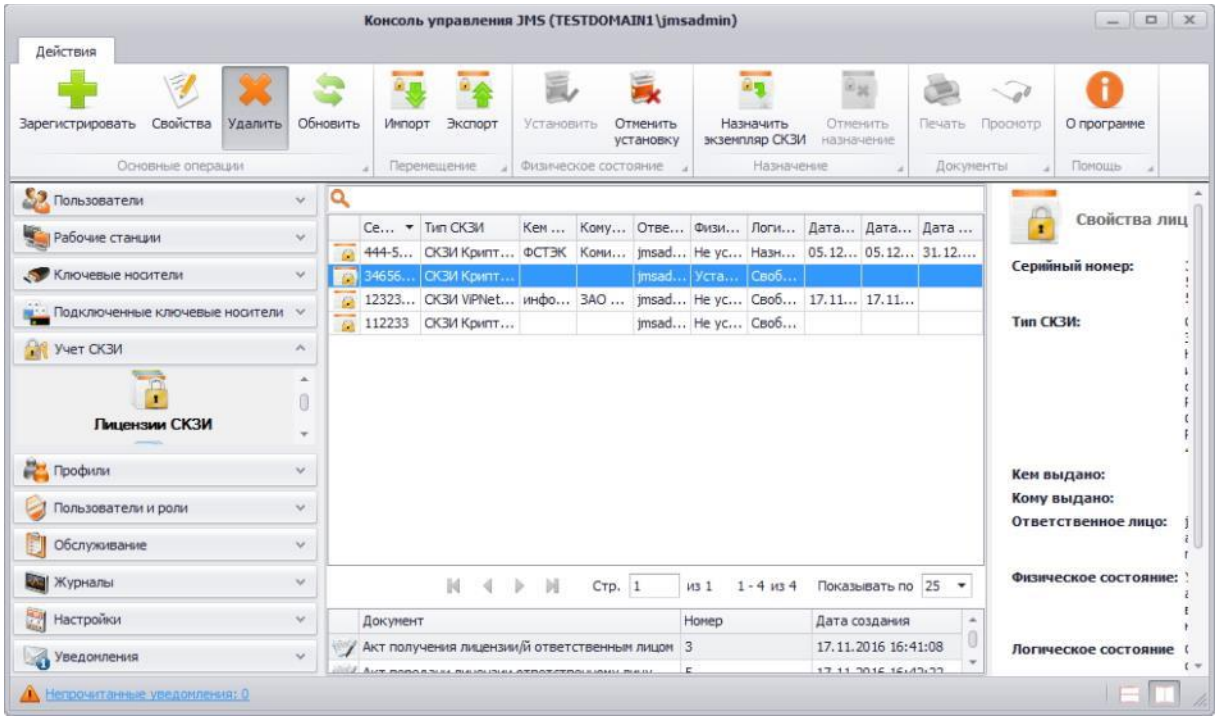


Рис. 348 – Окно удаления лицензии

3.11.7 Ключевые документы

Ключевой документ – это объект JMS, соответствующий сертификату, создаваемому при выпуске электронного ключа следующими удостоверяющими центрами:

- КриптоПро УЦ 1.5;
- КриптоПро УЦ 2.0;
- ViPNet УЦ

и записываемый на выпущенный электронный ключ.

Действия, выполнение которых возможно в разделе **Учет СКЗИ** -> **Ключевые документы**, перечислены в таблице 63.

При просмотре списка ключевых документов отображаются свойства, описание которых представлено в таблице 72.

Табл. 72

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)

Наименование свойства	Описание
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** (см. рис. 349).

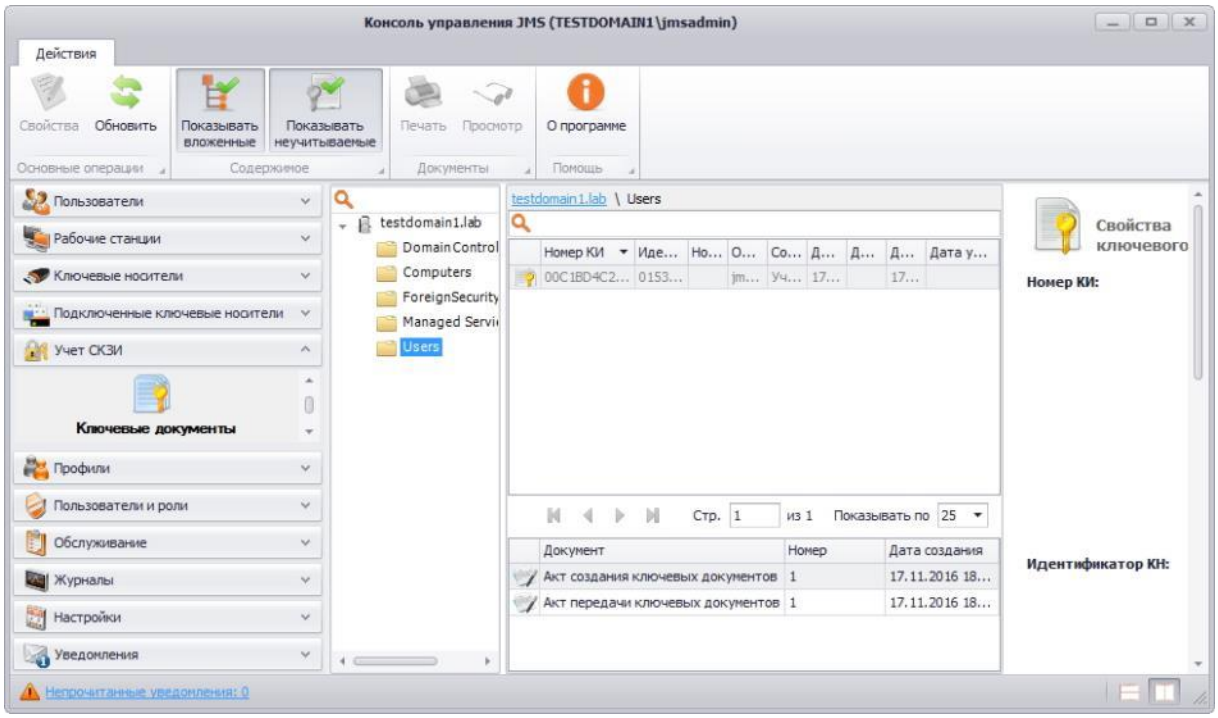


Рис. 349 – Окно в разделе Учет СКЗИ – Ключевые документы

При просмотре списка ключевых документов в верхней панели консоли управления JMS доступны дополнительные опции просмотра. Описание дополнительных опций просмотра представлено в таблице 73.

Табл. 73

Наименование опции	Описание
Содержимое -> **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
Содержимое -> **Показывать неучитываемые**	При выборе этой опции в списке ключевых документов отображаются те документы, учет которых был прекращен

3.11.8 Нормативная документация

Действия, выполнение которых возможно в разделе **Учет СКЗИ** -> **Нормативная документация** перечислены в таблице 63.

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** (поле **Текущий номер**). 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*. Данный шаблон задается в поле **Шаблон номера документа** в разделе **Учет СКЗИ** –> **Типы нормативных документов**.

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 74.

Табл. 74

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
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** (см. рис. 350).

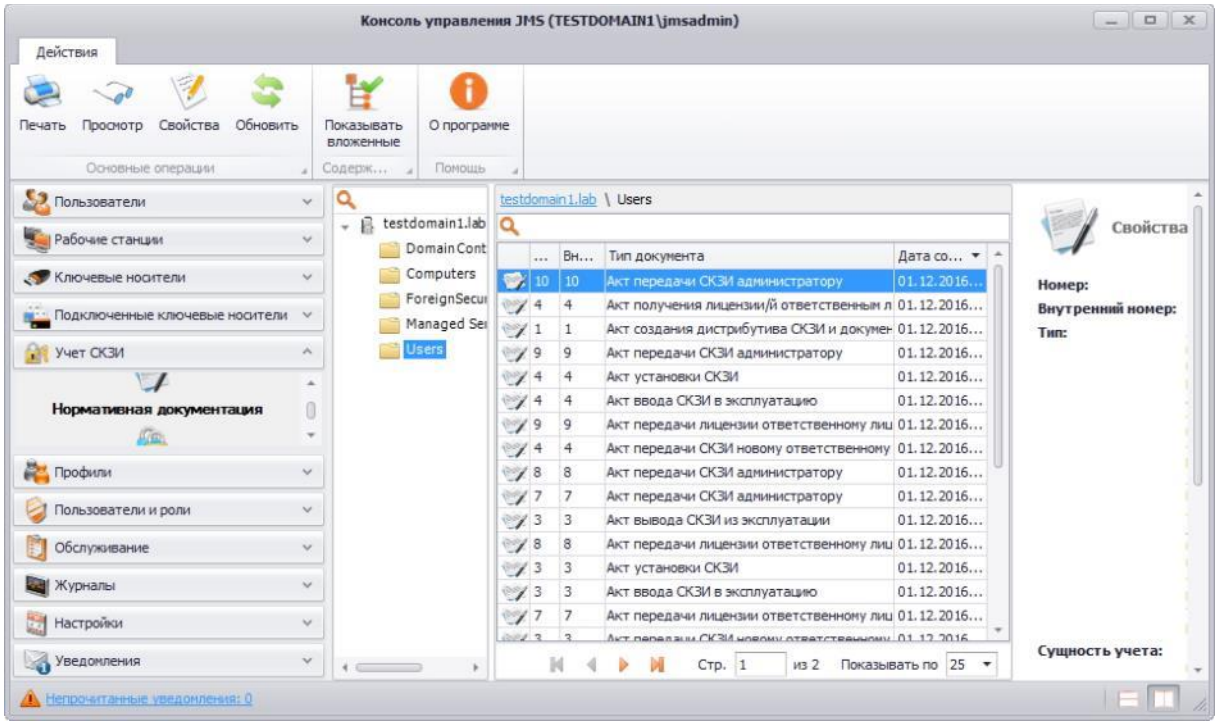


Рис. 350 – Окно в разделе Учет СКЗИ – Нормативная документация

Примечание. При просмотре списка нормативных документов в верхней панели консоли управления JMS доступна дополнительная опция просмотра: **Содержимое** –> **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.

3.11.9 Журнал событий (учета СКЗИ)

JMS позволяет просматривать все события, произошедшие в процессе жизненного цикла СКЗИ.

При просмотре списка событий отображаются свойства, описание которых представлено в таблице 75.

Табл. 75

Наименование свойства	Описание
Дата	Дата и время возникновения события
Событие	Описание произошедшего события
Пользователь	Имя пользователя, учетная запись которого использовалась при совершении события

Для того чтобы просмотреть список событий, произошедших в процессе учета СКЗИ, перейдите в раздел **Учет СКЗИ** -> **Журнал событий** (см. рис. 351).

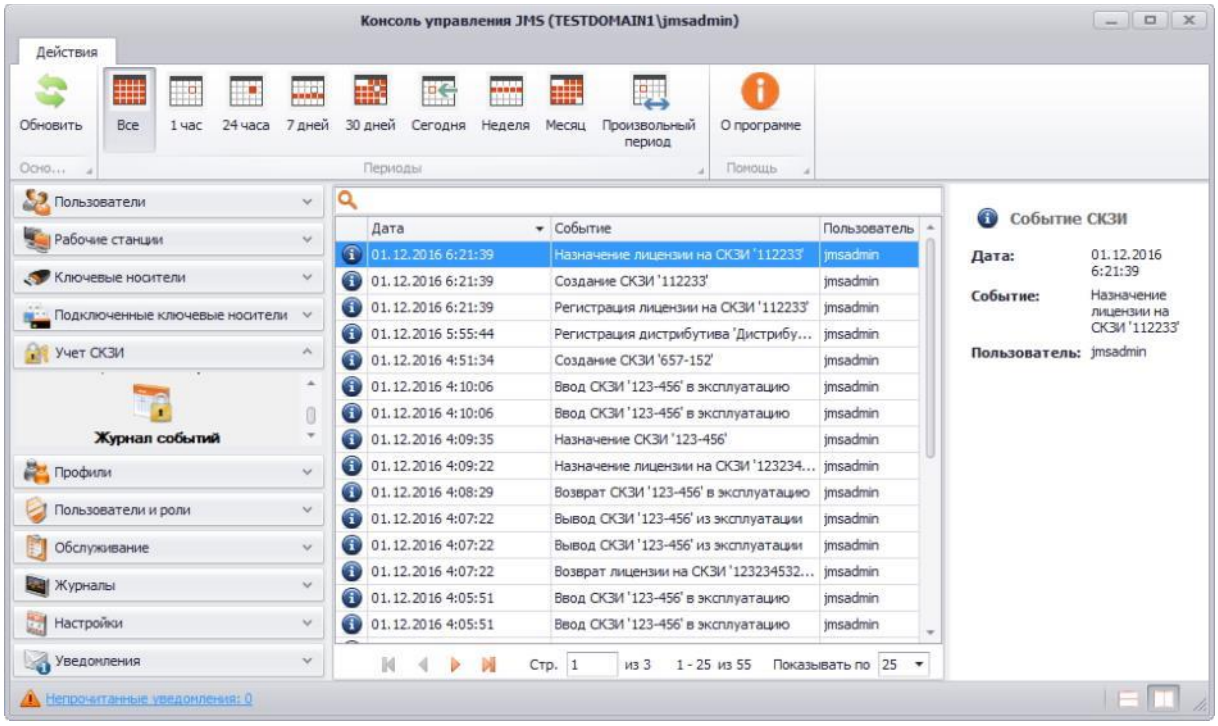


Рис. 351 – Окно журнала событий, связанных с учетом СКЗИ

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 этого, имеется возможность поиска по столбцу **Пользователь**.

3.12 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.

3.12.1 Создание шаблона печати

Для создания шаблона печати выполните следующие действия:

1. Перейдите в раздел **Настройки** -> **Шаблоны печати** и нажмите **Создать** (см. рис. 352).

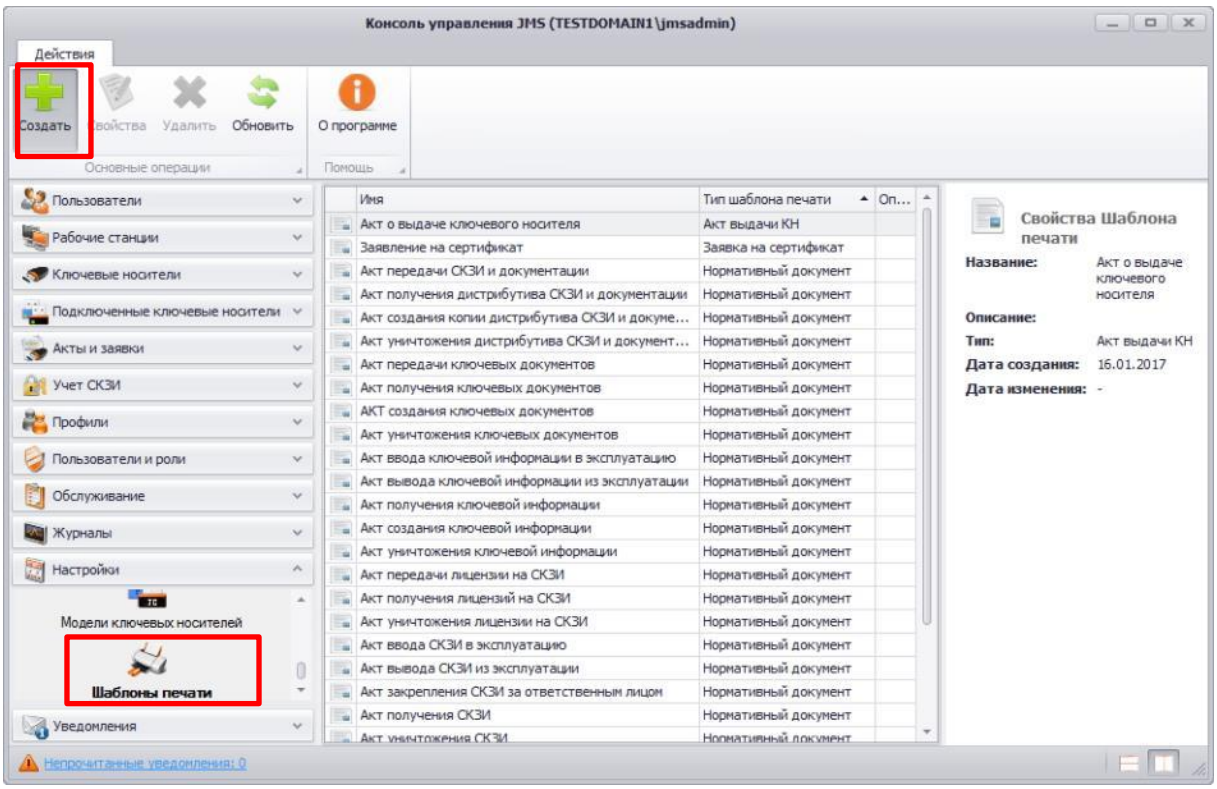


Рис. 352 – Создание шаблона печати

2. В появившемся окне (см. рис. 353) на вкладке **Общие** введите **Имя шаблона** и при необходимости заполните поле **Описание** и перейдите на вкладку **Настройки** (см. рис. 354).

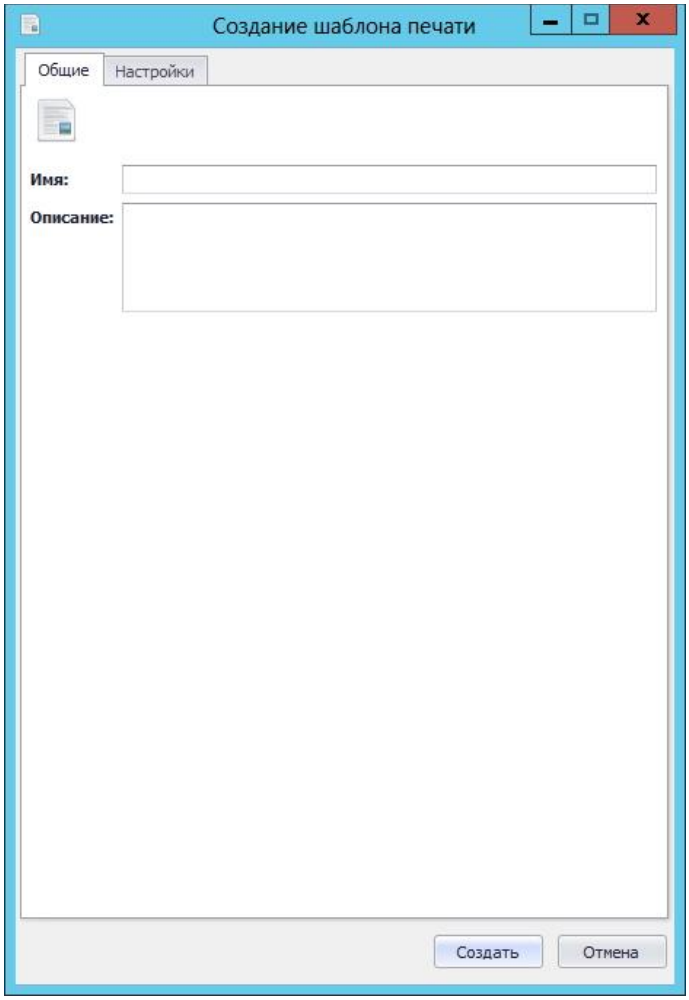


Рис. 353 – Окно создание шаблона печати

3. В окне на вкладке **Настройки** (см. рис. 354) выберите тип шаблона и нажмите **Импорт.** Описание типов шаблонов, появляющихся в раскрывающемся списке представлено в табл. 76.

Табл. 76 – Описание типов шаблонов

Тип шаблона	Описание
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.
Акт выдачи КН	Содержит ФИО, логин, адрес электронной почты и др. персональные данные, а так же лицо, выдавшее и лицо, получившее КН.
Заявка на сертификат	Содержит текст заявления с просьбой об изготовлении сертификата ключа проверки электронной подписи, а так же указанием необходимых для этого персональных данных.
Сертификат	Содержит данные пользователя (ФИО, аккаунт, адрес электронной почты и др.) и данные сертификата (номер версии, серийный номер, даты срока действия и др.).

Тип шаблона	Описание
Нормативный документ	Содержит сведения, отражающие различные события, возникающие в процессе учета СКЗИ. Данный тип шаблона используется только в рамках учета СКЗИ.

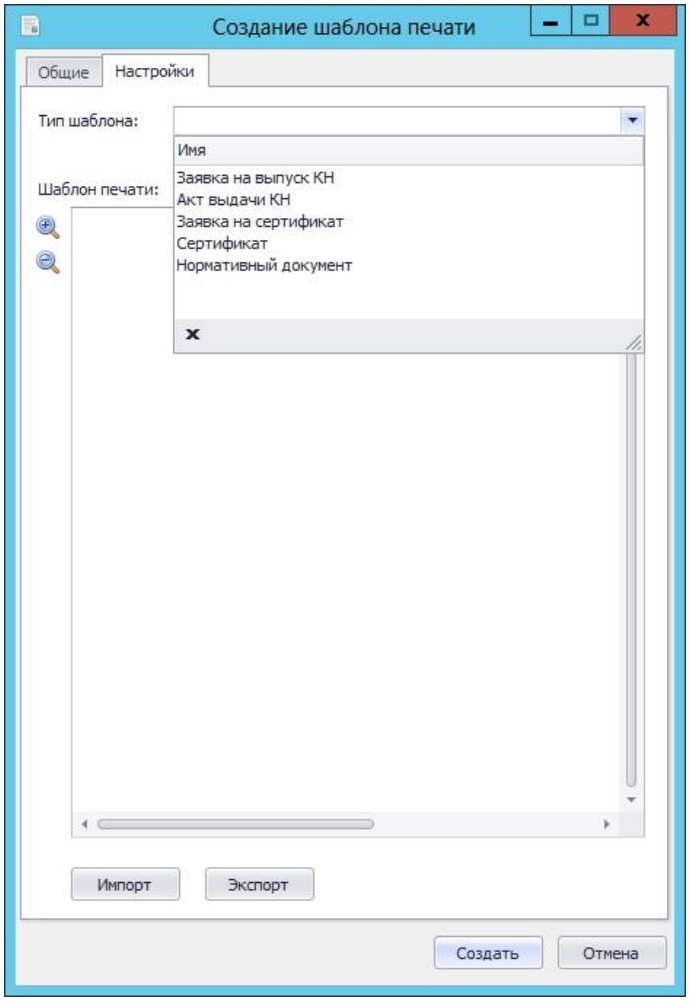


Рис. 354 – Вкладка Настройки в окне создания шаблона печати

4. Укажите место расположения файла шаблона (файла в формате .rtf) и нажмите **Открыть**.

Подробнее о создании файла шаблона в формате .rtf см. Создание файлов шаблонов в формате RTF.

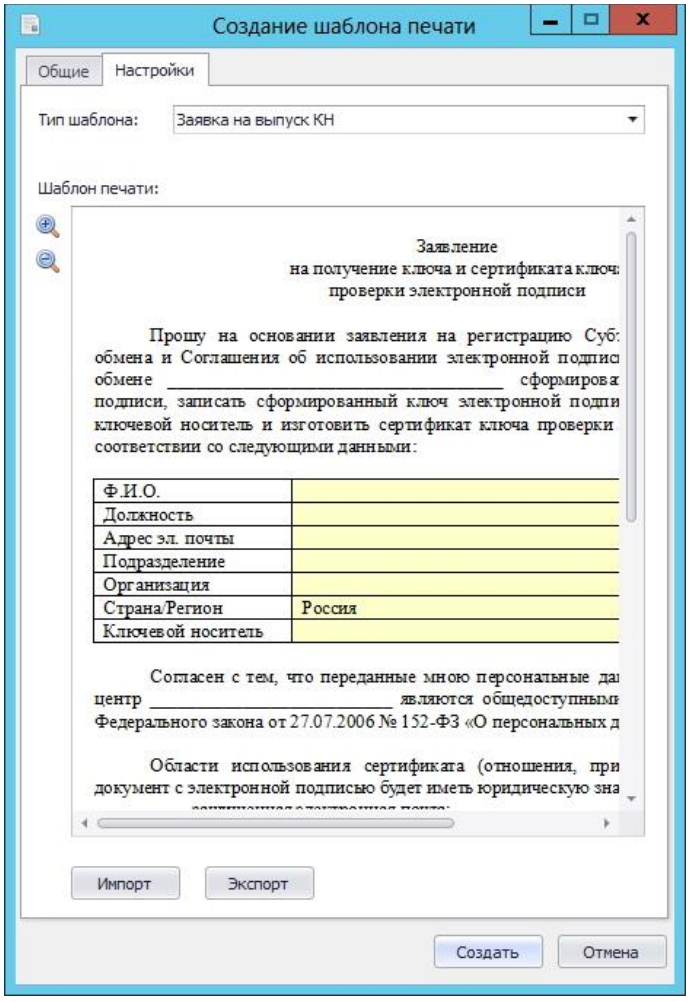


Рис. 355 – Окно создания шаблона печати после импорта шаблона печати

В появившемся окне (см. рис. 355) отобразится загруженный файл шаблона, содержимое которого можно просмотреть, используя полосу прокрутки и кнопки изменения масштаба "+" и "-".

5. Нажмите **Создать**. Созданный шаблон печати отобразится в списке шаблонов печати консоли управления JMS.

3.12.2 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.

В настоящем документе для примера используется Microsoft Word 2010.

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. 356);

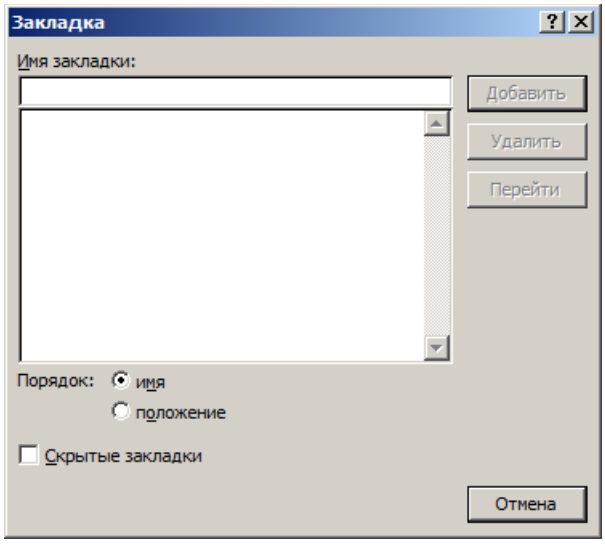


Рис. 356 – Добавление закладки в документ Microsoft Word

2.4. в поле **Имя закладки** введите имя, соответствующее названию поля в базе данных JMS (см. например, Табл. 77, below).

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 настройках подсистемы печати, в разделе реестра: **`HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Server\JaCarta Management System\default\PrintingManager`**

с помощью параметра **`MaxBookmarkIndex`** (тип REG_DWORD). Значение данного параметра по умолчанию – 100.

3.12.2.1 Создание шаблонов документов для выпуска КН и сертификата

Перечень доступных закладок, используемых в документах выпуска КН и сертификатов, представлен в табл. 77.

Табл. 77 – 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	+	+	+	+

Закладка/поле	Описание	Типы шаблона:			
		Заявка на выпуск КН	Акт выдачи КН	Заявка на сертификат	Сертификат
Department	Подразделение	+	+	+	+
Title	Должность	+	+	+	+
IssueDate	Дата выпуска (при печати подставляется текущая дата)	+	+	+	+
GlobalId	Идентификатор ключевого носителя	+	+	+	+
TokenSerialNumber	Серийный номер электронного ключа	+	+	+	+
PublicKey	Значение открытого ключа в сертификате			+	
IssuerName	Сертификат: издатель				+
SerialNumber	Сертификат: серийный номер				+
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	+	+	+	+

Закладка/поле	Описание	Типы шаблона:			
		Заявка на выпуск КН	Акт выдачи КН	Заявка на сертификат	Сертификат
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				+
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				+

Закладка/поле	Описание	Типы шаблона:			
		Заявка на выпуск КН	Акт выдачи КН	Заявка на сертификат	Сертификат
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				+

3.12.2.1.1 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 внести в реестр.

Для создания такого перечня следует создать (если отсутствует) раздел реестра:

`HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Server\JaCarta Management System\default\PrintingManager`

в котором необходимо создать (если отсутствует) мультистроковый параметр **`CertificateDnMappings`**.

В параметре **`CertificateDnMappings`** каждое соответствие задается отдельной строкой следующего формата:

<OID компонента>=<Обозначение компонента >

Например:

```
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
```

По умолчанию (при отсутствии параметра **CertificateDnMappings** в реестре) используются соответствия, указанные в Табл. 78.

Табл. 78 – 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
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 реестре параметра **CertificateDnMappings** все планируемые к использованию OID-идентификаторы «по умолчанию» необходимо указать в нем явно (в перечне соответствий) в соответствии с Табл. 78.

3.12.2.2 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. 79.

Табл. 79 – 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**	**+**	**+**	**+**	**+**	**+**	**+**
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**		+	+	+	+	+

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
DestroyDate	**Дата уничтожения**						+
StateMask	**Состояние**	+	+	+	+	+	+
Description	**Описание СКЗИ**	+	+	+	+	+	+
CryptoDeviceType	**Тип СКЗИ**	+	+	+	+	+	+
ReceivedFrom	**От кого получено**	+	+	+	+	+	+

3.12.2.3 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. 80.

Табл. 80 – 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**	+	+	+	+

3.12.2.4 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. 81.

Табл. 81 – 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			+

3.12.2.5 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. 82.

Табл. 82 – 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				+

3.12.2.6 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. 83.

Табл. 83 – 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					+

б) нажмите **Добавить** – окно добавления закладки закроется автоматически;

в) при необходимости повторите нужные действия для других закладок.

2. 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.
3. В ленточном меню Microsoft Word перейдите на вкладку **Файл** и выберите пункт **Параметры**.
4. В левой части окна выберите **Дополнительно**.
5. В секции **Показывать содержимое документа** справа установите флаг **Показывать закладки**.
6. Нажмите **ОК**, чтобы сохранить изменения.
7. Закладки будут отображены серым значком I.
8. Сохраните документ Microsoft Word в формате RTF.

3.13 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 каталогу пользователей **Users** (Пользователи), то по умолчанию (без применения глобальных групп JMS) этот профиль будет применяться ко всем пользователям этого каталога и ко всем рабочим станциям, зарегистрированным в JMS. Если создать глобальную группу и включить в нее только определенных пользователей каталога **Users** (Пользователи) 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 **Пользователи и роли -> Глобальные группы** и в верхней панели нажмите **Создать**.
   Отобразится следующее окно.

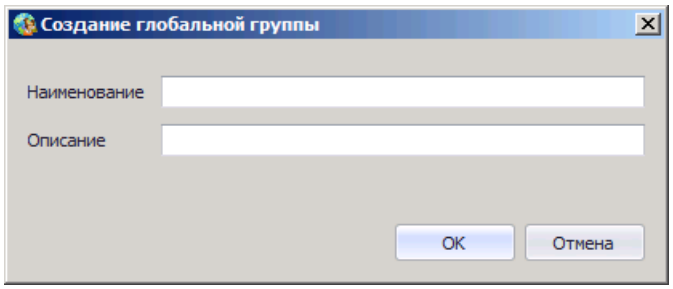


Рис. 357 – Создание новой глобальной группы

2. Введите наименование и описание глобальной группы в соответствующих полях, после чего нажмите **ОК**.

Новая глобальная группа отобразится в окне консоли управления JMS.

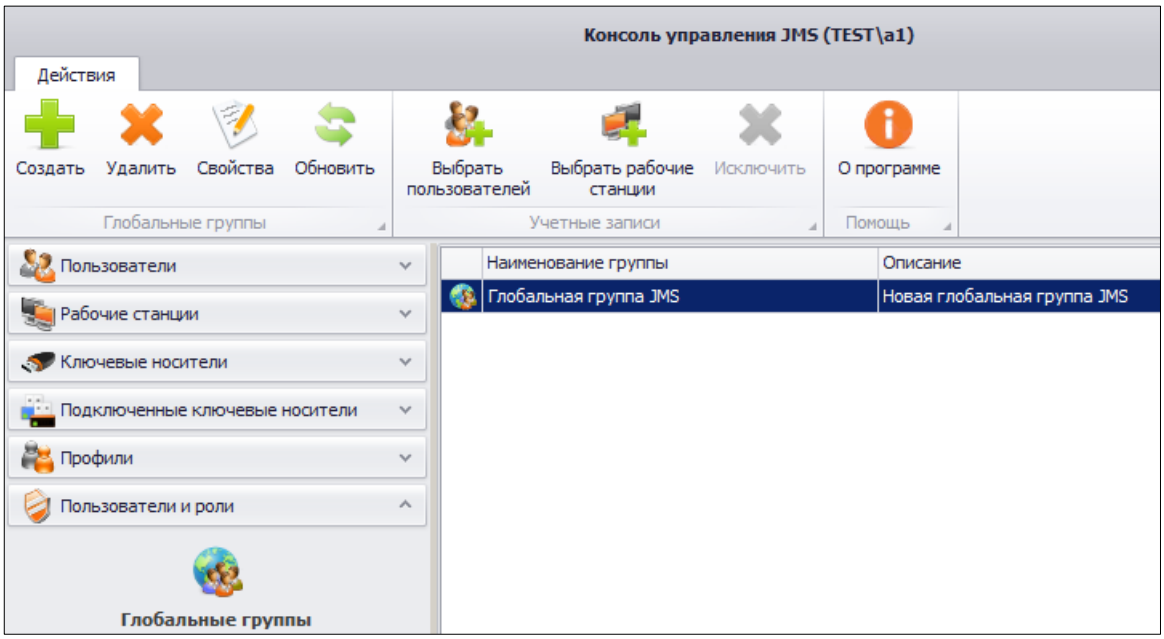


Рис. 358 – Созданная глобальная группа отображается в списке

3. Чтобы добавить в созданную глобальную группу пользователей, отметьте эту глобальную группу и в верхней панели нажмите **Выбрать пользователей**.
   Отобразится следующее окно.

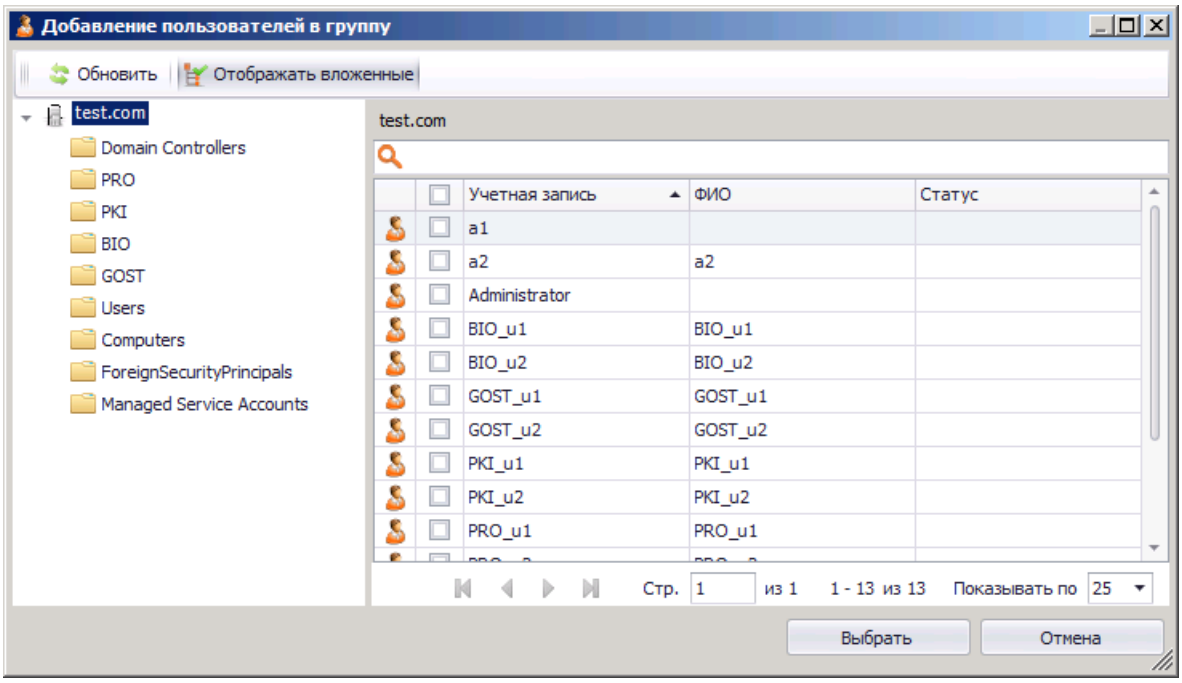


Рис. 359 – Добавление пользователей в глобальную группу

4. Отметьте пользователей, которых вы хотите добавить в глобальную группу, и нажмите **Выбрать**.
5. Чтобы добавить в глобальную группу рабочие станции, в верхней панели консоли управления JMS нажмите **Выбрать рабочие станции**.

Отобразится следующее окно.

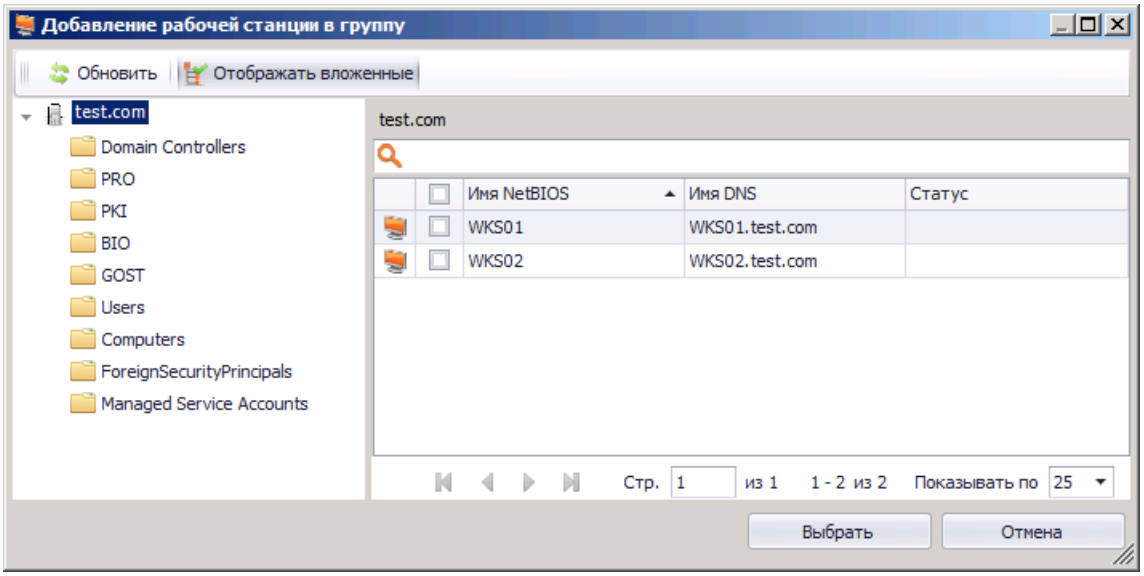


Рис. 360 – Добавление рабочих станций в глобальную группу

6. Отметьте рабочие станции, которые вы хотите добавить в глобальную группу, и нажмите **Выбрать**.
   Список добавленных пользователей и рабочих станций будет отображен в окне консоли управления JMS.

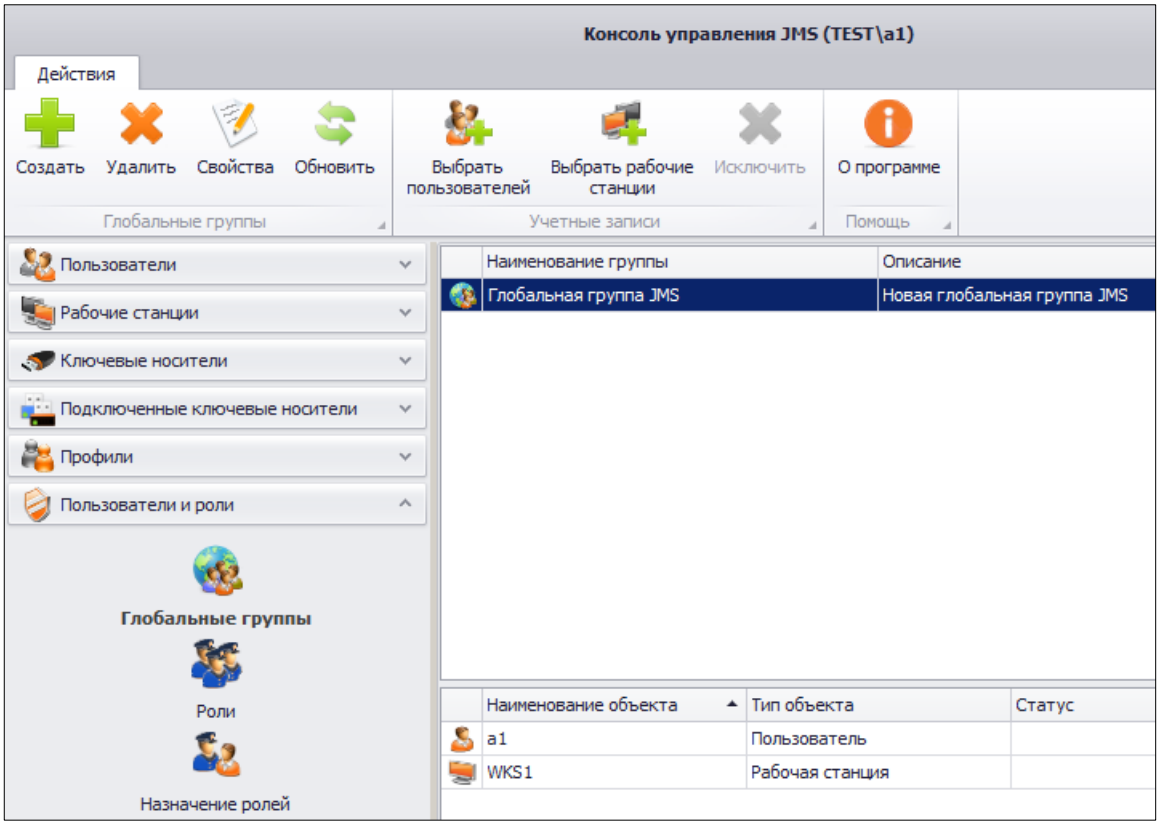


Рис. 361 – Список добавленных пользователей и рабочих станций

Созданную глобальную группу можно применять для ограничения действия привязки профилей JMS (см. «Ограничение действия профилей через группы домена/глобальные группы JMS», с. 299).

3.14 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 **Пользователи и роли -> Роли** консоли управления JMS.

Классификация операций, права на выполонение которых составляют полномочия разлчных ролей, и описание этих операций приведены в приложении «Приложение 3. Права на выполнение операций», с. 670.

Чтобы посмотреть, какие операции включены в ту или иную роль, отметьте нужную роль, затем в верхней панели консоли управления JMS нажмите **Свойства** в секции **Роли**, после чего в отобразившемся окне перейдите на вкладку **Операции** (см. рис. 362).

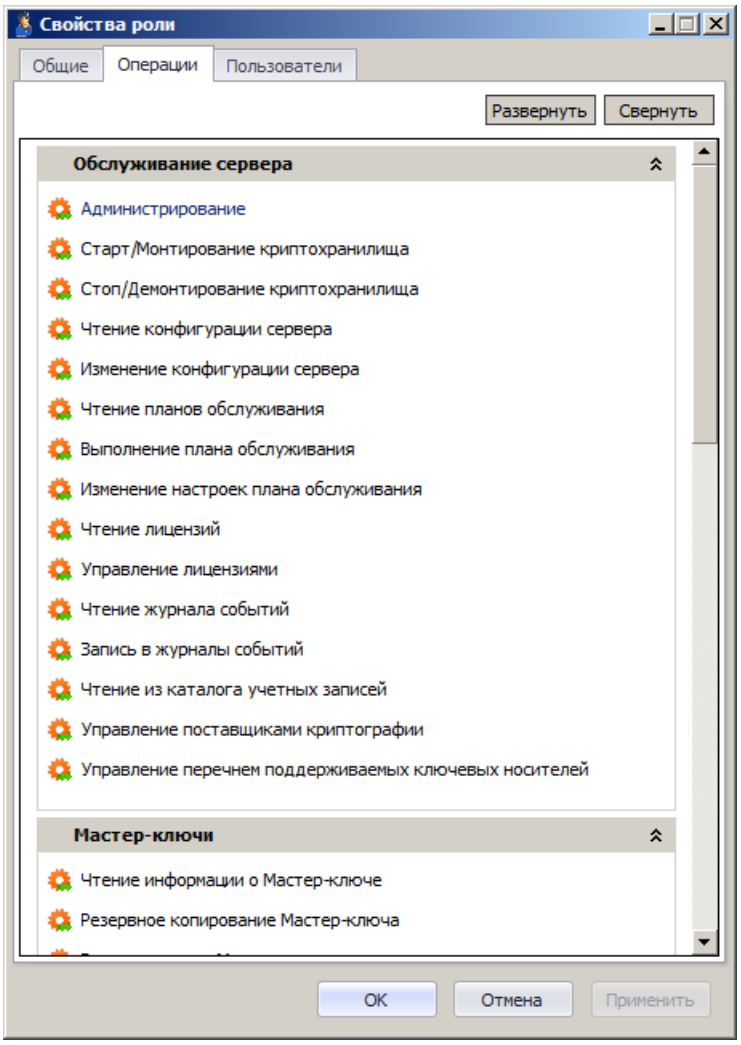


*Рис. 362 – Операции, включенные в роль **Оператор***

Для стандартных 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. 390.

1. Чтобы просмотреть список пользователей, которым назначена выбранная роль, перейдите на вкладку **Пользователи**.

Окно примет следующий вид.

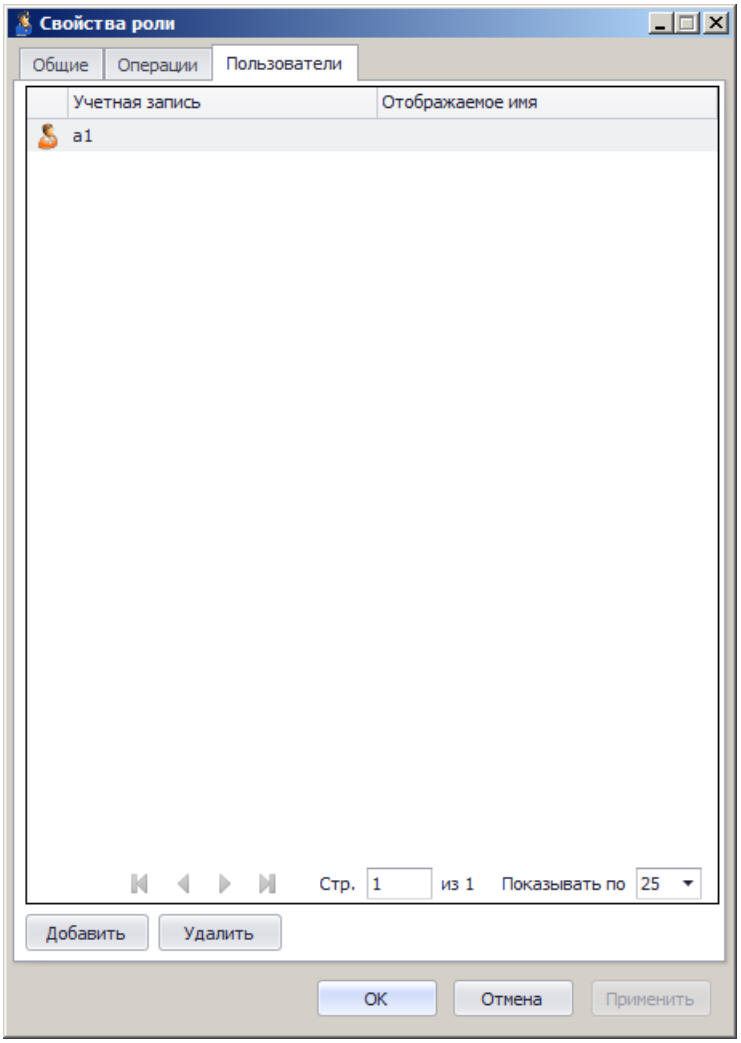


Рис. 363 – Список пользователей, которым назначена выбранная роль

2. Воспользовавшись кнопками **Добавить** или **Удалить**, вы можете, соответственно, назначить выбранную роль другим пользователям или снять назначение роли.
3. Нажмите **OK**, чтобы сохранить изменения и закрыть окно.

3.14.1 Создание новой роли JMS

Чтобы создать новую роль JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Пользователи и роли -> Роли** и в верхней панели нажмите **Создать**.

Отобразится следующее окно.

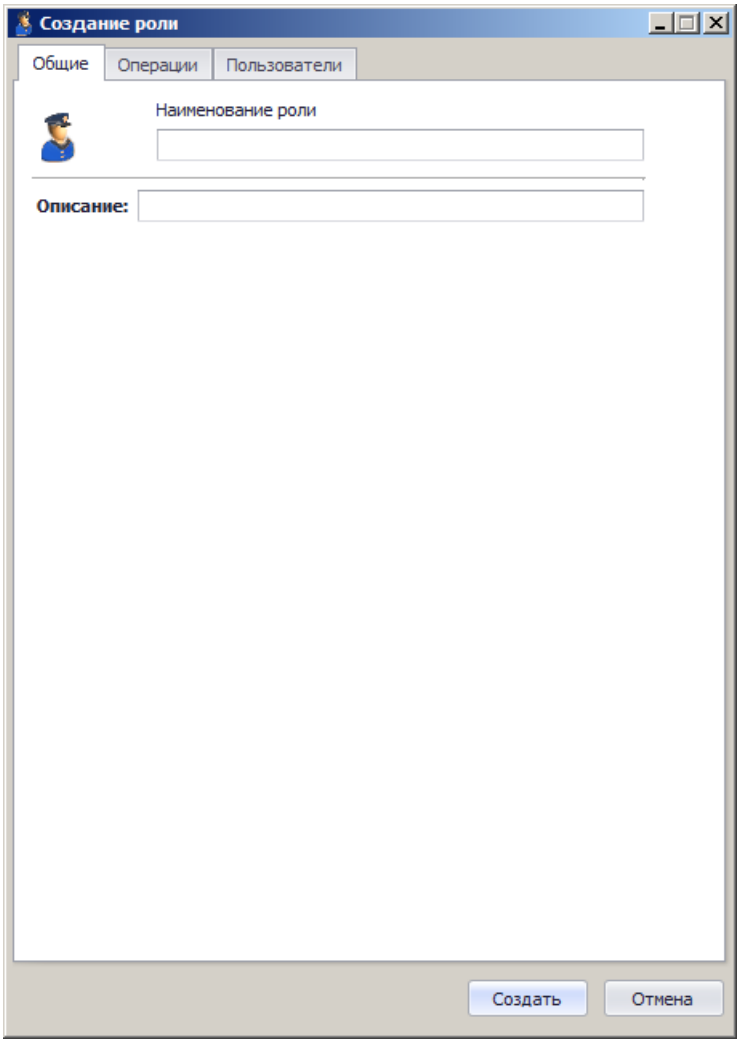


Рис. 364 – Создание новой роли

2. Введите наименование и описание роли в соответствующих полях, после чего перейдите на вкладку **Операции**.

Окно примет следующий вид.

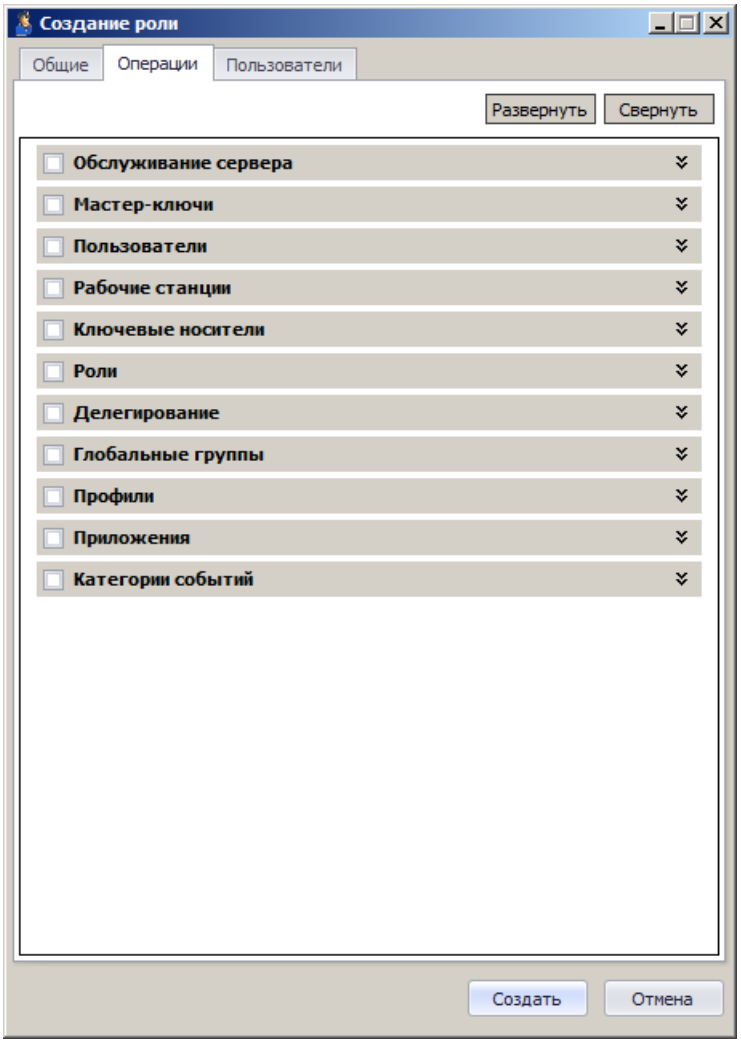


Рис. 365 – Список операций по категориям

3. Выполните одно из следующих действий:

   - отметьте нужные категории – в этом случае в роль будут включены все операции из отмеченных категорий;
   - нажмите **Развернуть** и отметьте отдельные операции, которые будут включены в роль.

4. Перейдите на вкладку **Пользователи**.

Окно примет следующий вид.

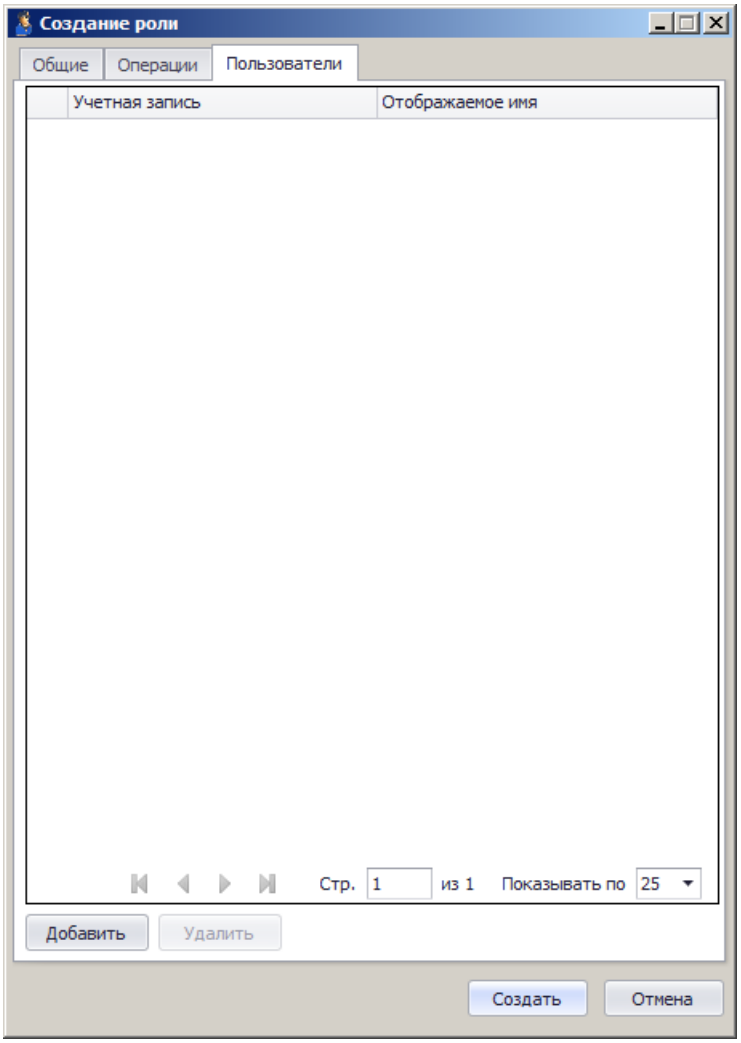


Рис. 366 – Назначение роли пользователям

5. Нажмите **Добавить** и выполните следующие действия:

5.1. в отобразившемся окне выберите пользователей, которым будет назначена созданная роль;
5.2. нажмите **Выбрать** в отобразившемся окне, чтобы подтвердить выбор.

Выбранные пользователи отобразятся в окне создания роли.

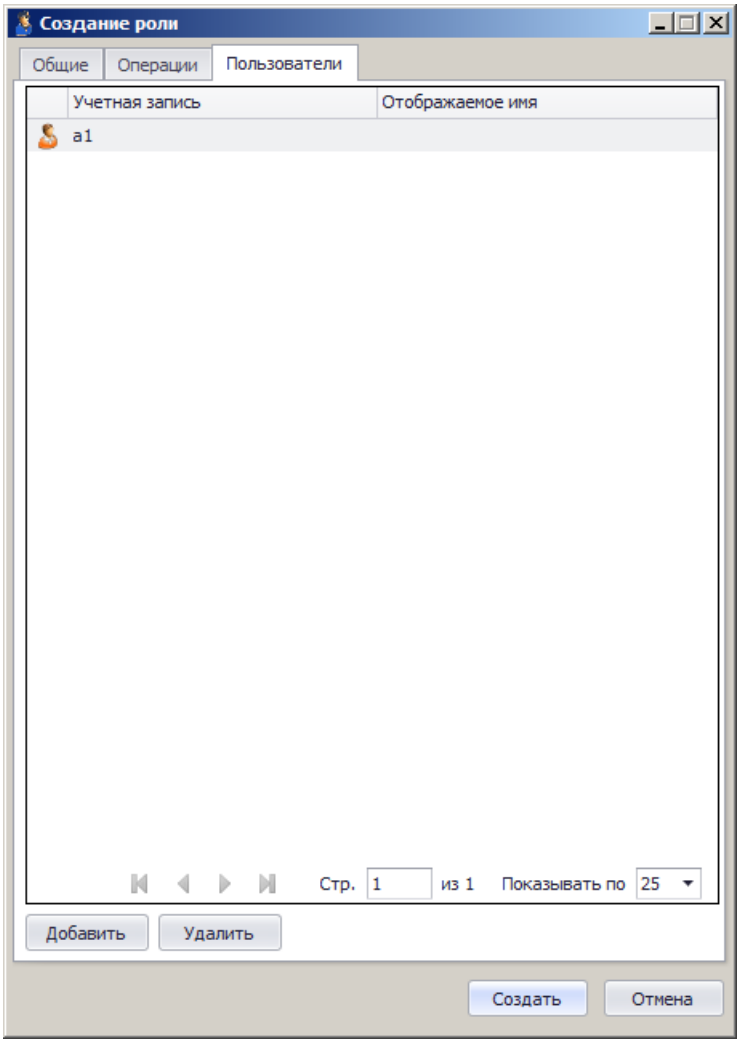


Рис. 367 – Список пользователей, которым назначена роль

6. Нажмите **Создать**, чтобы сохранить изменения и закрыть окно создания роли.

Созданная роль отобразится в окне консоли управления JMS (см. рис. 368).

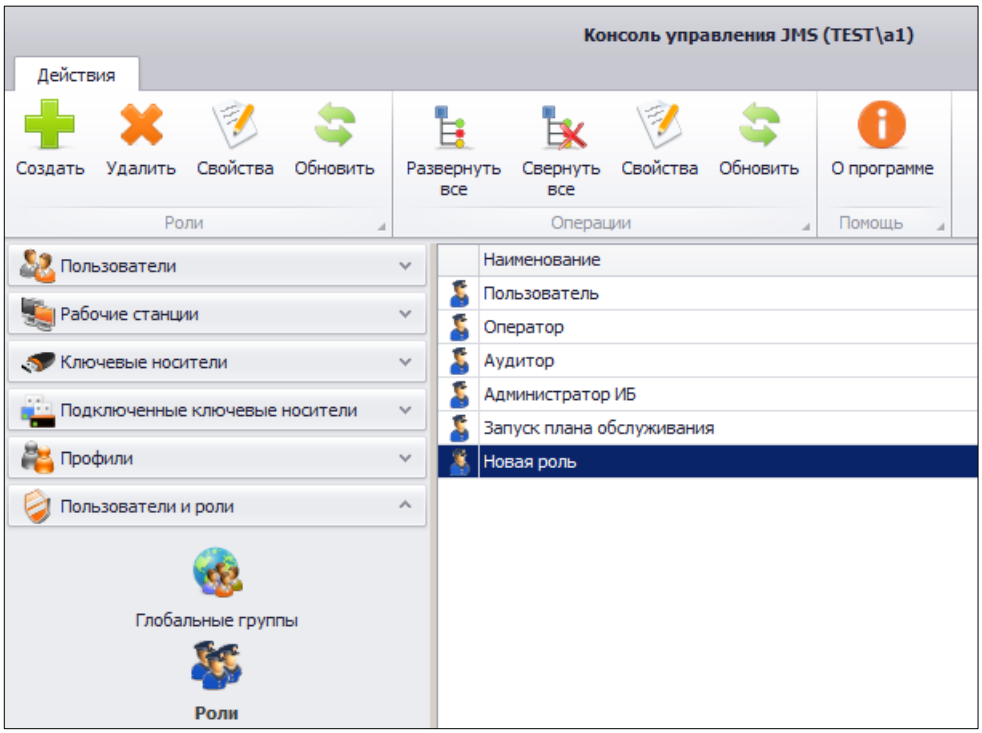


Рис. 368 – Новая роль добавлена

Теперь эту роль можно назначать пользователям JMS (см. «Назначение ролей пользователям JMS»).

3.14.2 Назначение ролей пользователям JMS

Чтобы назначить роль пользователям JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Пользователи и роли -> Назначение ролей**.

Окно консоли будет выглядеть следующим образом.

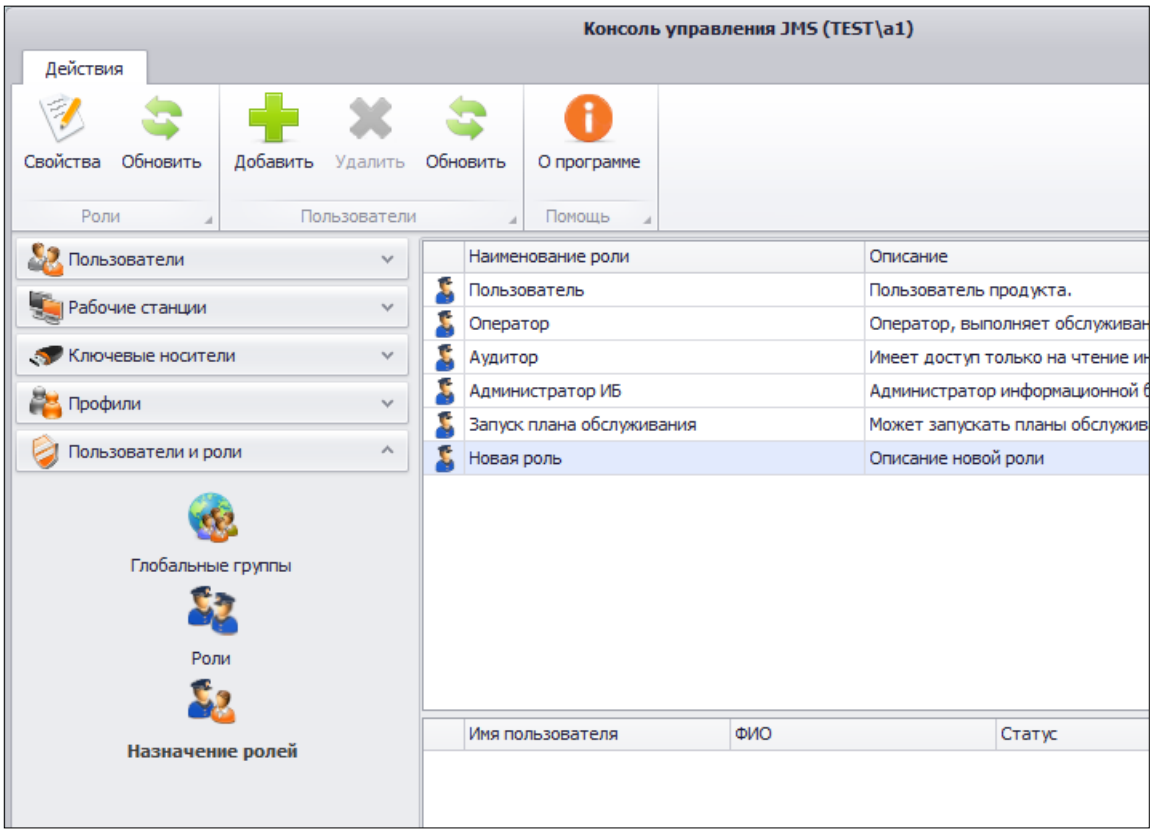


Рис. 369 – Назначение роли пользователям JMS

2. В центральной части окна отметьте роль, которую вы хотите назначить пользователям JMS, после чего в верхней панели нажмите **Добавить**.
   Отобразится следующее окно.

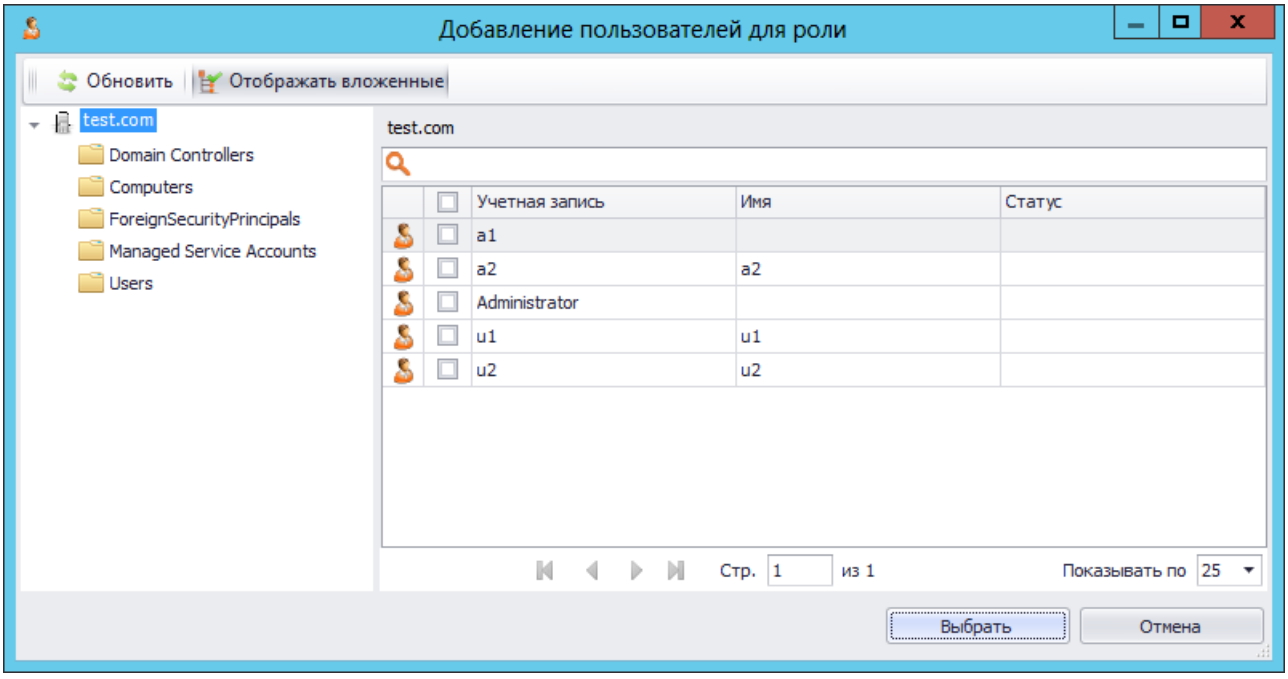


Рис. 370 – Назначение роли пользователям JMS

3. Отметьте пользователей, которым необходимо назначить выбранную роль, после чего нажмите **Выбрать**.
   Список пользователей, которым назначена роль, отобразится в окне консоли управления JMS.

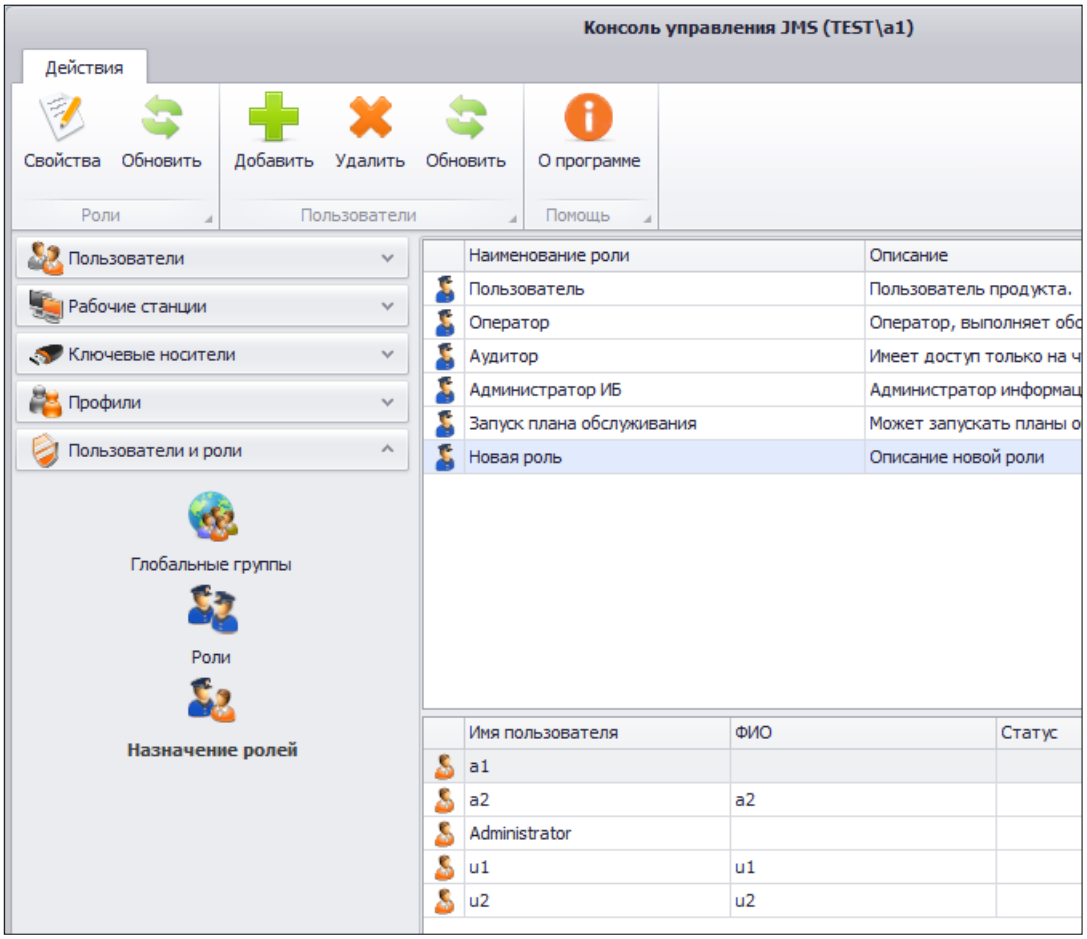


Рис. 371 – Список пользователей, которым назначена выбранная роль

3.14.3 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 3. Права на выполнение операций», с. 670.

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 центральной части интерфейса отметьте контейнер ресурсной системы, для которого вы хотите делегировать управление.
3. В верхней панели нажмите **Делегировать управления**.

Отобразится следующее окно.

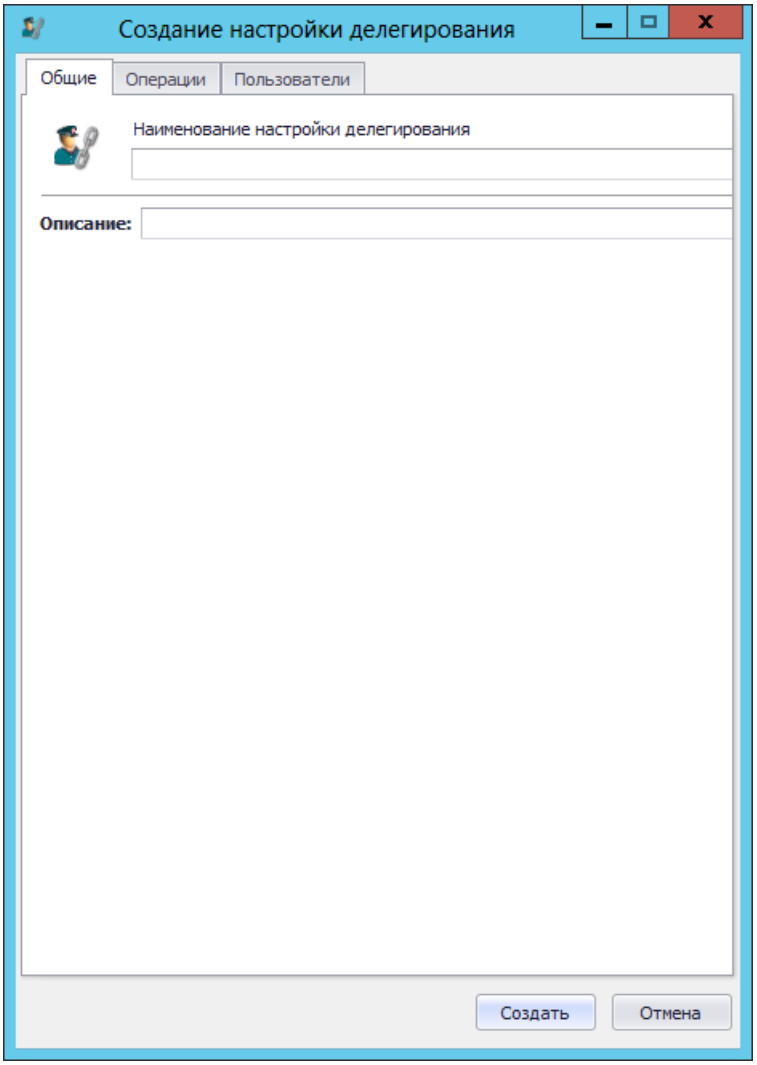


*Рис. 372 – Вкладка **Общие** настройки делегирования*

4. В соответствующих полях введите наименование и описание настройки делегирования, после чего переходите на вкладку **Операции**.

Окно примет следующий вид.

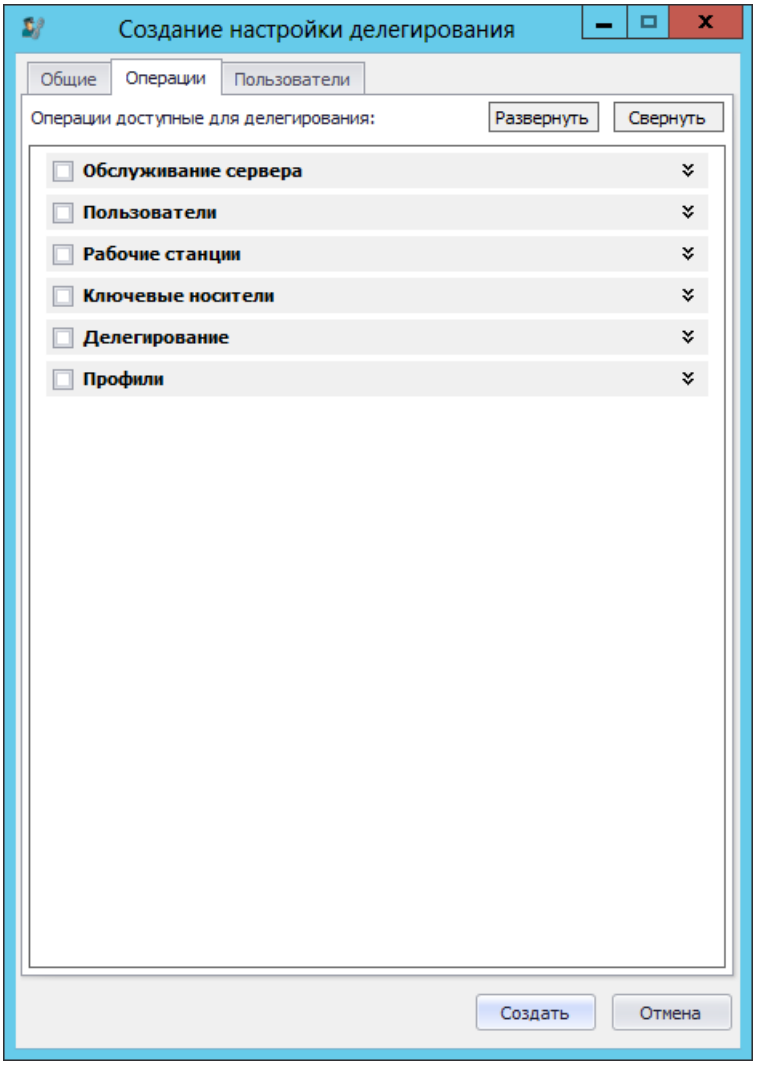


Рис. 373 – Список делегируемых операций

5. Отметьте операции, которые смогут совершать над контейнером пользователи, которым будет делегировано управление, после чего переходите на вкладку **Пользователи**.

Окно примет следующий вид.

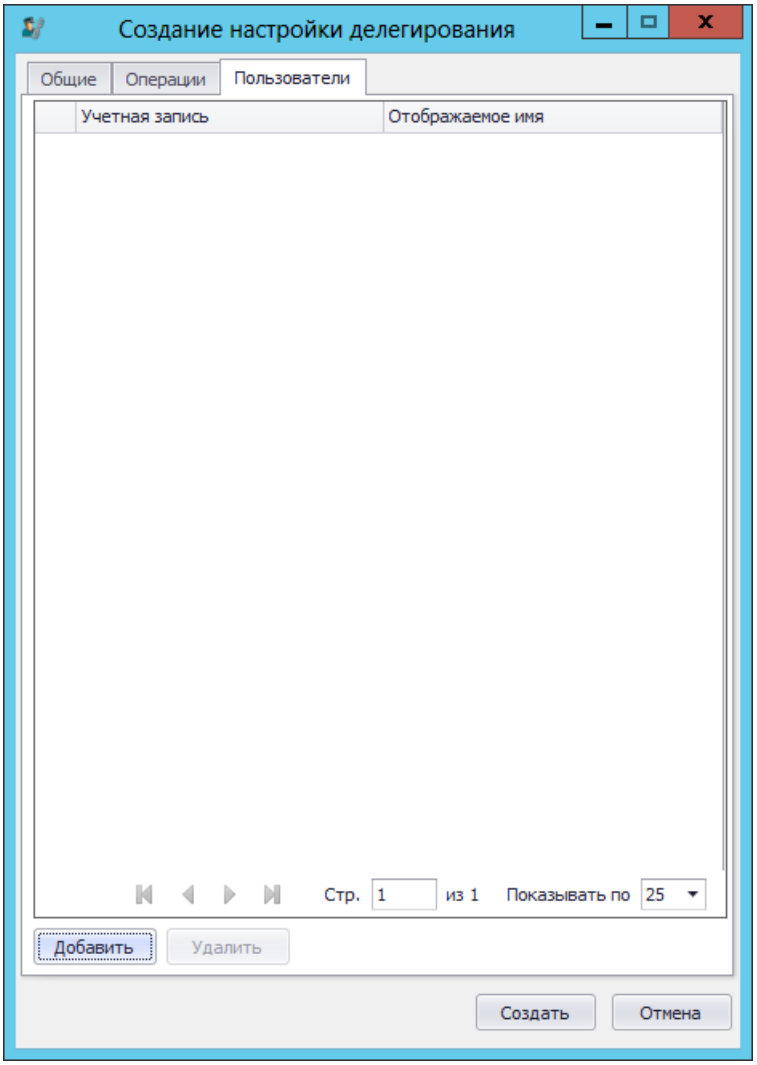


Рис. 374 – Добавление пользователей в настройку делегирования

6. Нажмите **Добавить**.

Отобразится следующее окно.

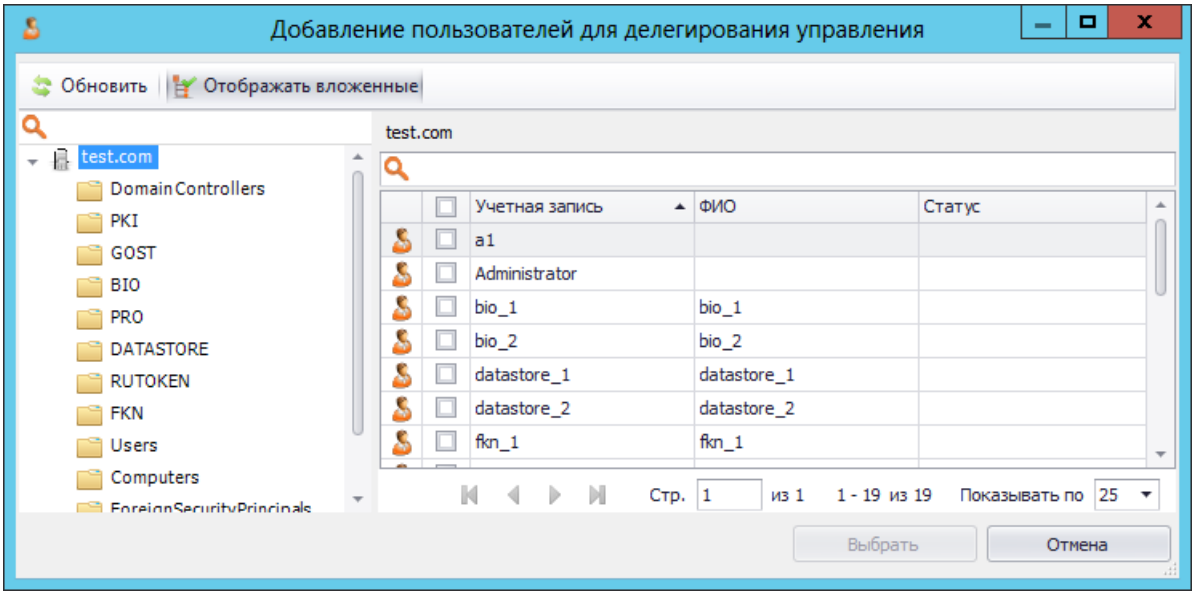


Рис. 375 – Выбор пользователей для делегирования

7. Отметьте пользователей, которым будут делегировано управление, после чего нажмите **Выбрать**.

Выбранные пользователи отобразятся на вкладке **Пользователи** настройки делегирования (см. рис. 376).

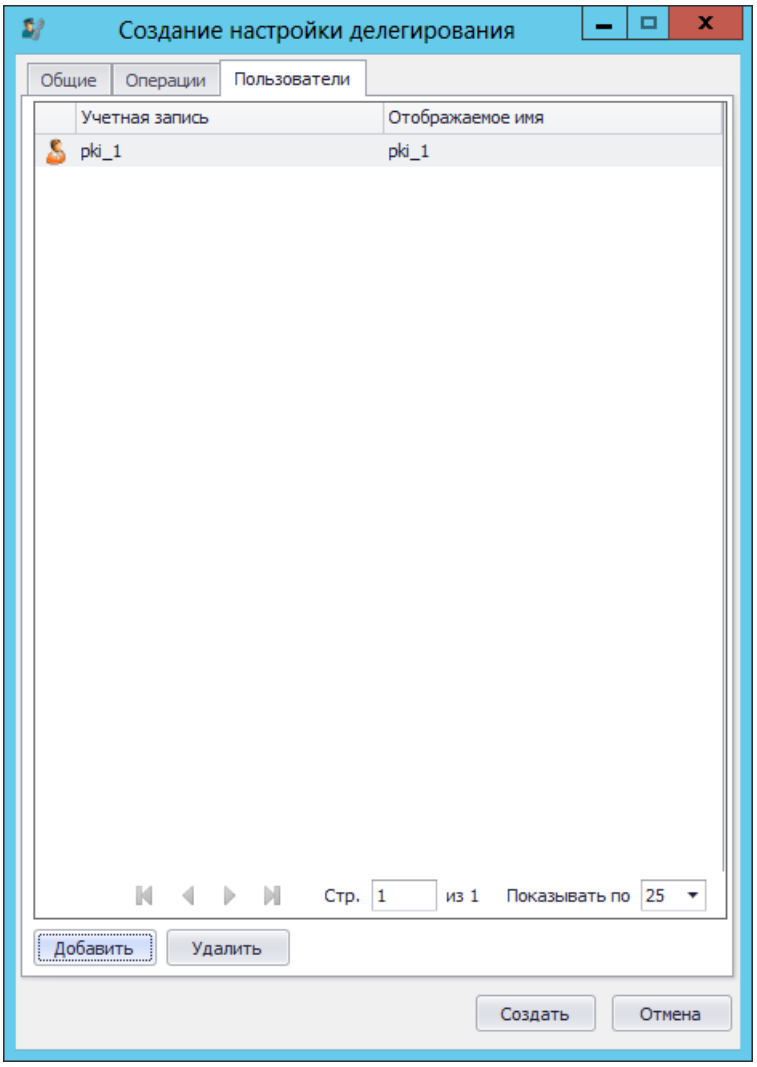


Рис. 376 – Пользователь добавлен в настройку делегирования

8. Нажмите **Создать**.

Созданная настройка делегирования отобразится в интерфейсе консоли управления JMS (см. рис. 377).

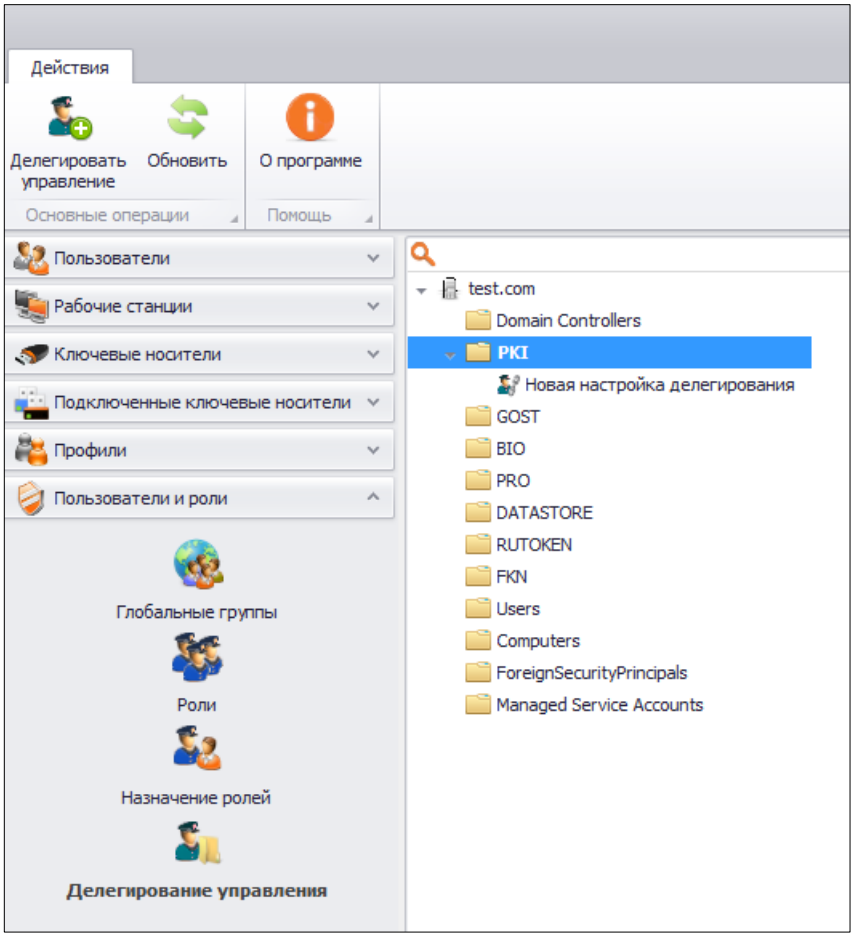


Рис. 377 – Созданная настройка делегирования в интерфейсе консоли управления JMS

3.15 Планы обслуживания

План обслуживания – процедура, предназначенная для выполнения регулярных операций массового обслуживания над объектами JMS, такими как учетные записи пользователей, электронные ключи, сертификаты, рабочие станции и др.

- план обслуживания OTP-токенов (см. «План обслуживания жизненного цикла OTP-токенов», с. 410);
- план обслуживания ключевых носителей (см. «План обслуживания ключевых носителей», с. 411);
- план обслуживания по умолчанию (см. «План обслуживания по умолчанию», с. 413);
- план обслуживания сертификатов (см. «План обслуживания сертификатов», с. 418);
- план обслуживания рабочих станций (см. «План обслуживания рабочих станций», с. 416);
- план обслуживания объектов интеграции с КриптоПро DSS (см. «План обслуживания «Синхронизация КриптоПро DSS»», с. 418).

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. 404).

План обслуживания по умолчанию следует запускать в первую очередь (см. «Запуск и просмотр результатов планов обслуживания из Консоли управления JMS», с. 405).

В настоящем подразделе рассматривается ручное управление планами обслуживания через графический интерфейс консоли управления JMS. Также существует возможность запускать планы обслуживания с помощью утилиты MaintenancePlanRunner из состава JMS. Использование утилиты MaintenancePlanRunner в частности позволяет настроить регулярный автоматический запуск планов обслуживания. Подробнее см. «Запуск планов обслуживания с помощью утилиты MaintenancePlanRunner», с. 422.

3.15.1 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 **Обслуживание -> Планы обслуживания**. Окно консоли будет выглядеть следующим образом.

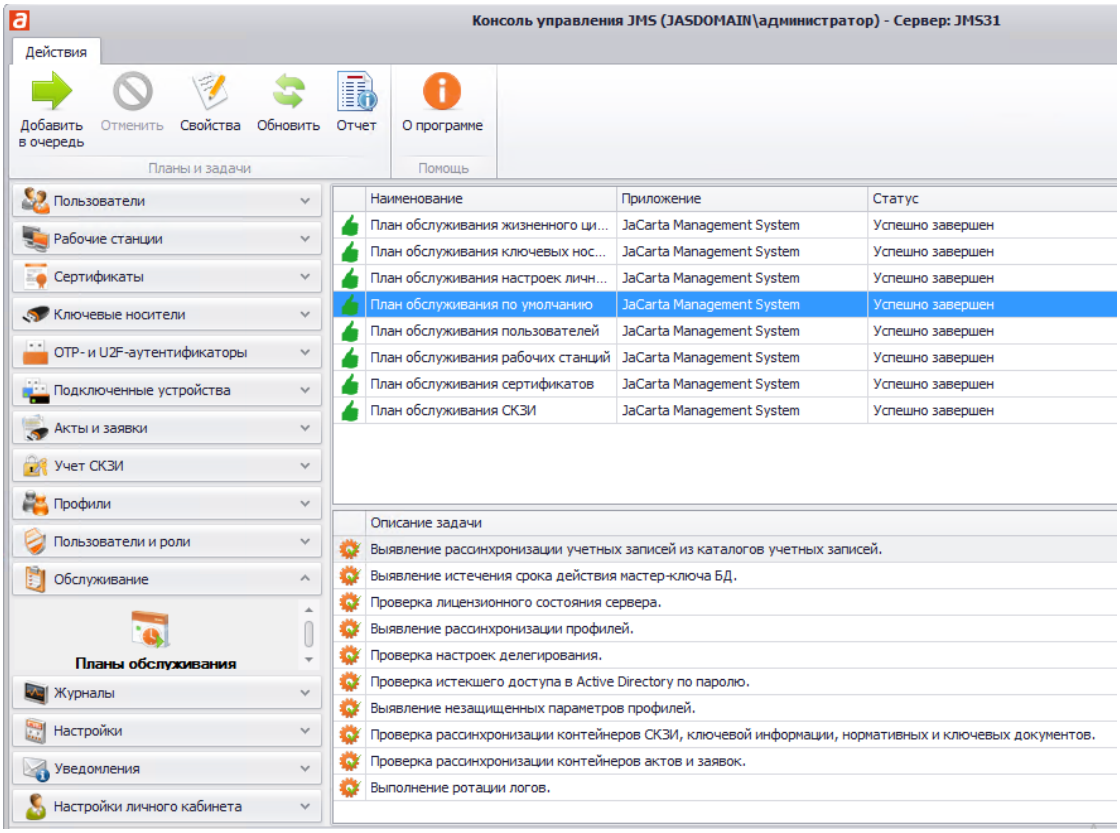


Рис. 378 – Планы обслуживания JMS

2. В центральной части окна выберите нужный план обслуживания.
3. В нижней части окна в секции **Описание задачи** выберите нужную задачу, после чего в верхней панели консоли управления JMS нажмите **Свойства**.
4. В отобразившемся окне выберите вкладку **Параметры**.

Окно примет следующий вид.

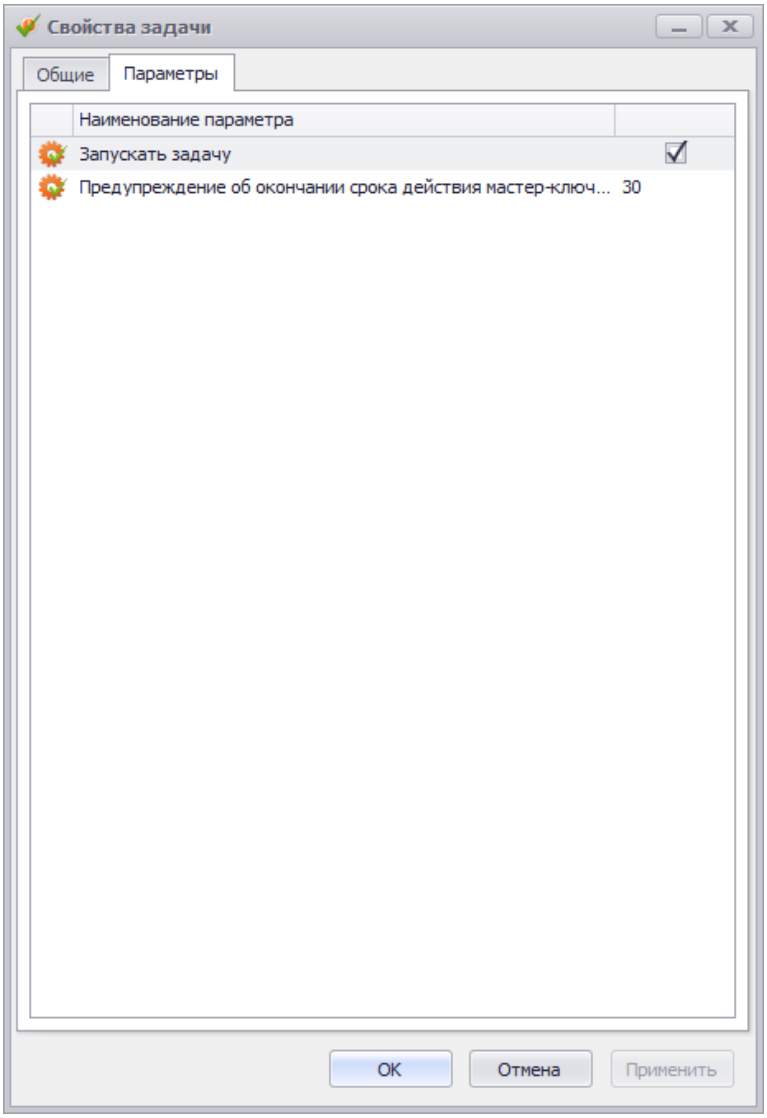


Рис. 379 – Параметры задачи

5. В зависимости от того, требуется ли выполнять задачу в рамках данного плана обслуживания, установите/сбросьте флаг **Запускать задачу**. В случае если задача должна запускаться, настройте остальные параметры, после чего нажмите **OK**.

3.15.2 Запуск и просмотр результатов планов обслуживания из Консоли управления JMS

Примечание. Запуск планов обслуживания возможен также с помощью специальной утилиты, позволяющей планировать и автоматизировать процесс обслуживания объектов JMS, подробнее см. раздел «Запуск планов обслуживания с помощью утилиты MaintenancePlanRunner», с. 422 .

Чтобы запустить выполнение плана обслуживания, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Обслуживание -> Планы обслуживания**.
2. В центральной части окна выберите нужный план обслуживания, после чего в верхней панели консоли управление JMS нажмите **Добавить в очередь**.

3. Если вы запускаете **План обслуживания пользователей**, **План обслуживания рабочих станций** или **План обслуживания жизненного цикла OTP-токенов**, отобразится окно, как на Рис. 380, после чего следуйте дальнейшему описанию. В противном случае переходите к шагу 11.

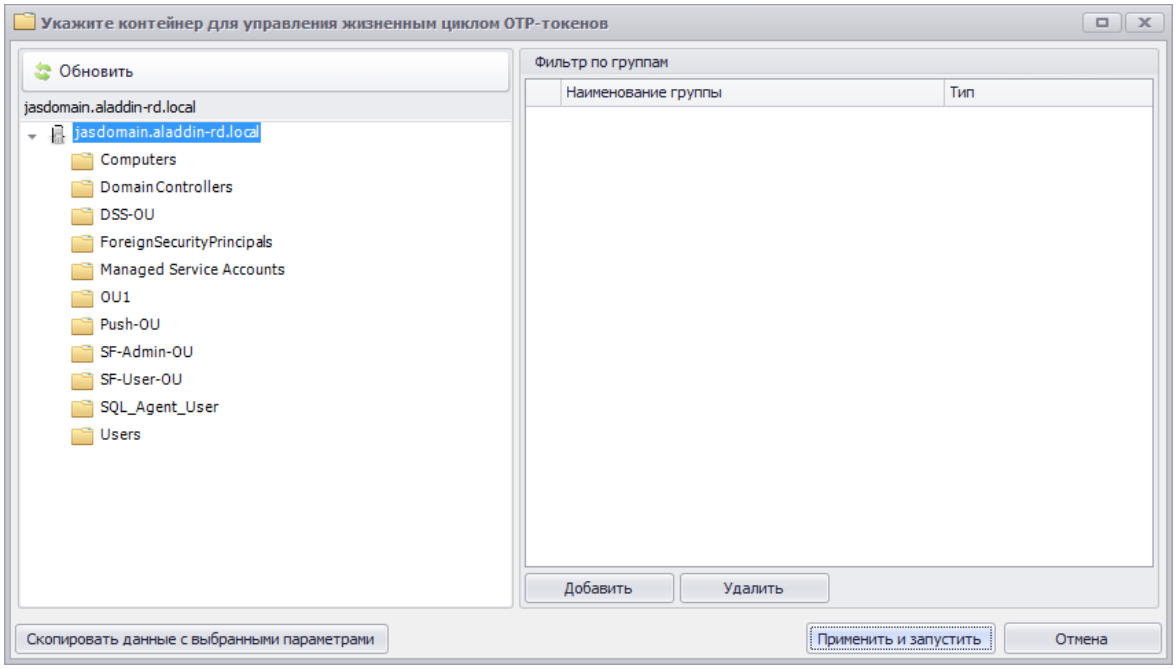


Рис. 380 – Окно фильтрации объектов обслуживания

4. В левой части окна выберите контейнер ресурсной системы, в котором содержатся объекты, подлежащие обслуживанию с помощью данного плана. (При необходимости допускается выбор корневого объекта, например домена AD).
5. При необходимости добавить к объектам выбранного контейнера объекты, относящиеся к доменным группам (группам домена Active Directory) или глобальным группам JMS (см. раздел «Глобальные группы JMS», с. 386), в правой половине окна нажмите **Добавить**.

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).

Отобразится окно следующего вида.

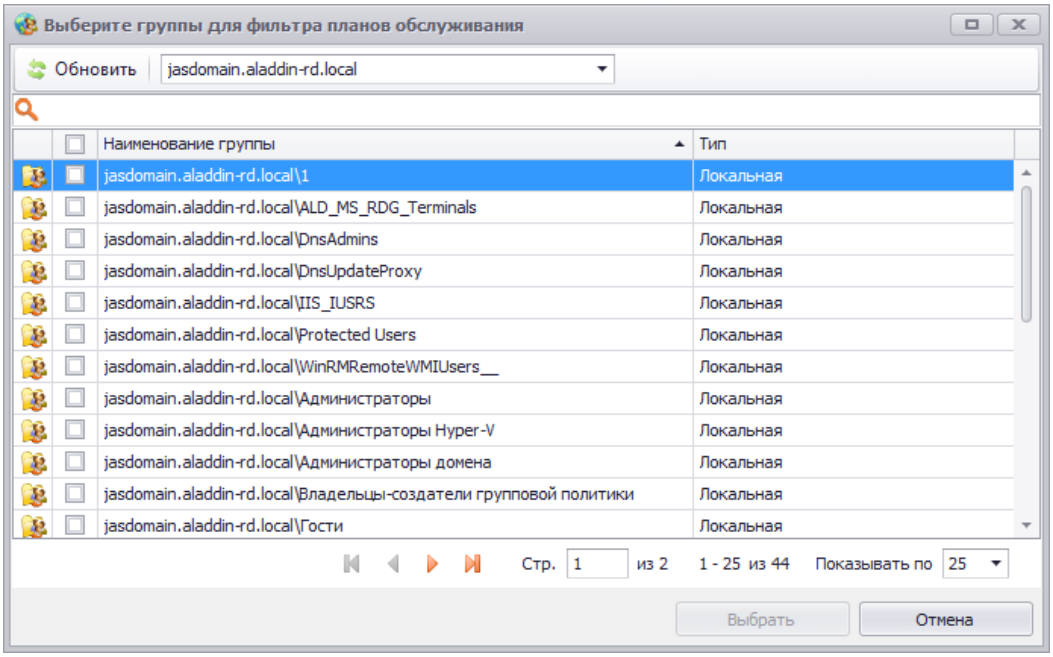


Рис. 381 – Окно добавления объектов, относящихся к доменным и/или глобальным группам

6. Для добавления объектов, относящихся к доменным группам, выберите (отметьте в левом столбце) доменные группы AD, объекты которых должны быть обработаны в ходе выполнения плана обслуживания.
7. Для добавления объектов, относящихся к глобальным группам, вверху окна нажмите раскрывающийся список.

Примечание. Возможность добавления объектов (пользователей) за счет *глобальных групп JMS* реализована только для **Плана обслуживания жизненного цикла OTP-токенов**.

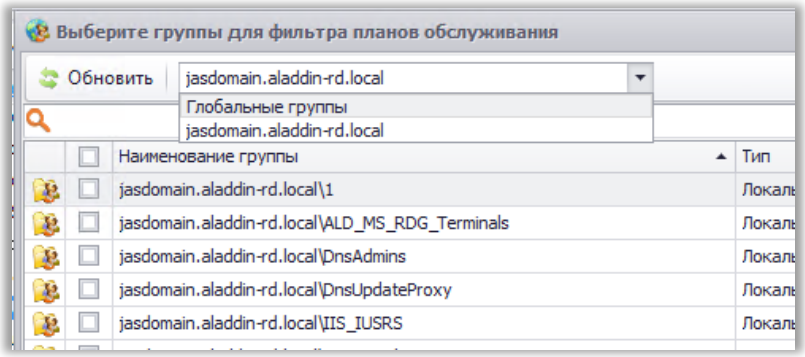


Рис. 382 – Выбор пункта Глобальные группы в окне фильтрации объектов

8. Выберите пункт **Глобальные группы**.

Отобразится окно следующего вида.

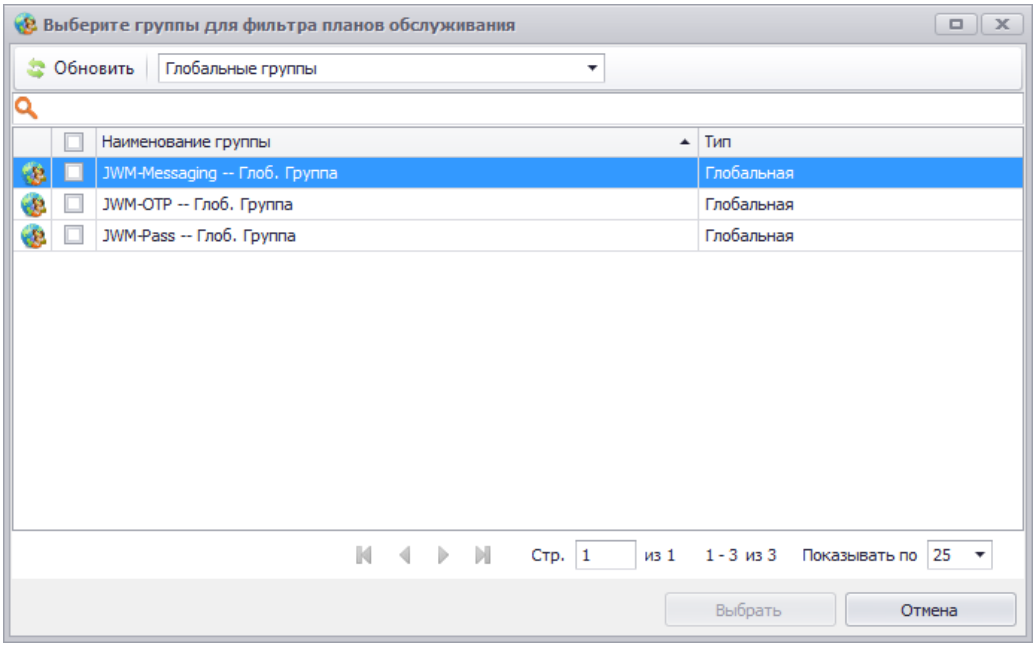


Рис. 383 – Выбор пункта Глобальные группы в окне фильтрации объектов

9. Для добавления объектов, относящихся к глобальным группам, выберите (отметьте в левом столбце) глобальные группы, объекты которых должны быть обработаны в ходе выполнения плана обслуживания.
10. Нажмите **Выбрать**.
11. В исходном окне фильтрации (Рис. 380, с. 406) нажмите **Применить и запустить**.

При успешном выполнении плана обслуживания напротив его названия отобразится значок (см. рис. 384), а в столбце **Статус** будет отображен статус **Успешно завершен**.

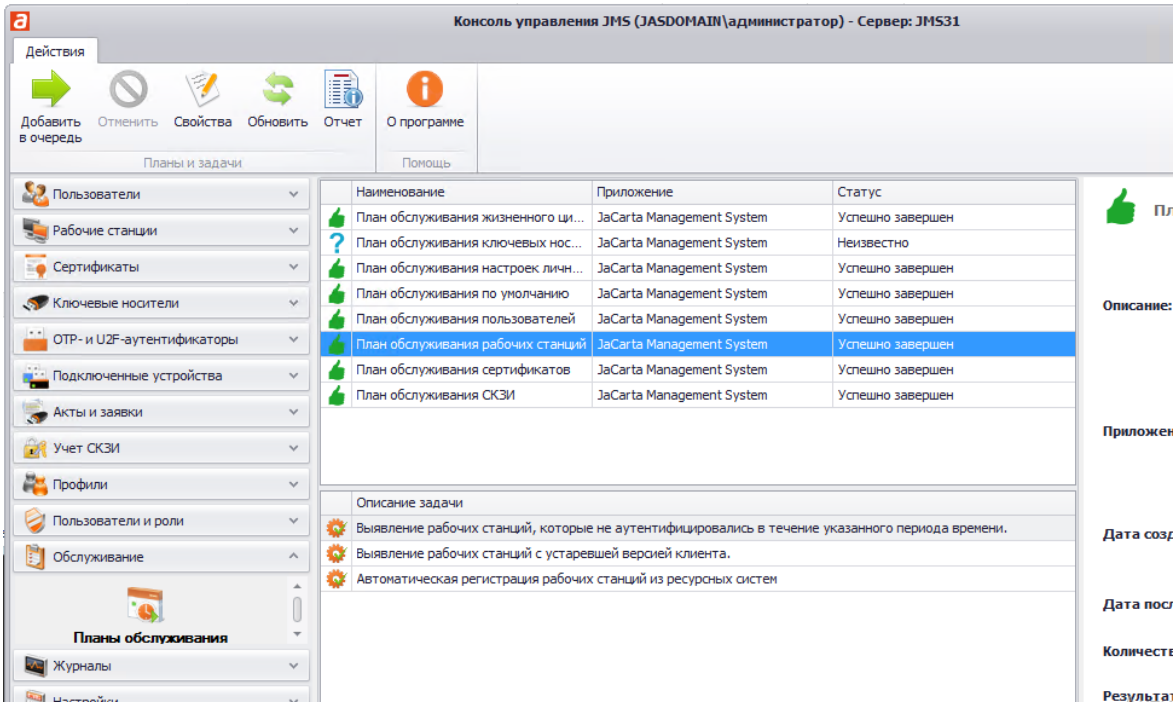


Рис. 384 – Результат выполнения плана обслуживания

12. Чтобы отобразить отчет о выполнении плана обслуживания, в верхней панели консоли управления JMS нажмите **Отчет**.
Отчет отобразится в отдельном окне.

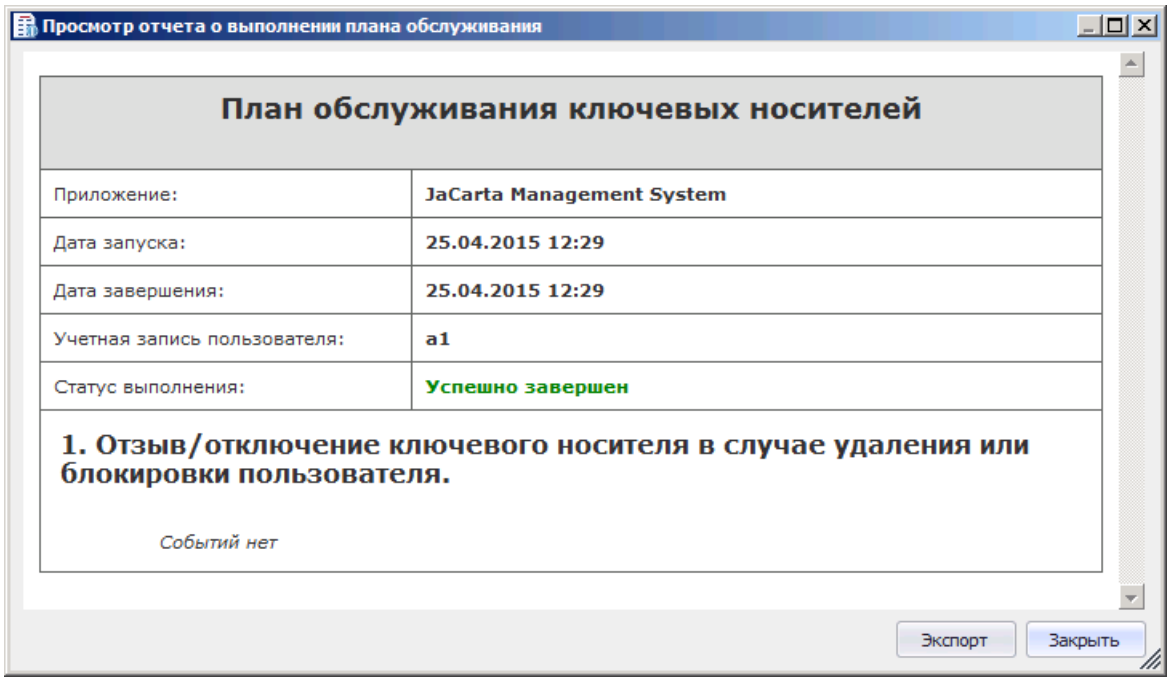


Рис. 385 – Отображение отчета о выполнении плана обслуживания

3.15.3 План обслуживания жизненного цикла OTP-токенов

План обслуживания жизненного цикла OTP-токенов содержит следующие задачи (см. 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

Примечание. Для удобства автоматизации запуска плана обслуживания можно использовать функцию автоматической генерации параметров запуска утилиты MaintanancePlanRunner (подробнее см. «Автоматическая генерация параметров запуска утилиты MaintenancePlanRunner», с. 422).

Табл. 84 – План обслуживания жизненного цикла OTP-токенов

Название задачи	Описание и параметры задачи
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. 262). По окончании выполнения данной задачи выпущенные токены переходят в состояние **Используется**. Параметры: **Запускать задачу** – определяет, будет ли задача 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. 269). По окончании выполнения данной задачи выпущенные токены переходят в состояние **Используется**. Параметры: **Запускать задачу** – определяет, будет ли задача 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. 254). По окончании выполнения данной задачи выпущенные токены переходят в состояние **Используется**. Параметры: **Запускать задачу** – определяет, будет ли задача 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. 275). По окончании выполнения данной задачи выпущенные токены переходят в состояние **Используется**. Параметры: **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания.

Название задачи	Описание и параметры задачи
Удаление Push OTP-токенов	Данная задача выполняет удаление Push OTP-токенов из связанной подсистемы A2FA. **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: • **Запускать задачу** – определяет, будет ли задача 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**).

3.15.4 План обслуживания ключевых носителей

План обслуживания ключевых носителей содержит следующие задачи (см. табл. 85).

Табл. 85 – 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. 413,задача **Выявление рассинхронизации учетных записей из каталогов учетных записей**). По окончании выполнения данной задачи, электронные ключи заблокированных пользователей переходят в состояние **Отключен**. Параметры: **Запускать задачу** – определяет, будет ли задача 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. Параметры: • **Запускать задачу** – определяет, будет ли задача 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.

Название задачи	Описание и параметры задачи
	Параметры: • **Запускать задачу** – определяет, будет ли задача 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 чило таких ключей меньше порогового значения, которое задается в параметрах задачи, то будет сгенерировано соответствующее уведомление в журнале предупреждений. Параметры: • **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания. • **Порог минимального количества свободных ключевых носителей** – пороговое значение, при снижении ниже которого генерируется уведомление
Проверка привязки назначенных ридеров смарт-карт к контейнеру	В рамках задачи анализируются все зарегистрированные ридеры смарт-карт, назначенные пользователям: • если пользователь был перемещен в новый контейнер ресурсной системы, туда же будут перемещены его карт-ридеры; • если пользователь был удален вместе с контейнером, его карт-ридер будет перемещен в корневой контейнер ресурсной системы. Параметры: • **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания.
Проверка привязки неназначенных ридеров смарт-карт к контейнеру	В данной задаче анализируются все зарегистрированные, но еще не назначенные пользователю карт-ридеры. Если контейнер ресурсной системы, к которой привязан карт-ридер, удален из ресурсной системы, данный ридер перемещается в корневой контейнер ресурсной системы. Параметры: • **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания.
Включение ключевого носителя разблокированного пользователя	В рамках задачи заблокированные электронные ключи, принадлежащие незаблокированным пользователям будут автоматически разблокированы, даже если электронный ключ был заблокирован вручную администратором. Параметры: • **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания.

3.15.5 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. 293) в свойства объектов *Пользователь*, к которым привязан данный профиль.

План обслуживания настроек личного кабинета содержит следующие задачи (см. Табл. 86)

Табл. 86 – План обслуживания настроек личного кабинета

Название задачи	Описание и параметры задачи
Синхронизация прав доступа	Позволяет синхронизировать права доступа в личный кабинет пользователя на JWM, настройенные профиле **Доступ в личный кабинет** (см. раздел «Настройка

Название задачи	Описание и параметры задачи
	профиля доступа в личный кабинет JWM», с. 293) со свойствами объектов *Пользователь*, к которым привязан данный профиль. Задача содержит следующие параметры: • **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания.

3.15.6 План обслуживания по умолчанию

План обслуживания по умолчанию содержит следующие задачи (см. табл. 87)

Табл. 87 – 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: • **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания; • **Блокировать зарегистрированных пользователей и рабочие станции** – 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** – если флаг установлен, то при выполнении плана обслуживания учетные записи пользователей, не заблокированных в ресурсной системе, будут разблокированы и в JMS (если по какой-то причине они были заблокированы). Значение по умолчанию: не установлен • **Разблокировать рабочие станции, на момент выполнения плана обслуживания не заблокированные в ресурсной системе** – если флаг установлен, то при выполнении плана обслуживания учетные записи рабочих станций, не заблокированных в ресурсной системе, будут разблокированы и в JMS (если по какой-то причине они были заблокированы). Значение по умолчанию: не установлен
Выявление истечения срока действия мастер-ключа БД	Осуществляет проверку срока действия текущего мастер-ключа БД. Задача имеет следующие параметры: • **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания; • **Предупреждение об окончании срока действия мастер-ключа БД** – позволяет указать, за сколько дней до истечения срока действия мастер-ключа БД в отчете о выполнении плана обслуживания будет отображаться соответствующее предупреждение.
Проверка лицензионного состояния сервера	Задача имеет следующие параметры: • **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания; • **Предупреждение об окончании срока действия лицензии за 90 дней** – позволяет указать, за сколько дней до истечения срока действия лицензии в отчете о выполнении плана обслуживания будет отображаться соответствующее предупреждение.

Название задачи	Описание и параметры задачи
	• **Предупреждение об исчерпании лимита рабочих станций** – в текущей версии продукта данный параметр не используется (при установке значения никаких действий не производится)
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: • **Запускать задачу** – определяет, будет ли задача 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 в Active Directory), выполняется отмена этого делегирования. В журнал плана обслуживания (журнал **Отчеты планов обслуживания**) заносится соответствующее событие. Параметры: • **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания.
Проверка истекшего доступа в Active Directory по паролю	Отменяет временный доступ в Active Directory по паролю, если срок такого доступа истек. Параметры: • **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания.
Выявление назащищенных параметров профилей	Выявляет и помещает в криптохранилище 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 криптохранилище, или при создании новой базы данных). • **Запускать задачу** – определяет, будет ли задача 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: • **Запускать задачу** – определяет, будет ли задача 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:

Название задачи	Описание и параметры задачи
	• **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания.
Выполнение ротации логов	Задача имеет следующие параметры: • **Запускать задачу** – определяет, будет ли задача 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).**

3.15.7 План обслуживания пользователей

План обслуживания пользователей содержит следующие задачи (см. Табл. 88).

План обслуживания применяется только к объектам в выбранном контейнере соответствующей ресурсной системы. Выбор ресурсной системы и ее контейнера выполняется в момент запуска плана обслуживания.

Примечание. Для удобства автоматизации запуска плана обслуживания можно использовать функцию автоматической генерации параметров запуска утилиты MaintanancePlanRunner (подробнее см. «Автоматическая генерация параметров запуска утилиты MaintenancePlanRunner», с. 422).

Табл. 88 – 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. Задача содержит следующие параметры: • **Запускать задачу** – определяет, будет ли задача 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 ресурсными системами Active Directory и Remote Active Directory, 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 Remote 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 пользователей по дате создания.**

Название задачи	Описание и параметры задачи
	Фильтр эффективен только в случае регулярного автоматического запуска плана обслуживания средствами утилиты MaintenancePlanRunner 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**.

3.15.8 План обслуживания рабочих станций

Внимание! План обслуживания рабочих станций не предусмотрен в версии *CA Edition* продукта JMS (см. «Руководство администратора. Часть 1» [2], раздел «Версии поставки продукта и лицензионные опции»).

План обслуживания рабочих станций содержит следующие задачи (см. Табл. 89).

План обслуживания применяется только к объектам в выбранном контейнере соответствующей ресурсной системы. Выбор ресурсной системы и ее контейнера выполняется в момент запуска плана обслуживания.

Примечание. Для удобства автоматизации запуска плана обслуживания можно использовать функцию автоматической генерации параметров запуска утилиты MaintanancePlanRunner (подробнее см. «Автоматическая генерация параметров запуска утилиты MaintenancePlanRunner», с. 422).

Табл. 89 – 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. В разделе **Рабочие станции** консоли управления строка с учетной записью такой рабочей станции подсвечивается желтым цветом. • 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. В разделе **Рабочие станции** консоли управления строка с учетной записью такой рабочей станции подсвечивается красным цветом (Рис. 386, ниже). Задача содержит следующие параметры: • **Запускать задачу** – определяет, будет ли задача 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).

Название задачи	Описание и параметры задачи
	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: • **Запускать задачу** – определяет, будет ли задача 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]`
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: • **Запускать задачу** – определяет, будет ли задача 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 и Remote 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 утилиты *MaintenancePlanRunner* 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**.

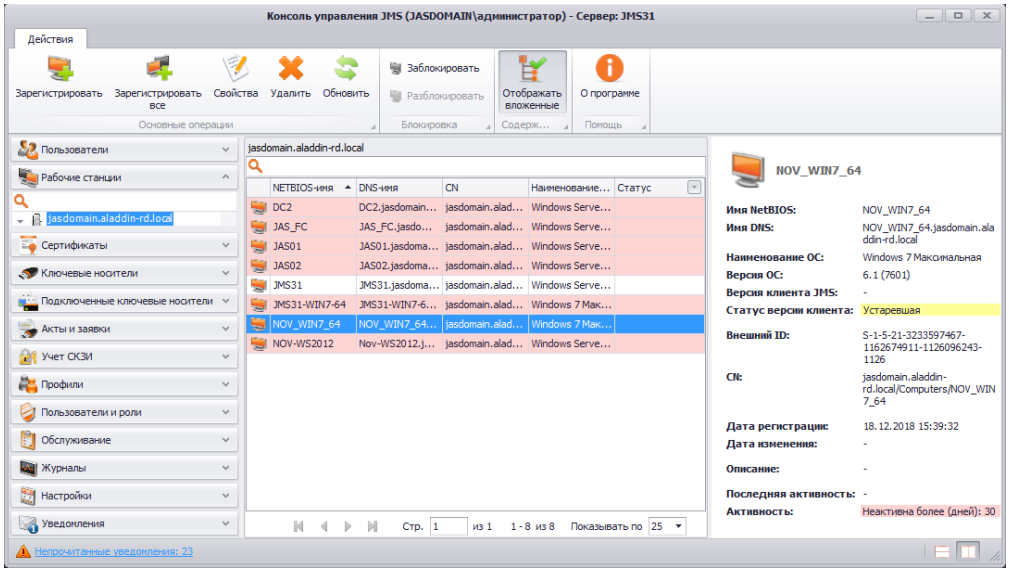


Рис. 386 – Цветовое выделение рабочих станций, у которых превышен срок выполнения последней аутентификации (активности)

3.15.9 План обслуживания сертификатов

План обслуживания сертификатов содержит следующие задачи (см. таблицу 90).

Табл. 90 – 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: • **Запускать задачу** – определяет, будет ли задача 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 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: • **Запускать задачу** – определяет, будет ли задача 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

Название задачи	Описание и параметры задачи
	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: • **Запускать задачу** – определяет, будет ли задача 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: • **Запускать задачу** – определяет, будет ли задача 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. 432) данному пользователю будет отправлено уведомление по электронной почте. Задача содержит следующие параметры: • **Запускать задачу** – определяет, будет ли задача 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 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

Название задачи	Описание и параметры задачи
	(см. «Уведомления о событиях, связанных с использованием JMS», с. 432) данному пользователю будет отправлено уведомление по электронной почте. Задача содержит следующие параметры: • **Запускать задачу** – определяет, будет ли задача 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. 432) данному пользователю будет отправлено уведомление по электронной почте. Задача содержит следующие параметры: • **Запускать задачу** – определяет, будет ли задача 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	В рамках данной задачи будут проанализированы все внешние сертификаты, взятые под управление, у которых в профиле установлена опция **Опубликовать сертификат в ресурсную систему** (см. раздел «Создание и настройка профиля Внешние объекты», с. 239), но которые по каким-то причинам не были опубликованы. Все выявленные сертификаты будут повторно опубликованы в ресурсную систему. Задача содержит следующие параметры: • **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания
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 помечены в БД JMS, как удалённые. Задача содержит следующие параметры: • **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания

3.15.10 План обслуживания СКЗИ

План обслуживания СКЗИ содержит следующие задачи (см. Табл. 91).

Табл. 91 – План обслуживания СКЗИ

Название задачи	Описание и параметры задачи
Автоматический ввод в эксплуатацию программных СКЗИ	Позволяет автоматически вводить в эксплуатацию экземпляры программных СКЗИ, которые привязаны к лицензии и назначены пользователям. Задача содержит следующие параметры: • **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания

3.15.11 План обслуживания «Синхронизация КриптоПро DSS»

План обслуживания «Синхронизация КриптоПро DSS» содержит следующие задачи (см. Табл. 92).

Табл. 92 – План обслуживания «Синхронизация КриптоПро DSS»

Название задачи	Описание и параметры задачи
Синхронизация учетных записей пользователей	Данная задача выполняет перенос/синхронизацию информации о пользователях из JMS в КриптоПро DSS в соответствии с активными профилями **Пользователь КриптоПро DSS** (см. раздел «Настройка профиля пользователя КриптоПро DSS», с. 281). В процессе выполнения задачи выполняется также установка контроля над пользователями, существовавшими в КриптоПро DSS до интеграции с JMS (см. раздел «Взятие под управление пользователей КриптоПро DSS», с. 459) Параметры: **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания.
Синхронизация сертификатов пользователей	Данная задача выполняет запуск выпуска сертификатов для пользователей КриптоПро DSS в соответствии с активными профилями **Выпуск сертификатов на КриптоПро DSS**. Параметры: **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания.
Рассылка оповещений об учетных записях	Данная задача выполняет рассылку оповещений пользователей КриптоПро DSS (о назначении паролей и др. аутентификаторов), определенных активными профилями **Пользователь КриптоПро DSS** (см. раздел «Настройка профиля пользователя КриптоПро DSS», с. 281). Параметры: **Запускать задачу** – определяет, будет ли задача выполнена во время выполнения плана обслуживания.

3.15.12 Запуск планов обслуживания с помощью утилиты MaintenancePlanRunner

3.15.12.1Сведения об утилите

В состав JMS входит утилита MaintenancePlanRunner (полное наименование **Aladdin.EAP.MaintenancePlanRunner.exe**), которая используется для управления процессом запуска плана обслуживания. В сочетании с планировщиком задач Microsoft Windows утилита позволяет настроить регулярный автоматический запуск планов обслуживания JMS.

Утилита расположена в каталоге установки JMS Server, по умолчанию:

c:\Program Files\Enterprise Management System Server\Aladdin.EAP.MaintenancePlanRunner.exe.

Утилита **Aladdin.EAP.MaintenancePlanRunner.exe** используется для управления процессом запуска плана обслуживания. Используя Планировщик заданий из состава Microsoft Windows, можно настроить автоматический регулярный запуск планов обслуживания JMS.

Конфигурационный файл **Aladdin.EAP.MaintenancePlanRunner.exe.config** утилиты расположен в той же папке, что и сама утилита.

3.15.12.2Автоматическая генерация параметров запуска утилиты MaintenancePlanRunner

В некоторых планах обслуживания, предусматривающих ограничение сферы их действия за счет выбора контейнера ресурсной системы и доменных и глобальных групп (на данный момент это планы обслуживния пользователей и рабочих станций, а также **План обслуживания жизненного цикла OTP-токенов**), администратору предоставляется сервис автоматической генерации параметров запуска утилиты *MaintenancePlanRunner*.

Для получения таких параметров выполните следующие действия (приведены на примере **Плана обслуживания пользователей**).

1. Запустите план обслуживания на выполнение. Для этого в разделе **Планы обслуживания** выберите соответствующий план (например, **План обслуживания пользователей**) и в верхней панели нажмите **Добавить в очередь** (Рис. 378, с. 404).
   Отобразится окно следующего вида.

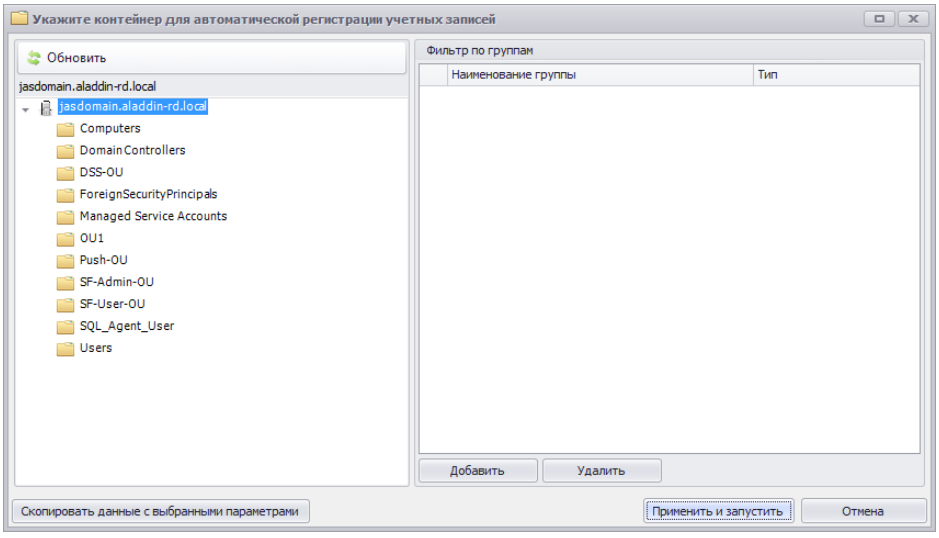


Рис. 387 – Окно ограничения области действия плана обслуживания

2. Выполните настройку в окне ограничения области действия плана обслуживания так, как это описано в разделе «Запуск и просмотр результатов планов обслуживания из Консоли управления JMS», с. 405, до шага запуска плана обслуживания (т.е. до нажатия на кнопку

Применить и запустить), после чего нажмите **Скопировать данные с выбранными параметрами**. При этом параметры запуска утилиты *MaintenancePlanRunner* будут скопированы в буфер обмена.

3. В любом текстовом редакторе вставьте из буфера обмена текстовое содержимое следующего вида:

```
Информация о выбранном контейнере:

Имя ресурсной системы:           jasdomain.aladdin-rd.local
Идентификатор ресурсной системы: 1
Имя контейнера:                  Users
Идентификатор контейнера:        3590bcab-f394-4952-8b7e-733502e664b6

Для запуска плана обслуживания из командной строки используйте следующие параметры:
Aladdin.EAP.MaintenancePlanRunner.exe -run 12860255-34a2-67a1-2027-83644a5f39ba
"OtpSyncActionBase.AccountSystemName=jasdomain.aladdin-
rd.local;OtpSyncActionBase.ParentObjectId=3590bcab-f394-4952-8b7e-733502e664b6"
```

4. Используйте предоставленные параметры при настройке автоматического регулярного запуска данного плана обслуживания (см. раздел «Настройка автоматического регулярного запуска», ниже)

3.15.12.3Настройка автоматического регулярного запуска

Чтобы настроить автоматический запуск плана обслуживания по расписанию, выполните следующие действия.

Для успешной настройки на сервере JMS должна быть запущена служба **Планировщик заданий.** Кроме того, настройка задания на автоматический запуск утилиты MaintenancePlanRunner в планировщике заданий из состава Microsoft Windows должна производиться от имени пользователя с полномочиями администратора.

Описание приводится на примере Microsoft Windows Server 2012 R2.

1. Запустите планировщик заданий Microsoft Windows (для этого в панели управления выберите **Администрирование -> Планировщик заданий**).

Отобразится следующее окно.

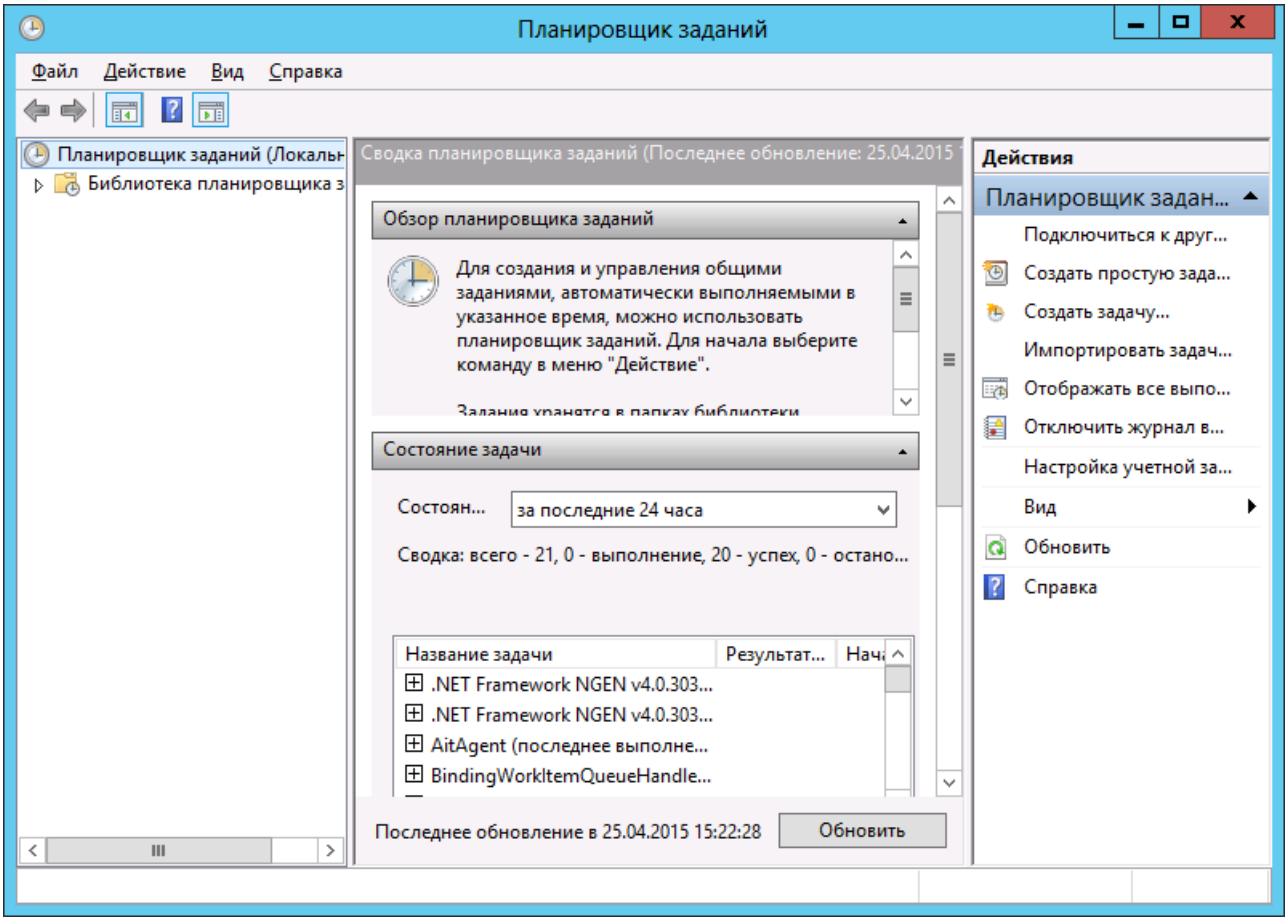


Рис. 388 – Планировщик заданий

2. В верхнем меню выберите **Действие -> Создать задачу**.

Отобразится следующее окно.

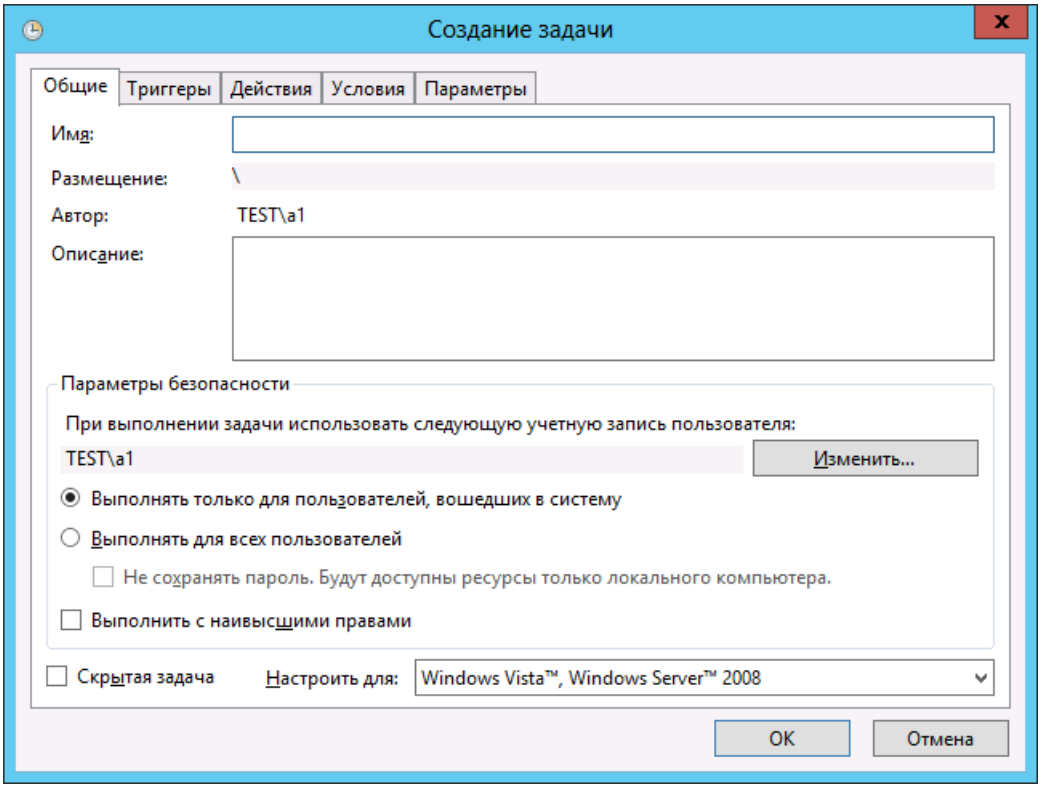


Рис. 389 – Окно создания задачи

3. В полях **Имя** и **Описание** введите соответственно имя и описание создаваемой задачи.
4. В секции **Параметры безопасности** нажмите **Изменить** и в отобразившемся окне укажите учетную запись, от имени которой будет осуществляться запуск утилиты планов обслуживания.

⚠ Для корректного выполнения автоматического запуска планов обслуживания необходимо, чтобы процесс запускался от имени одной из следующих учетных записей **SYSTEM** (Система), **LOCAL SERVICE** (Локальная служба), **NETWORK SERVICE** (Сетевая служба). Автоматический запуск также может выполняться от имени учетной записи оператора JMS, однако этот вариант не рекомендуется, так как предполагает хранение пароля оператора JMS в реестре (хоть и в зашифрованном виде).

5. В окне выбора учетной записи нажмите **OK**.
6. В окне создания задачи на автоматический запуск плана обслуживания перейдите на вкладку **Триггеры**.

Окно примет следующий вид.

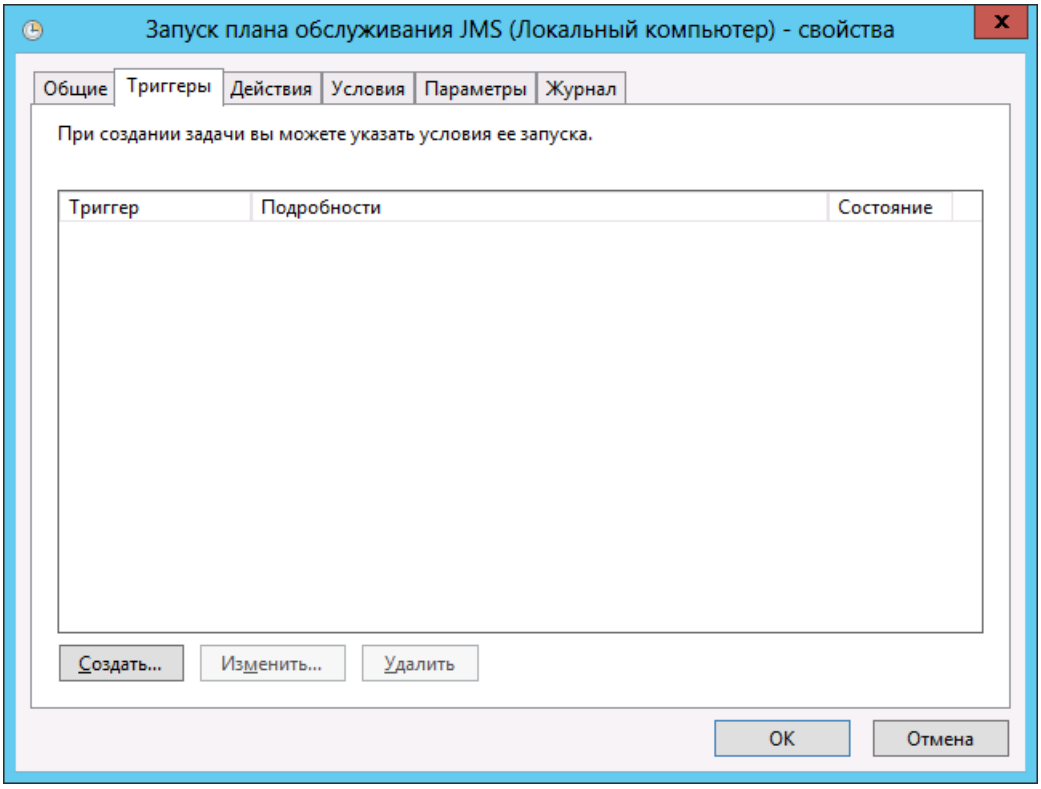


*Рис. 390 – Вкладка **Триггеры***

7. Нажмите **Создать**.

Отобразится следующее окно.

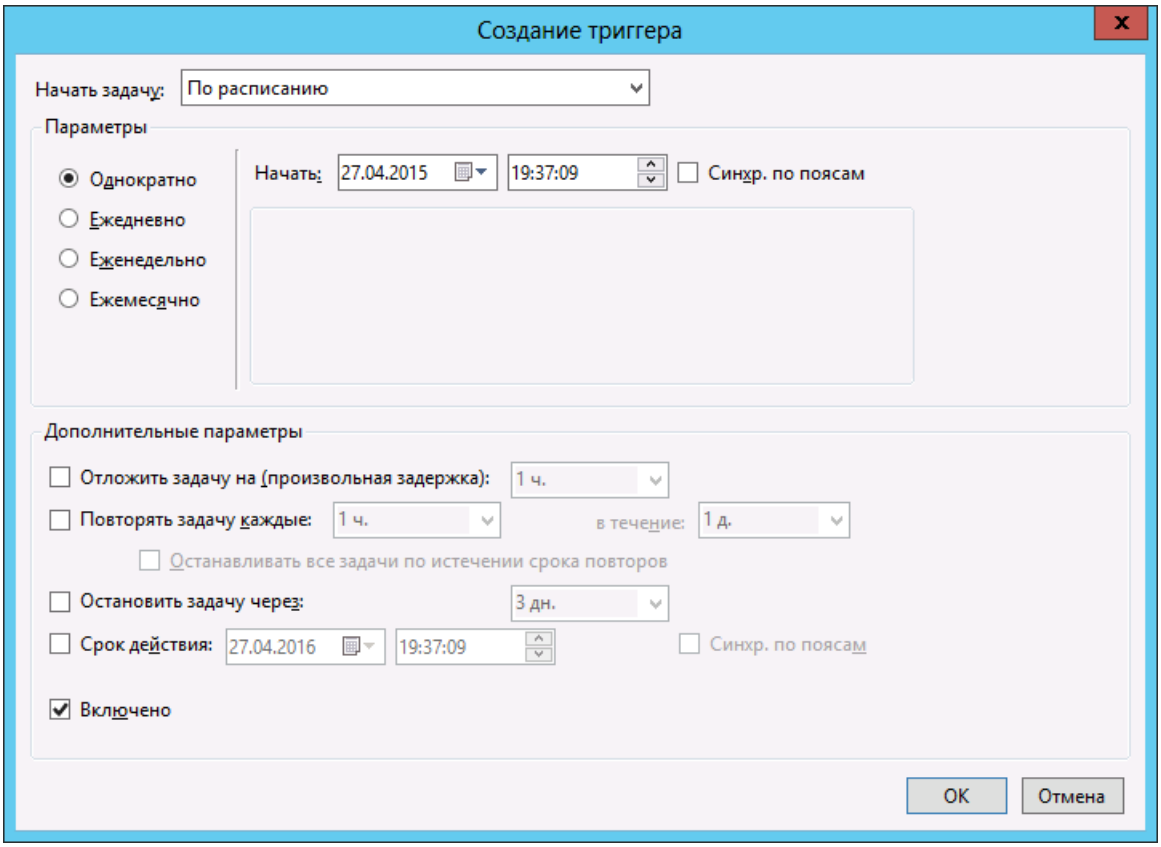


Рис. 391 – Выбор периодичности запуска

8. Настройте периодичность запуска плана обслуживания.

Рекомендуется установить следующие время и периодичность запуска планов обслуживания - ежедневно в нерабочее время, когда на сервер приходится минимальная нагрузка, например, в 3:30 ночи. Также, план обслуживания по умолчанию следует запускать перед планом обслуживания ключевых носителей.

Окно создания триггера после настройки будет выглядеть следующим образом.

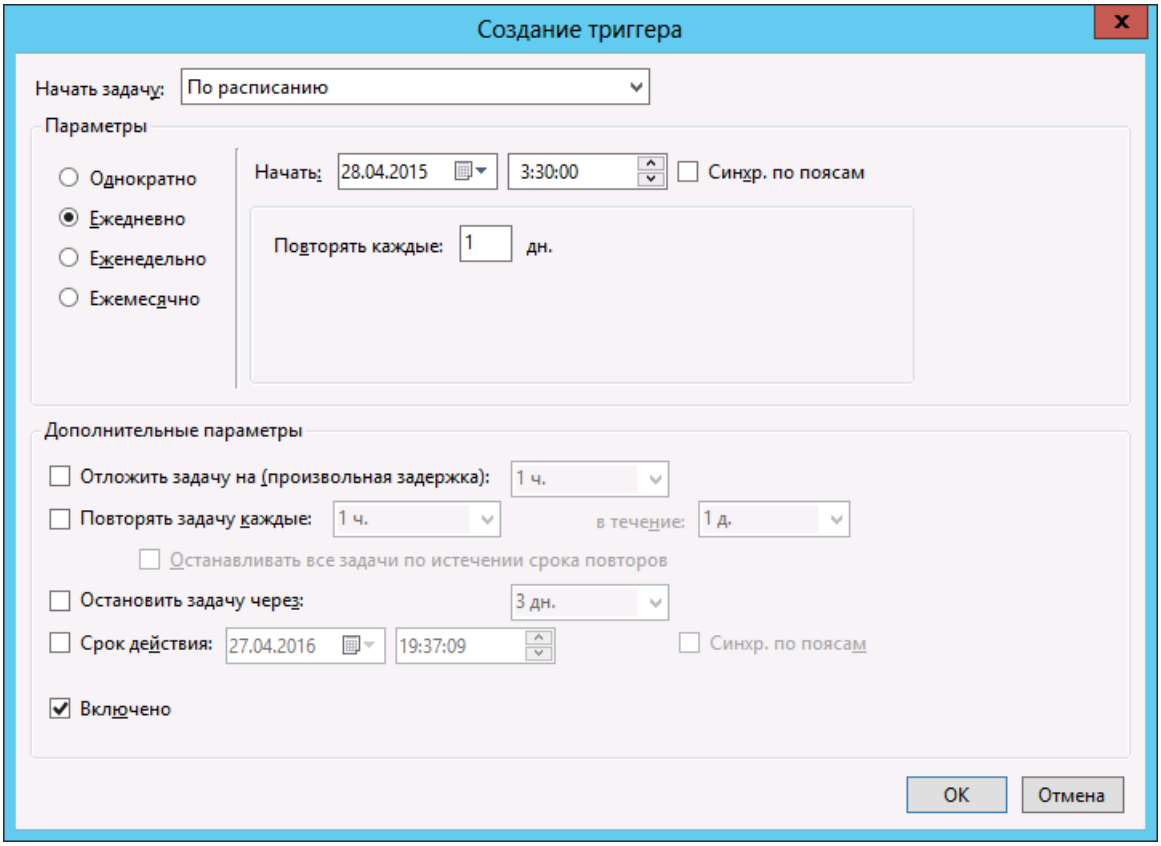


Рис. 392 – Время и периодичность запуска плана обслуживания

9. Нажмите **OK** и в окне создания задачи на автоматический запуск плана обслуживания перейдите на вкладку **Действия**.

Окно примет следующий вид.

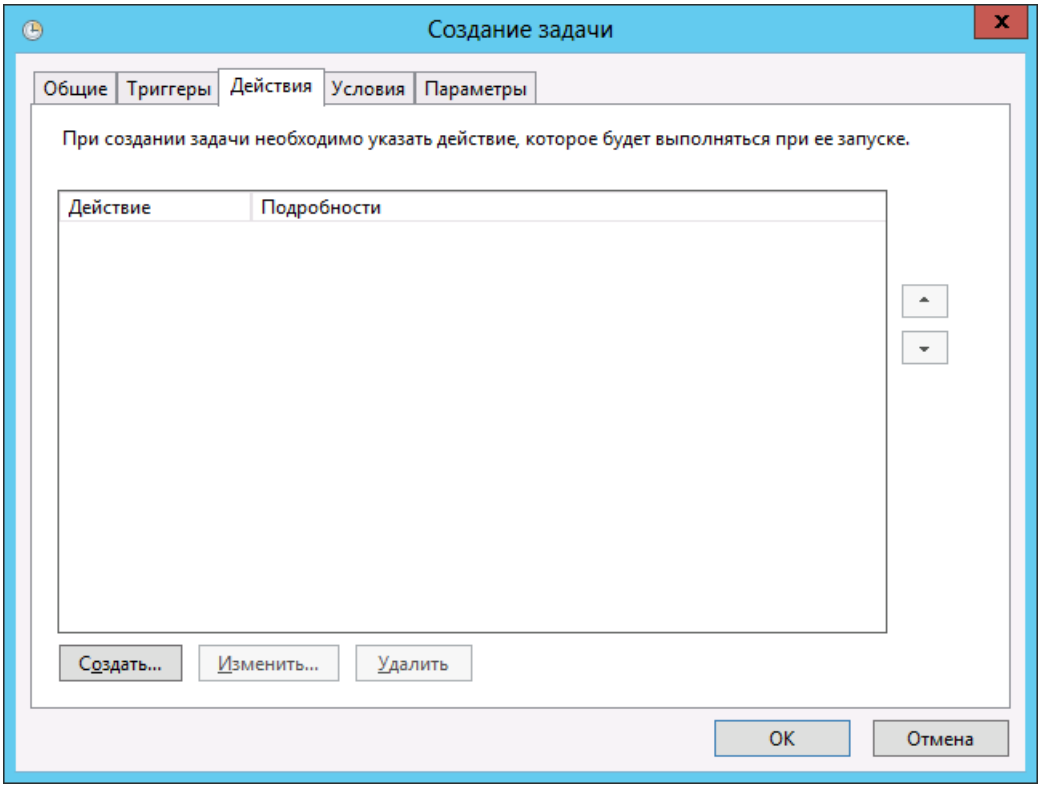


Рис. 393 – Параметры ежедневного запуска задания

10. Нажмите **Создать**.

Отобразится следующее окно.

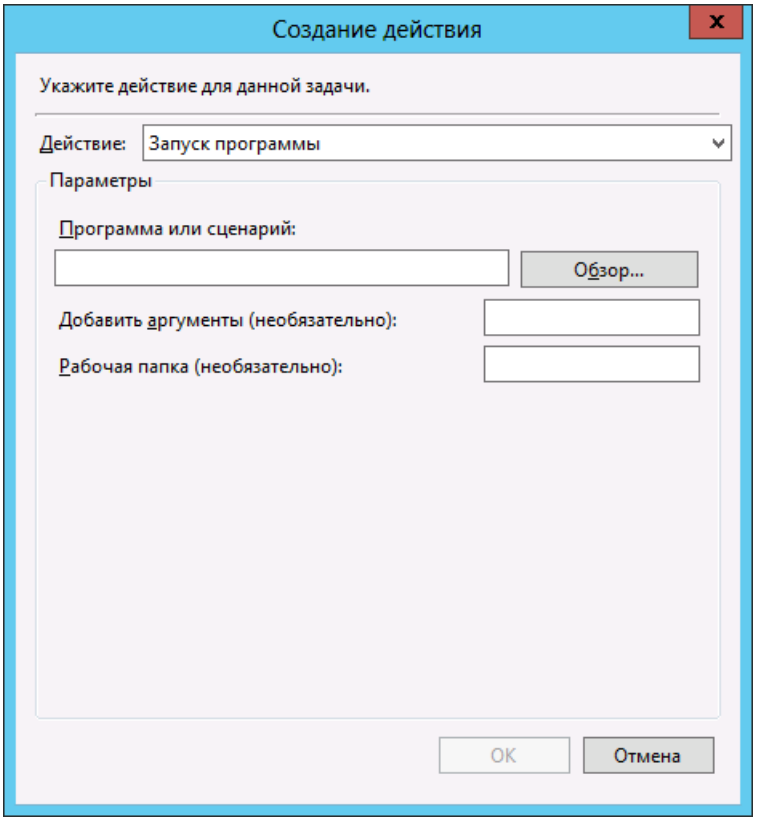


Рис. 394 – Выбор действия для задачи

11. В списке **Действие** оставьте выбранным пункт Запуск программы, после чего выполните настройки, руководствуясь табл. 93.

Табл. 93 – Параметры автоматического регулярного запуска плана обслуживания JMS

Настройка	Описание
Программа или сценарий	Укажите в этом поле путь к утилите запуска планов обслуживания. Если компонент JMS Server был установлен в каталог по умолчанию, утилита находится по следующему пути: **c:\Program Files\Enterprise Management System Server\Aladdin.EAP.MaintenancePlanRunner.exe**
Добавить аргументы	В этом поле введите: **-run <значение>** где <значение> - идентификатор плана обслуживания: • 553AA527-94C4-40EF-84BE-1DE5B4BFB7A7 – план обслуживания по умолчанию; • 4578A30A-E423-F2EF-B235-75E564B8B679 – план обслуживания ключевых носителей; • B786028A-22AA-47AE-A024-C36F4AFF19FC – план обслуживания сертификатов; • 3288FD0D-2F4B-412A-BD8C-292A1E11FC05 – план обслуживания рабочих станций; • 78960243-7a21-62aa-a02b-73622a5f39b1 – план обслуживания пользователей; • 12860255-34a2-67a1-2027-83644a5f39ba – план обслуживания жизненного цикла OTP-токенов; • 6239de18-3c2b-4c99-884e-b833cc841c8c - План обслуживания настроек личного кабинета; • 55960255-1521-56AA-8025-E36AAFFF39B2 – План обслуживания СКЗИ. **Примечания:**

Настройка	Описание
	1. Если вы настраиваете автоматический запуск плана обслуживания по умолчанию, идентификатор плана обслуживания указывать необязательно – достаточно указать аргумент **-run**. 2. Если план обслуживания применяется только к выбранным контейнерам (например, **План обслуживания жизненного цикла OTP-токенов** или **План обслуживания пользователей/рабочих станций**), то для удобства можно воспользоваться готовыми параметрами, полученными в окне выбора контейнера (подробнее см. раздел «Автоматическая генерация параметров запуска утилиты MaintenancePlanRunner», с. 422)
Рабочая папка	В этом поле укажите рабочий каталог установки JMS Server. По умолчанию этот каталог расположен по следующему пути: **c:\Program Files\Enterprise Management System Server** Если в поле **Программа или сценарий** вы указали полный путь к утилите планов обслуживания, это поле можно не заполнять.

12. Нажмите **OK**.
Созданное действие отобразится в окне **Создание задачи** (см. рис. 395).

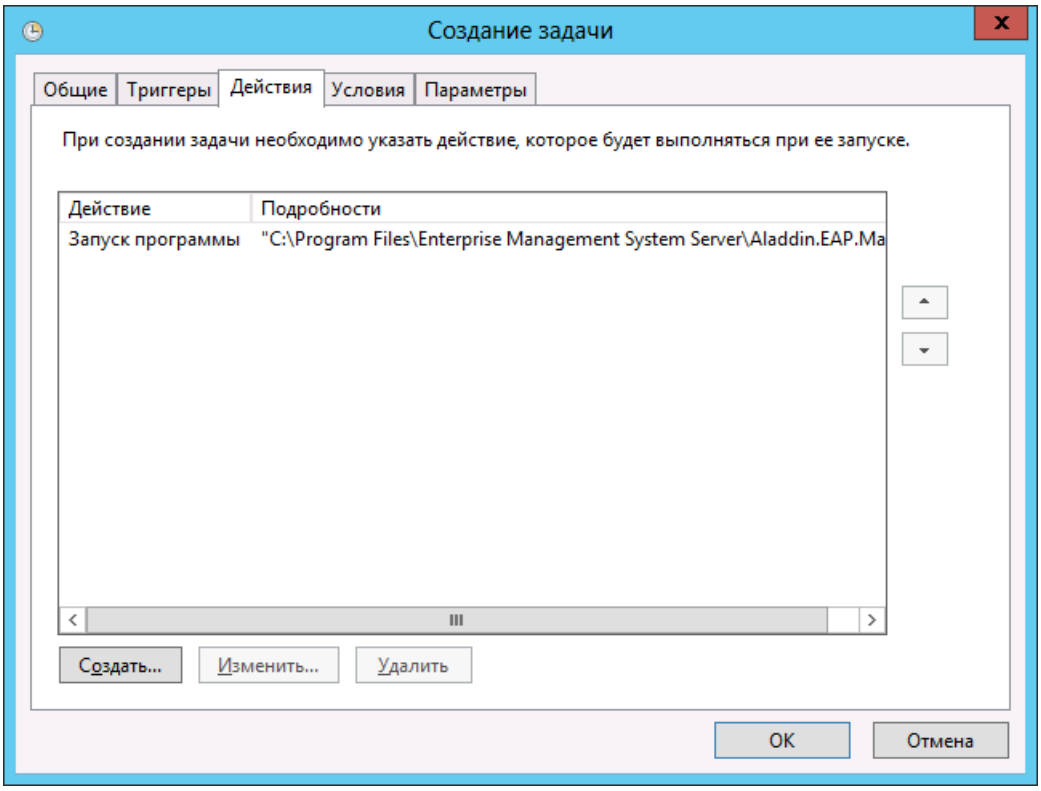


Рис. 395 – Действие отображено в списке

13. Нажмите **OK**.
Созданная задача отобразится в библиотеке планировщика заданий (см. рис. 396).

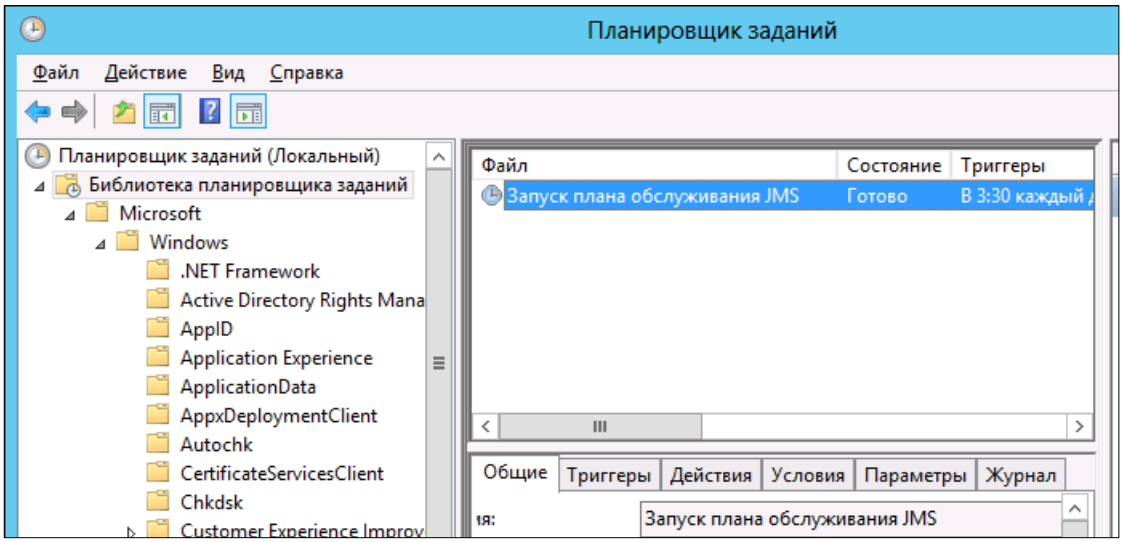


Рис. 396 – Библиотека планировщика заданий

Результаты выполнения планов обслуживания можно посмотреть в интерфейсе консоли управления JMS (см. «Запуск и просмотр результатов планов обслуживания из Консоли управления JMS», с. 405).

3.15.12.4Автоматическая организация очередей выполнения заданий планов обслуживания

Утилита MaintenancePlanRunner позволяет организовывать очередь выполнения заданий планов обслуживания. Очередь организуется в порядке поступления заявок на выполнение (в порядке последовательных запусков команды MaintenancePlanRunner).

При этом в очередь могут быть поставлены несколько заданий на выполнение одного и того же плана обслуживания (например с разными параметрами).

3.16 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

3.16.1 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. 397).

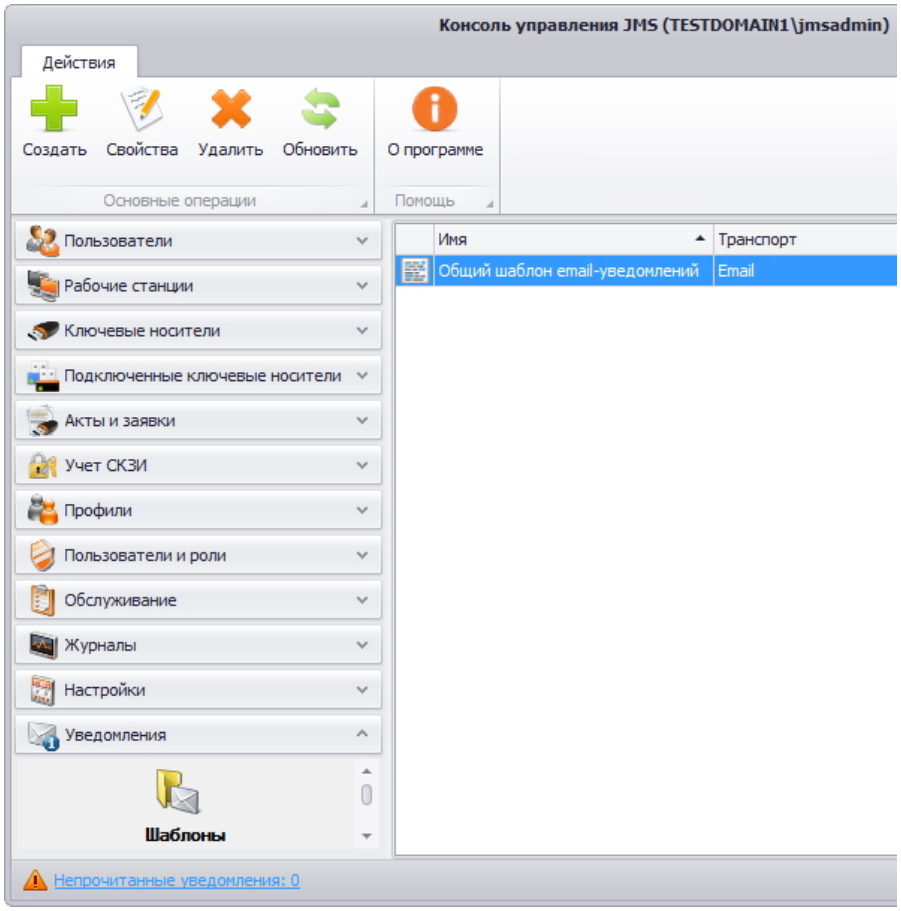


Рис. 397 – Список доступных шаблонов уведомлений

Шаблон уведомлений представляет собой HTML-файл, содержащий переменные, которые заменяются соответствующими значениями события JMS. На рис. 398 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. 398 – Шаблон уведомлений по умолчанию

В шаблонах уведомлений о событиях JMS можно использовать шесть переменных (см. табл. 94) – все они включены в стандартный шаблон из состава JMS (**Общий шаблон email-уведомлений**).

Табл. 94 – 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. рис. 398, с. 433 и табл. 94, с. 434);
- отредактировать стандартный шаблон уведомлений (**Общий шаблон email-уведомлений**) – для этого вам следует экспортировать стандартный шаблон (см. «Экспорт шаблона уведомлений из JMS», с. 434), внести изменения, после чего импортировать отредактированный шаблон в JMS (см. «Загрузка/замена шаблонов уведомлений в JMS», с. 435);
- создать шаблон уведомлений вручную, после чего импортировать его в JMS (см. «Загрузка/замена шаблонов уведомлений в JMS», с. 435).

По завершении подготовки шаблона уведомлений переходите к настройке параметров рассылки административных и пользовательских уведомлений – см. «Настройка рассылки административных/пользовательских уведомлений», с. 437.

3.16.1.1 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»).

3.16.1.2 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 верхней панели нажмите **Создать**.
   – если вы хотите отредактировать шаблон уведомлений, уже загруженный в JMS (например, **Общий шаблон email-уведомлений**), выберите этот шаблон и в верхней панели нажмите **Свойства**.

   Отобразится следующее окно.

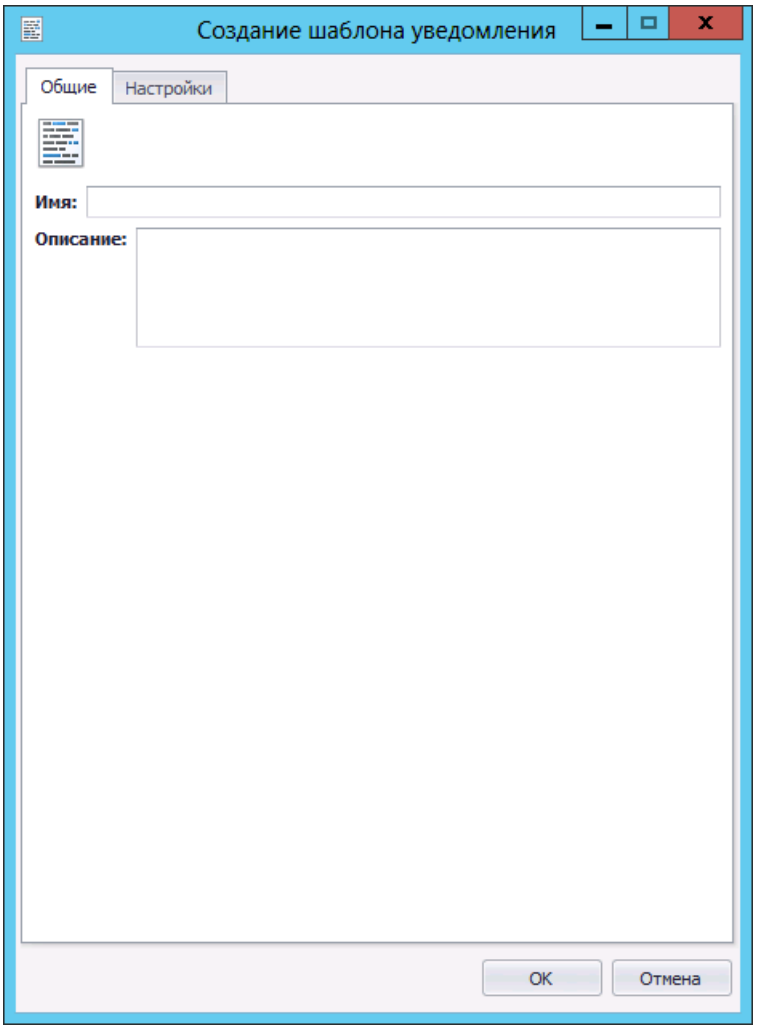


*Рис. 399 – Вкладка **Общие** окна свойств создаваемого/заменяемого шаблона уведомлений*

3. Введите/отредактируйте в соответствующих полях имя и описание создаваемого/заменяемого шаблона, после чего перейдите на вкладку **Настройки**.

Окно примет следующий вид.

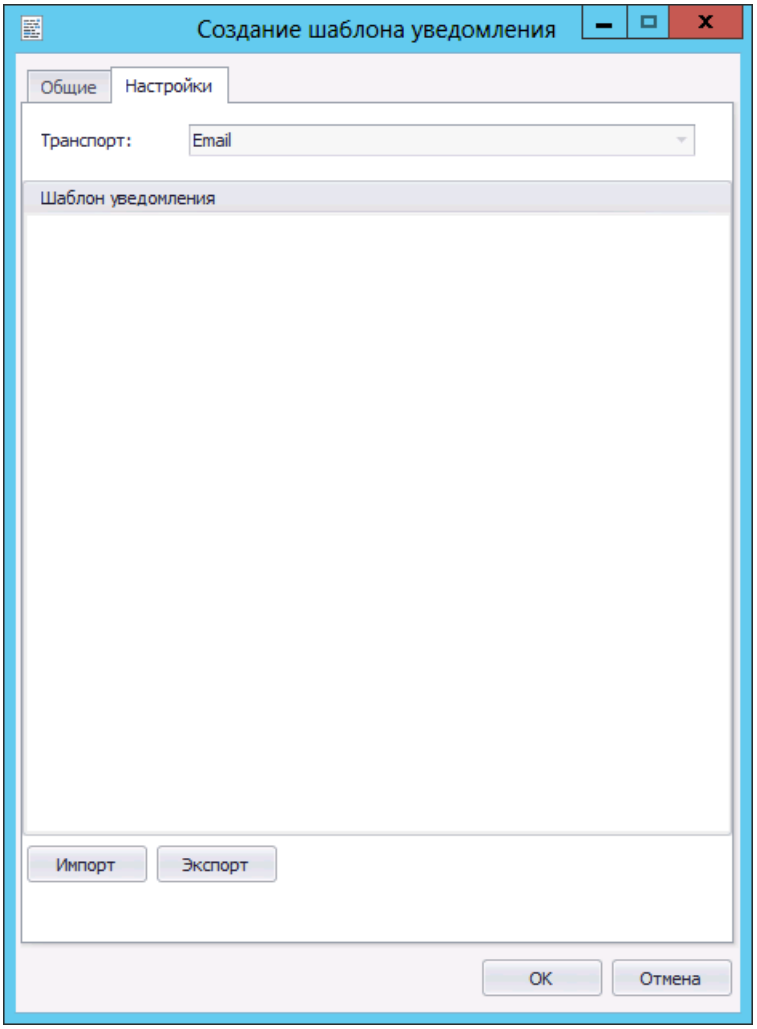


*Рис. 400 – Вкладка **Настройки** окна свойств создаваемого/заменяемого шаблона уведомлений*

4. Чтобы загрузить новый шаблон, нажмите **Импорт**, после чего укажите путь к созданному шаблону уведомлений.

Если вы заменяете уже существующий шаблон, он будет отображен в секции **Шаблон уведомления**.

Новый шаблон отобразится в окне.

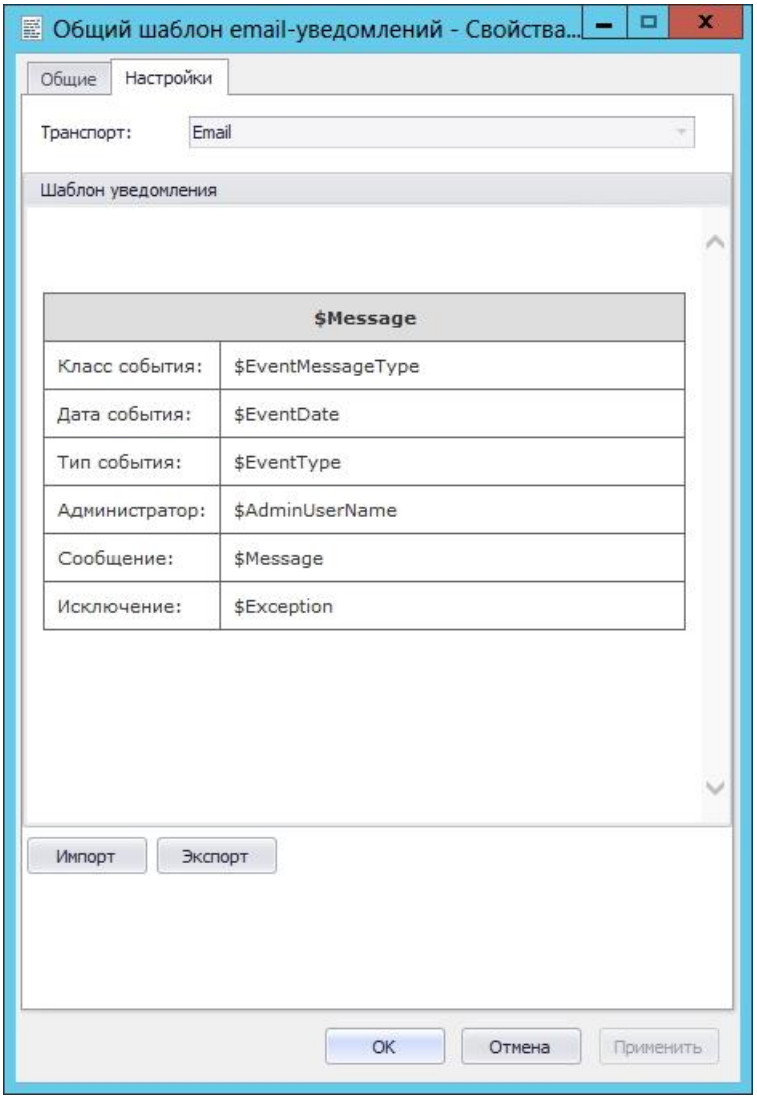


*Рис. 401 – Шаблон уведомлений отображается на вкладке **Настройки***

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

3.16.2 Настройка рассылки административных/пользовательских уведомлений

В JMS поддерживаются уведомления для следующих категорий событий:

- журнал аудита;
- предупреждения;
- клиентские события.

Так же уведомления делятся на две группы – пользовательские и административные (см. рис. 402). 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 тоже 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. 95).

Для категории событий **Предупреждения** и категории **Клиентские события** поддерживаются только административные уведомления.

Табл. 95 – Группы уведомлений

Пользовательские уведомления	Административные уведомления
• Журнал аудита (часть событий журнала)	• Журнал аудита (все события журнала) • Предупреждения • Клиентские события

Одно или несколько уведомлений могут быть отражены в правилах рассылки.

Чтобы создать или отредактировать правило рассылки уведомлений о событиях JMS, выполните следующие действия:

В правилах рассылки административных/пользовательских уведомлений по умолчанию отсутствуют события, по наступлении которых отправляются уведомления. Таким образом, если вы собираетесь использовать правила по умолчанию, необходимо их отредактировать, отметив те события, по наступлении которых будут рассылаться уведомления.

1. В консоли управления JMS перейдите в раздел. **Уведомления -> Административные правила рассылки/Пользовательские правила рассылки** (см. рис. 402).

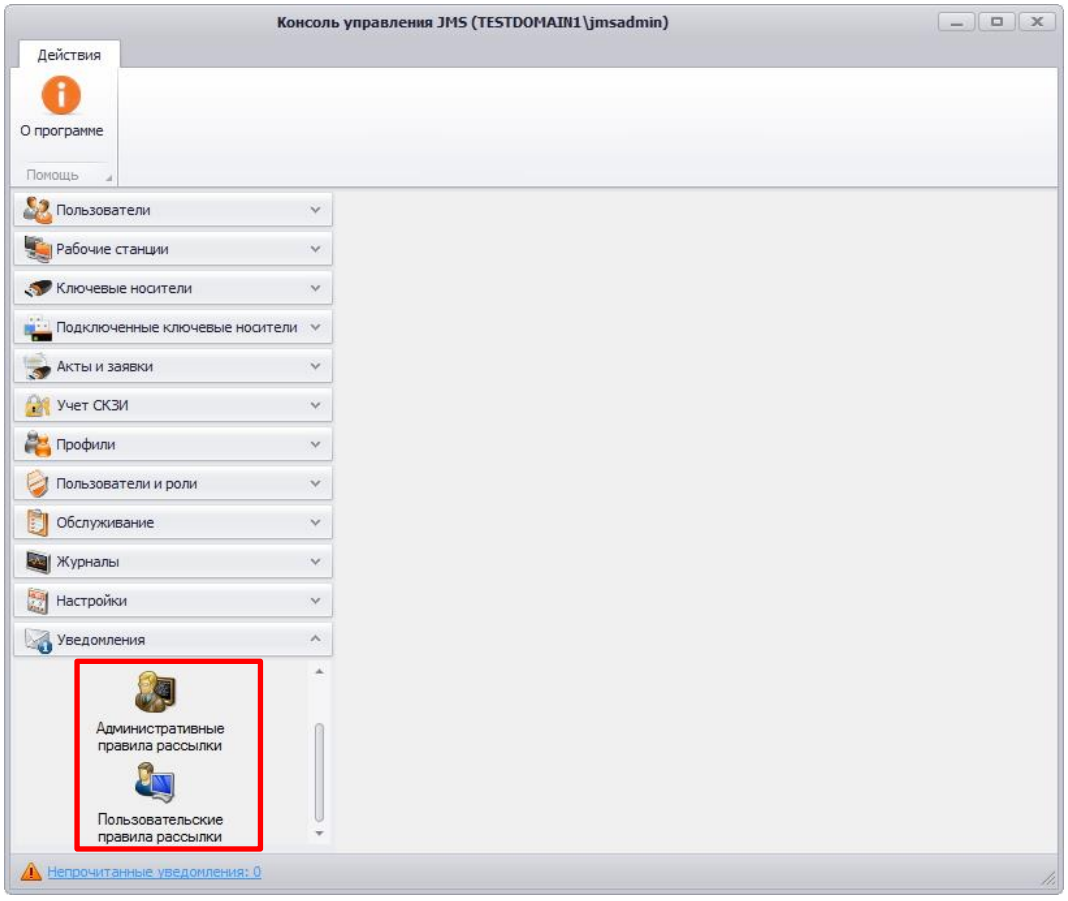


*Рис. 402 – Вкладка **Уведомления***

2. Выполните одно из следующих действий:

   - если вы хотите отредактировать существующее правило, выберите его в центральной части окна и в верхней панели нажмите **Свойства**.
   - если вы хотите создать новое правило, в верхней панели нажмите **Создать** (см. рис. 403).

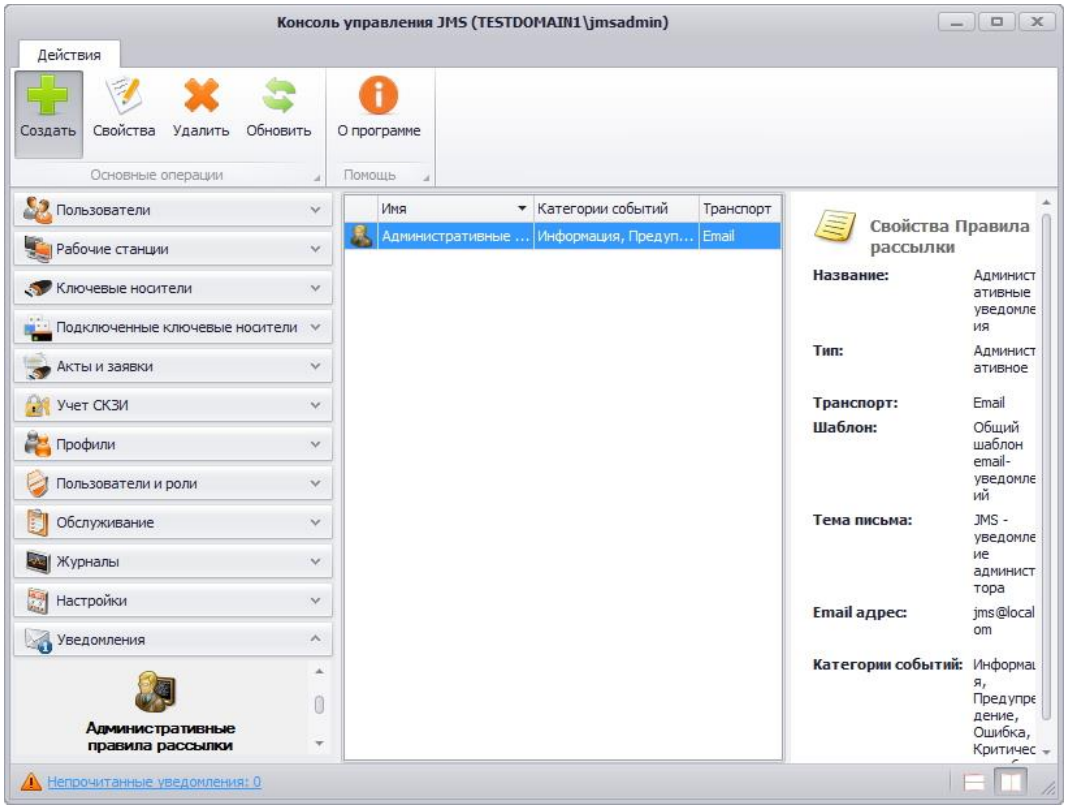


*Рис. 403 – Вкладка **Уведомления – Административные правила рассылки***

В случае выбора опции **Административные правила рассылки** отобразится окно следующего вида (см. рис. 404).

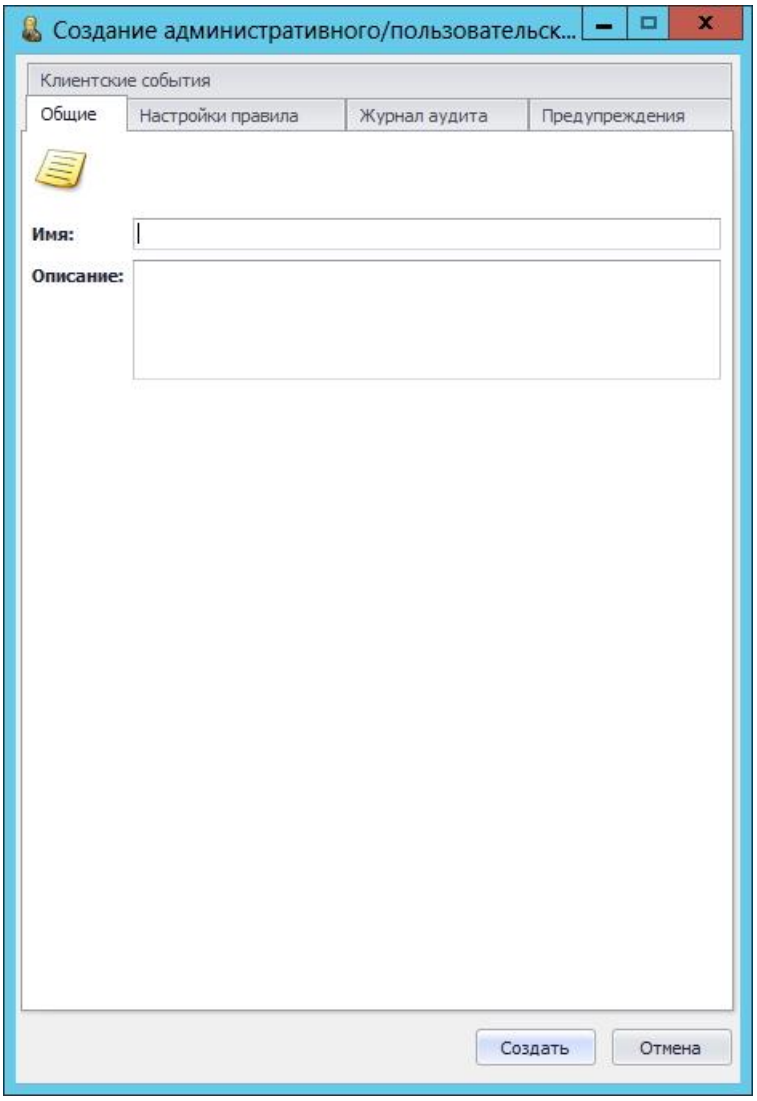


*Рис. 404 – Вкладка **Общие***

3. Введите или отредактируйте имя и описание правила рассылки уведомлений в соответствующих полях, после чего перейдите на вкладку **Настройки правила**.

Окно примет следующий вид.

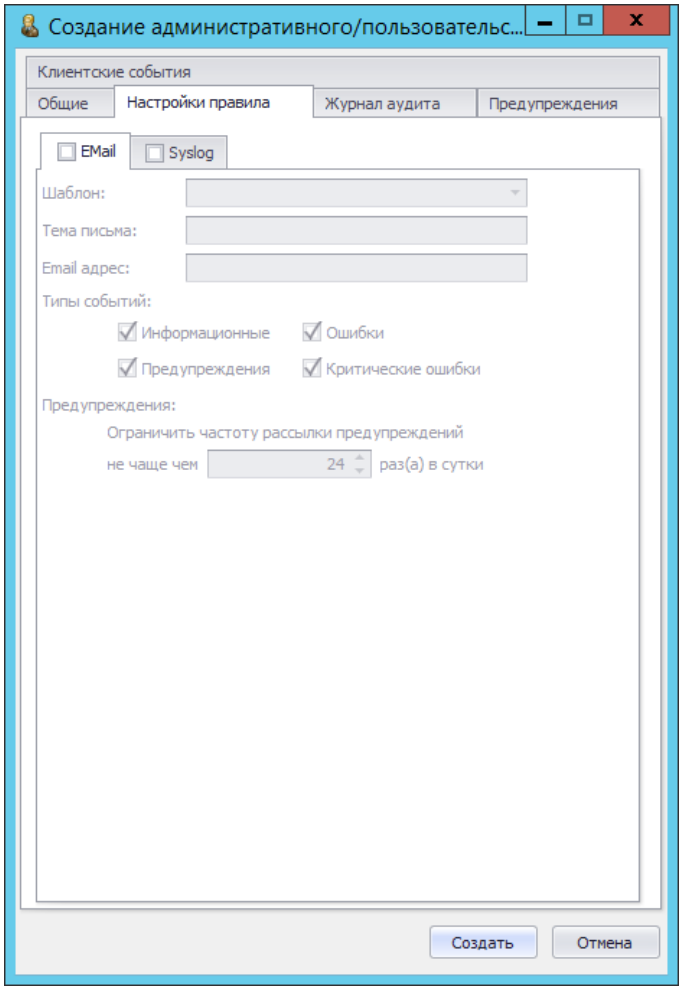


*Рис. 405 – Вкладка **Настройки правила** в части Email-транспорта*

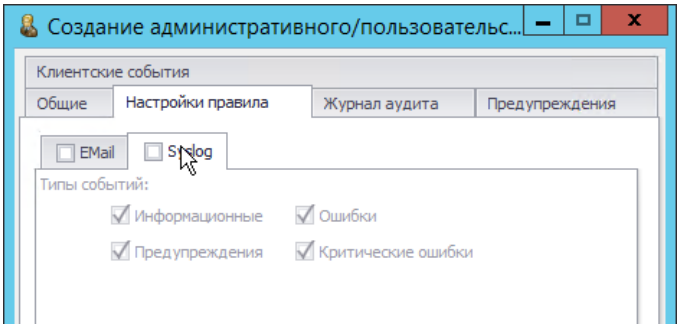


*Рис. 406 – Вид вкладки **Настройки правила** в части Syslog-транспорта*

4. Выполните настройку, руководствуясь табл. 96.

Табл. 96 – Настройка правила уведомлений о событиях JMS

Настройка	Описание
Email	Установите флаг, если в качестве одного из транспортов уведомлений следует использовать электронную почту.

Настройка	Описание
	Примечание. Для обеспечения работы уведомлений по электронной почте в серверном агенте JMS должен быть настроен соответствующий транспорт (см. описание вкладки **Настройка** -> **Настройка транспорта** –> **Настройка SMTP** в руководстве по установке и настройке JMS [2])
Syslog	Установите флаг, если в качестве одного из транспортов уведомлений следует использовать сервер Syslog. **Примечание.** Для обеспечения передачи уведомлений в сервер Syslog в серверном агенте JMS должен быть настроен соответствующий транспорт (см. описание вкладки **Настройка** -> **Настройка транспорта** –> **Настройка Syslog** в руководстве по установке и настройке JMS [2])
Шаблон (только для Email-транспорта)	Подготовленный шаблон уведомлений (см. «Шаблоны уведомлений», с. 433).
Тема письма (только для Email-транспорта)	Текст, который будет отображаться в поле **Тема** сообщения электронной почты.
Email адрес (только для Email-транспорта)	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.
Типы событий	Позволяет отметить, при наступлении каких типов событий будет отправляться уведомление: • **Информационные**; • **Ошибки**; • **Предупреждения**; • **Критические ошибки**.
Предупреждения (только для Email-транспорта)	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.

5. Перейдите на вкладку **Журнал аудита**.

Окно примет следующий вид.

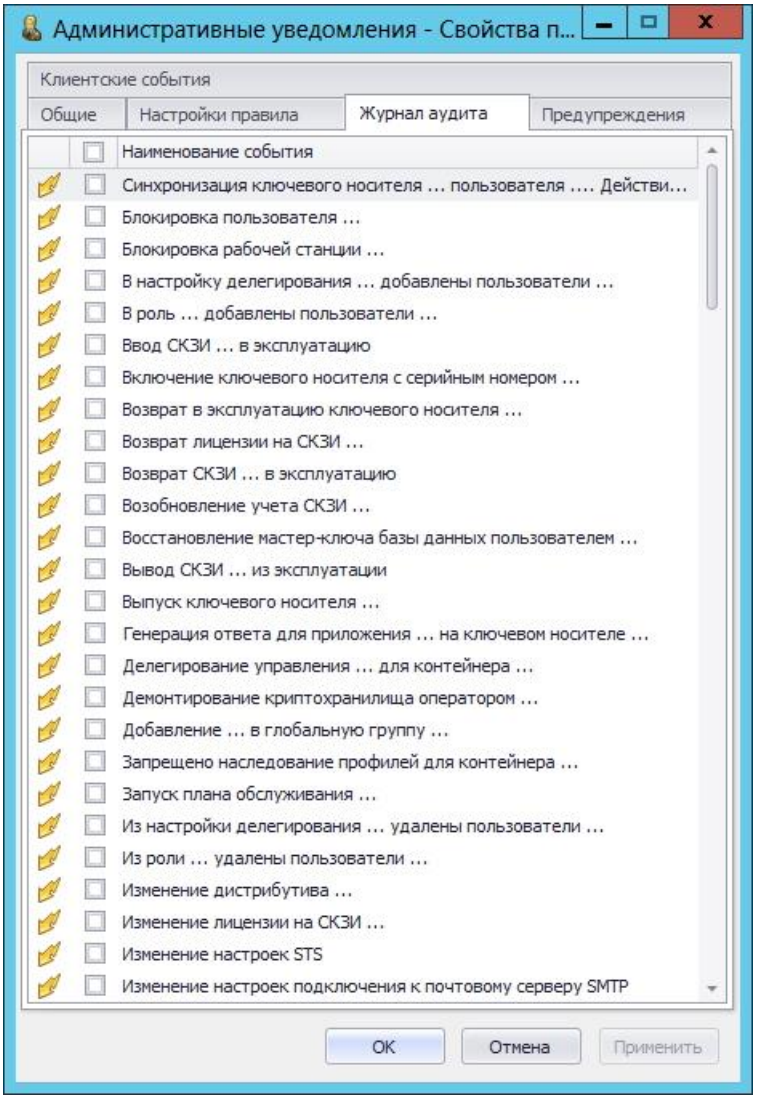


*Рис. 407 – Вкладка **Журнал аудита***

6. Установите флаги напротив событий, по поводу которых вы хотите получать уведомления (чтобы отметить все события, установите флаг напротив пункта **Наименование события**).

Чтобы уведомление было отправлено, тип отмеченного события должен совпадать с одним из типов, отмеченным на вкладке **Настройки правила** (см. табл. 96, с. 441). Например, если на вкладке **Настройки правила** в секции **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. Нажмите **OK**, чтобы сохранить изменения.

Список событий на вкладке **Журнал аудита** представлен в таблице 97 .

Табл. 97 – Список событий на вкладке Журнал аудита

Наименование события	Административные уведомления	Пользовательские уведомления
Синхронизация ключевого носителя … пользователя … Действий по синхронизации не потребовалось	Да	Да
Блокировка пользователя …	Да	Да
Блокировка рабочей станции …	Да	Нет
В настройку делегирования … добавлены пользователи …	Да	Нет
В роль … добавлены пользователи …	Да	Нет
Ввод СКЗИ … в эксплуатацию	Да	Нет
Включение ключевого носителя с серийным номером …	Да	Да
Возврат в эксплуатацию ключевого носителя …	Да	Да
Возврат лицензии на СКЗИ …	Да	Нет
Возврат СКЗИ … в эксплуатацию	Да	Нет
Возобновление учета СКЗИ …	Да	Нет
Восстановление мастер-ключа базы данных пользователем …	Да	Нет
Вывод СКЗИ … из эксплуатации	Да	Нет
Выпуск ключевого носителя …	Да	Да
Генерация ответа для приложения … на ключевом носителе	Да	Да
Делегирование управления … для контейнера …	Да	Нет
Демонтирование криптохранилища оператором …	Да	Нет
Добавление … в глобальную группу …	Да	Нет
Запрещено наследование профилей для контейнера …	Да	Нет
Запуск плана обслуживания …	Да	Нет
Из настройки делегирования … удалены пользователи …	Да	Нет
Из роли … удалены пользователи …	Да	Нет
Изменение дистрибутива …	Да	Нет
Изменение лицензии на СКЗИ …	Да	Нет

Наименование события	Административные уведомления	Пользовательские уведомления
Изменение настроек STS	Да	Нет
Изменение настроек подключения к почтовому серверу SMTP	Да	Нет
Изменение настроек регистрации каталога учетных записей	Да	Нет
Изменение настройки делегирования …	Да	Нет
Изменение пароля пользователя …	Да	Да
Изменение роли …	Да	Нет
Изменение свойства привязки профиля … к контейнеру …	Да	Нет
Изменение СКЗИ …	Да	Нет
Изменение шаблона печати …	Да	Нет
Импорт ключевого носителя … с идентификатором …	Да	Нет
Импорт резервной копии сертификата (субъект: … , отпечаток: …) . Сертификат выпущен на ключевой носитель … , принадлежащий пользователю …	Да	Нет
Импорт экземпляра профиля …	Да	Нет
Миграция ключевого носителя … из контейнера … в новый контейнер …	Да	Нет
Модификация экземпляра профиля …	Да	Нет
Монтирование криптохранилища оператором …	Да	Нет
Назначение дистрибутива … экземпляру СКЗИ …	Да	Нет
Назначение ключевого носителя … пользователю …	Да	Да
Назначение лицензии на СКЗИ …	Да	Нет
Назначение СКЗИ …	Да	Нет
Настроено делегирование управления … для контейнера …	Да	Нет
Обновление атрибутов внедоменной рабочей станции …	Да	Нет
Обновление глобальной группы …	Да	Нет
Обновление немашиночитаемых атрибутов ключевого носителя …	Да	Нет
Обновление правила рассылки уведомлений …	Да	Нет

Наименование события	Административные уведомления	Пользовательские уведомления
Обновление шаблона уведомлений ...	Да	Нет
Отвязка пользователя ... от учетной записи ресурсной системы ...	Да	Да
Отзыв ключевого носителя ... по причине ...	Да	Да
Отзыв ключевого носителя ... по причине ... с восстановлением на ключевом носителе ...	Да	Да
Отзыв мастера-ключа базы данных оператором ...	Да	Нет
Отключение ключевого носителя с серийным номером ...	Да	Да
Отключение принудительного входа по смарт-карте для пользователя ...	Да	Да
Отмена временного доступа по паролю для пользователя ...	Да	Да
Отмена назначения дистрибутива ... от экземпляра СКЗИ ...	Да	Нет
Отмена опции принудительной смены PIN-кода для приложения ... на ключевом носителе ... , принадлежащем пользователю ...	Да	Да
Ошибка выпуска ключевого носителя ...	Да	Да
Ошибка синхронизации ключевого носителя ...	Да	Да
План обслуживания ... завершен с ошибками	Да	Нет
План обслуживания ... успешно завершен	Да	Нет
План обслуживания ... успешно отменен	Да	Нет
Получение PIN-кода администратора для приложения ... на ключевом носителе ...	Да	Нет
Пользователь ... добавлен в роли ...	Да	Да
Пользователь ... удален из ролей ...	Да	Да
Пользователь ... удален из ролей ... и добавлен в роли ...	Да	Да
Пользователю отказано в выполнении операции ... - отсутствуют необходимые разрешения	Да	Нет
Пользователю отказано в выполнении операции ... - отсутствуют права на контейнер ...	Да	Нет
Предоставление временного доступа по паролю для пользователя ...	Да	Да

Наименование события	Административные уведомления	Пользовательские уведомления
Прекращение учета СКЗИ ...	Да	Нет
Привязка пользователя ... к учетной записи ресурсной системы ...	Да	Да
Привязка профиля ... к контейнеру ...	Да	Нет
Разблокировка пользователя ...	Да	Да
Разблокировка рабочей станции ...	Да	Нет
Разрешено наследование профилей для контейнера ...	Да	Нет
Регистрация внедоменной рабочей станции ...	Да	Нет
Регистрация дистрибутива ...	Да	Нет
Регистрация каталога учетных записей ...	Да	Нет
Регистрация ключевого носителя с серийным номером ...	Да	Нет
Регистрация лицензии на СКЗИ ...	Да	Нет
Регистрация новой лицензии ...	Да	Нет
Регистрация операторского сертификата для ...	Да	Нет
Регистрация пользователя ...	Да	Нет
Регистрация рабочей станции ...	Да	Нет
Регистрация типа СКЗИ ...	Да	Нет
Регистрация экземпляра профиля ...	Да	Нет
Резервное копирование мастер-ключа базы данных пользователем ...	Да	Нет
Сбой при добавлении в настройку делегирования ... пользователей ...	Да	Нет
Сбой при добавлении в роль ... пользователей ...	Да	Нет
Сбой при добавлении пользователя ... в роли ...	Да	Нет
Сбой при удалении из настройки делегирования ... пользователей...	Да	Нет
Сбой при удалении из роли ... пользователей ...	Да	Нет
Сбой при удалении пользователя ... из ролей ...	Да	Нет

Наименование события	Административные уведомления	Пользовательские уведомления
Сброс пароля пользователя …	Да	Да
Синхронизация ключевого носителя … пользователя …	Да	Да
Смена мастер-ключа оператором …	Да	Нет
Создание глобальной группы …	Да	Нет
Создание правила рассылки уведомлений …	Да	Нет
Создание роли …	Да	Нет
Создание СКЗИ …	Да	Нет
Создание шаблона печати …	Да	Нет
Создание шаблона уведомлений …	Да	Нет
Тиражирование дистрибутива …	Да	Нет
Удален сохраненный объект с ключевого носителя … пользователя … …	Да	Да
Удаление из глобальной группы …	Да	Нет
Удаление дистрибутива …	Да	Нет
Удаление лицензии …	Да	Нет
Удаление лицензии на СКЗИ …	Да	Нет
Удаление назначения ключевого носителя … пользователю …	Да	Нет
Удаление операторского сертификата для …	Да	Нет
Удаление плана обслуживания … из очереди на выполнение	Да	Нет
Удаление пользователя … из роли …	Да	Да
Удаление правила рассылки уведомлений	Да	Нет
Удаление регистрации ключевого носителя с серийным номером …	Да	Нет
Удаление регистрации пользователя …	Да	Да
Удаление регистрации рабочей станции …	Да	Нет
Удаление роли …	Да	Нет

Наименование события	Административные уведомления	Пользовательские уведомления
Удаление СКЗИ …	Да	Нет
Удаление типа СКЗИ …	Да	Нет
Удаление шаблона печати	Да	Нет
Удаление шаблона уведомлений	Да	Нет
Удаление экземпляра профиля …	Да	Нет
Уничтожение СКЗИ …	Да	Нет
Установка опции принудительной смены PIN-кода для приложения … на ключевом носителе … , принадлежащем пользователю …	Да	Да
Установка пароля для пользователя … Срок действия - …	Да	Нет
Установка PIN-кода администратора для приложения … на ключевом носителе …	Да	Нет
Установка принудительного входа по смарт-карте для пользователя …	Да	Нет
Физическая разблокировка ключевого носителя …	Да	Да
Экспорт дистрибутива …	Да	Нет
Экспорт ключевого носителя … с идентификатором …	Да	Нет
Экспорт лицензии на СКЗИ …	Да	Нет
Экспорт резервной копии сертификата (субъект: … , отпечаток: …). Сертификат выпущен на ключевой носитель … , принадлежащий пользователю …	Да	Нет
Экспорт экземпляра профиля …	Да	Нет

8. Перейдите на вкладку **Предупреждения**.

Окно примет следующий вид.

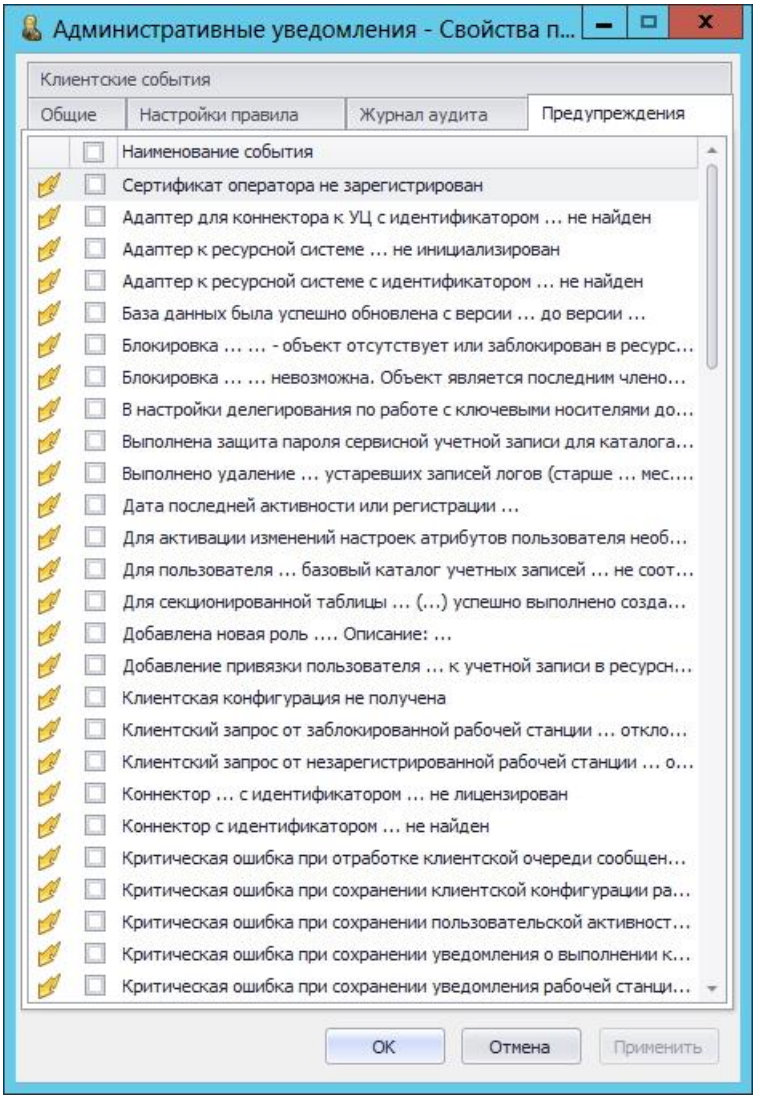


Рис. 408 – Вкладка Предупреждения

9. Установите флаги напротив событий, по поводу которых вы хотите получать уведомления (чтобы отметить все события, установите флаг напротив пункта **Наименование события**).

Чтобы уведомление было отправлено, тип отмеченного события должен совпадать с одним из типов, отмеченным на вкладке **Настройки правила** (см. табл. 96, с. 441). Например, если на вкладке **Настройки правила** в секции **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.

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

Список событий на вкладке **Предупреждения** представлен в таблице 98.

Табл. 98 – Список событий на вкладке Предупреждения

Наименование события
Сертификат оператора не зарегистрирован
Адаптер коннектора к УЦ с идентификатором … не найден
Адаптер к ресурсной системе … не найден
База данных была успешно обновлена с версии … до версии …
Блокировка … … - объект отсутствует или заблокирован в ресурсной системе
Блокировка … … невозможна. Объект является последним членом некоторых из системных ролей. Если объект был заблокирован в ресурсной системе рекомендуется его разблокировать
В настройки делегирования по работе с ключевыми носителями добавлена операция Ключевые носители:: Чтение
Выполнена защита пароля сервисной учетной записи для каталога учетных записей…
Выполнено удаление … устаревших записей логов (старше … мес.) из таблицы … (…).
Дата последней активности или регистрации…
Для активации изменений настроек атрибутов пользователя необходимо выполнить план обслуживания сервера
Для пользователя … базовый каталог учетных записей … не соответствует правилам привязки. Рекомендуется перерегистрировать пользователя вручную
Для секционированной таблицы … (…) успешно выполнено создание новой секции с границей … и удаление старой секции …
Добавлена новая роль … Описание: …
Добавление привязки пользователя … к учетной записи в ресурсной системе …
Клиентская конфигурация не получена
Клиентский запрос от заблокированной рабочей станции … отклонен
Клиентский запрос от незарегистрированной рабочей станции … отклонен
Коннектор … с идентификатором … не лицензирован
Коннектор с идентификатором … не найден
Критическая ошибка при отработке клиентской очереди сообщений рабочей станции
Критическая ошибка при сохранении клиентской конфигурации рабочей станции … Обновление конфигурации будет выполнено позднее
Критическая ошибка при сохранении пользовательской активности рабочей станции …

Наименование события
Критическая ошибка при сохранении уведомления о выполнении клиентской операции рабочей станции …
Критическая ошибка при сохранении уведомления рабочей станции…
Кумулятивная лицензия содержит несколько ресурсов … с различными типами валидации…
Лицензия не действительна
Мастер-ключ базы данных был отозван оператором …
Мастер-ключ базы данных был сменен оператором …
Не задана роль Пользователь
Не удалось зарегистрировать в БД существующие лицензии. Необходимо зарегистрировать лицензии вручную при помощи Агента
Не удалось обработать клиентское уведомление от рабочей станции … Информация - …
Не удалось сохранить информацию о свободных литерах дисков и пользователях для рабочей станции …
Недопустимый параметр ротации логов. Возможные значения периода хранения записей логов - 1-36 месяцев. Ротация лога … (…) невозможна
Неизвестное событие
Нет добавленных ролей
Оператор не обладает правом монтирования криптохранилища
Отзыв ключевого носителя … пользователя …в связи с истечением срока действия
Отзыв ключевого носителя … удаленного пользователя …
Отключение ключевого носителя … заблокированного пользователя …
Ошибка аутентификации … при обращении с рабочей станции …
Ошибка восстановления объектов ключевого носителя … из резервной копии
Ошибка переключений секций для таблицы … (…)
Ошибка при блокировке объекта ключевого носителя … в УЦ
Ошибка при блокировке пользователя … в связи с его неактивностью
Ошибка при блокировке рабочей станции … в связи с ее неактивностью
Ошибка при обновлении объекта ключевого носителя … в УЦ

Наименование события
Ошибка при первоначальном разбиении на секции таблицы … (…)
Ошибка при переразбиении секции таблицы … (…). Период хранения данных в журнале - … мес., количество секций - …
Ошибка при проверке отозванности объекта ключевого носителя… в УЦ
Ошибка при проверке приостановки действия объекта ключевого носителя … в УЦ
Ошибка при разблокировке объекта ключевого носителя в УЦ
Ошибка при синхронизации … … из ресурсной системы
Ошибка при синхронизации … … из ресурсной системы – объект не найден в БД
Ошибка при смене мастер-ключа базы данных оператором …
Ошибка при создании объекта ключевого носителя … в УЦ
Ошибка при удалении устаревших записей логов из таблицы … (…)
Ошибка регистрации внедоменной рабочей станции … с идентификатором …
Ошибка синхронизации учетных записей … … из ресурсной системы
Первоначальное разбиение на секции таблицы … (…) успешно завершено. Период хранения данных в журнале - … мес., количество секций - …
Перемещение ключевого носителя … в контейнер …
Перемещение пользователя … в корневой контейнер …
Переразбиение на секции таблицы … (…) успешно завершено. Период хранения данных в журнале - … мес., количество секций - …
Получено уведомление от рабочей станции … с указанием недействительного идентификатора пользователя …
Получено уведомление от рабочей станции … с указанием недействительного идентификатора приложения …
Пользователь … был длительное время неактивен. Количество дней отсутствия активности: более …
Пользователь … был неактивен с момента регистрации более … дней
Пользователь … заблокирован
Пользователь … заблокирован в связи с неактивностью с момента регистрации. Количество дней отсутствия активности: более …
Пользователь … заблокирован в связи с неактивностью. Количество дней отсутствия активности: более …
Пользователь … не зарегистрирован

Наименование события
Пользователь … не имеет прав для обращения к серверу. Проверьте входит ли пользователь в роль "Пользователь".
После установки сервера необходимо прописать его адрес в DNS
После установки сервера необходимо сконфигурировать планировщик задач Windows для автоматизированного запуска планов обслуживания
Превышен лимит основного количества зарегистрированных рабочих станций. Лимит: … , Зарегистрировано: … Возможно зарегистрировать дополнительно: … Необходимо обновить лицензию
Проверьте учетную запись …. … - объект отсутствует или заблокирован в ресурсной системе
Рабочая станция…. была длительное время неактивна. Количество дней отсутствия активности: более …
Рабочая станция … была неактивна с момента регистрации более… дней
Рабочая станция … заблокирована в связи с неактивностью с момента регистрации. Количество дней отсутствия активности: более …
Рабочая станция … заблокирована в связи с неактивностью. Количество дней отсутствия активности: более …
Регистрация внедоменной рабочей станции … с идентификатором …
Сертификат пользователя не зарегистрирован
Синхронизация … … из ресурсной системы
Синхронизация учетных записей … из ресурсной системы
Срок действия JMS сертификата истек - … …
Срок действия JMS сертификата скоро истекает (дней): … - … …
Срок действия внешнего сертификата истек - … …
Срок действия внешнего сертификата скоро истекает (дней): … - … …
Срок действия лицензии истекает. Количество дней до истечения лицензии: менее …
Срок действия мастер-ключа базы данных истек. Криптохранилище демонтировано
Срок действия мастер-ключа базы данных истекает. Количество дней до истечения срока действия ключа: менее …
Срок действия сертификата оператора истек
Срок действия сертификата пользователя истек
Срок действия унаследованного сертификата истек- … …
Срок действия унаследованного сертификата скоро истекает (дней): … - … …

Наименование события
Существующие лицензии успешно зарегистрированы в БД. Необходимо проверить их валидность
Уведомление для … не было доставлено в течение выделенного интервала времени
Удаление привязки пользователя … к учетной записи в ресурсной системе …

11. Перейдите на вкладку **Клиентские события**.

Примечание. Вкладка **Клиентские события** отсутствует в версии *CA Edition* продукта JMS (см. «Руководство администратора. Часть 1» [2], раздел «Версии поставки продукта и лицензионные опции»).

Окно примет следующий вид.

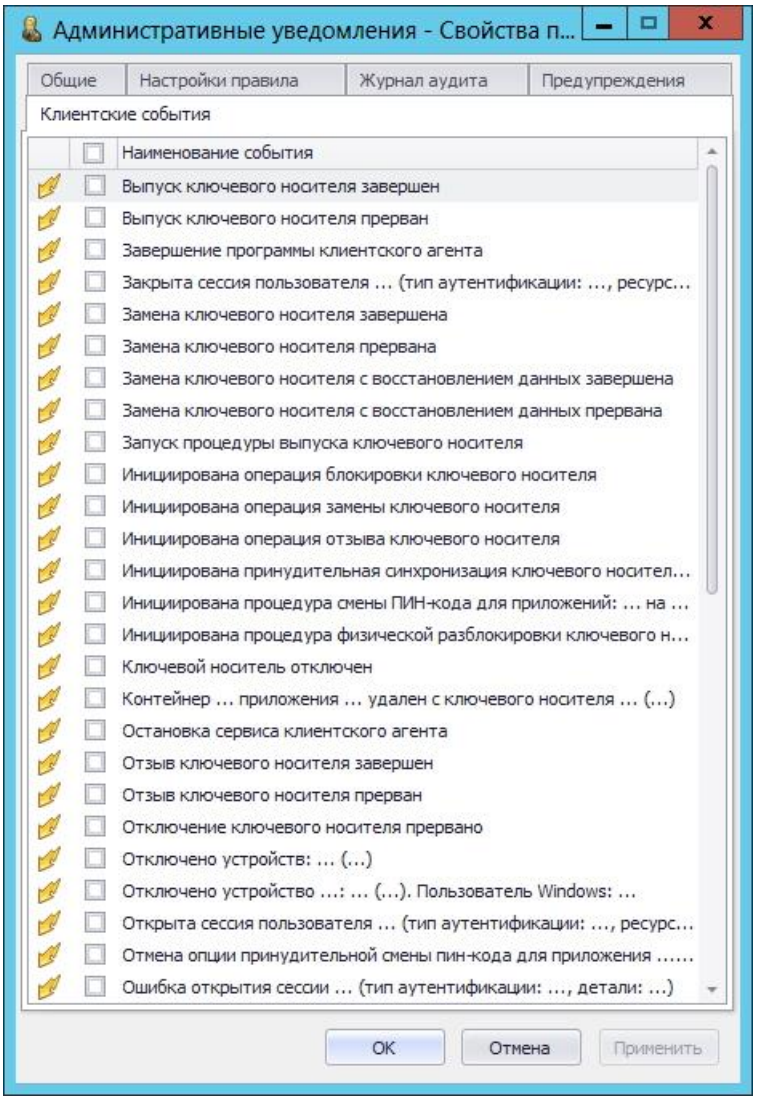


Рис. 409 – Вкладка Клиентские события

12. Установите флаги напротив событий, по поводу которых вы хотите получать уведомления (чтобы отметить все события, установите флаг напротив пункта **Наименование события**).

Чтобы уведомление было отправлено, тип отмеченного события должен совпадать с одним из типов, отмеченным на вкладке **Настройки правила** (см. табл. 96, с. 441). Например, если на вкладке **Настройки правила** в секции **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 произошло ошибка или критическая ошибка.

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

Список событий на вкладке **Клиентские события** представлен в таблице 99.

Табл. 99 – Список событий на вкладке Клиентские события

Наименование события
Выпуск ключевого носителя завершен
Выпуск ключевого носителя прерван
Завершение программы клиентского агента
Закрыта сессия пользователя … (тип аутентификации: … , ресурсная система: … , детали: …)
Замена ключевого носителя завершена
Замена ключевого носителя прервана
Замена ключевого носителя с восстановлением данных завершена
Замена ключевого носителя с восстановлением данных прервана
Запуск процедуры выпуска ключевого носителя
Инициирована операция блокировки ключевого носителя
Инициирована операция замены ключевого носителя
Инициирована операция отзыва ключевого носителя
Инициирована принудительная синхронизация ключевого носителя … : … (…)
Инициирована процедура смены PIN-кода для приложений: … на ключевом носителе … (…)
Инициирована процедура физической разблокировки ключевого носителя … : … (…)
Ключевой носитель отключен
Контейнер … приложения … удален с ключевого носителя … (…)
Остановка сервиса клиентского агента
Отзыв ключевого носителя завершен

Наименование события
Отзыв ключевого носителя прерван
Отключение ключевого носителя прервано
Отключено устройств: … (…)
Отключено устройство … : … (…). Пользователь Windows: …
Открыта сессия пользователя … (тип аутентификации: … , ресурсная система: … , детали: …)
Отмена опции принудительной смены PIN-кода для приложения … на ключевом носителе … (…) без смены PIN-кода т.к. приложение инициализировано с типом доступа Биометрия
Ошибка открытия сессии … (тип аутентификации: … , детали: …)
PIN-код сменен для приложения … на ключевом носителе … (…)
Подключено устройств: … (…)
Подключено устройство …: … (…). Пользователь Windows: …
Принудительная синхронизация ключевого носителя …: … (…) завершена
Принудительная синхронизация ключевого носителя …: … (…) завершена – действий по синхронизации не потребовалось
Принудительная синхронизация ключевого носителя …: … (…) прервана
Произошел сбой выпуска ключевого носителя
Произошел сбой замены ключевого носителя
Произошел сбой отзыва ключевого носителя
Произошел сбой синхронизации ключевого носителя … : … (…)
Произошел сбой смены PIN-кода для приложения … на ключевом носителе … (…)
Произошел сбой смены PIN-кода контейнера … в приложении … на ключевом носителе … (…)
Произошел сбой удаления контейнера … в приложении … с ключевого носителя … (…)
Произошел сбой физической разблокировки ключевого носителя … : … (…)
Процедура смены PIN-кода на ключевом носителе … (…) завершена. PIN-код сменен для контейнеров: … Смена PIN-кода пропущена для контейнеров: …
Процедура смены PIN-кода на ключевом носителе … (…) завершена. PIN-код сменен для приложений: … Смена PIN-кода пропущена для приложений: …
Процедура физической разблокировки ключевого носителя … : … … (…) завершена

Наименование события
Процедура физической разблокировки ключевого носителя … : … … (…) прервана
Сбой при отключении ключевого носителя
Смена PIN-кода контейнера … в приложении … на ключевом носителе … (…) завершена
Старт программы клиентского агента
Старт сервиса клиентского агента

4. Взятие под управление JMS внешних объектов

4.1 Взятие под управление 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 центра сертификации Microsoft. 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 удостоверяющим центрам (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 КриптоПро УЦ 1.5;
- сертификаты, выпущенные КриптоПро УЦ 2.0;
- сертификаты, выпущенные ViPNet УЦ 4.6;
- сертификаты на рабочих станциях пользователей (в качестве электронного ключа выступает *виртуальный электронный ключ «Хранилище пользователя»*);
- сертификаты, зарегистрированные для пользователя в КриптоПро DSS (в качестве электронного ключа выступает *виртуальный электронный ключ «Хранилище сервера КриптоПро DSS»*);
- профили SecurLogon.

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. 158) 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. 100 ниже), в противном случае – в память электронного ключа будет записан новый объект.

Примечание. В случае взятия под управления «виртуального электронного ключа» (см. «Виртуальный электронный ключ «Хранилище пользователя», с. 118) при наличии в хранилище пользователя нескольких сертификатов, удовлетворяющим требованиям для взятия под управление (табл. 100 ниже) будет выбран сертификат с наиболее поздней датой действительности сертификата.

Табл. 100 – Условие взятия под управление без повторного выпуска объектов

Тип объекта	Шаблон сертификата пользователя	Атрибуты пользователя
Сертификаты, выпущенные удостоверяющим центрами Microsoft CA и КриптоПро УЦ 1.5/2.0.	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.
Профиль SecurLogon	Неприменимо	
Сертификаты, выпущенные ViPNet УЦ 4.6	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 – ViPNet УЦ** (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.

4.2 Взятие под управление пользователей КриптоПро DSS

По аналогии с управлением электронными ключами, выпущенными вне JMS, система также позволяет устанавливать контроль (администрировать параметры аутентификации и функционирования) над объектами пользователей, зарегистрированными в КриптоПро DSS. Для взятия пользователей под управление необходимо, чтобы в соответствующем профиле (см. раздел «Настройка профиля пользователя КриптоПро DSS», с. 281) был выставлен флаг **Брать под управление существующие учетные записи** (см. Табл. 60, с. 291), а идентификаторы пользователей КриптоПро DSS (список и критерий сопоставления которых также устанавливается в данном профиле) совпадали с соответствующими атрибутами пользователей в одной из ресурсных систем JMS.

При установлении контроля JMS над пользователями КриптоПро DSS (т.е. при первой синхронизации посредством плана обслуживания **Синхронизация КриптоПро DSS**) действуют следующие правила:

- в случае если в КриптоПро DSS до первой синхронизации у пользователя настроены те же методы первичной аутентификации (например **Аутентификация по паролю**, **Аутентификация по сертификату** и т.п.), что и в профиле, то значение аутентификатора (пароль, сертификат и т.п.) для данного метода аутентификации сохраняется; если же в профиле какой-либо метод аутентификации отключен, то у пользователя в КриптоПро DSS данный метод аутентификации также будет отключен с потерей аутентификатора;
- все остальные параметры пользователя КриптоПро DSS, устанавливаются в соответствии с профилем (ранее установленные значения параметров игнорируются).

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. 239.
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. 158 «Привязка профилей», с. 296.

 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 электронного ключа администратором», с. 75.

 Если электронный ключ выпускается через JMS Client, 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 JMS Client.

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 следующие КН:

- электронные ключи компании Аладдин (обозначения приложения в JMS – **ГОСТ**, **ГОСТ 2**);
- электронные ключи «Рутокен ЭЦП» (обозначение приложения в JMS –**RuToken ECP**);
- электронные ключи «JaCarta CryptoPro» (обозначение приложения в JMS –**ФКН**);
- электронные ключи «ESMART ГОСТ» (обозначение приложения в JMS –**ESMART ГОСТ**).

Все операции над ключевыми носителями как аппаратными СКЗИ осуществляются в разделах **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. 410.

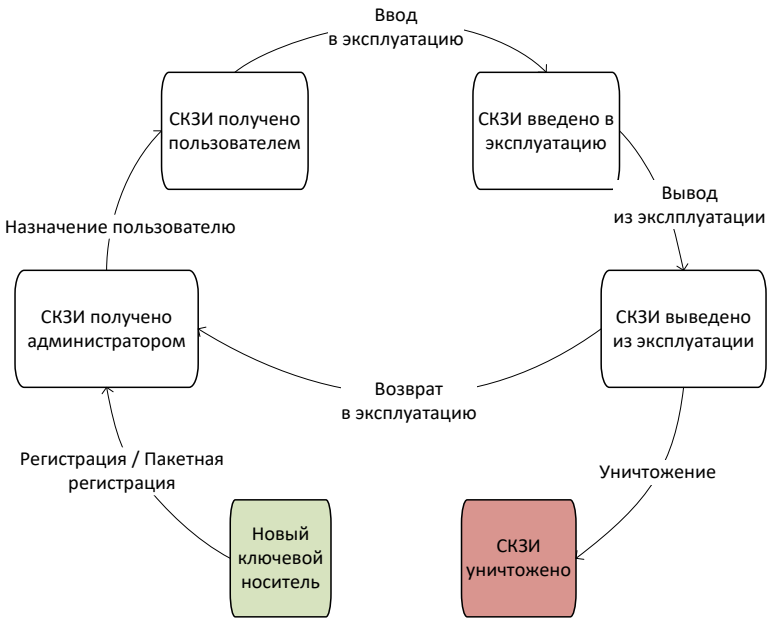


Рис. 410 – Жизненный цикл ключевого носителя как аппаратного СКЗИ

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** на верхней панели нажмите **Зарегистрировать** (подробнее см. в «Регистрация подсоединенных

электронных ключей в JMS», с. 57). 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. 367)

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) электронных ключей в JMS», с. 68). 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 электронного ключа пользователю», с . 71).

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 в верхней панели нажмите **Зарегистрировать и выпустить** (подробнее см. «Выпуск электронного ключа администратором», с. 75).

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 электронного ключа администратором», с. 75 (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. 164 и «Привязка профилей», с. 296)

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 и в верхней панели нажмите **Отозвать** (подробнее см. «Отзыв электронного ключа», с . 88).

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 **Ключевые носители** выберите выведенный из эксплуатации КН и в верхней панели нажмите **Вернуть в эксплуатацию** (подробнее см. «Возврат в эксплуатацию электронного ключа», с. 95).

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. 410, с. 461);
- 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 **Подключенные устройства -> Ключевые носители** (или **Ключевые носители**) выберите КН, предварительно выведенный из эксплуатации, и в верхней панели на вкладке **Действия** нажмите **Удалить**.

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.

6.2 Порядок управления программным СКЗИ

Управление программным СКЗИ осуществляется в соответствии с жизненным циклом, изображенным на Рис. 411.

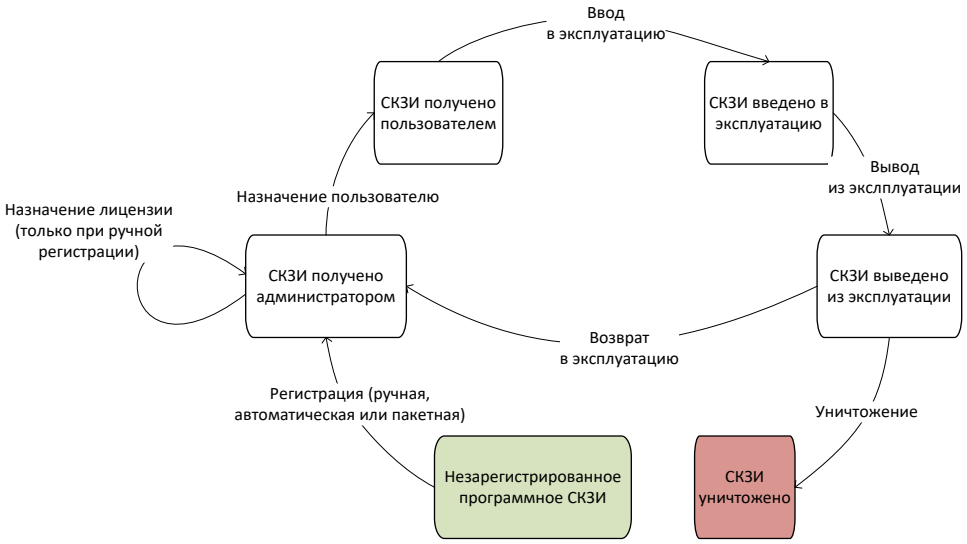


Рис. 411 – Жизненный цикл программного СКЗИ

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 **СКЗИ -> Экземпляры СКЗИ** необходимо выполнить следующие действия**:**

1. На верхней панели нажмите **Зарегистрировать** и выполните необходимые действия по регистрации (подробнее см. в «Регистрация экземпляра СКЗИ», с. 328).
2. В списке экземпляров СКЗИ выберите только что зарегистрированное СКЗИ, на верхней панели нажмите **Лицензии** и выберите **Назначить** (подробнее см. в разделе «Лицензия», с. 332).

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. 318), при регистрации его лицензии в консоли администрирования JMS (см. в раздел «Регистрация лицензии СКЗИ», с. 352), 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. 318), при пакетной регистрации лицензий СКЗИ такого типа (см. раздел «Импорт лицензий (пакетная регистрация)», с. 354), 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. 357.

Автоматическая регистрация программных СКЗИ, установленных на рабочих станциях

Экземпляры программных СКЗИ типа КриптоПро CSP и ViPNet CSP (кроме экземпляров СКЗИ КриптоПро CSP с *демонстрационной лицензией* производителя) создаются в JMS автоматически при обнаружении их инсталляций на рабочих станциях с установленным и подключенным клиентом JMS.

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. 367). 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 **СКЗИ -> Экземпляры СКЗИ** выберите необходимый экземпляр СКЗИ со статусом *Получен администратором* и в верхней панели нажмите **Назначить ответственное лицо** (подробнее см. «Назначить ответственное лицо», с . 333).

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 **СКЗИ -> Экземпляры СКЗИ** выберите необходимый экземпляр СКЗИ со статусом *Получен пользователем* и в верхней панели нажмите **Ввести в эксплуатацию** (подробнее см. «Ввести в эксплуатацию», с . 333).

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 ответственном у лицу».

6.2.4 Порядок вывода программного СКЗИ из эксплуатации

Для вывода программного СКЗИ из эксплуатации в разделе **СКЗИ -> Экземпляры СКЗИ** выберите необходимый экземпляр СКЗИ со статусом *Введен в эксплуатацию* и в верхней панели нажмите **Вывести из эксплуатации** (подробнее см. «Порядок вывода КН-СКЗИ из эксплуатации», с . 462).

В результате вывода из эксплуатации:

- экземпляру СКЗИ будет присвоен статус **Выведен из эксплуатации**;
- в JMS будет автоматически сгенерированы следующие нормативные документы:
  - «Акт передачи лицензии ответственном у 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 **СКЗИ -> Экземпляры СКЗИ** выберите необходимый экземпляр СКЗИ со статусом *Выведен из эксплуатации* и в верхней панели нажмите **Вернуть в эксплуатацию** (подробнее см. «Вернуть в эксплуатацию», с . 336).

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. 411, с. 464);
- 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 **СКЗИ -> Экземпляры СКЗИ** выберите экземпляр программного СКЗИ со статусом *Выведен из эксплуатации* и в верхней панели нажмите **Уничтожить** (подробнее см. в разделе «Уничтожить», с. 336).

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. 410, с. 461 и Рис. 411, с. 464). 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, на верхней панели нажмите **Управление учетом** и выберите **Прекратить**. 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** выберите в списке необходимый экземпляр СКЗИ со статусом *Учет прекращен*, на верхней панели нажмите **Управление учетом** и выберите **Возобновить**. 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*, на верхней панели нажмите **Управление учетом** и выберите **Удалить учетную запись**. Учетная запись данного экземпляра СКЗИ будет удалена из базы данных JMS.

Примечание. Удаление из JMS учетной записи экземпляра СКЗИ со статусом *Уничтожен* невозможно.

7. Настройка параметров ведения журнала диагностики JMS

Файлы журнала диагностики JMS в зависимости от компонента записываются в следующие каталоги (см. табл. 101).

Табл. 101 – Каталоги записи файлов журнала диагностики JMS

Компонент	Каталог записи файлов журнала диагностики JMS
Серверная служба JMS	На компьютере с установленным компонентом JMS Server: **%ALLUSERSPROFILE%\Application Data\Aladdin\Enterprise Management System\Logs**.
Серверный агент JMS	На компьютере с установленным компонентом JMS Server: **%APPDATA%\Aladdin\Enterprise Management System\Logs**.
Административный клиент JMS	На компьютере с установленным компонентом JMS Admin: **%APPDATA%\Aladdin\Enterprise Application Platform\Logs\Admin**.
Клиентская служба JMS	На компьютере с установленным компонентом JMS Client: **%ALLUSERSPROFILE%\Application Data\Aladdin\Enterprise Application Platform\Logs\Client**.
Клиентский агент JMS	На компьютере с установленным компонентом JMS Client: **%APPDATA%\Aladdin\Enterprise Application Platform\Logs\Client**.

По умолчанию ведение журнала диагностики JMS включено. Чтобы отключить ведение журнала диагностики JMS, необходимо внести изменения в файл конфигурации, например, с помощью программы **Блокнот** (см. табл. 102).

Табл. 102 – Включение/отключение ведения журнала диагностики JMS

Компонент	Расположение файла конфигурации и необходимые действия
Серверная служба JMS	На компьютере с установленным компонентом JMS Server: **<каталог установки JMS Server>\Aladdin.EAP.Engine.exe.config** Чтобы отключить ведение журнала: 1. найдите в файле значение **<log4net>** и замените его на **<log4net threshold="OFF">**; 2. перезапустите службу **Aladdin EAP Engine Service – default.**

Компонент	Расположение файла конфигурации и необходимые действия
Серверный агент JMS	На компьютере с установленным компонентом JMS Server: **<каталог установки JMS Server>\Aladdin.EAP.Agent.exe.config** Чтобы отключить ведение журнала: 1. найдите в файле значение <log4net threshold="**ALL**"> и замените его на <log4net threshold="**OFF**">; 2. в области уведомлений щелкните правой кнопкой на значке и выберите **Выход**, после чего снова запустите утилиту **Сервер JMS** (**Пуск -> JaCarta Management System -> Сервер JMS**).
Административный клиент JMS	На компьютере с установленным компонентом JMS Admin: **<каталог установки JMS Admin>\Aladdin.EAP.Admin.UI.exe.config** Чтобы отключить ведение журнала: 1. найдите в файле значение **<log4net>** и замените его на **<log4net threshold="OFF">**; 2. перезапустите консоль управления JMS.
Клиентская служба JMS	На компьютере с установленным компонентом JMS Client: **<каталог установки JMS Client>\Aladdin.EAP.ClientSTS.Service.exe.config** Чтобы отключить ведение журнала: 1. найдите в файле значение **<log4net>** и замените его на **<log4net threshold="ALL">**; 2. перезапустите службу отображаемое имя: **Aladdin EAP Client - default**.
Клиентский агент JMS	На компьютере с установленным компонентом JMS Client: **<каталог установки JMS Client>\Aladdin.EAP.ClientSTS.UI.exe.config** Чтобы отключить ведение журнала: 1. найдите в файле значение **<log4net>** и замените его на **<log4net threshold="OFF">**; 2. перезапустите утилиту Клиент JMS – для этого в области уведомлений щелкните правой кнопкой на значке и выберите Выход, после чего снова запустите утилиту (**Пуск -> Все программы -> JaCarta Management System -> Клиент JMS**).

8. Отображение имен компьютеров при взаимодействиях в JMS

Для визуальной идентификации многочисленных компонентов JMS (клиентов, консолей управления и серверов) в процессе их взаимодействия в системе реализована индикация имен компьютеров, на которых данные компоненты функционируют. Такая индикация предусмотрена:

- в пользовательском интерфейсе:
  - в консоли управления JMS (отображение сервера, к которому консоль управления в данный момент подключена, Рис. 412);
  - в клиенте JMS (отображение сервера, на котором клиентский агент в данный момент аутентифицирован, Рис. 413);
- в журналах JMS (журнале аудита – Рис. 414; журнале клиентских событий – Рис. 415).

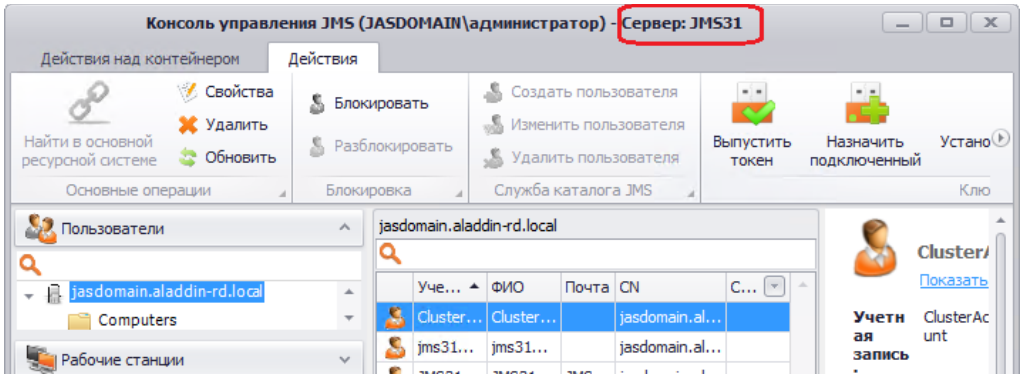


Рис. 412 – Индикация имени сервера JMS, к которому консоль управления в данный момент подключена

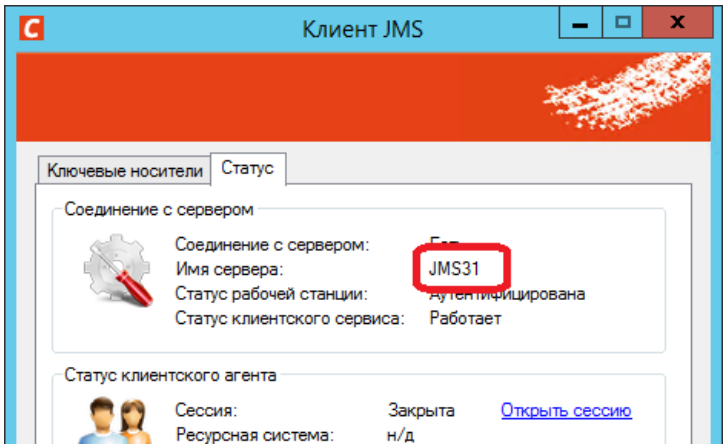


Рис. 413 – Индикация имени сервера JMS, на котором JMS-клиент в данный момент аутентифицирован

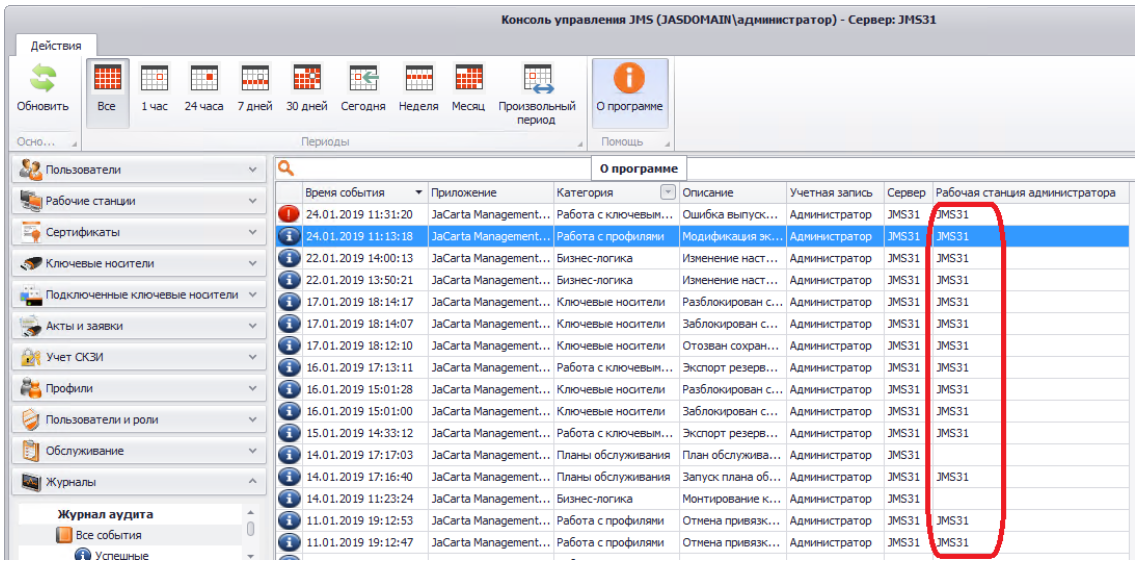


Рис. 414 – Отображение имени рабочей станции, на которой работает консолью управления JMS, в журнале аудита

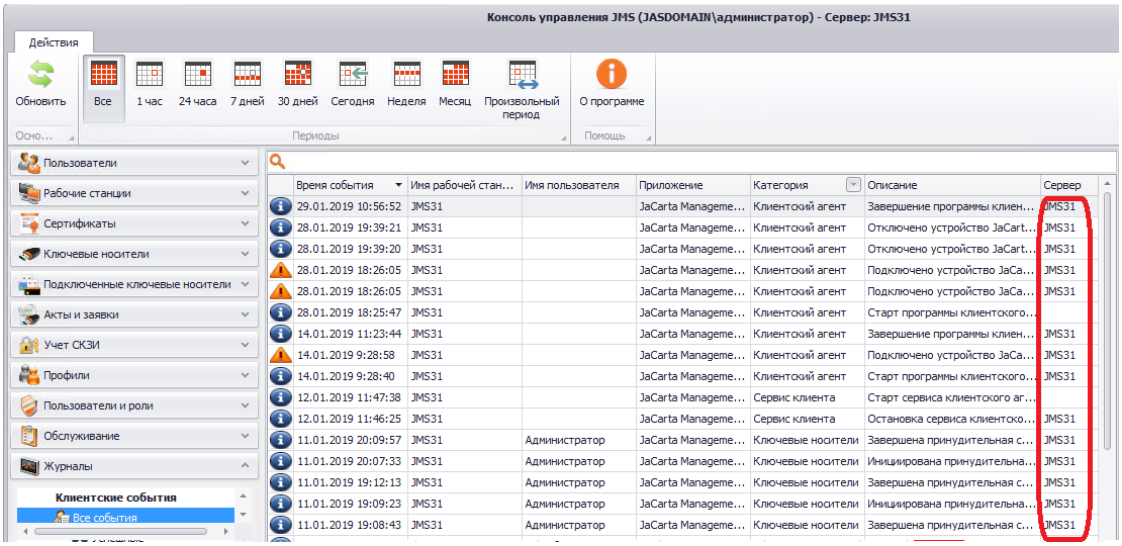


Рис. 415 – Отображение имени сервера JMS, на котором аутентифицирован JMS-клиент, в журнале клиентских событий

При работе в кластерной конфигурации данная функциональность позволяет проанализировать, с каким именно узлом кластера в данный момент взаимодействует консоль управления или JMS-клиент.

Передача и отображение имен компьютеров при взаимодействиях в рамках JMS реализована, начиная с версии 3.5 продукта. Введенная функциональность не нарушает обратной совместимости клиентов и серверов JMS. Например, при взаимодействии новой версии сервера со старым клиентами имя машины в журнале клиентских событий будет считаться неизвестным (поле остается незаполненным).

9. Управление журналом Предупреждения в JMS

В целях сокращения объема публикуемых событий в журнале **Предупреждения** (такое ограничение актуально на этапах внедрения JMS, когда возникает большой объем событий типа Предупреждение, приводящий к перегрузке сервера базы данных), в JMS предусмотрен механизм регулирования объема журналируемых событий типа Предупреждение.

Для регулирования объема публикуемых событий в журнале **Предупреждения** (раздел консоли управления **Журналы**) в конфигурационном файле службы сервера:

`<каталог установки JMS Server>\Aladdin.EAP.Engine.exe.config`

параметру AlertPublishLevel необходимо присвоить одно из следующих значений:

- **All** (значение по умолчанию) – публиковать все события в журнале **Предупреждения**;
- **Selectively** – исключить из публикации события типа Предупреждение, перечисленные в Табл. 103;
- **None** – не публиковать никаких событий в журнале **Предупреждения.**

Например:

```
<!-- Режим публикации предупреждений (All|Selectively|None) -->
<add key="AlertPublishLevel" value="All"/>
```

Важно! После внесения изменения в конфигурационный файл Aladdin.EAP.Engine.exe.config следует перезапустить службу JMS (**Aladdin EAP Engine Service - default**).

Табл. 103 – События типа Предупреждение, подлежащие регулированию

№ п/п	Название события
1	Ошибка аутентификации … при обращении с рабочей станции …
2	Регистрация внедоменной рабочей станции … с идентификатором …
3	Ошибка регистрации внедоменной рабочей станции … с идентификатором …
4	Клиентский запрос от незарегистрированной рабочей станции … отклонен.
5	Клиентский запрос от заблокированной рабочей станции … отклонен.
6	Получено уведомление от рабочей станции … с указанием недействительного идентификатора пользователя …
7	Пользователь … заблокирован.
8	Пользователь … не имеет прав для обращения к серверу. Проверьте входит ли пользователь в роль "Пользователь".
9	Пользователь … заблокирован

10. Управление журналом Клиентские события

10.1 Поиск записей в журнале клиентских событий

Журнал клиентских событий предназначен для протоколирования событий, возникающих в связи с эксплуатацией ПО Клиент JMS, устанавливаемого на рабочих станциях. Чтобы открыть журнал в консоли управления JMS выберите раздел **Журналы** -> **Клиентские события** -> **Все события** (Рис. 171).

Примечание. Журнал **Клиентские события** отсутствует в версии *CA Edition* продукта JMS (см. «Руководство администратора. Часть 1» [2], раздел «Версии поставки продукта и лицензионные опции»).

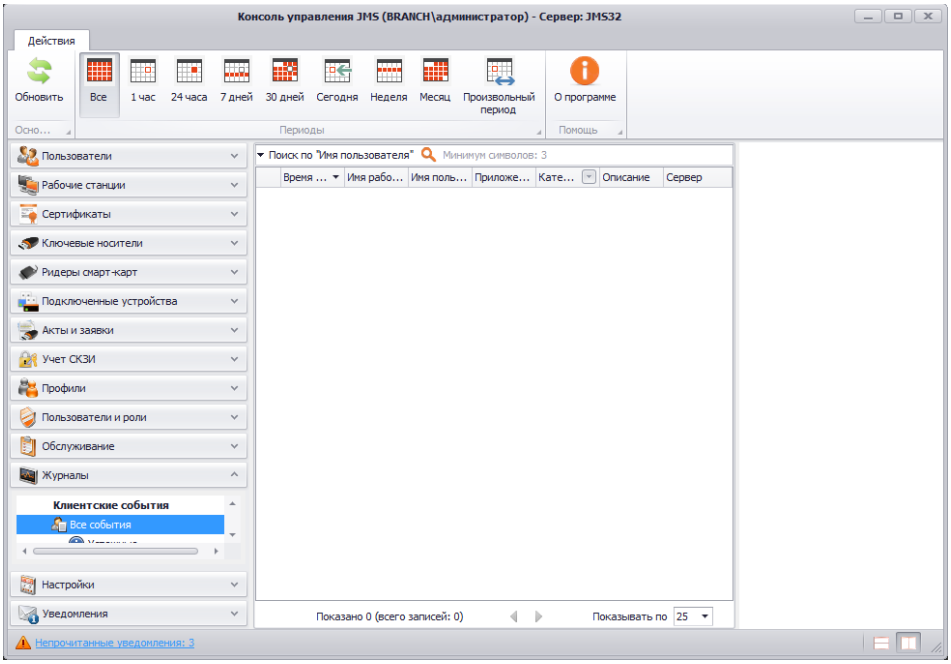


Рис. 416 – Раздел с журналом клиентских событий в Консоли управления JMS

Для поиска записей в журнале клиентских событий в поле **Поиск по "*<имя поля>*"** выберите поле, по которому должен осуществляться поиск (например, по полю **Имя пользователя**); в поле поиска введите строку поиска (не менее 3 символов) и нажмите **Ввод**. Поиск совпадения в текстовых полях осуществляется только начиная с первого символа значения поля.

10.2 Ограничение числа записей в журнале клиентских событий

В случае если необходимо ограничить число фиксируемых в журнале клиентских событий (т.е. событий, возникающих в связи с эксплуатацией ПО Клиент JMS, устанавливаемого на рабочих станциях), можно воспользоваться функцией фильтрации таких событий.

В консоли управления JMS откройте раздел **Настройки** -> **Журналы** (Рис. 417).

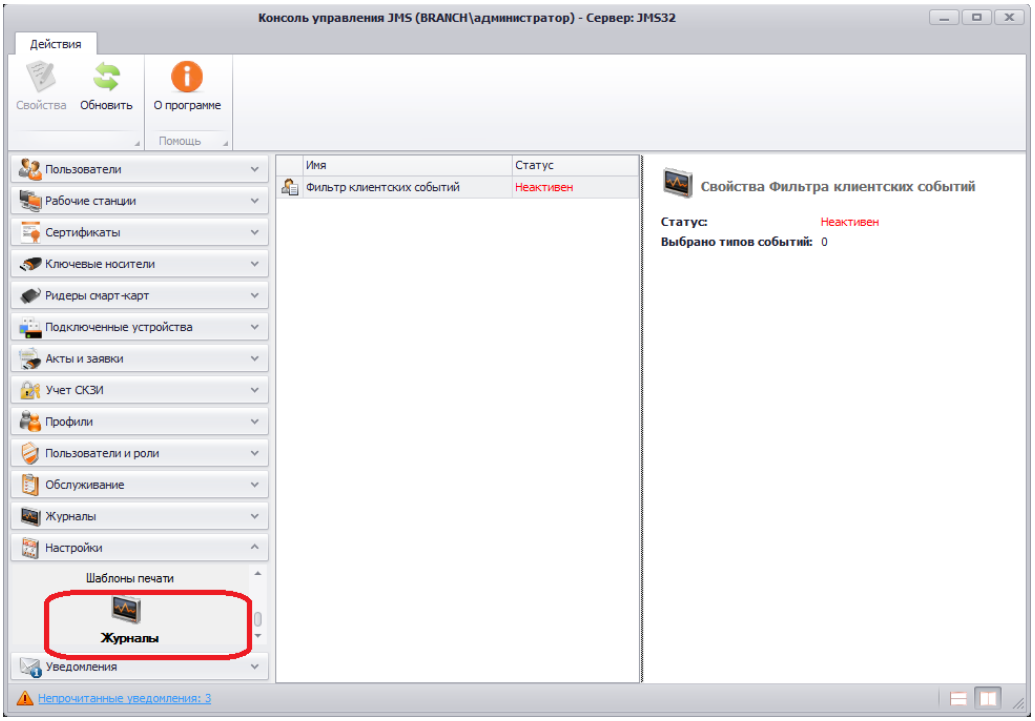


Рис. 417 – Выбор настройки фильтрации записи клиентских событий

В центральной части окна выберите **Фильтр клиентских событий** и верхней панели нажмите **Свойства**.

Откроется окно следующего вида:

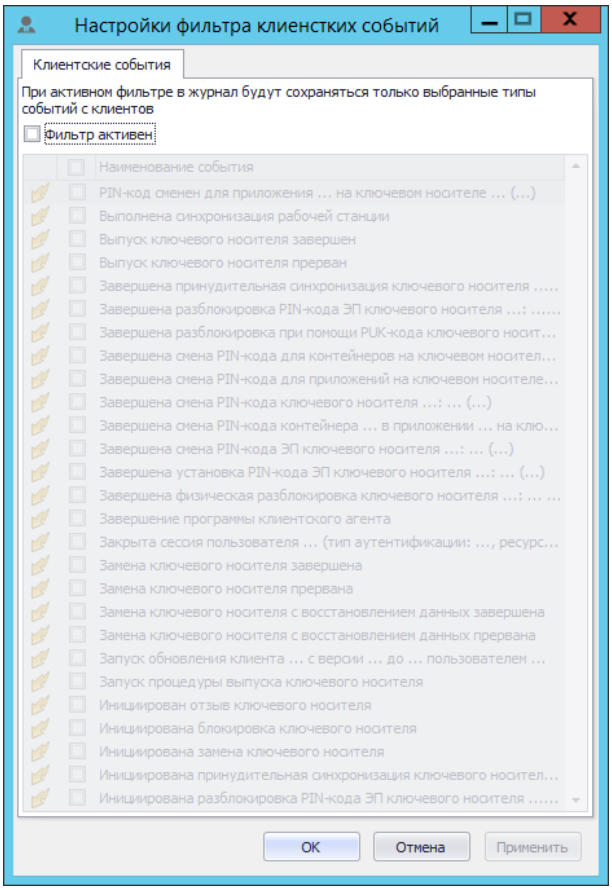


Рис. 418 – Настройка фильтрации событий в журнал клиентских событий

Выполните настройки, руководствуясь Табл. 104.

Табл. 104 – Настройки фильтра клиентских событий

Настройка	Описание
Фильтр активен	Установите флаг, если требуется ограничить число типов событий, записываемых в журнал клиентских событий. По умолчанию флаг не установлен (в журнал записываются клиентские события всех типов).
<Название события>	Установите флаг напротив событий, которые должны быть записаны в журнал клиентских событий

Важно! При установке фильтра клиентских событий следует иметь в виду, что на те события, которые в результате настроек перестанут попадать в журнал, не будет также рассылаться уведомления (о настройках уведомлений см. в разделе «Настройка рассылки административных/пользовательских уведомлений», с. 437).

11. Администрирование удаленных экземпляров JMS

В поставку JMS (компонент JMS Admin) входит оснастка, позволяющая осуществлять администрирование удаленных экземпляров JMS. Это может понадобиться, если в разных отделениях организации установлены разные экземпляры JMS.

Для администрирования удаленных экземпляров JMS, выполните следующие действия.

1. На компьютере, на котором установлен компонент JMS Admin, из командной строки выполните команду **mmc**.
   Отобразится следующее окно.

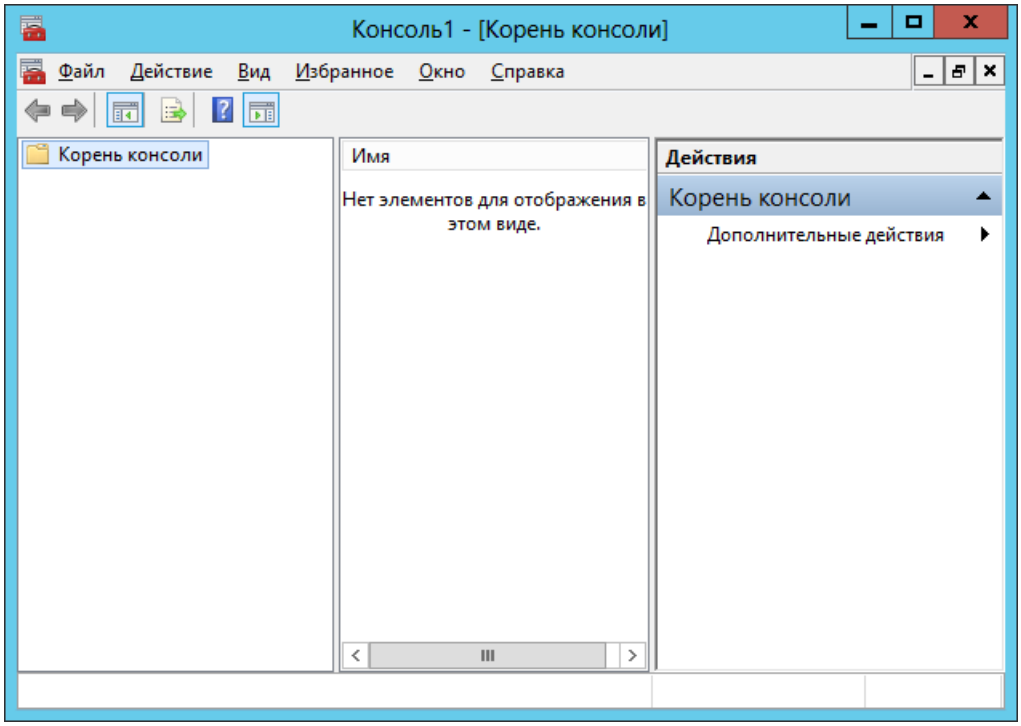


Рис. 419 – Корень консоли оснасток

2. Нажмите сочетание клавиш CTRL+M.
   Отобразится следующее окно.

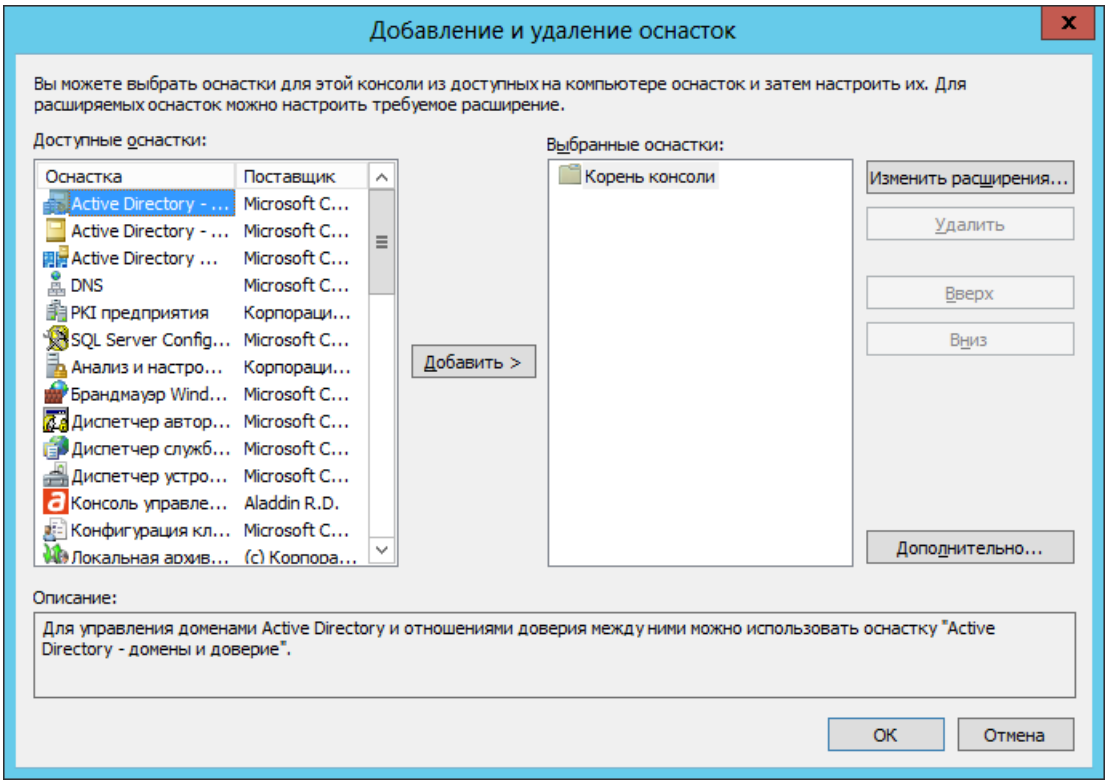


Рис. 420 – Окно добавления и удаления оснасток

3. Выполните одно из следующих действий:

   - если вы хотите создать иерархию экземпляров JMS в организации (чтобы они отображались в разных папках оснастке), переходите к следующему шагу процедуры;
   - если вы хотите, чтобы все удаленные экземпляры JMS располагались в корневом каталоге консоли, переходите к шагу 8 настоящей процедуры.

4. Щелкните на кнопке **Дополнительно** справа.
   Отобразится следующее окно.

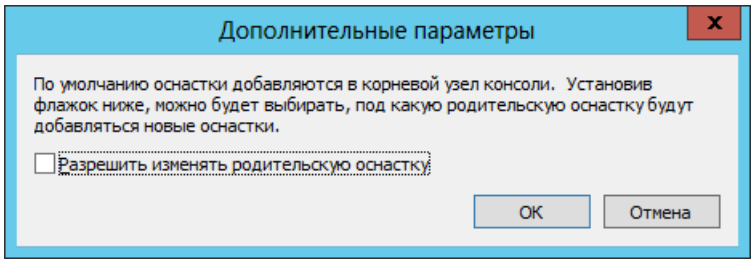


Рис. 421 – Окно дополнительных параметров

5. Установите флаг **Разрешить изменять родительскую оснастку** и нажмите **OK**.
6. В окне **Добавление и удаление оснасток** в списке **Доступные оснастки** выберите пункт **Папка** и нажмите **Добавить**.

Окно примет следующий вид.

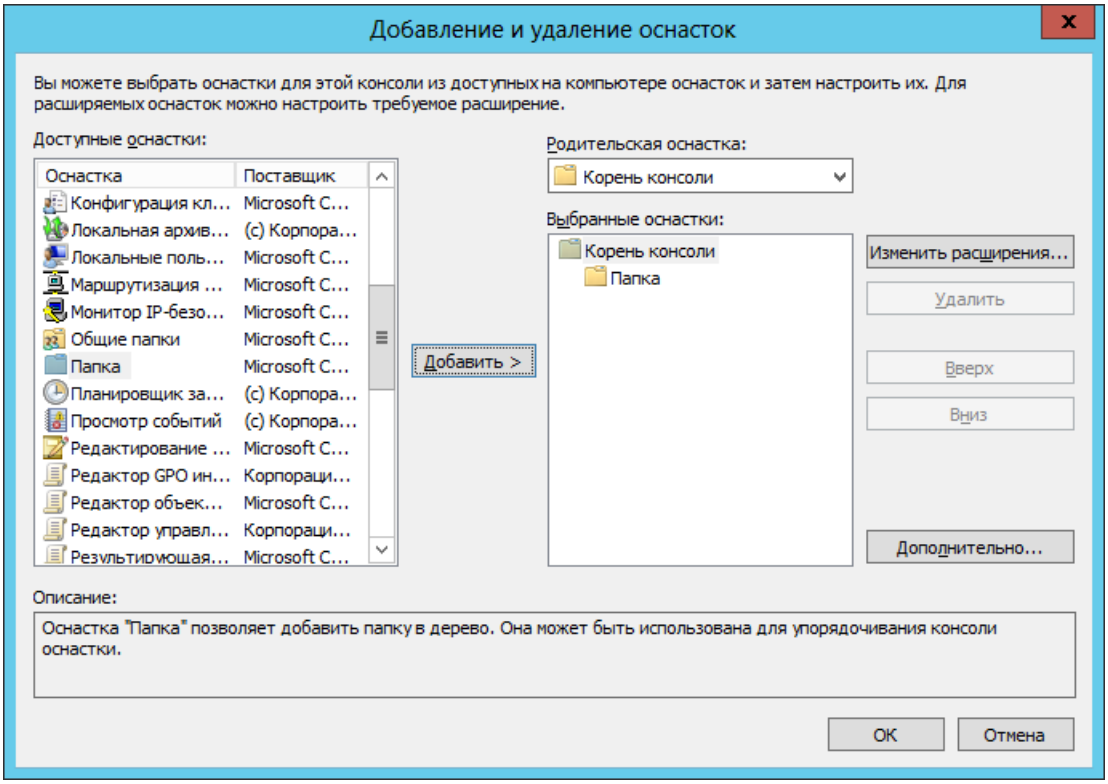


Рис. 422 – В корень консоли добавлена папка

7. Добавьте необходимое количество папок (например, одна папка может означать населенный пункт, в котором находятся филиалы организации).
8. Чтобы добавить оснастку администрирования удаленного экземпляра JMS, выполните следующие действия.
   Если вы добавляли папки в корень консоли:

8.1. в списке **Родительская оснастка** справа выберите папку, в которую будет помещена оснастка управления сервером JMS;
8.2. в списке **Доступные оснастки** слева выберите **Консоль управления JMS** и нажмите **Добавить**.

Если вы не добавляли дополнительных папок в корень консоли:

8.1. в списке **Доступные оснастки** слева выберите **Консоль управления JMS** и нажмите **Добавить**.

Отобразится следующее окно.

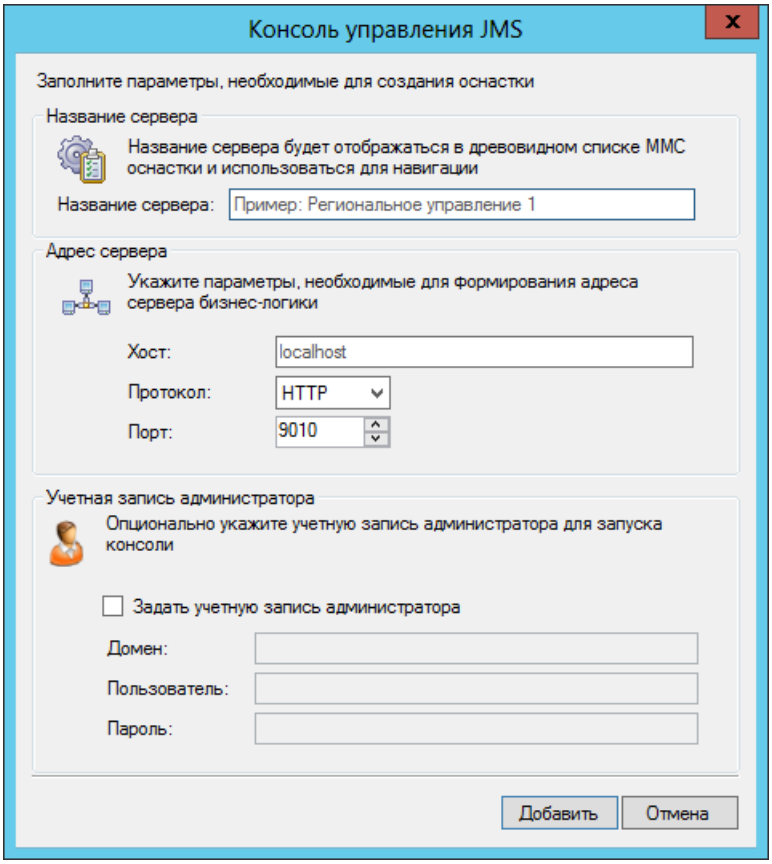


Рис. 423 – Настройка параметров соединения

9. Выполните настройки, руководствуясь табл. 105.

Табл. 105 – Настройка подключения для оснастки администрирования удаленного экземпляра JMS

Секция	Настройка	Описание
Название сервера	**Название сервера**	Введите название сервера, которое будет отображаться в оснастке.
Адрес сервера	**Хост**	Введите IP-адрес удаленного сервера JMS.
	Протокол	В списке протокол выберите протокол подключения к удаленному сервера JMS: • **HTTP**; • **HTTPS**.
	Порт	Укажите порт подключения к удаленному экземпляру сервера JMS. Подробнее см. «Руководство администратора. Часть 1» [2], раздел «Централизованная настройка подключения к серверу JMS», таблица «Настройка записи ресурса».
Учетная запись администратора	**Задать учетную запись администратора**	Флаг позволяет задать учетные данные, которые будут использоваться для администрирования удаленного экземпляра JMS.

Секция	Настройка	Описание
	Домен	Позволяет указать домен (например, **test.com**) членом которого является администратор, который будет управлять удаленным сервером JMS.
	Пользователь	Позволяет указать имя пользователя администратора, который будет управлять удаленным сервером JMS.
	Пароль	Позволяет указать пароль администратора, который будет управлять удаленным сервером JMS.

При явном указании учетной записи администратора, пароль учетной записи шифруется при помощи пароля текущего пользователя. Если изменить пароль текущего пользователя, изменится и ключ шифрования, таким образом, все сохраненные пароли необходимо будет ввести повторно.

10. Повторите необходимые действия необходимое количество раз, добавив нужно число оснасток удаленного администрирования экземплярами JMS.
11. В окне **Консоль управления JMS** нажмите **OK**.
    Отобразится окно оснасток.

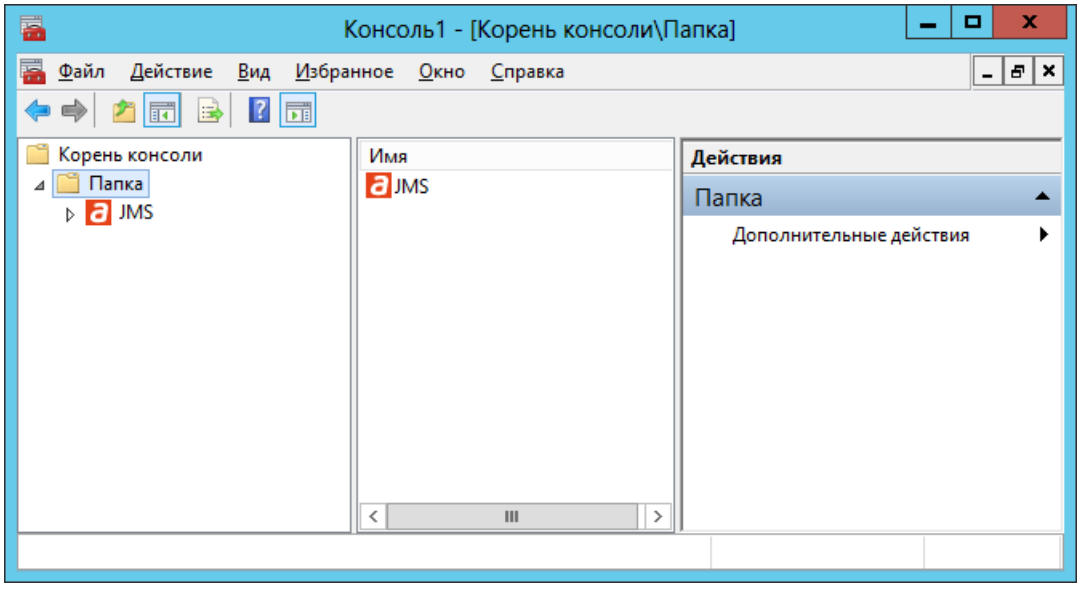


Рис. 424 – Оснастки администрирования удаленных экземпляров JMS

12. Если вы рассортировывали удаленные экземпляры JMS по папкам, вы можете переименовать их, щелкнув на них правой кнопкой и выбрав пункт **Переименовать**.
13. Чтобы запустить консоль управления удаленного экземпляра JMS, в левой панели выберите нужный экземпляр JMS.

Центральная часть окна примет следующий вид.

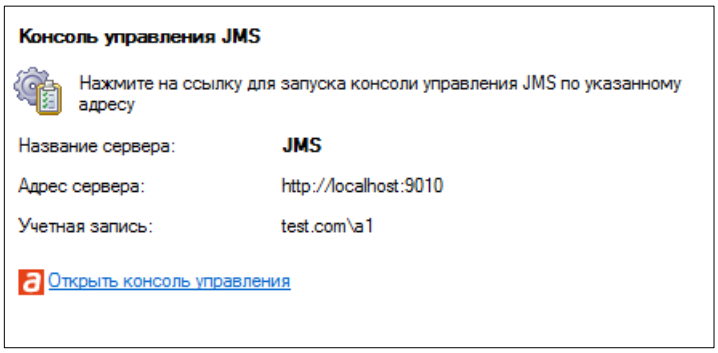


Рис. 425 – Центральная часть окна оснастки удаленного администрирования

14. Для запуска щелкните на ссылке **Открыть консоль управления**.
15. Завершив работу, сохраните созданную консоль оснасток администрирования удаленных экземпляров JMS для удобства последующих запусков.

12. Импорт резервных копий сертификатов в JMS

В состав компонента JMS Server входит утилита, позволяющая осуществлять импорт резервных копий сертификатов в JMS. По умолчанию утилита расположена в папке сервера JMS по следующему пути:

C:\Program Files\Enterprise Management System Server\Aladdin.EMS.CertificateBackupImportTool.exe.

12.1 Начало процедуры импорта

Чтобы выполнить импорт резервных копий сертификатов, выполните следующие действия.

1. Запустите утилиту импорта данных.
   Отобразится следующее окно.

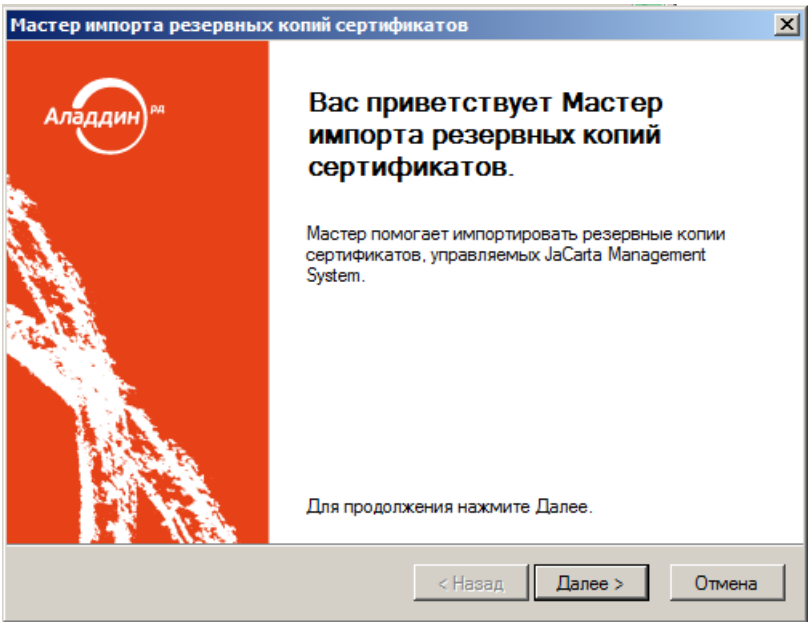


Рис. 426 – Окно приветствия мастера импорта резервных копий сертификатов

2. Нажмите **Далее**.

Отобразится следующее окно.

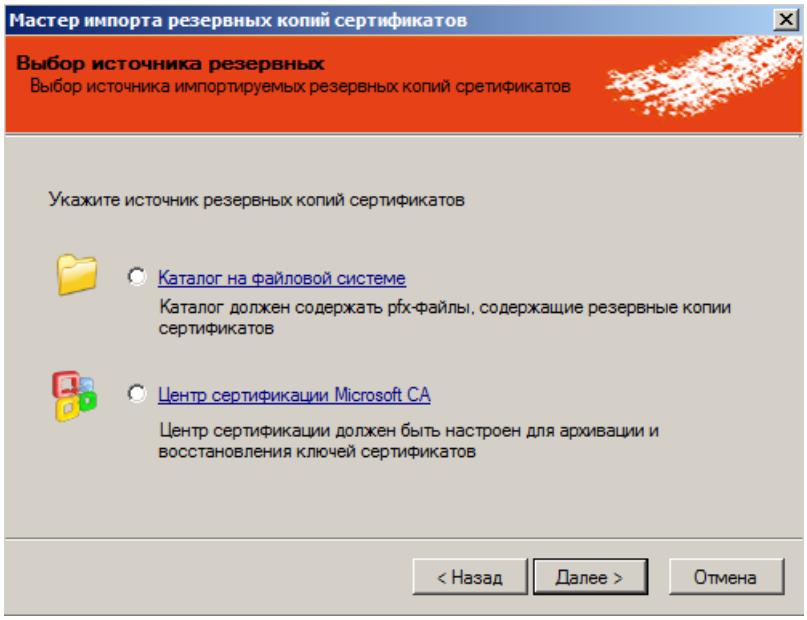


Рис. 427 – Выбор источника резервных копий сертификатов

3. Выберите один из источников копий резервных сертификатов и нажмите **Далее**. Продолжите процедуру в зависимости от сделанного выбора:

   – См. «Каталог на файловой системе»;
   – См. «Центр сертификации Microsoft CA», с. 482.

12.2 Каталог на файловой системе

Отобразится следующее окно.

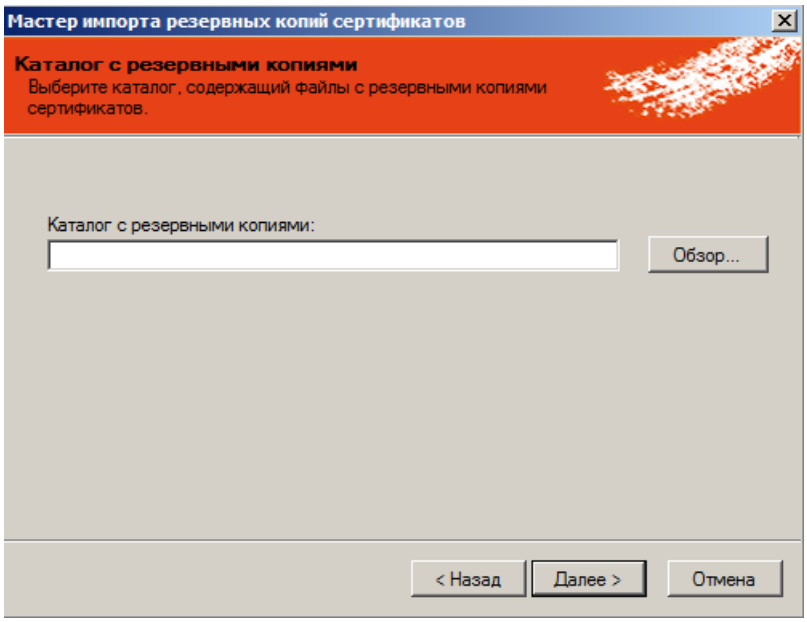


Рис. 428 – указание пути к каталогу с резервными копиями

1. Воспользуйтесь кнопкой **Обзор**, чтобы указать путь к каталогу с резервными копиями.
2. Нажмите **Далее**.

Отобразится следующее окно.

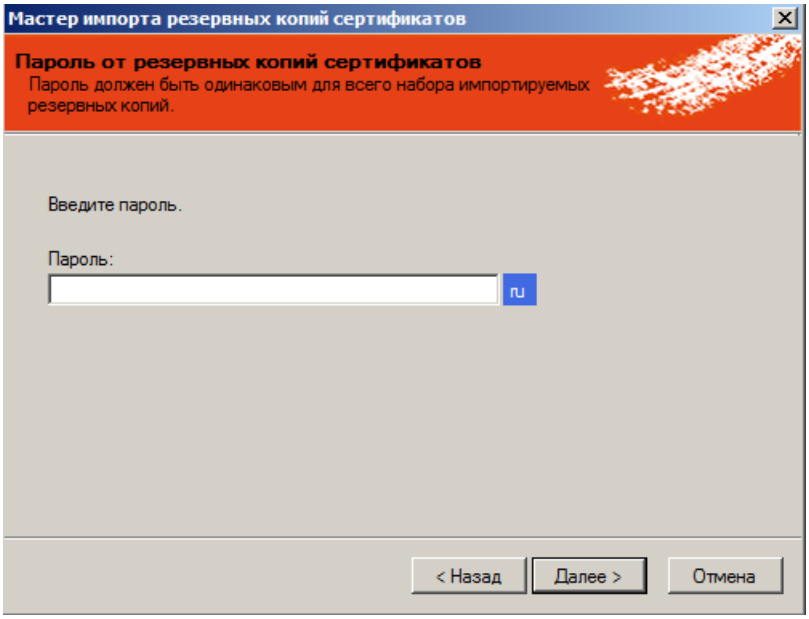


Рис. 429 – Указание пароля резервных копий сертификатов

3. В поле **Пароль** укажите пароль для импорта резервных копий сертификатов.

⚠ Пароль должен совпадать для все резервных копий сертификатов, которые вы собираетесь импортировать.

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

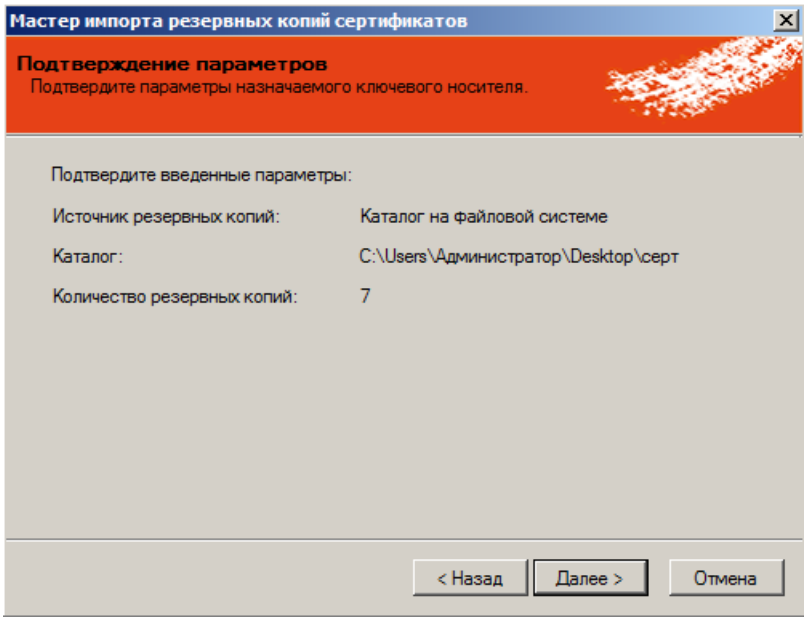


Рис. 430 – Подтверждение параметров импорта

5. Нажмите **Далее** и переходите к завершению процедуры импорта – см. «Завершение процедуры импорта», с. 483.

12.3 Центр сертификации Microsoft CA

Отобразится следующее окно.

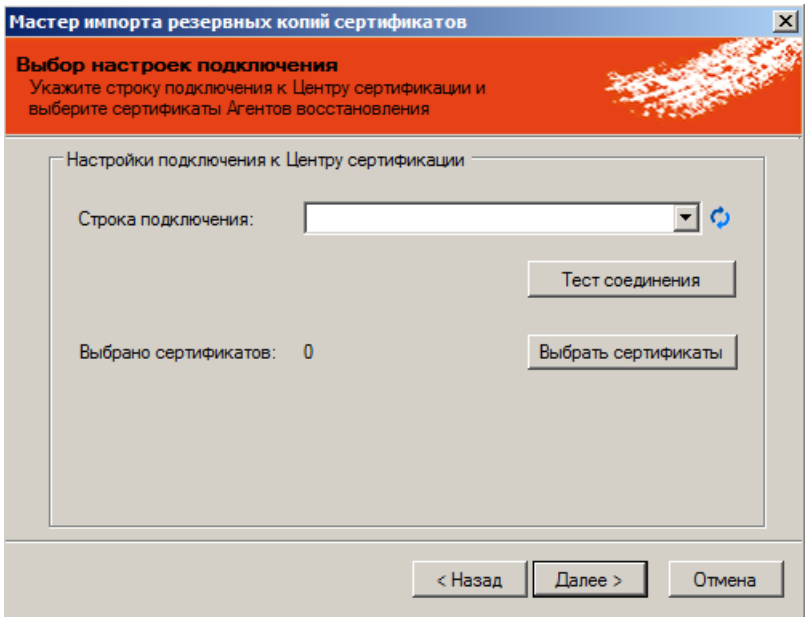


Рис. 431 – Настройка подключения к центру сертификации Microsoft

1. В поле **Строка подключения** укажите строку подключения к центру сертификации Microsoft.
2. При необходимости проверьте соединение, воспользовавшись кнопкой **Тест соединения**.
3. Щелкните на кнопке **Выбрать сертификаты**.
   Отобразится следующее окно.

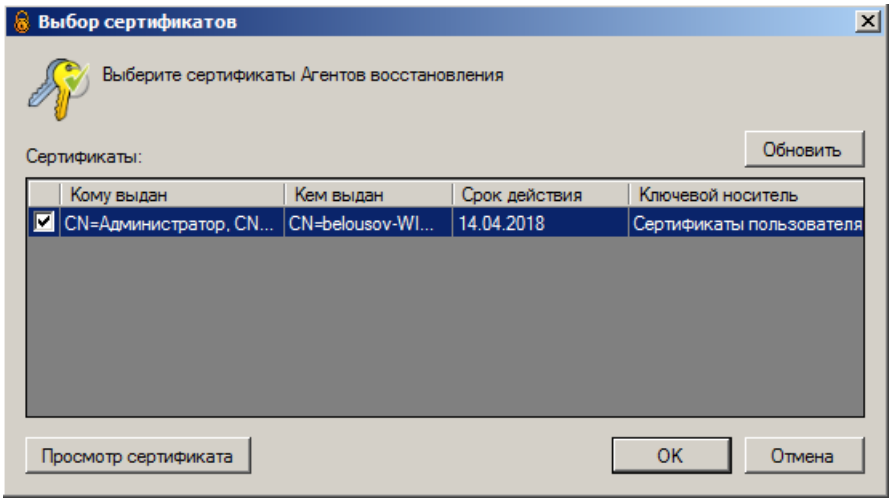


Рис. 432 – Выбор сертификата агента восстановления сертификатов

4. Отметьте сертификат агента восстановления сертификатов, который будет использоваться для импорта резервных копий сертификатов, после чего нажмите **OK**.
5. В окне настройки подключения к центру сертификации нажмите **Далее**.

Отобразится следующее окно.

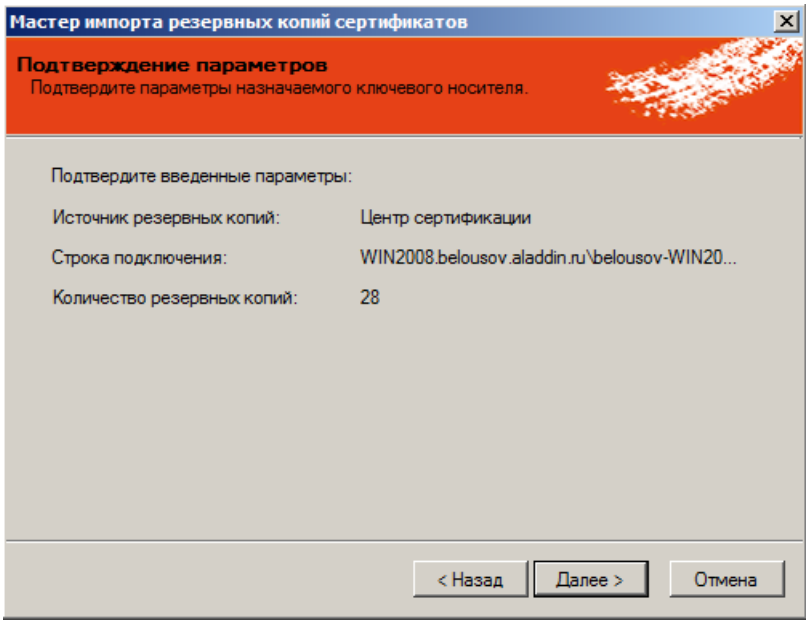


Рис. 433 – Подтверждение параметров импорта

6. Нажмите **Далее** и переходите к завершению процедуры импорта – см. «Завершение процедуры импорта».

12.4 Завершение процедуры импорта

Отобразится следующее окно.

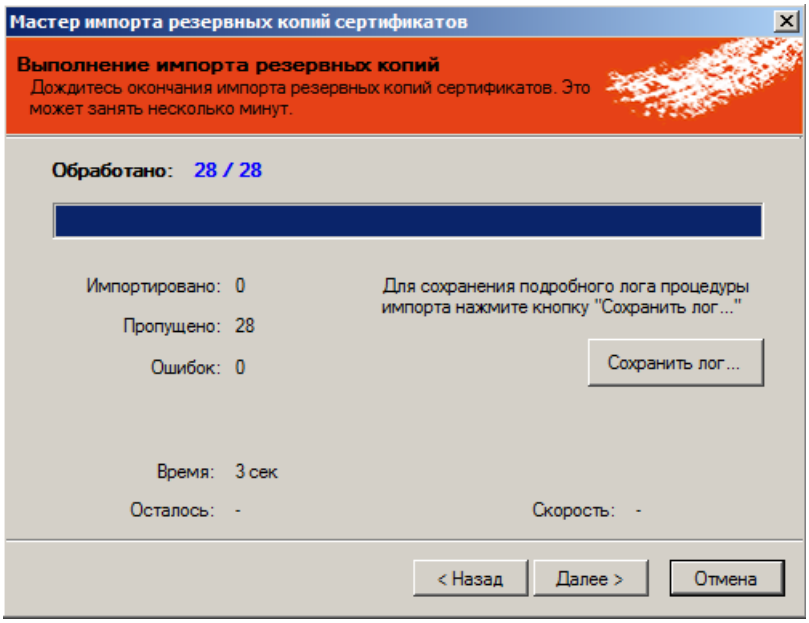


Рис. 434 – Импорт выполнен

1. При необходимости нажмите **Сохранить лог**, чтобы указать путь сохранения журнала импорта.
2. Нажмите **Далее**.

Отобразится следующее окно.

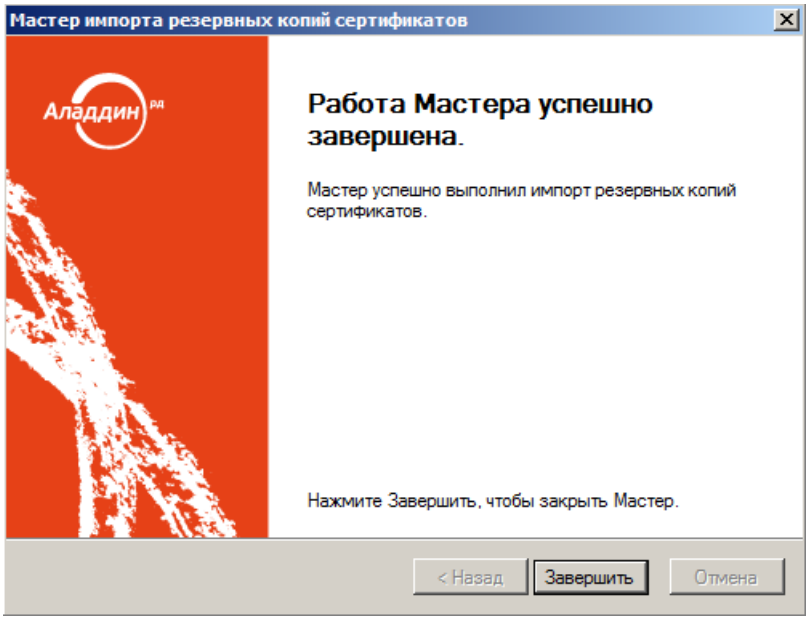


Рис. 435 – Завершение работы мастера импорта резервных копий сертификатов

3. Нажмите **Завершить** для завершения процедуры.

13. Диагностика JMS

В состав каждого из компонентов JMS (JMS Server, JMS Admin, JMS Client) входит утилита диагностирования, которая позволяет произвести диагностику установленного компонента. Чтобы выполнить диагностику, выполните следующие действия.

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

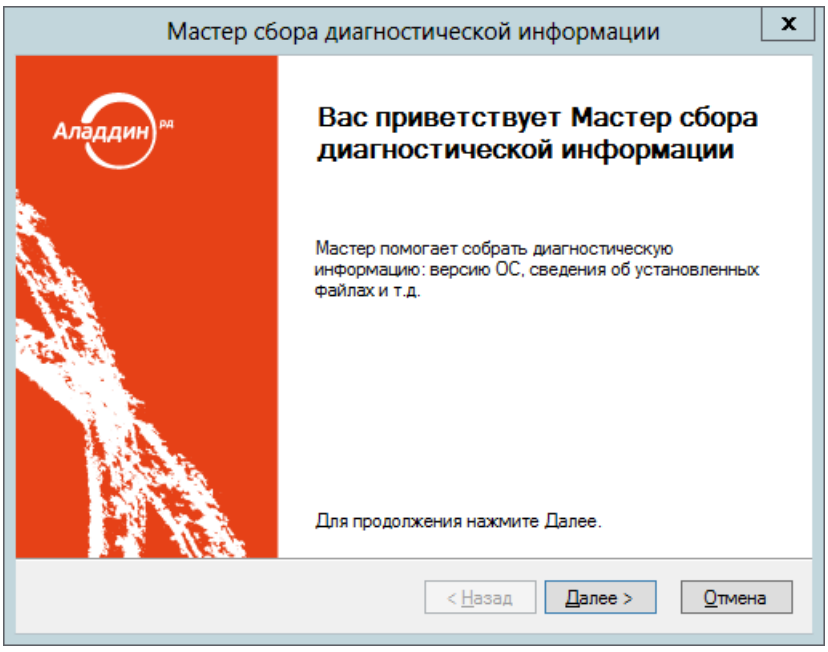


Рис. 436 – Окно приветствия мастера сбора диагностической информации

2. Нажмите **Далее**.

Отобразится следующее окно.

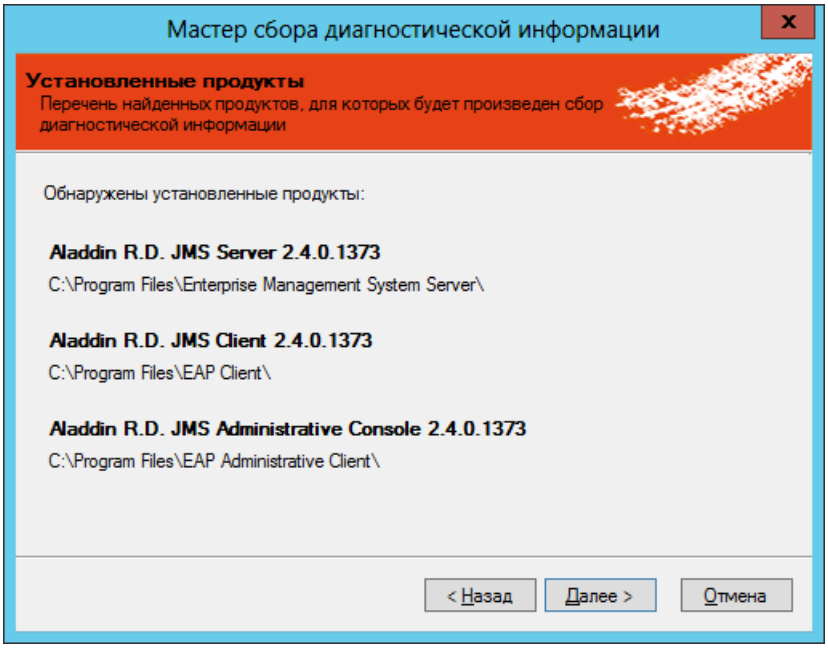


Рис. 437 – Список установленных компонентов JMS

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

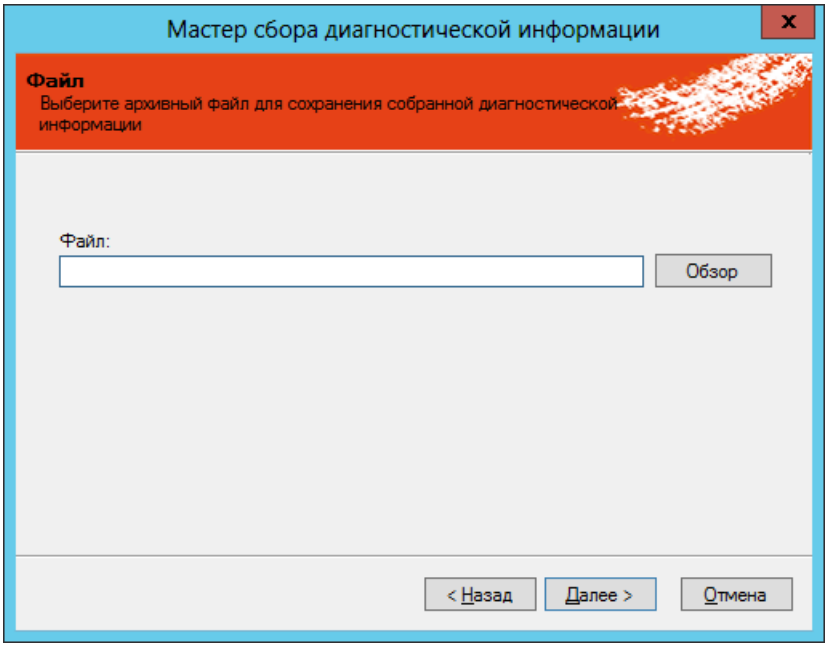


Рис. 438 – Указание пути сохранения диагностического отчета

4. Воспользуйтесь кнопкой **Обзор**, чтобы указать путь и файл сохранения архива диагностического отчета, после чего нажмите **Далее**.

По завершении диагностики отобразится следующее окно.

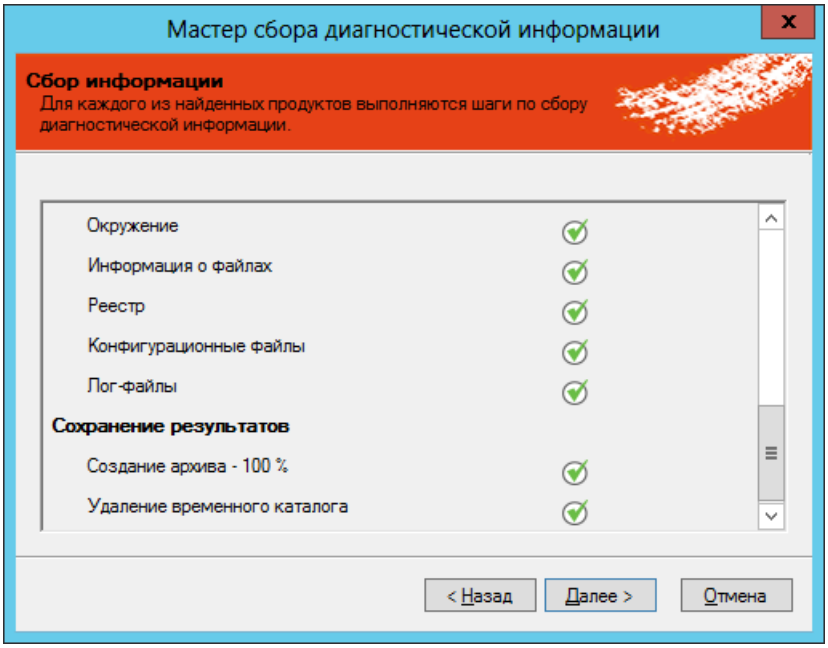


Рис. 439 – Результаты диагностики

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

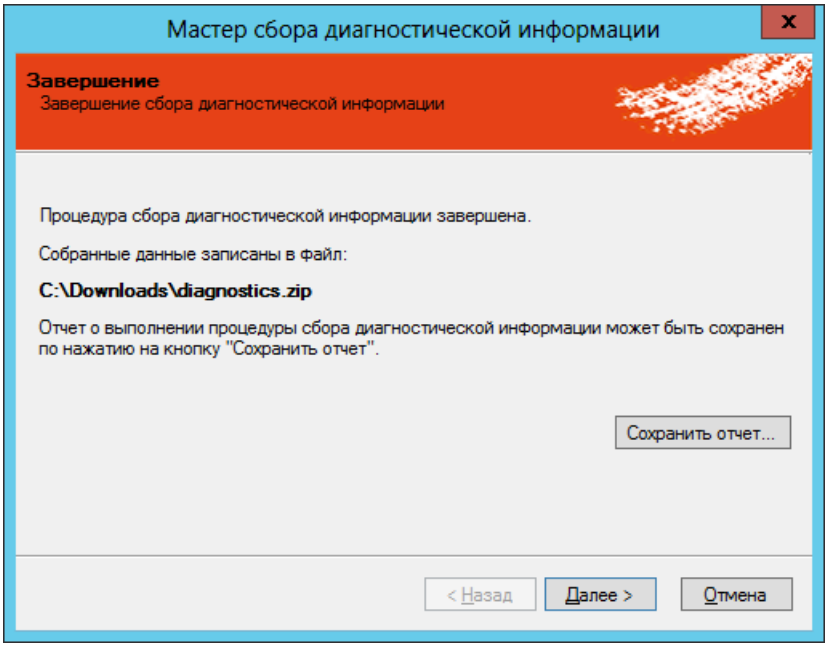


Рис. 440 – Завершение сбора диагностической информации

6. Нажмите **Далее**.

Отобразится следующее окно.

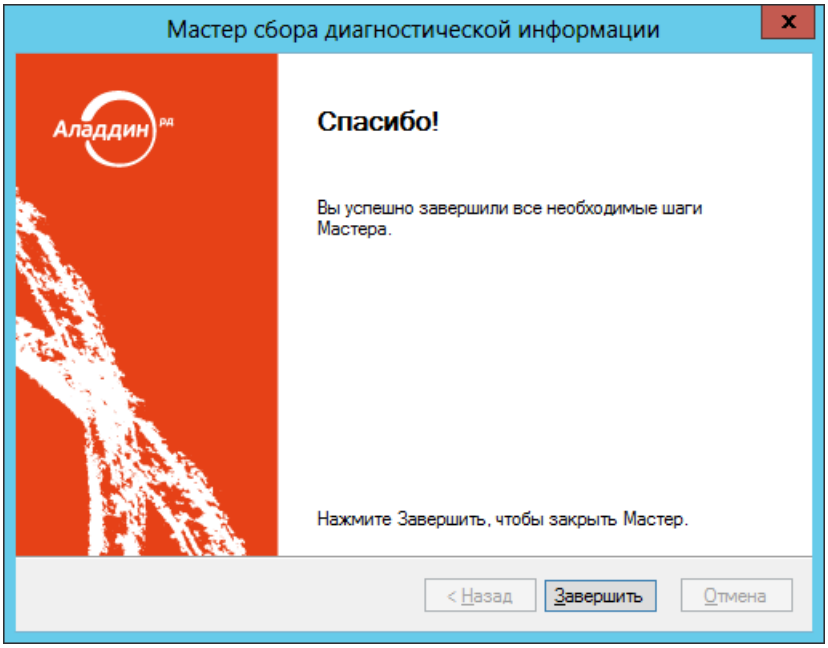


Рис. 441 – Окно завершения работы мастера сбора диагностической информации

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

14. JMS Web Manager (JWM)

JMS Web Manager (JWM) – компонент JMS, предоставляющий возможность удаленного администрирования JMS и выполнения пользовательских функций через корпоративную сеть или Интернет с помощью web-браузера по протоколам http и https.

Установка и настройка JWM и его специальаного 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 раделе «Настройки личного кабинета», ниже.
- **внутренний web-портал самообслуживания пользователей**, представляющий собой web-модификацию JMS-клиента и предназначенный для использования внутри корпоративной сети (подробнее см. в руководстве пользователя [1], раздел «Web-портал самообслуживания пользователей»);
- **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»).

14.1 Настройки личного кабинета

Важно! Раздел **Настройки личного кабинета** (Рис. 442) 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*.

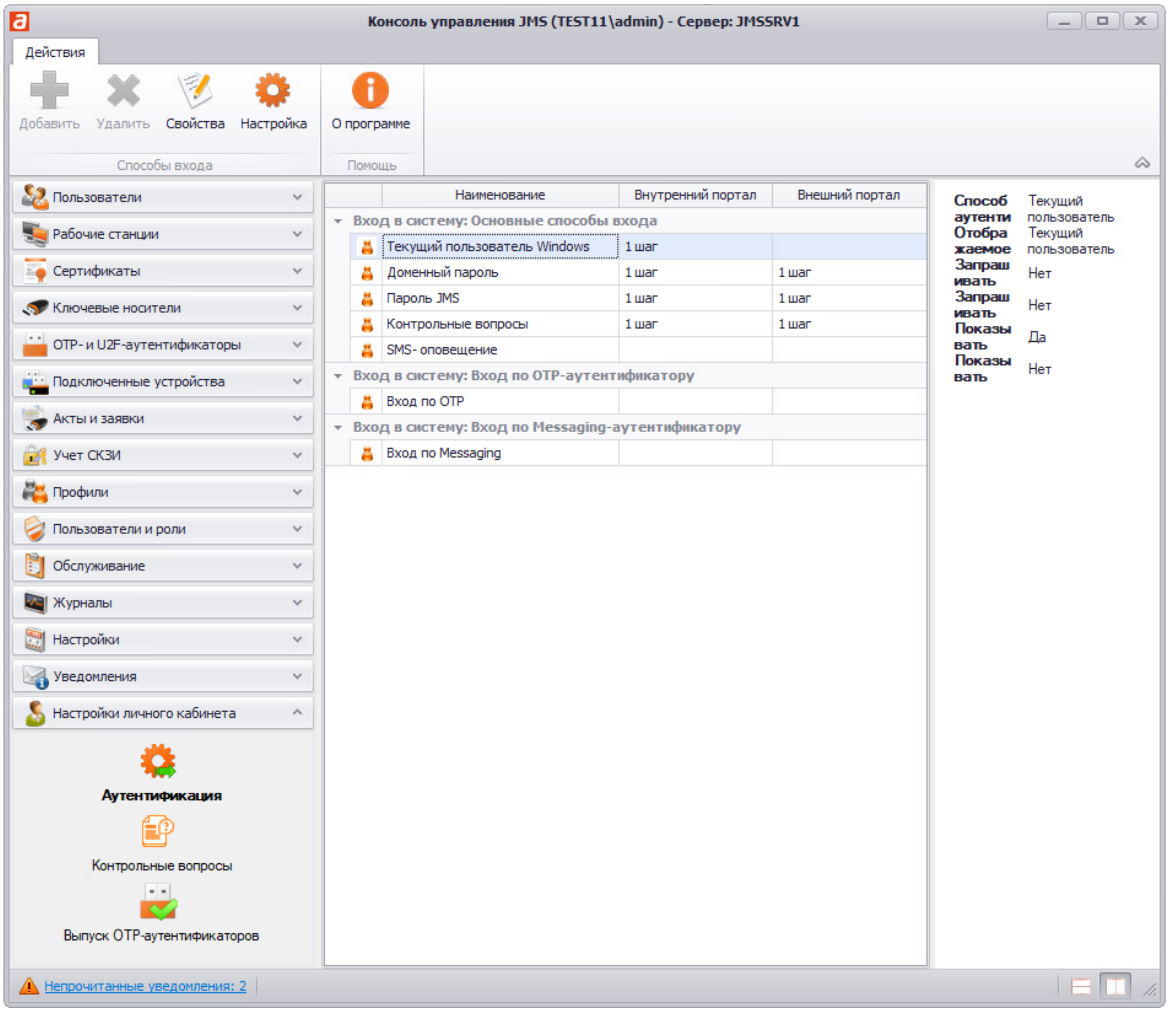


*Рис. 442 –Раздел **Настройки личного кабинета** консоли управления*

Раздел содержит следующие пункты:

- **Аутентификация** (см. «Раздел Аутентификация», ниже);
- **Контрольные вопросы** (см. «Раздел Контрольные вопросы», с. 514);
- **Выпуск OTP-аутентификаторов** (см. «Раздел Выпуск OTP-аутентификаторов», с. 518).

14.1.1 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. 443, подробнее см. руководство пользователя [1]).

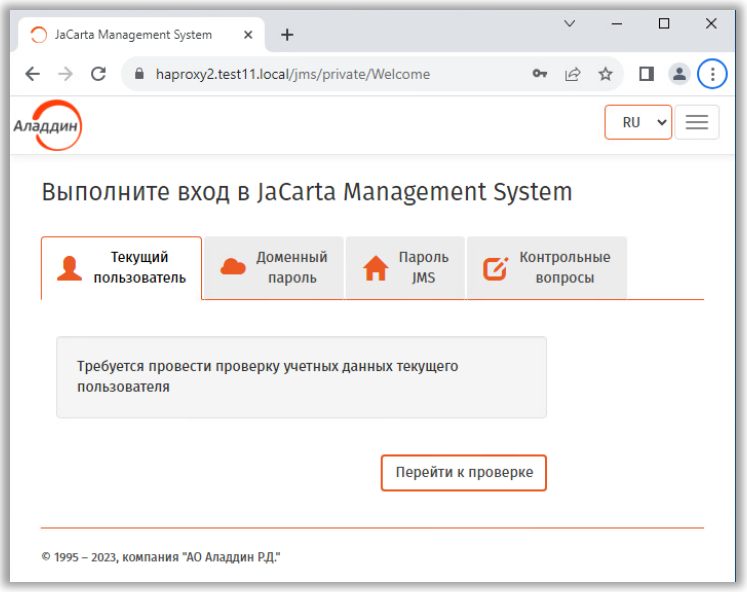


Рис. 443 –Пример страницы аутентификации пользователя на внутреннем Web-портале JWM

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.

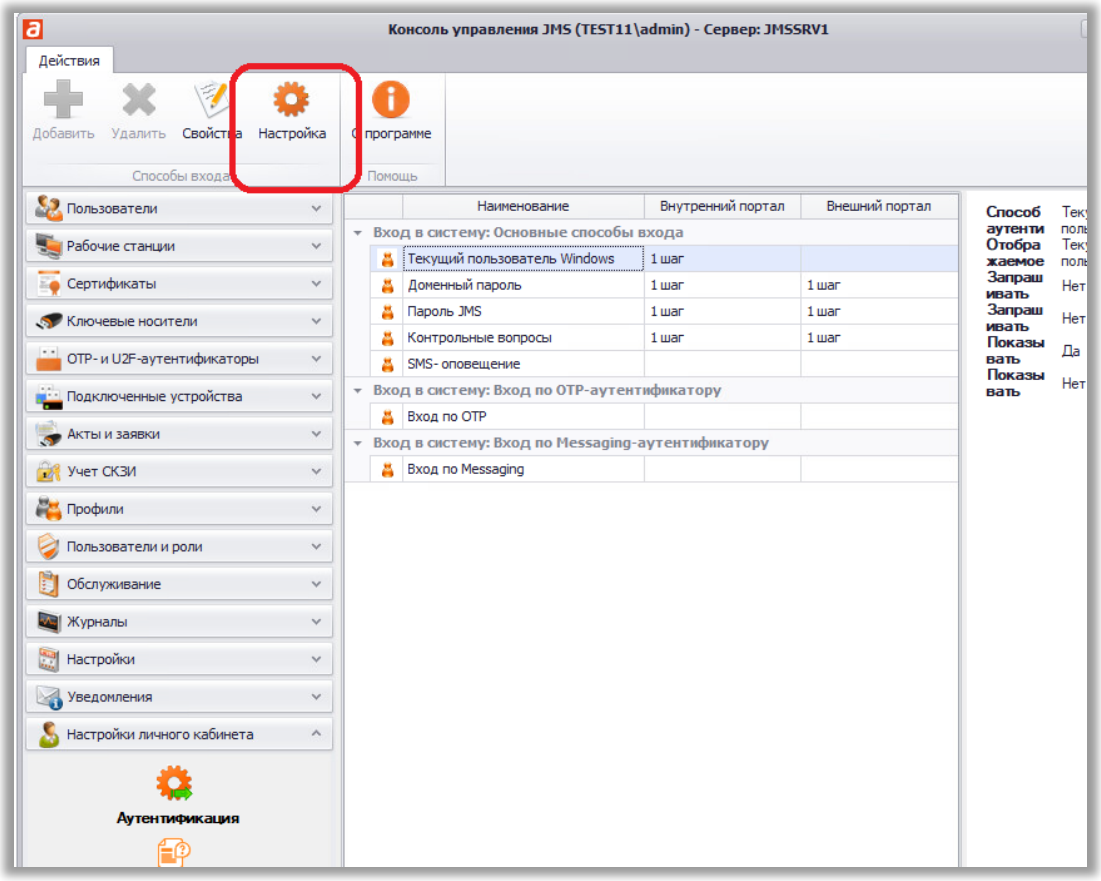


*Рис. 444 – Настройка раздела **Авторизация** личного кабинета (JWM)*

2. Для выполнения общих настроек аутентификации нажмите **Настройка** на верхней панели.

Отобразится следующее окно.

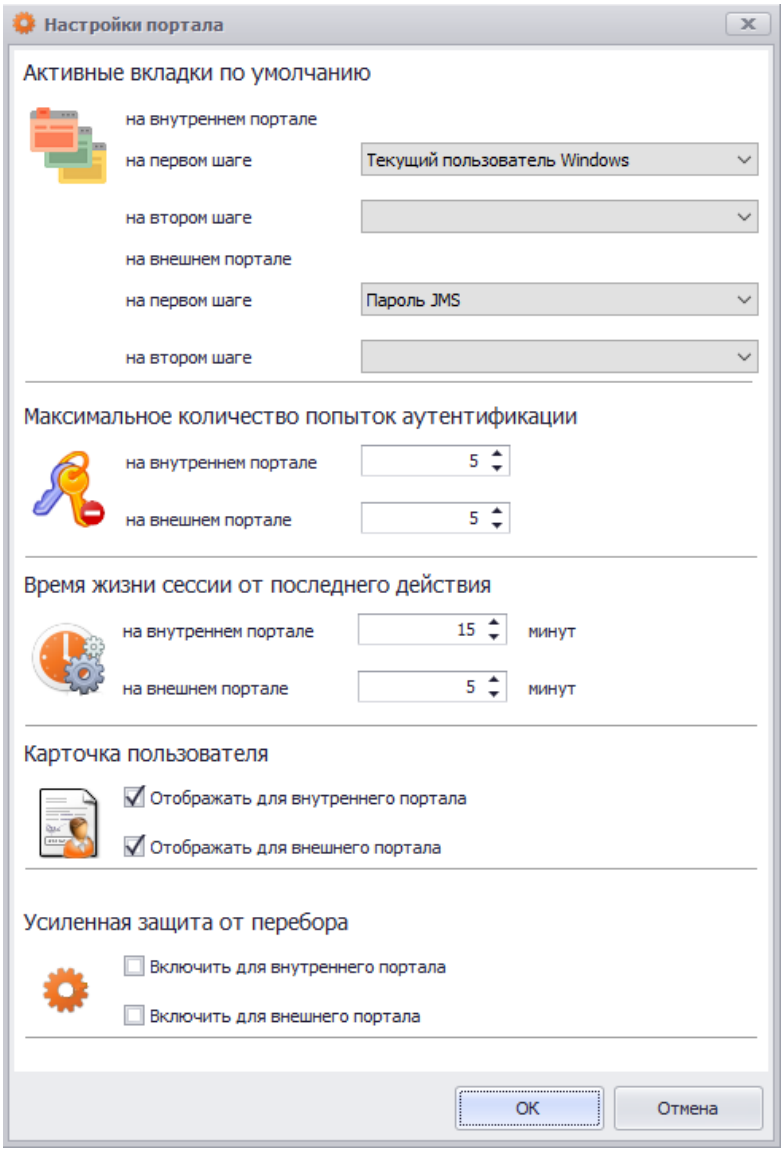


Рис. 445 – Окно настроек аутентификации в ЛК на портале JWM

3. Выполните общие настойки аутентификации в ЛК руководствуясь Табл. 106.

Табл. 106 – Общие настройки аутентификации в ЛК на портале JWM

Настройка	Описание
	<Секция> **Активные вкладки по умолчанию**
на внутреннем портале **на первом шаге**	Выберите вкладку с типом аутентификации, которая будет установлена в качестве **первого шага** *двухфакторной аутентификации пользователя* по умолчанию на внутреннем портале. Предлагаются выбор одного из следующих способов: • **Текущий пользователь Windows** • **SMS-оповещение** • **Вход по OTP** • **Вход по Messaging** • **Пароль JMS**

Настройка	Описание
	• **Доменный пароль** • **Контрольные вопросы**
на внутреннем портале **на втором шаге**	Выберите вкладку с типом аутентификации (отличную от выбранной на первом шаге), которая будет установлена в качестве **второго шага** *двухфакторной аутентификации пользователя* по умолчанию на внутреннем портале. Выбор предлагается из тог же списка.
на внешнем портале **на первом шаге** **на втором шаге**	Сделайте выбор вкладок по умолчанию, отражающих шаги *двухфакторной аутентификации пользователя* в ЛК на внешнем портале JWM по аналоги с тем, как это было описано выше для внутреннего портала.
<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**, (см. раздел «Общие настройки аутентификации по контрольным вопросам», Табл. 119, с. 516). 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	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	Та же настройка для внешнего портала. 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.

Настройка	Описание
Отображать для внешнего портала	Та же настройка для внешнего портала
<Секция> **Усиленная защита от перебора**	
Включить для внутреннего портала	Флаг отключения на странице входа детализированной информации об ошибках аутентификации, облегчающей злоумышленникам выполнять взлом логина путем перебора. На любые ошибки ввода неверной аутентификационных данных выдается унифицированное сообщение вида "Неверное имя пользователя или пароль". По умолчанию флаг защиты отключен.
Включить для внутреннего портала	Та же настройка для внешнего портала

4. Для настройки вкладок страницы аутентификации пользователя выберите соответствующую строку с названием пункта настроек в центральной части экрана (Рис. 444, с.489) и нажмите **Свойства** на верхней панели (или откройте свойства пункта двойным нажатием мыши). Выполните настройку, руководствуясь Табл. 107.

Табл. 107 – Пункты настроек вкладок на web-странице аутентификации пользователя в JWM

Название пункта	Описание
<Секция> **Вход в систему: основные способы входа**	
Текущий пользователь Windows	Данный пункт предназначен для настройки вкладки **Текущий пользователь Windows** Вкладка используется для авторизации пользователя, уже прошедшего процедуру аутентификации в ОС Windows. 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 Windows», с. 493.
Доменный пароль	Данный пункт предназначен для настройки вкладки **Доменный пароль** Вкладка используется для аутентификации пользователя в ЛК путем ввода доменного (AD) имени и пароля. Порядок настройки описан в разделе «Настройка вкладки Доменный пароль», с. 496
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. 41). Порядок настройки описан в разделе «Настройка вкладки Пароль JMS», с. 497

Название пункта	Описание
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. 500
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. 503 **Примечание.** Подробнее о настройке аутентификации с помощью SMS-оповещения см. в разделе «Настройка аутентификации пользователя в JWM по SMS-оповещению» с. 506).
<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. Порядок настройки описан в разделе «Настройка вкладки Вход по OTP», с. 507
<Секция> **Вход в систему: Вход по Messaging-аутентификатору**	
Вход по Messaging	Порядок настройки описан в разделе «Настройка вкладки Вход по Messaging», с. 511

14.1.1.1 Настройка вкладки Текущий пользователь Windows

Для настройки вкладки выполните следующие действия.

1. Окно параметров вкладки **Текущий пользователь Windows** выглядит следующим образом.

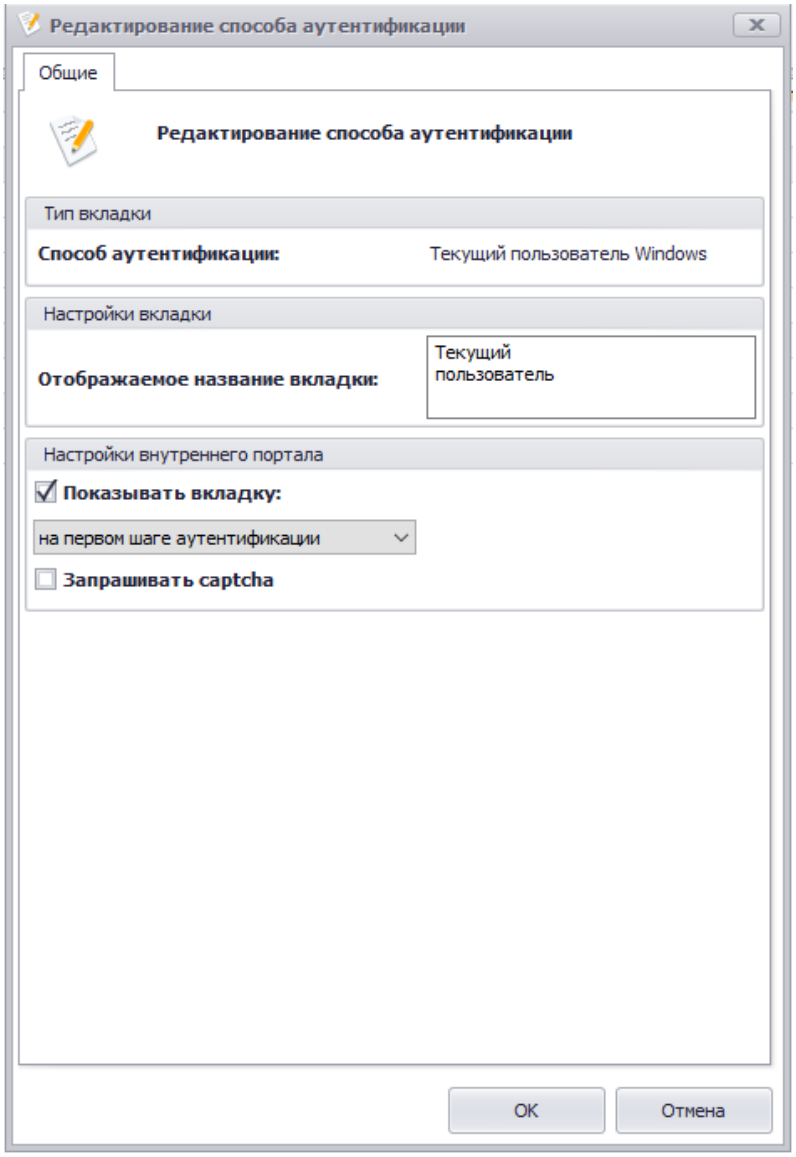


Рис. 446 – Настройка вкладки Текущий пользователь Windows

2. Выполните настройку, руководствуясь Табл. 108.

Табл. 108 – Параметры настройки вкладки Текущий пользователь Windows

Параметр	Описание
<Секция> **Тип вкладки**	
Способ аутентификации	(Нередактируемое поле) Текущий пользователь
<Секция> **Настройки вкладки**	
Отображаемое название вкладки	При необходимости отредактируйте отображаемое в web-интерфейсе название вкладки.

Параметр	Описание
	Значение по умолчанию: **Текущей пользователь**
<Секция> **Настройки внутреннего портала**	
Показывать вкладку	Установите флаг, если вкладка должна отображаться при аутентификации пользователя на внутреннем портале JWM. 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. По умолчанию не установлен.

3. По окончании настройки нажмите **ОК** для сохранения изменений.

14.1.1.2 Настройка вкладки Доменный пароль

1. Окно параметров вкладки **Доменный пароль** выглядит следующим образом.

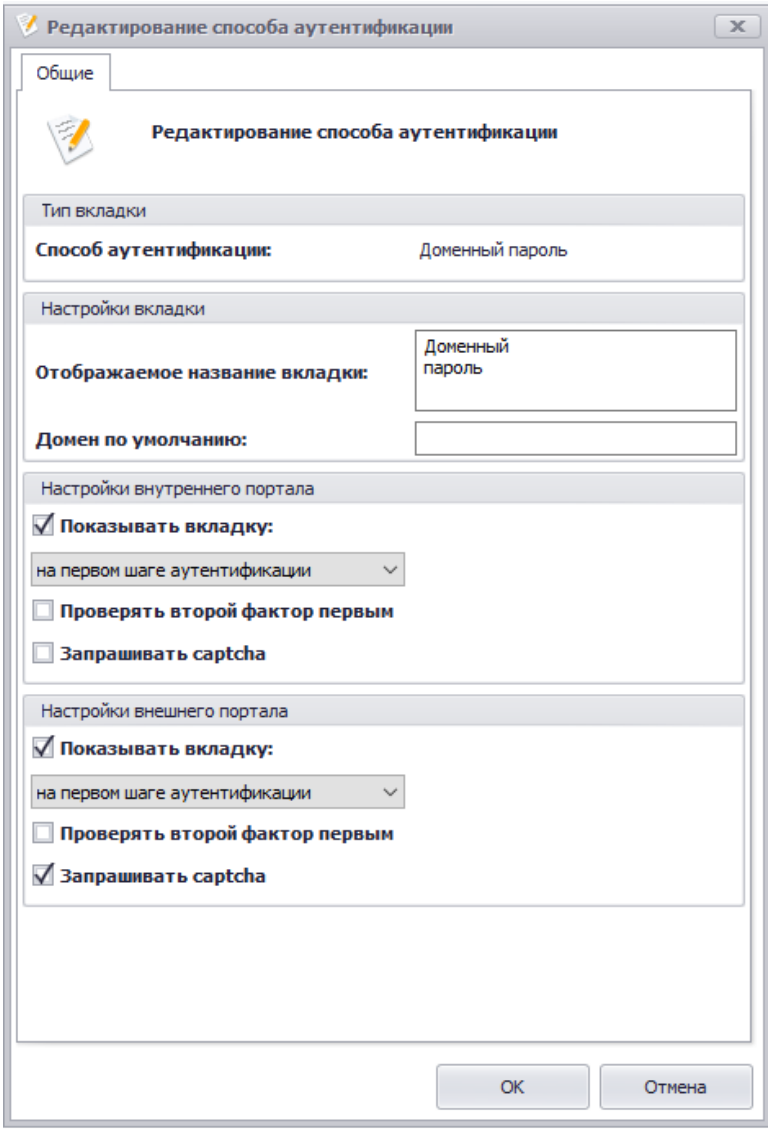


*Рис. 447 – Настройка вкладки **Доменный пароль***

2. Выполните настройку, руководствуясь Табл. 109.

Табл. 109 –Настройки вкладки Доменный пароль

Параметр	Описание
<Секция> **Тип вкладки**	
Способ аутентификации	(Нередактируемое поле) Доменный пароль
<Секция> **Настройки вкладки**	
Отображаемое название вкладки	При необходимости отредактируйте отображаемое в web-интерфейсе название вкладки.

Параметр	Описание
	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> **Настройки 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;
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> **Настройки 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 **OK** для сохранения изменений.

14.1.1.3 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. 41).

1. Окно параметров вкладки **Пароль JMS** выглядит следующим образом.

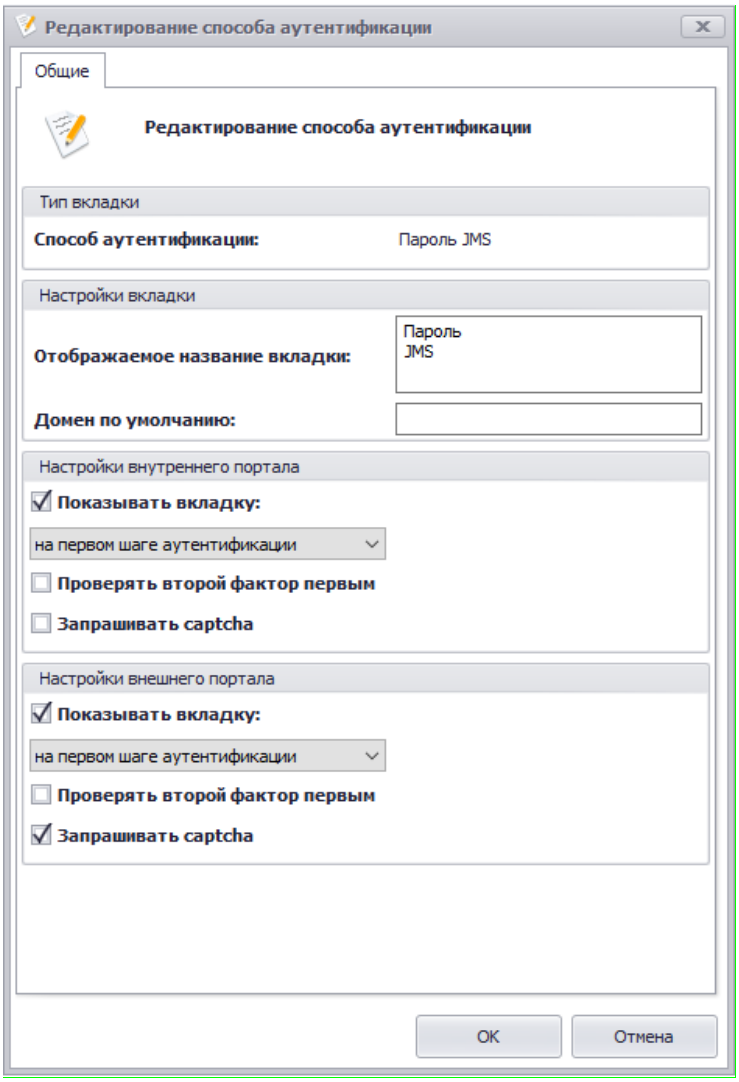


*Рис. 448 – Настройка вкладки **Пароль JMS***

2. Выполните настройку, руководствуясь Табл. 110.

Табл. 110 –Настройки вкладки Пароль JMS

Параметр	Описание
<Секция> **Тип вкладки**	
Способ аутентификации	(Нередактируемое поле) Пароль JMS
<Секция> **Настройки вкладки**	
Отображаемое название вкладки	При необходимости отредактируйте отображаемое в web-интерфейсе название вкладки. Значение по умолчанию: **Пароль JMS**

Параметр	Описание
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> **Настройки 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
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> **Настройки 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 **OK** для сохранения изменений.

14.1.1.4 Настройка вкладки Контрольные вопросы

1. Окно настройки параметров **Контрольные вопросы** включает в себя две вкладки и выглядит следующим образом.

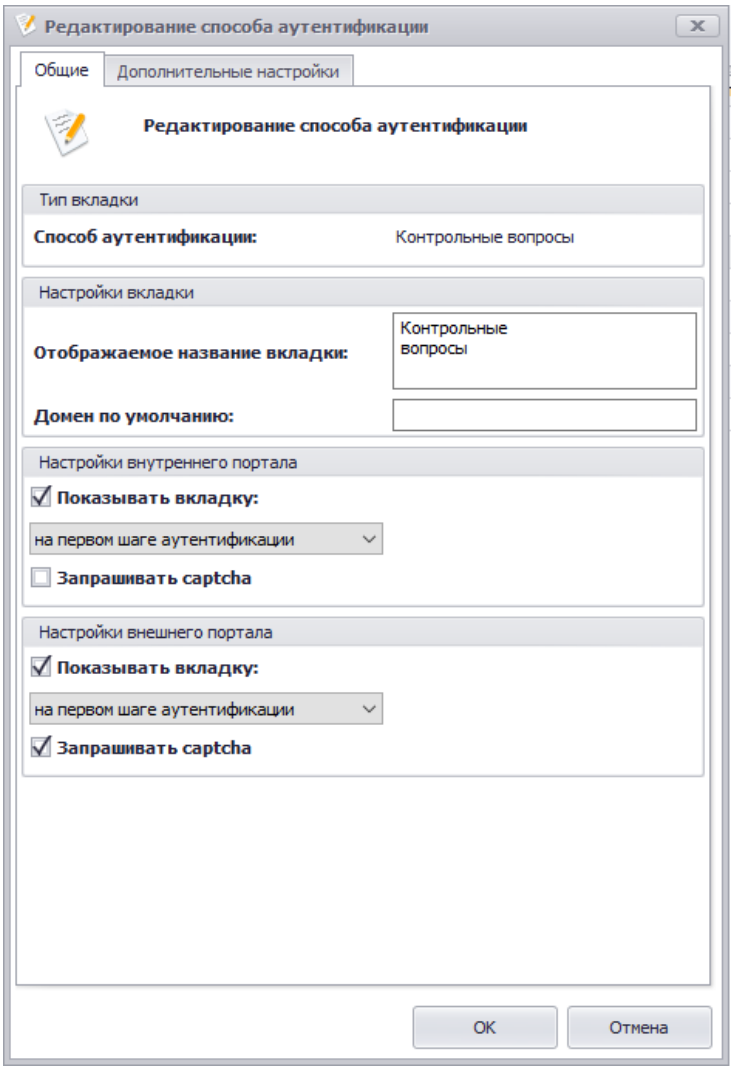


*Рис. 449 –Раздел **Общие** настроек вкладки Контрольные вопросы*

Рис. 450 –Раздел Дополнительных настроек вкладки Контрольные вопросы

2. Выполните настройки на двух вкладках, руководствуясь Табл. 111 и Табл. 112 соответственно.

Табл. 111 –Общие настройки вкладки Контрольные вопросы

Параметр	Описание
<Секция> **Тип вкладки**	
Способ аутентификации	(Нередактируемое поле) Контрольные вопросы
<Секция> **Настройки вкладки**	
Отображаемое название вкладки	При необходимости отредактируйте отображаемое в web-интерфейсе название вкладки. Значение по умолчанию: **Контрольные вопросы**
<Секция> **Настройки внутреннего портала**	
Показывать вкладку	Установите флаг, если вкладка должна отображаться при аутентификации пользователя на внутреннем портале JWM. Значение по умолчанию: установлен

Параметр	Описание
	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> **Настройки 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

Табл. 112 –Дополнительные настройки вкладки Контрольные вопросы

Параметр	Описание
<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 (см. разделы «Настройка вкладки Вход по OTP», с. 507 и «Настройка вкладки Вход по Messaging», с. 511). **Примечание.** Отмена проверки по *Контрольным вопросам* проявляется в отсутствии соответствующей вкладки на web-странице аутентификации пользователя. Значение по умолчанию: не установлен

3. По окончании настройки нажмите **ОК** для сохранения изменений.

14.1.1.5 Настройка вкладки SMS-оповещение

1. Окно настройки параметров **SMS-оповещение** включает в себя две вкладки и выглядит следующим образом.

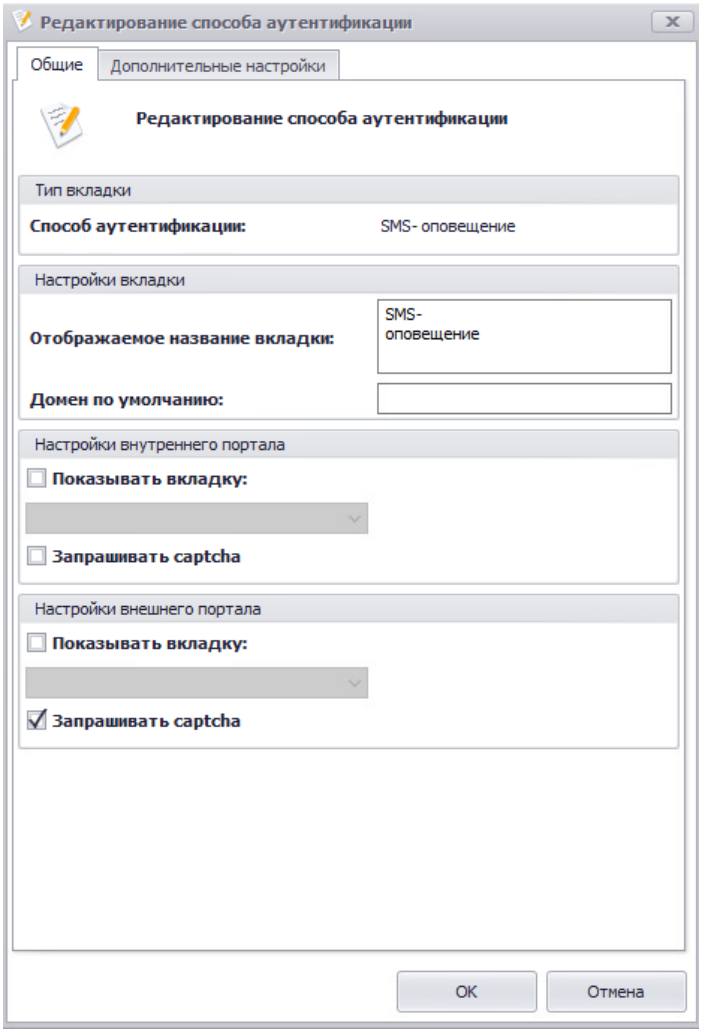


*Рис. 451 –Раздел **Общие** настроек вкладки SMS-оповещение*

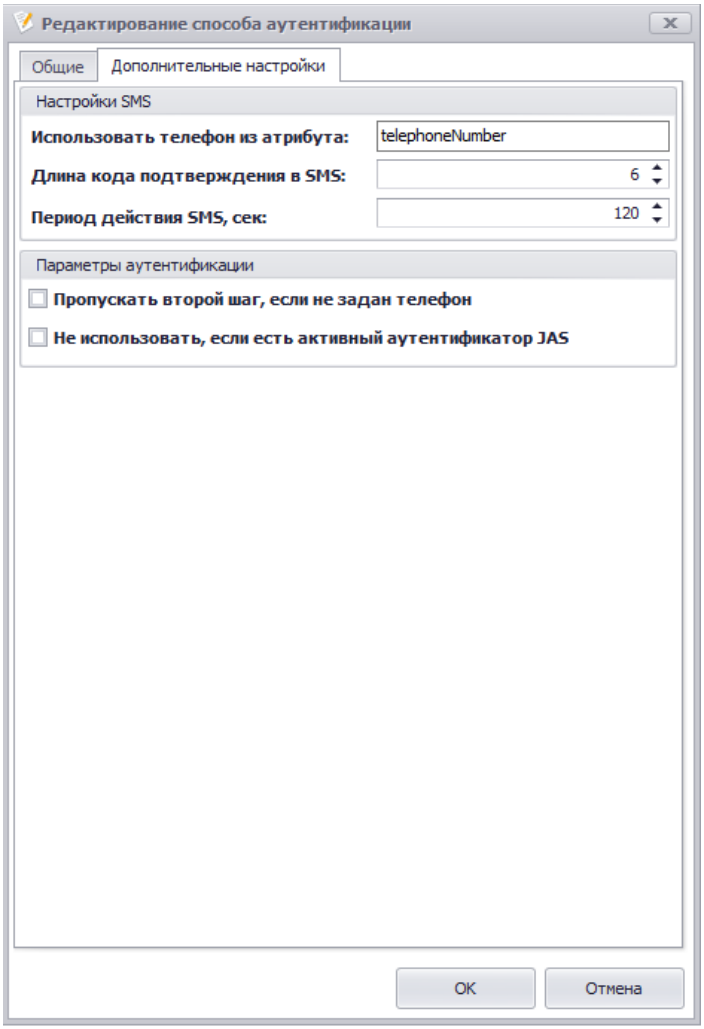


Рис. 452 –Раздел Дополнительных настроек вкладки SMS-оповещение

2. Выполните настройки на двух вкладках, руководствуясь Табл. 113 и Табл. 114 соответственно.

Табл. 113 – Общие настройки вкладки SMS-оповещение

Параметр	Описание
<Секция> **Тип вкладки**	
Способ аутентификации	(Нередактируемое поле) SMS-оповещение
<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.

Параметр	Описание
	Значение по умолчанию: пустая строка
<Секция> **Настройки 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> **Настройки 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

Табл. 114 – Дополнительные настройки вкладки SMS-оповещение

Параметр	Описание
<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. 506)
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. 506)
Период действия SMS, сек	Параметр устанавливает время действия кода из SMS для аутентификации пользователя на портале (в секундах) Значение по умолчанию: 120

Параметр	Описание
<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. **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-токен (см. разделы «Настройка вкладки Вход по OTP», с. 507 и «Настройка вкладки Вход по Messaging», с. 511). **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 **OK** для сохранения изменений.

14.1.1.6 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. 503).

   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 системы с JMS посредством выполнения плана обслуживания по умолчанию (см. раздел «План обслуживания по умолчанию», с. 413).

2. Выполните настройки Messaging-транспорта в серверном агенте JAS согласно руководству по установке и настройке JAS [3] (раздел «Настройки Messaging-транспорта»).

Примечание. Сервис аутентификации пользователей в JWM по SMS-оповещению использует тот же транспорт, что и Messaging-токены.

14.1.1.7 Настройка вкладки Вход по OTP

1. Окно настройки параметров **Вход по OTP** включает в себя две вкладки и выглядит следующим образом.

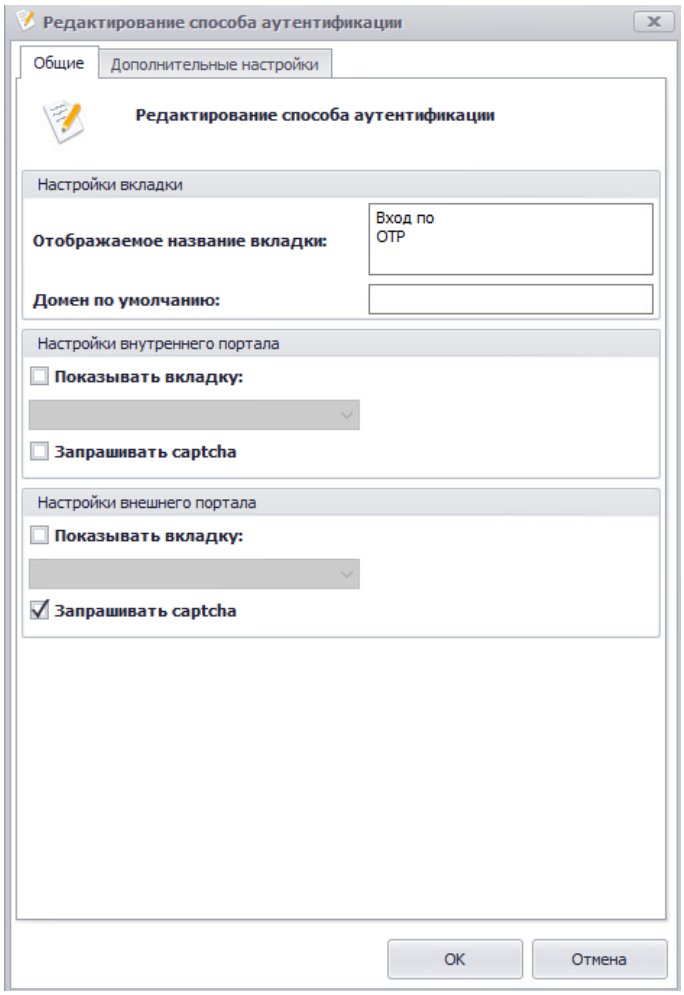


*Рис. 453 –Раздел **Общие** настроек вкладки **Вход по OTP***

*Рис. 454 –Раздел **Дополнительных** настроек вкладки **Вход по OTP***

2. Выполните настройки на двух вкладках, руководствуясь Табл. 115 и Табл. 116 соответственно.

Табл. 115 – Общие настройки вкладки Вход по OTP

Параметр	Описание
<Секция> **Тип вкладки**	
Способ аутентификации	(Нередактируемое поле) Вход по OTP
<Секция> **Настройки вкладки**	
Отображаемое название вкладки	При необходимости отредактируйте отображаемое в web-интерфейсе название вкладки. Значение по умолчанию: **Вход по OTP**
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.

Параметр	Описание
	Значение по умолчанию: пустая строка
<Секция> **Настройки 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> **Настройки 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

Табл. 116 –Дополнительные настройки вкладки Вход по OTP

Параметр	Описание
<Секция> **Настройки OTP**	
Запрашивать OTP-PIN-код	Флаг необходимости указания пользователями PIN-кода для OTP при аутентификации на портале **Важно!** В текущей версии JMS при установке запроса PIN-кода OTP следует убедиться, что во всех профилях, на основе которых были выпущены аппаратные и программные OTP-токены, в режиме аутентификации присутствует запрос PIN-кода OTP (например **OTP PIN-код + OTP**, либо **Доменный пароль + OTP PIN-код + OTP**).
Запрашивать доменный пароль	Флаг необходимости указания пользователями доменного пароля при аутентификации на портале **Важно!** В текущей версии JMS при установке запроса доменного пароля следует убедиться, что во всех профилях, на основе которых были выпущены аппаратные и программные OTP-токены, в режиме аутентификации присутствует запрос **Доменный пароль** (например **Доменный пароль + OTP**, либо **Доменный пароль + OTP PIN-код + OTP**).

Параметр	Описание
<Секция> **Параметры аутентификации** **Пропускать второй шаг:** **Примечание.** По факту полная отмена второго шага (с превращением в однофакторную аутентификацию) произойдет лишь если для второго шага определён единственный способ (Вход по OTP). В общем же случае пользователю будут предложены альтернативные способы аутентификации для второго шага, если они были определены.	
если пользователь не имеет аутентификатора JAS	Флаг отмены второго шага двухфакторной аутентификации, если такой аутентификатор не выпущен для данного пользователя в JMS. Значение по умолчанию: не установлен
если аутентификатор JAS не активирован	То же, но для случая, когда OTP-аутентификатор пользователю выпущен, но не активирован. Значение по умолчанию: не установлен

3. По окончании настройки нажмите **OK** для сохранения изменений.

14.1.1.8 Настройка вкладки Вход по Messaging

1. Окно настройки параметров **Вход по Messaging** включает в себя две вкладки и выглядит следующим образом.

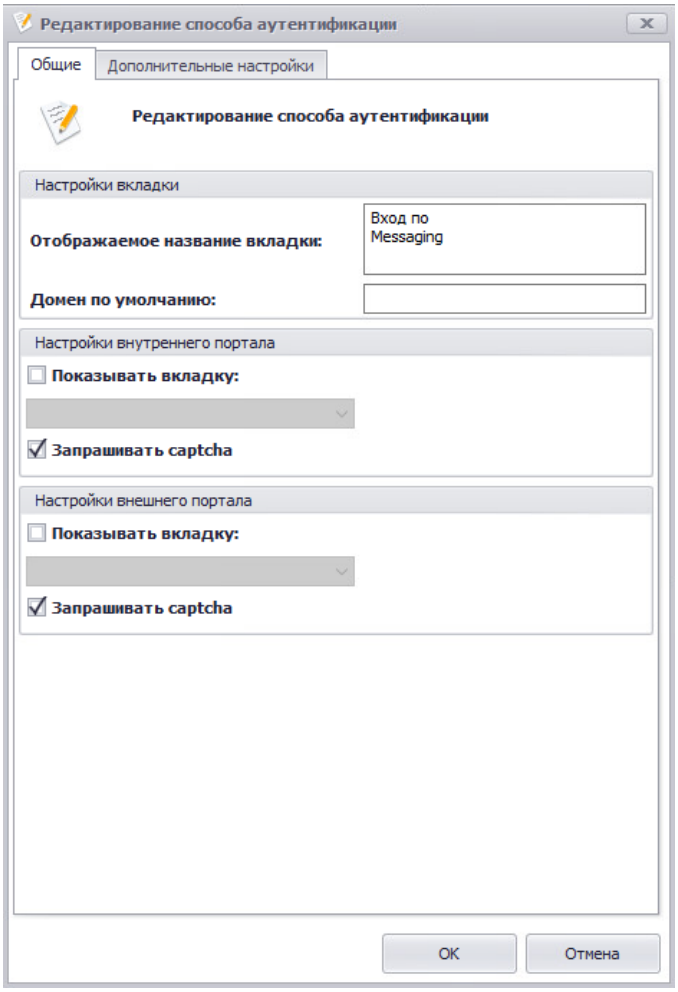


*Рис. 455 –Раздел **Общие** настроек вкладки **Вход по Messaging***

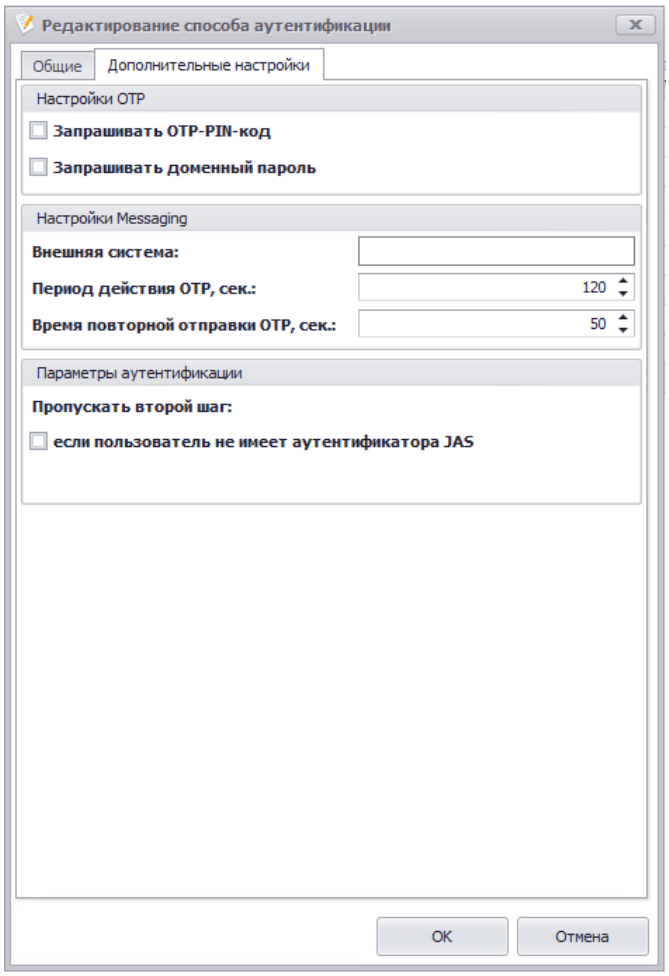


*Рис. 456 –Раздел **Дополнительных** настроек вкладки **Вход по Messaging***

2. Выполните настройки на двух вкладках, руководствуясь Табл. 117и Табл. 118 соответственно.

Табл. 117 – Общие настройки вкладки Вход по Messaging

Параметр	Описание
<Секция> **Настройки вкладки**	
Отображаемое название вкладки	При необходимости отредактируйте отображаемое в web-интерфейсе название вкладки. Значение по умолчанию: **Вход по Messaging**
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> **Настройки внутреннего портала**	
Показывать вкладку	Установите флаг, если вкладка должна отображаться при аутентификации пользователя на внутреннем портале JWM. Значение по умолчанию: не установлен

Параметр	Описание
	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: установлен
<Секция> **Настройки внешнего портала**	
Показывать вкладку **Запрашивать captcha**	Параметры имеют то же назначение, что и для случая внутреннего портала (выше).

Табл. 118 – Дополнительные настройки вкладки Вход по Messaging

Параметр	Описание
<Секция> **Настройки OTP**	
Запрашивать OTP-PIN-код	Флаг необходимости указания пользователями PIN-кода для OTP при аутентификации на портале **Важно!** В текущей версии JMS при установке запроса PIN-кода OTP следует убедиться, что во всех профилях, на основе которых были выпущены аппаратные и программные OTP-токены, в режиме аутентификации присутствует запрос PIN-кода OTP (например **OTP PIN-код + OTP**, либо **Доменный пароль + OTP PIN-код + OTP**).
Запрашивать доменный пароль	Флаг необходимости указания пользователями доменного пароля при аутентификации на портале **Важно!** В текущей версии JMS при установке запроса доменного пароля следует убедиться, что во всех профилях, на основе которых были выпущены аппаратные и программные OTP-токены, в режиме аутентификации присутствует запрос **Доменный пароль** (например **Доменный пароль + OTP**, либо **Доменный пароль + OTP PIN-код + OTP**).
<Секция> **Настройки Messaging**	
Внешняя система	Идентификатор JWM как «внешней системы», для которой организуется Messaging-аутентификация. Следует указать тот же идентификатор, который указан в поле **Внешняя система** профиля выпуска Messaging-токенов (должен быть создан специально для JWM), вкладка **Параметры выпуска** (см. Табл. 53, с. 271) **Важно!** Для корректной настройки JWM следует сначала создать профиль (профили) выпуска Messaging-токенов, предназначенный специально для аутентификации пользователей в JWM, с указанием одного и того же идентификатора внешней системы (JWM), и уже этот идентификатор указать в данном поле

Параметр	Описание
Период действия OTP, сек.	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: **120** **Примечание.** Данная настройка используется только при аутентификации пользователей на порталах JWM. Данная настройка имеет приоритет перед аналогичной настройкой из профиля выпуска messaging-токенов **Время жизни OTP** (настройка профиля игнорируется).
Время повторной отправки OTP, сек.	Определяет, через какое время (в секундах) с момента генерации предыдущего пароля OTP разрешается запрашивать следующий. Значение по умолчанию: **50** **Примечание.** Данная настройка используется только при аутентификации пользователей на порталах JWM. Данная настройка имеет приоритет перед аналогичной настройкой из профиля выпуска messaging-токенов **Задержка генерации OTP** (настройка профиля игнорируется).
<Секция> **Параметры аутентификации** **Пропускать второй шаг:** **Примечание.** По факту полная отмена второго шага (с превращением в однофакторную аутентификацию) произойдет лишь если для второго шага определён единственный способ (Вход по Messaging). В общем же случае пользователю будут предложены альтернативные способы аутентификации для второго шага, если они были определены.	
если пользователь не имеет аутентификатора JAS	Флаг отмены второго шага двухфакторной аутентификации, если такой аутентификатор не выпущен для данного пользователя в JMS. Значение по умолчанию: не установлен

3. По окончании настройки нажмите **OK** для сохранения изменений.

14.1.2 Раздел Контрольные вопросы

Контрольные вопросы – это один из способов аутентификации пользователя при обращении к JMS с внутреннего или внешнего портала JWM. В личном кабинете портала самообслуживания пользователь в процессе настройки своей учетной записи должен определить заданное число контрольных вопросов и ответов на них (см. раздел «Общие настройки аутентификации по контрольным вопросам», с. 515). Часть из этих контрольных вопросов он может выбрать из числа так называемых *стандартных* (предопределенных, созданных администратором) вопросов.

В разделе **Настройки личного кабинета -> Контрольные вопросы** можно:

- выполнить общие настройки аутентификации по контрольным вопросам;
- сформировать список *стандартных вопросов*.

14.1.2.1 Общие настройки аутентификации по контрольным вопросам

Чтобы произвести общие настройки для метода аутентификации *Контрольные вопросы* выполните следующие действия.

1. Откройте раздел **Настройки личного кабинета** -> **Контрольные вопросы** в консоли управления JMS.
   Отобразится следующее окно.

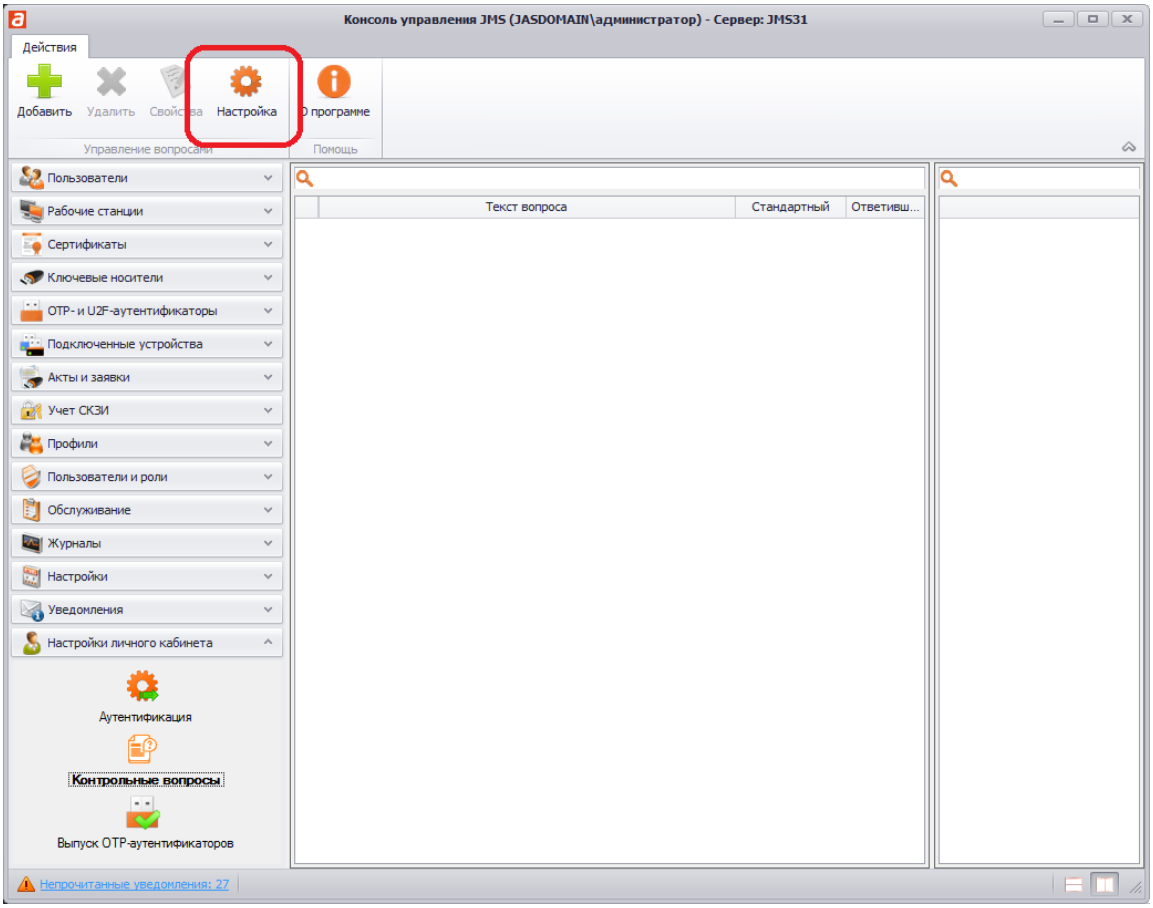


*Рис. 457 – Выбор общих настроек раздела **Контрольные вопросы***

2. Для выполнения общих настроек аутентификации по контрольным вопросам нажмите **Настройки** на верхней панели.

Отобразится следующее окно.

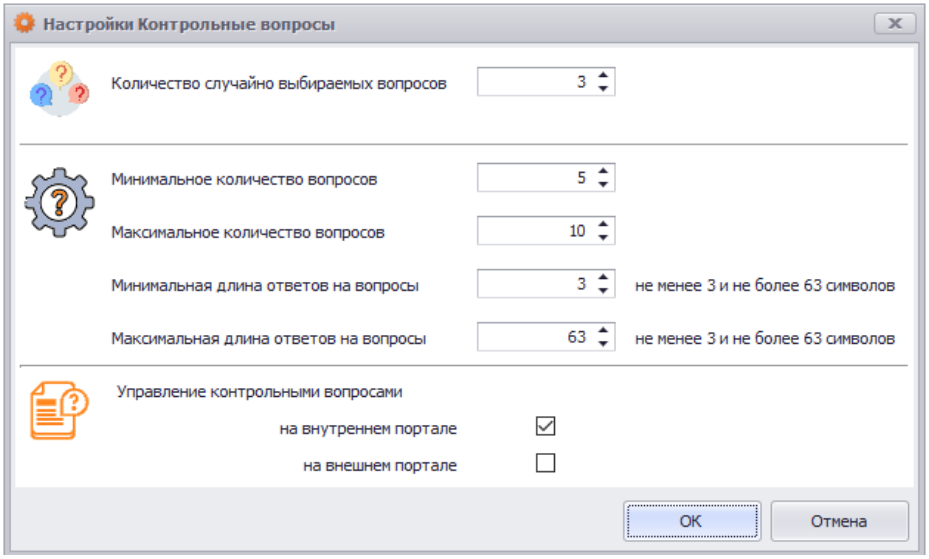


Рис. 458 – Окно общих настроек аутентификации в ЛК по контрольным вопросам

3. Выполните общие настойки аутентификации в ЛК по контрольным вопросам руководствуясь Табл. 119.

Табл. 119 – Общие настройки аутентификации в ЛК по контрольным вопросам

Настройка	Описание
Количество случайно выбираемых вопросов	Число контрольных вопросов, отображаемых на странице при аутентификации пользователя (вопросы выбираются случайным образом из полного списка контрольных вопросов, определенных пользователем; для успешной аутентификации необходимо дать верный ответ на каждый из вопросов). Значение по умолчанию: **3**
Минимальное количество вопросов	Минимальное число контрольных вопросов, которые должен определить (установить) пользователь в личных настройках. Значение по умолчанию: **5**
Максимальное количество вопросов	Максимальное число контрольных вопросов, которые может установить пользователь в личных настройках. Значение по умолчанию: **10**
Минимальное длина ответов на вопросы	Минимальное число символов в ответе на контрольный вопрос. Значение по умолчанию: **3**
Максимальная длина ответов на вопросы	Максимальное число символов в ответе на контрольный вопрос. Значение по умолчанию: **3**
	<секция> **Управление контрольными вопросами**
на внутреннем портале	Флаг, позволяющий отключить вкладку Вопросы в личном кабинете пользователя на внутреннем портале

Настройка	Описание
	Значение по умолчанию: не включен
на внешнем портале	То же для внешнего портала. Значение по умолчанию: включен

14.1.2.2 Формирование списка стандартных контрольных вопросов

Для формирования списка *стандартных* контрольных вопросов выполните следующие действия.

1. Откройте раздел **Настройки личного кабинета** -> **Контрольные вопросы** в консоли управления JMS.
   Отобразится следующее окно.

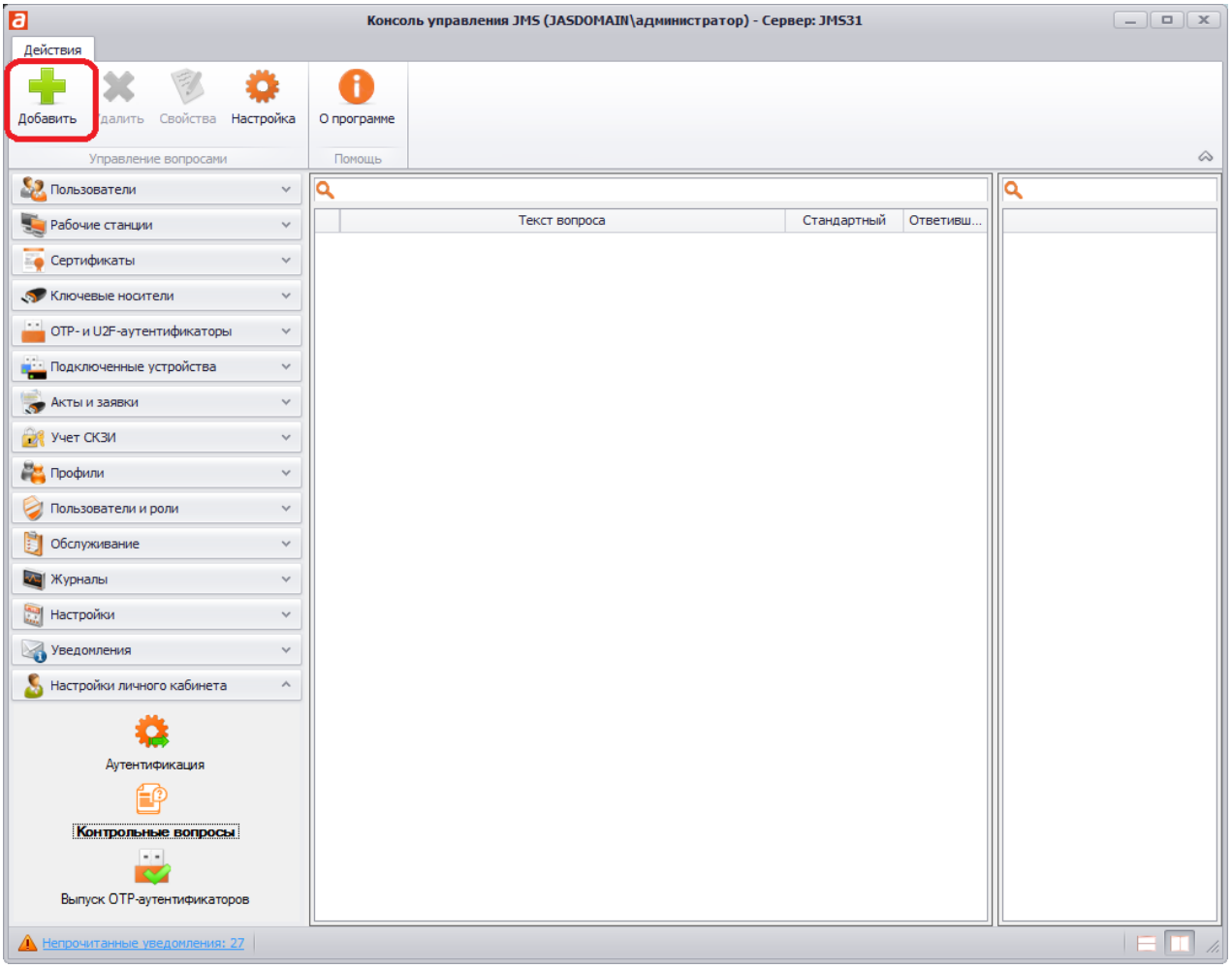


*Рис. 459 – Выбор общих настроек раздела **Контрольные вопросы***

2. Чтобы добавить контрольный вопрос нажмите. **Добавить** на верхней панели.

Отобразится следующее окно.

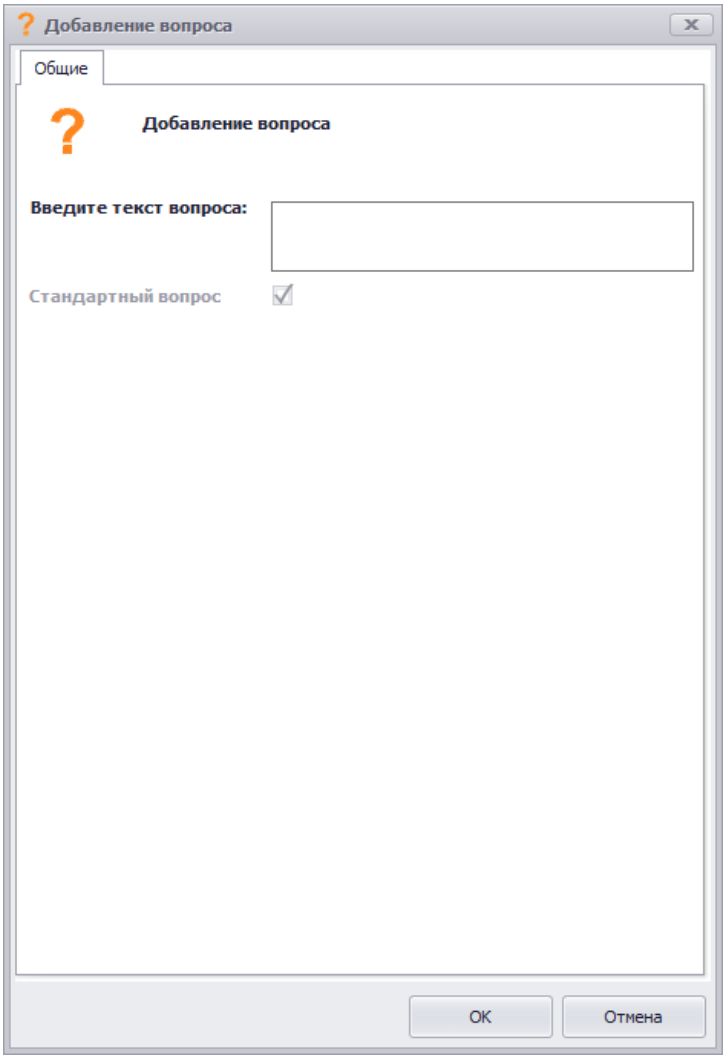


Рис. 460 – Окно общих настроек аутентификации в ЛК по контрольным вопросам

3. Введите текст вопроса в соответствующем поле, например «Кличка вашего домашнего питомца»
4. Нажмите **OK**, чтобы сохранить внесенные изменения.

Вопрос сохранится в списке стандартных контрольных вопросов JMS.

Если контрольный вопрос необходимо отредактировать или исключить из списка стандартных (т.е. предлагаемых в качестве таковых пользователю для формирования своего списка), выберите данный вопрос в списке, откройте на редактирование, нажав **Свойства** на верхней панели. При этом вы сможете отредактировать текст или снять флаг **Стандартный**.

Если контрольный вопрос необходимо удалить, нажмите **Удалить** на верхней панели.

14.1.3 Раздел Выпуск OTP-аутентификаторов

Данный раздел консоли управления JMS (Рис. 461) позволяет обеспечить дополнительную настройку профиля выпуска OTP-аутентификаторов, а именно – разрешить/отменить для пользователей, на которых распространяется данный профиль, возможность выпуска соответствующего OTP-аутентификатора.

Примечание. Под OTP-аутентификаторами подразумеваются программный OTP-, Messaging и Push OTP-токены.

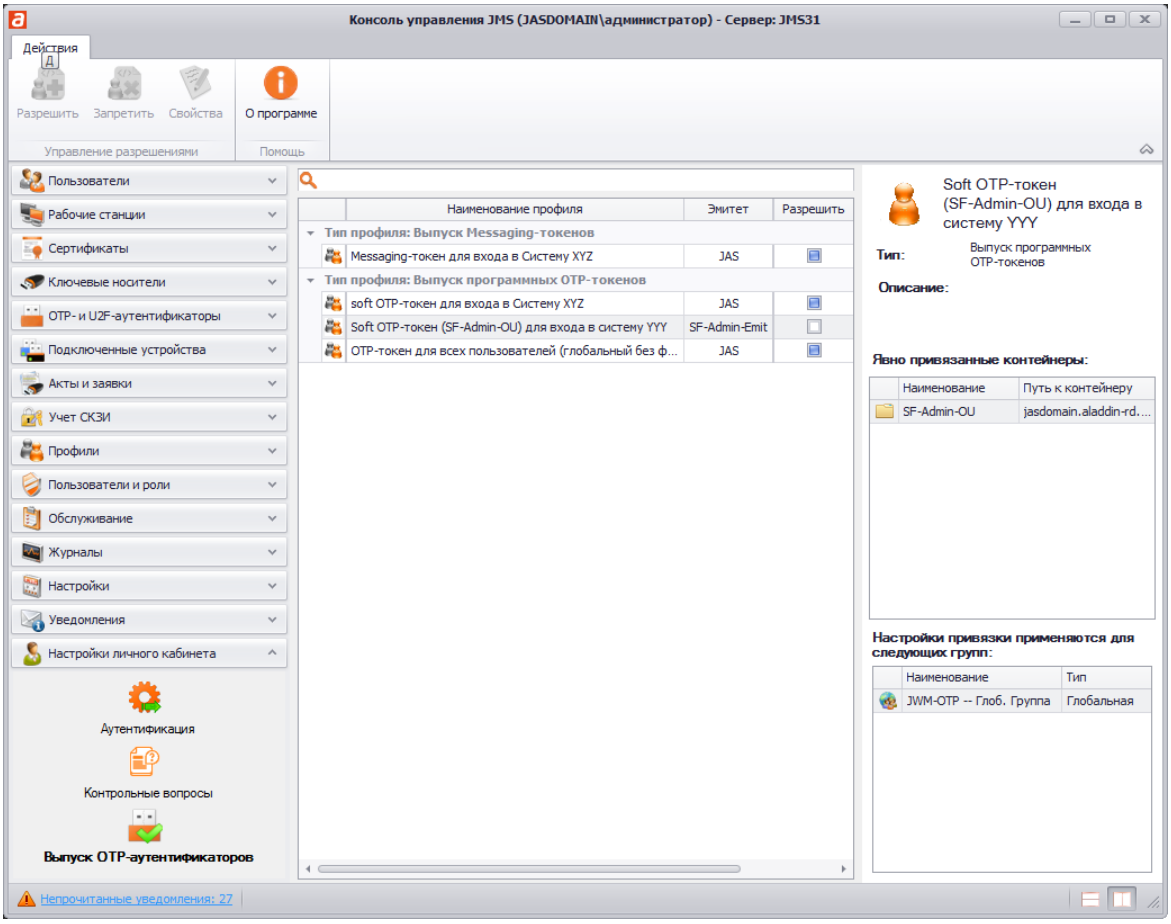


Рис. 461 – Общий вид раздела Выпуск OTP-аутентификатора

Для того чтобы выполнить такую настройку, предварительно следует создать соответствующий профиль (см. например «Настройка профиля выпуска программных OTP-токенов», с. 262).

Для того чтобы разрешить/отменить для пользователей, на которых распространяется профиль выпуска OTP-аутентификатора, возможность выпуска соответствующего OTP-аутентификатора выполните следующие действия.

1. В разделе **Настройки личного кабинета** -> **Выпуск OTP-аутентификатора** в центральной части экрана выберите необходимый профиль выпуска и откройте его двойным нажатием левой кнопки мыши.

Откроется окно следующего вида.

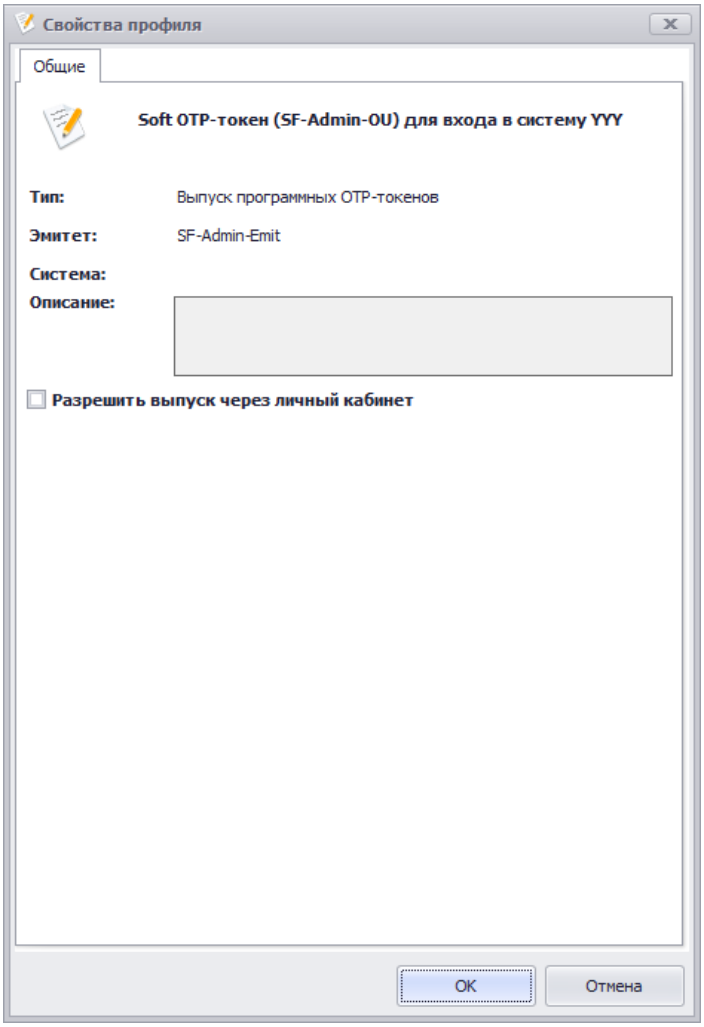


Рис. 462 – Окно настройки разрешения выпуска OTP-аутентификатора через ЛК

2. Если следует разрешить самостоятельный выпуск OTP-аутентификаторов по данному профилю установите флаг **Разрешить выпуск через личный кабинет** (в противном случае, оставьте данный флаг неустановленным).
3. Нажмите **OK** для завершения настройки.

В случае если в окне настройки профиля отображается предупреждение «Не указан фильтр по группе...» (Рис. 463), то при самостоятельном выпуске OTP-аутентификаторов из личного кабинета у пользователей не будет возможности отказаться от выпуска токена данного типа (он будет выпущен в любом случае). Опция отказа будет заблокирована (см. Рис. 464, с. 521).

Для того чтобы предотвратить такое поведение системы следует при привязке профиля выпуска OTP-аутентификатора создать фильтр по глобальной группе. Подробнее см. раздел «Порядок настройки самостоятельного выпуска пользователями OTP-аутентификатора», с. 310).

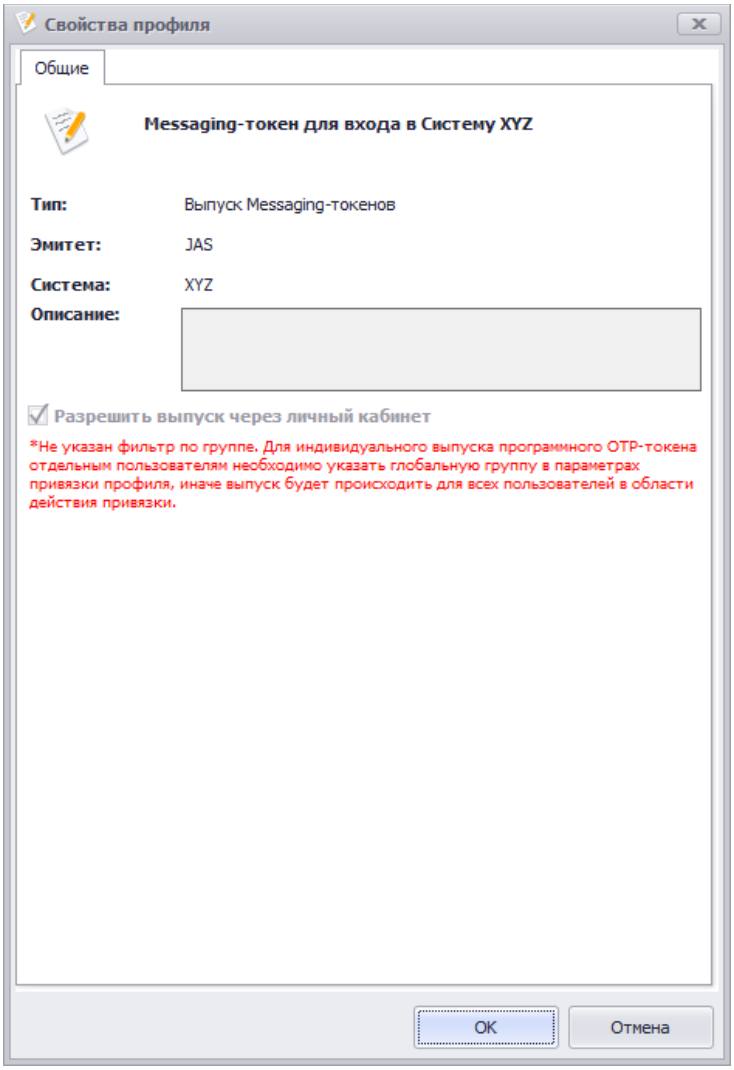


Рис. 463 – Предупреждение об отсутствии фильтрации по глобальной группе

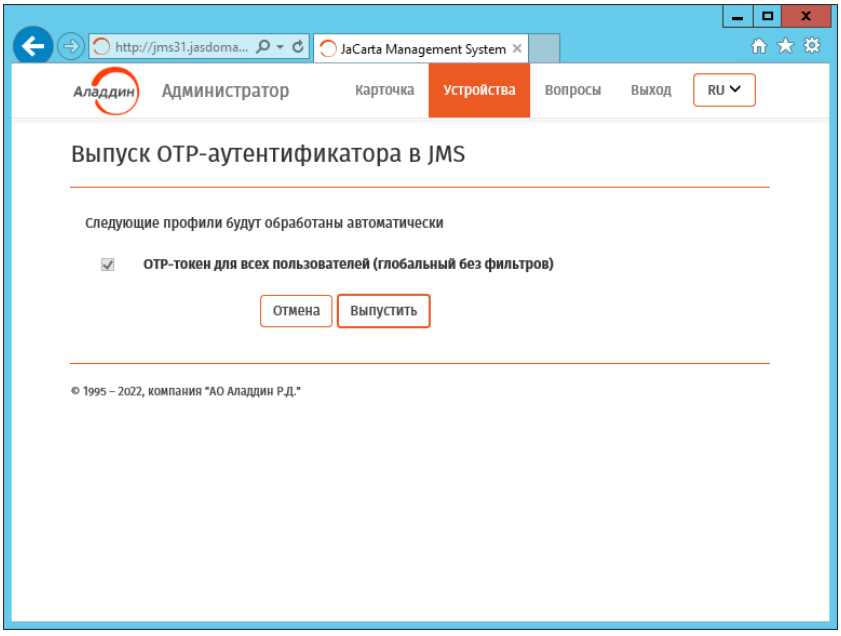


Рис. 464 – Возможность отказа от выпуска OTP-аутентификатора в ЛК заблокирована

15. Служба каталога JMS (JDS)

Служба каталога JMS (JMS Directory Service – JDS) представляет собой компонент JMS, позволяющий хранить информацию о пользователях и организационной структуре предприятия независимо от других ресурсных систем, таких как служба каталога Active Directory или удостоверяющий центр КриптоПро УЦ.

JDS обеспечивает тесную интеграцию с JMS и позволяет управлять объектами, хранящимися в службе каталога, непосредственно из консоли управления JMS.

JDS реализована в распределенной клиент-серверной архитектуре, включающей в себя 3 компонента:

- Служба каталога JMS (название компонента в мастере установки — «Служба каталога JMS»):
  - версия в виде службы Windows;
  - версия в виде приложения сервера IIS.
- Расширение для приложения Консоль управления JMS (название компонента в мастере установки — «Поддержка консоли управления JMS»). Компонент устанавливается на компьютере, на котором функционирует приложение *Консоль управления JMS*.
- Коннектор для сервера JMS (название компонента в мастере установки — «Поддержка Сервера JMS»). Компонент устанавливается на компьютере, на котором функционирует сервер JMS (компонент JMS Server).

Важно! Компонент «Поддержка консоли управления JMS» требует установки на каждом хосте, на котором функционирует приложение *Консоль управления JMS*.

Полный цикл установки и настройки JDS включает в себя 3 этапа:

1. Установка JDS (см «Установка JDS», с. 524)
2. Настройка JDS с помощью мастера настройки (см. «Настройка JDS», с. 529)
3. Настройка доступа к новой ресурсной системе (JDS) в серверном агенте (см. «Регистрация каталога учетных записей JDS на сервере JMS», с. 537)

Инсталлятор JDS способен автоматически определять наличие на хосте того типа приложения (сервера JMS или консоли управления), для которого требуется установить соответствующий компонент JDS. Нужный компонент JDS можно также выбрать вручную в режиме выборочной установки.

15.1 Дистрибутив

Дистрибутив компонента JDS состоит из одного файла *Aladdin.JMS.DirectoryService.msi*.

15.2 Системные требования для JDS

Табл. 120 – Системные требования для установки компонента JDS

Компонент среды функционирования	Требование
Процессор, оперативная память, дисковая память	Требования к процессору и оперативной памяти не отличаются от соответствующих системных требований к серверной операционной системе, на которой устанавливается компонент JDS

Компонент среды функционирования	Требование
Место на диске	Для установки компонента JDS требуется минимум 40 Мбайт свободного дискового пространства
Операционная система	• Microsoft Windows Server 2008 SP2 (64-битная платформа); • Microsoft Windows Server 2008 R2 SP1; • Microsoft Windows Server 2012; • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016
База данных	• MS SQL Server 2008 (SP1); • MS SQL Server 2008 R2; • MS SQL Server 2012. (Необходимый компонент - **SQL Server Database Engine**)
Дополнительное ПО	• Распространяемый пакет Visual C++ для Visual Studio 2015 версии 14.0.24215 или более поздней (Visual C++ Redistributable for Visual Studio 2015) • .NET Core Runtime 2.1 Hosting Bundle Installer (https://www.microsoft.com/net/download/dotnet-core/runtime-2.1.0) • Microsoft .NET Framework 4.6.2 или более поздние версии данного ПО (https://www.microsoft.com/ru-RU/download/details.aspx?id=53344) • Для установки JDS в варианте приложения IIS требуется также установка ПО Internet Information Server версии 7.0 или более поздней (в составе серверной ОС Windows) **Примечание.** Перед установкой дополнительного ПО убедитесь в том, что выполнено обновление ОС Window, в частности установлены следующие обновления: • KB2975061 (https://www.microsoft.com/en-us/download/details.aspx?id=43531) • KB2939087 (https://www.microsoft.com/en-us/download/details.aspx?id=42365) • KB2919355 (https://support.microsoft.com/en-us/kb/2919355) • KB2999226 (https://support.microsoft.com/en-us/kb/2999226)
Другие требования	Установка должна осуществляться от имени учётной записи с правами администратора
	Компонент JDS должен устанавливаться на сервере, принадлежащем тому же домену Windows, что и сервер JMS, к которому JDS будет подключен после настройки
	Если для обращения к программному интерфейсу JDS требуется установка защищенного канала (в конфигурации без использования IIS), то для хоста, на котором будет установлен JDS, следует выпустить сертификат по шаблону, описанному в документе «Руководство администратора. Часть 1» [2], раздел «Шаблон сертификата службы аутентификации JMS и серверов JMS/SQL».

15.3 Предварительные настройки

В случае если компонент JDS *Служба каталога JMS* устанавливается не на сервере JMS, а также в случае использования кластера JMS, компьютеру, на котором установлен компонент *Служба каталога JMS,* на уровне домена Active Directory необходимо делегировать право обращения от имени другого пользователя. Для этого на контроллере домена AD, в оснастке **Active Directory - Пользователи и компьютеры** (dsa.msc), в свойствах соответствующего компьютера (хоста со службой JDS), на вкладке **Делегирование** установите опцию **Доверять компьютеру делегирование любых служб (только Kerberos)**, см. Рис. 465.

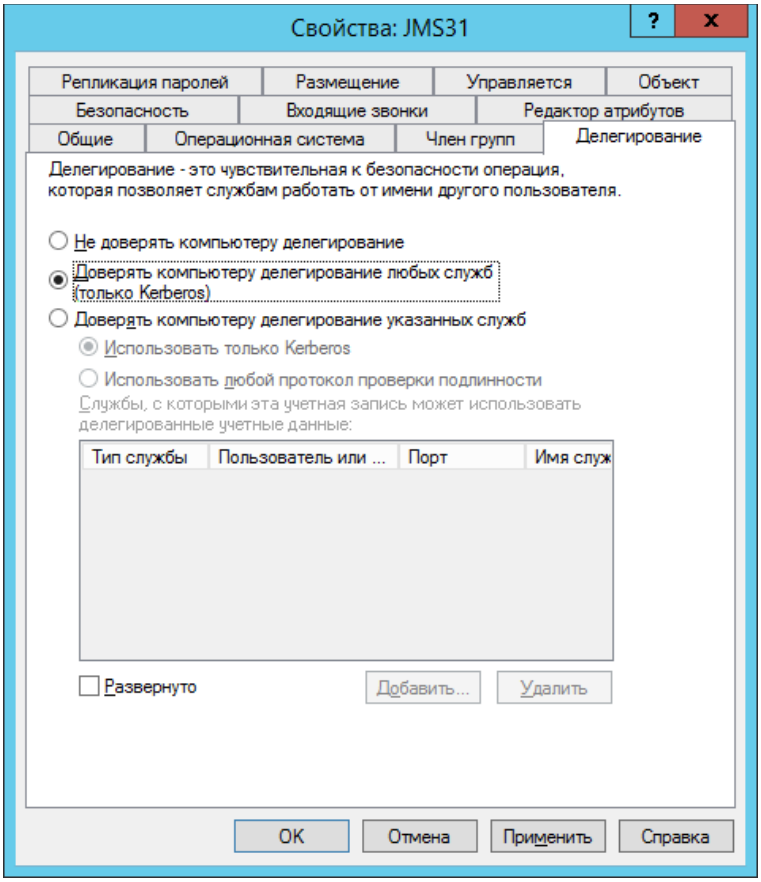


Рис. 465 – Настройка делегирвоания для службы JDS

15.4 Установка JDS

Чтобы установить компонент JDS, выполните следующие действия.

Примечание. В настоящем руководстве приводится пример установки для случая, когда сервер JMS, консоль управления и служба JDS располагаются на одном хосте.

1. Запустите на выполнение файл *Aladdin.JMS.DirectoryService.msi*.

Отобразится следующее окно.

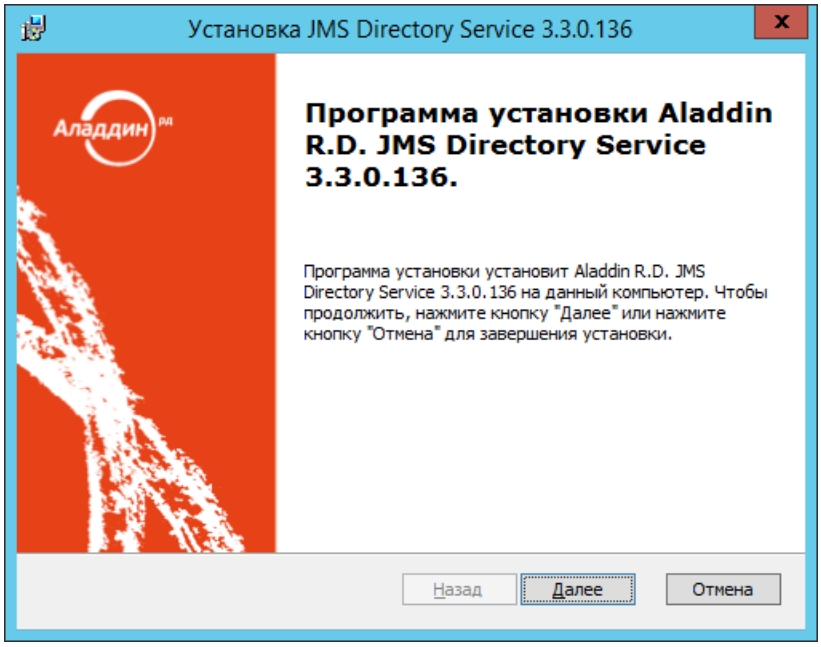


Рис. 466 – Окно приветствия мастера установки компонента JDS

2. Нажмите **Далее**.
   Отобразится следующее окно.

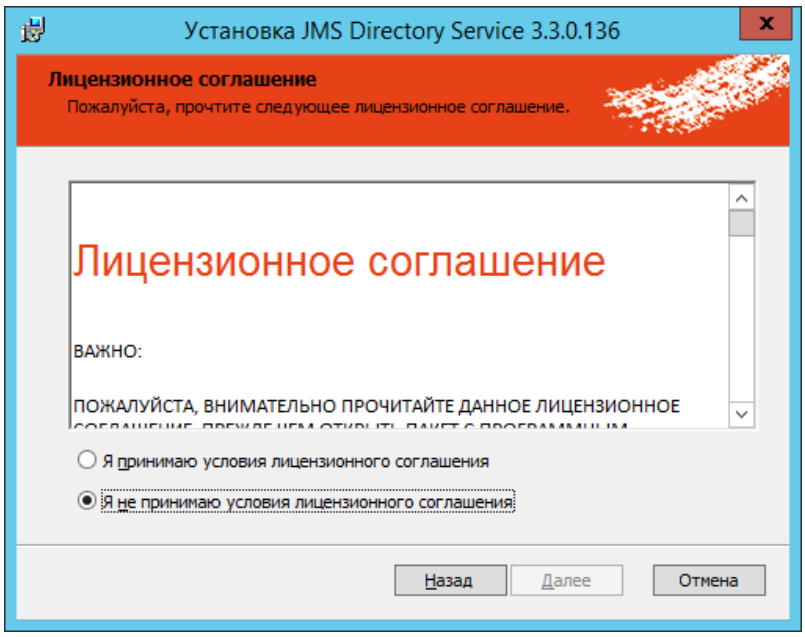


Рис. 467 – Окно лицензионного соглашения

3. Выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.

Отобразится следующее окно.

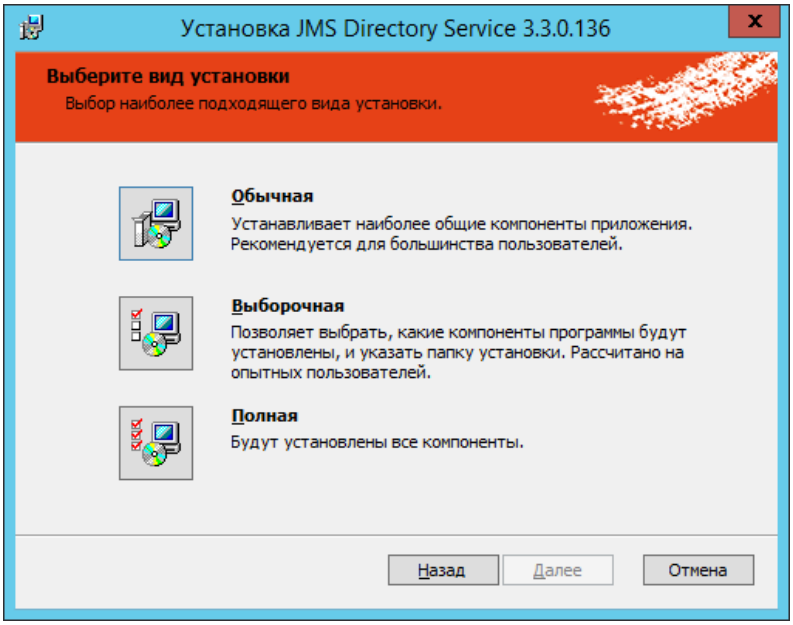


Рис. 468 – Окно выбора варианта установки

4. Выберите пункт **Выборочная**.

Примечание. В случае выбора пункта **Полная** у пользователя не будет возможности выбора варианта установки JDS, и последняя будет установлена только в варианте службы Windows.

Отобразится следующее окно.

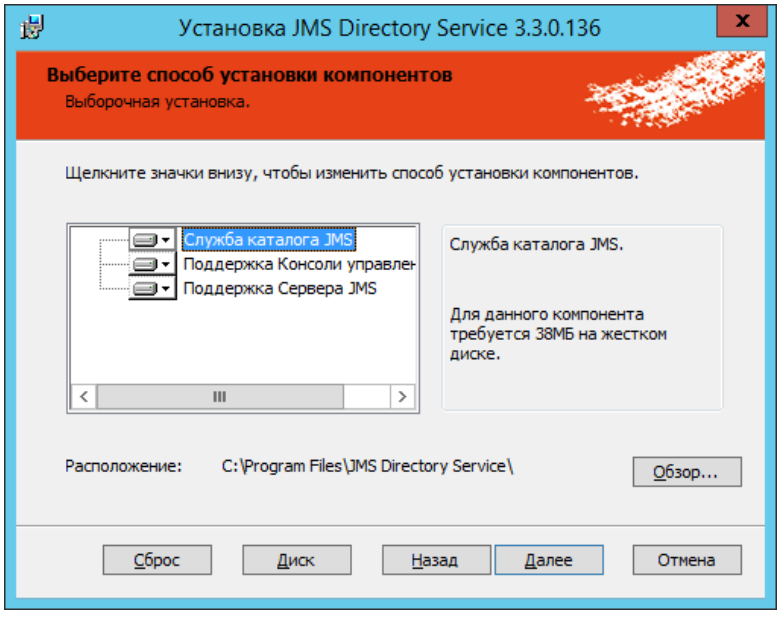


Рис. 469 – Окно выбора компонентов JDS

Примечания:

1. Чтобы задать путь установки, отличный от пути по умолчанию, напротив поля **Расположение** нажмите **Обзор** и внесите необходимые изменения.
2. В случае если необходимо установить компоненты JDS выборочно, отключите лишние компоненты, в противном случае автоматически будут установлены все компоненты JDS, применимые к данному хосту (например, если на

данном хосте установлено только приложение *Консоль управления JMS*, то из всего инсталляционного комплекта JDS будут установлены компоненты «Служба каталога JMS» и «Поддержка консоли управления»).

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

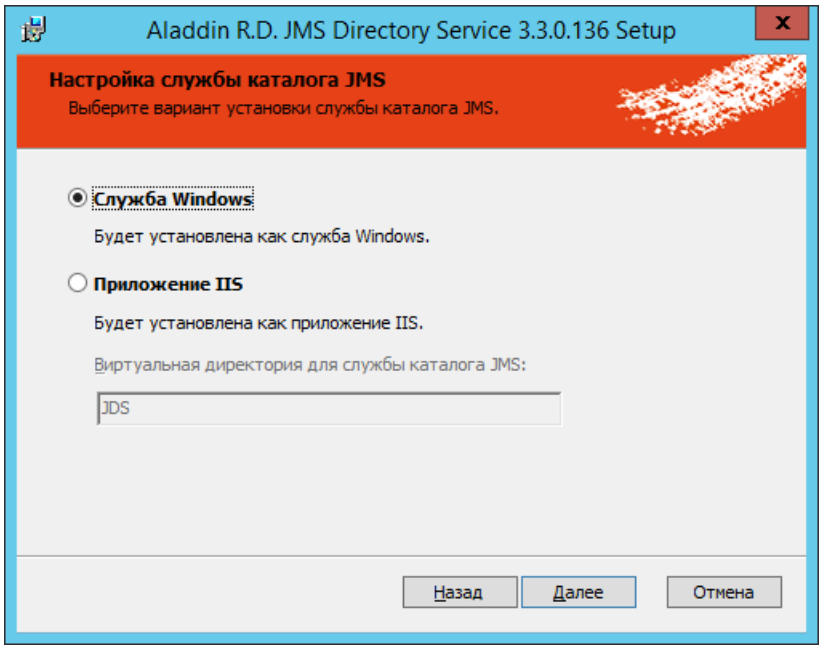


Рис. 470 – Окно выбора варианта установки JDS

6. В случае если JDS должна быть установлена в варианте приложения IIS, выберите **Приложение IIS** и при необходимости измените имя виртуального каталога (псевдонима) для службы JMS в IIS в поле **Виртуальная директория для службы каталога JMS**.

Примечание. Для установки JDS в варианте приложения IIS необходимо предварительно установить ПО Internet Information Server в соответствии с рекомендациями из Табл. 120, с. 522.

7. Нажмите **Далее**.

Отобразится следующее окно.

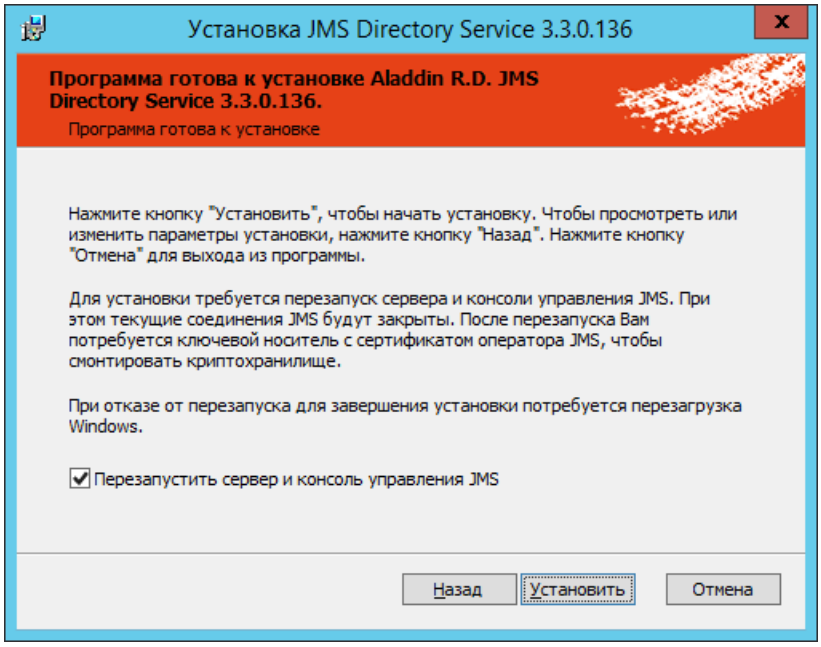


Рис. 471 – Окно готовности к установке

8. Для отмены автоматической перезагрузки сервера JMS и прекращения работы *Консоли управления JMS* сбросьте флаг **Перезапустить сервер и консоль управления JMS**. (В этом случае перезагрузку службы JMS, приложений *Сервер JMS* и *Консоль управления JMS* потребуется произвести вручную по окончании процесса установки и настройки компонента JDS).
9. Нажмите **Установить**.
10. В случае установленного флага **Перезапустить сервер и консоль управления JMS** (см. выше) отобразится окно запроса на перезагрузку сервера и консоли управления JMS (Рис. 472). (Если флаг не был установен перейдите к следующему шагу.)

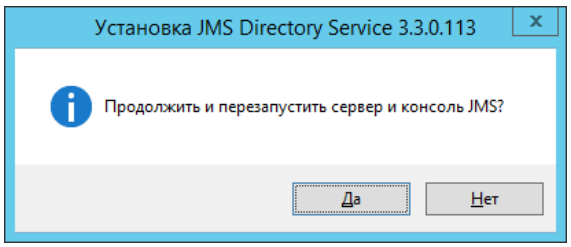


Рис. 472 – Окно запроса перезагрузки сервера

Нажмите **Да** для продолжения установки JDS.

11. По окончанию установки отобразится следующее окно.

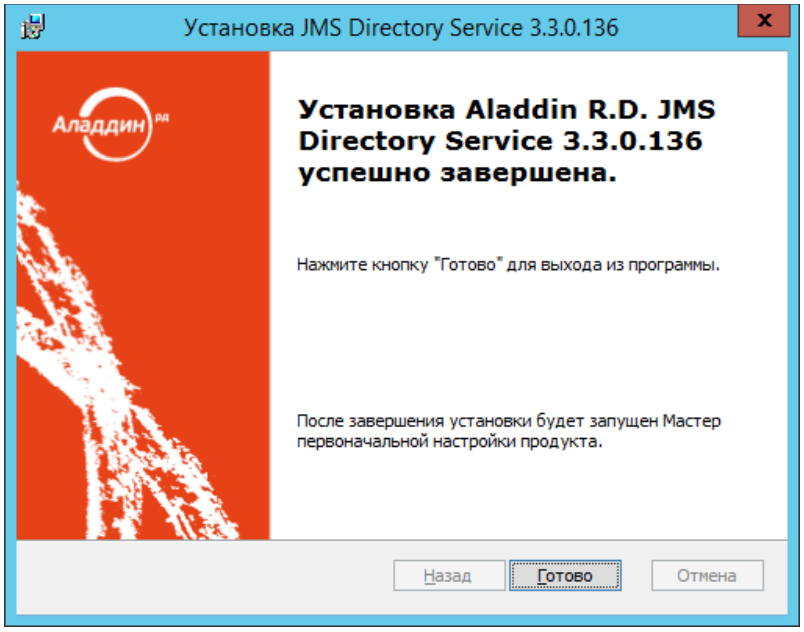


Рис. 473 – Окно завершения процедуры установки

12. Для завершения установки нажмите **Готово**.

После установки компонента JDS автоматически откроется окно мастера настройки JDS (см. «Настройка JDS», ниже)

15.5 Настройка JDS

Окно мастера настройки JDS открывается автоматически после установки компонента JDS.

Если вы закрыли окно мастера настройки JDS, к нему можно вернуться самостоятельно, запустив приложение **Настройка службы каталога JMS** (значок D) в разделе **JaCarta Management System** списка пользовательских приложений соответствующей версии операционной системы Windows Server.

Окно приветствия мастера настройки компонента JDS выглядит следующим образом.

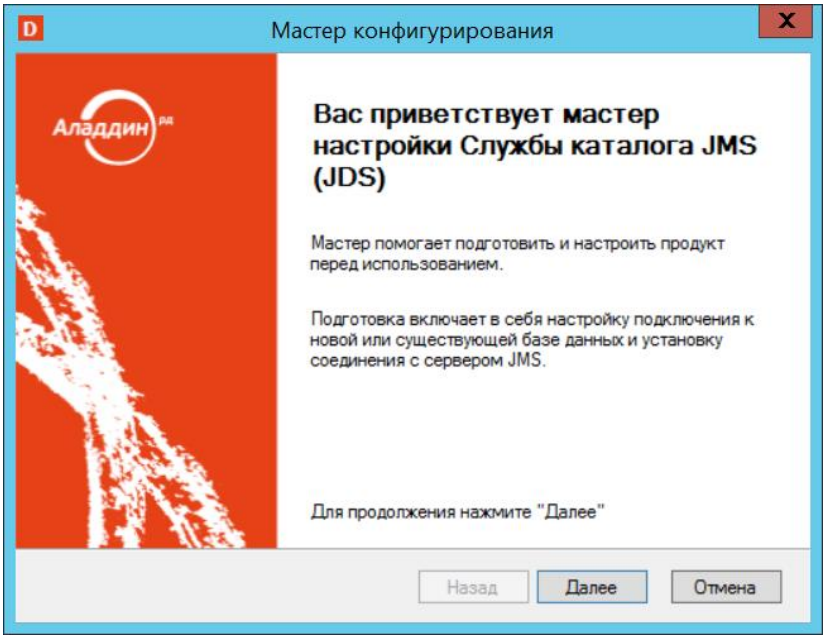


Рис. 474 – Окно приветствия мастера настройки JDS

1. Нажмите **Далее**.
   Отобразится следующее окно.

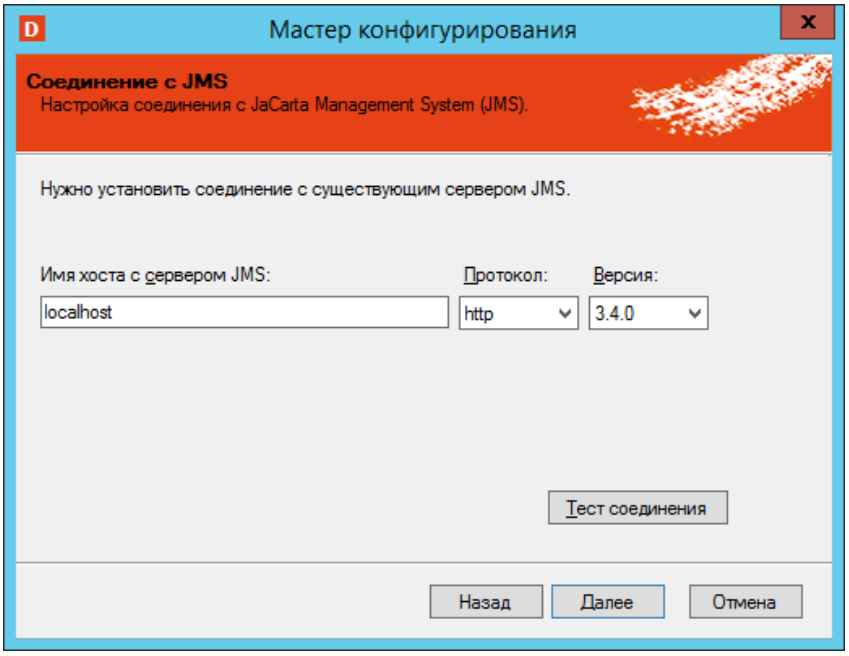


Рис. 475 – Окно настройки соединения с сервером JMS

2. Выполните настройку, руководствуясь Табл. 121.

Табл. 121 – Настройка соединения с сервером JMS

Настройка	Описание
Имя хоста с сервером JMS	Введите полное доменное имя (FQDN) компьютера, на котором установлен компонент JMS Server (например, *JMS31.jasdomain.aladdin-rd.local*)  **Примечания:** 1. В случае использования протокола https (см. настройку **Протокол**, ниже) имя хоста должно совпадать с именем, на которое был выпущен сертификат сервера JMS, используемый для SSL-соединения с административным агентом из состава Admin JMS. 2. В случае использования протокола http допускается указать NetBIOS-имя сервера JMS (при этом, если компонент JDS установлен на одном хосте с сервером JMS, в качестве имени можно указать *localhost*)
Протокол	Выберите протокол подключения к серверу JMS. Возможные значения: • **http** (значение по умолчанию) • **https**  **Примечание.** Для выбора протокола https на сервере JMS должна быть настроена поддержка SSL в части, касающейся связи JMS по SSL с административнвным агентом из состава JMS Admin (см. «Руководство администратора. Часть 1» [2], раздел «Настройка SSL-соединения на стороне сервера JMS»).
Версия	Выберите версию сервера JMS, с которым будет установлено соединение. Допустимые значения: • 3.3.0 (значение по умолчанию) • 3.4.0
Тест соединения	Для проверки корректности установки соединения указанного в предыдущих настройках нажмите **Тест соединения**. В случае корректной настройки в диалоговом окне будет сообщено об успешном установлении соединения.

3. Нажмите **Далее**.
   В зависимости от того, в каком варианте была установлена JDS – как служба Windows (Рис. 476), или как приложение IIS (Рис. 477) – отобразится соответствующее окно.

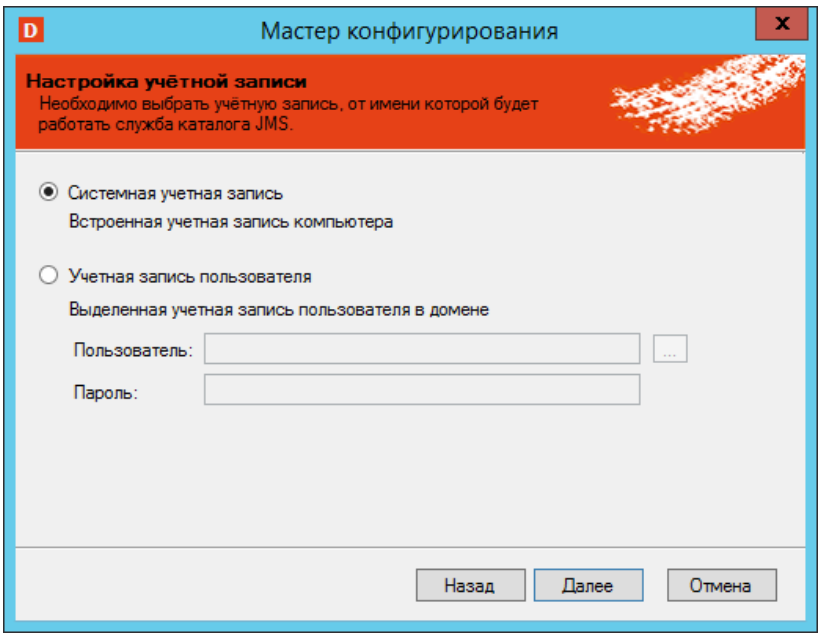


Рис. 476 – Окно выбора учетной записи для запуска JDS (для варианта установки JDS в качестве службы Windows)

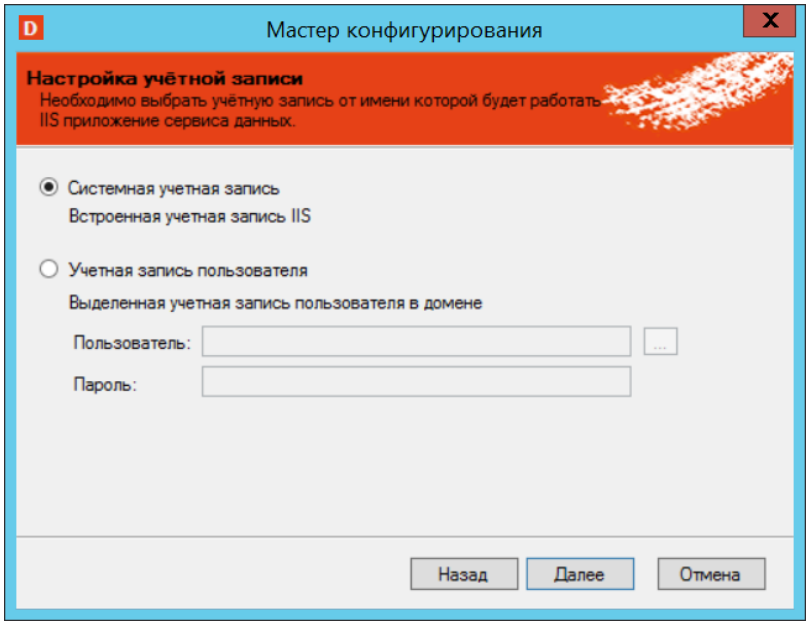


Рис. 477 – Окно выбора учетной записи для запуска JDS (для варианта установки JDS в качестве приложения IIS)

4. Выберите тип учетной записи, от имени которой будет запускаться JDS и выполните необходимые действия, руководствуясь Табл. 122.

Табл. 122 – Выбор учетной записи для запуска службы JDS

Тип учетной записи	Описание
Системная учетная запись	При выборе данной опции будет использоваться соответствующая системная учетная запись:

Тип учетной записи	Описание
	• В случае установки JDS как службы Windows -- встроенная учетная запись компьютера; • В случае установки JDS как приложения IIS -- встроенная учетная запись IIS
Учетная запись пользователя	В случае запуска JDS как Windows-службы при выборе данной опции следует указать пользователя и его пароль. Права на запуск JDS (как Windows службы или приложения IIS) и доступа к базе данных на сервере СУБД и будут предоставлены указанной учетной записи пользователя автоматически. **Примечание.** Чтобы обеспечить безопасный доступ к серверу СУБД, для запуска службы JDS (как Windows-службы или приложения IIS) следует выбрать учетную запись, отличную от учетной записи, созданной ранее для запуска сервера JMS (если такая была создана).

5. Нажмите **Далее**.
   В случае если JDS была установлена как служба Windows отобразится следующее окно. (В противном случае перейдите к шагу 7)

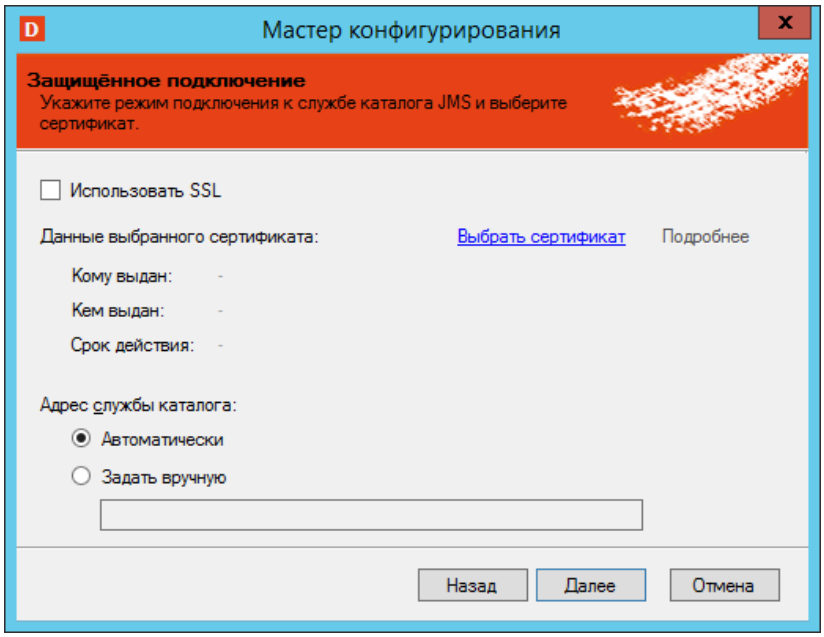


Рис. 478 – Окно настройки SSL для доступа к JDS

6. Выполните настройки в соответствии с Табл. 123.

Табл. 123 – Настройки подключения к базе данных JDS

Настройка	Описание
Использовать SSL	Установите флаг **Использовать SSL** в случае, если для обращения к службе JDS необходимо обеспечить защищенный канал. При установке флага **Использовать SSL** следует выбрать сертификат хоста JDS, выпущенный заблаговременно в соответствии с рекомендациями из Табл. 120, с. 522. **Важно!** После выбора сертификата, запомните (выпишите) DNS-имя хоста службы JDS (отображается в поле **Кому выдан**). Данный адрес понадобится при указании URL службы JDS на сервере JMS (см. «Регистрация каталога учетных записей JDS на сервере JMS»)

Настройка	Описание
Адрес службы каталога	Укажите адрес службы каталога JMS (JDS). Для этого выберите одну из следующих опций. • **Автоматически** – в случае выбора данной опции в настройках JDS будет установлен адрес службы JDS (т.е. хоста, на котором устанавливается компонент *Служба каталога JMS)* в следующем формате: `<протокол>://<FQDN_хоста>:5577`, где – <протокол> — http или https, в зависимости от значения опции **Использовать SSL** при установке JDS и настроек IIS; – <FQDN_хоста> — полное доменное имя хоста, на котором функционирует служба каталога JMS; • **Задать вручную** – при выборе данной опции задайте адрес службы вручную в следущем формате: `<протокол>://<FQDN_хоста>:<порт>`, где – <протокол> — http или https, в зависимости от значения опции **Использовать SSL** при установке JDS и настроек IIS; – <FQDN_хоста> — полное доменное имя хоста, на котором функционирует служба каталога JMS; – <порт> -- номер порта, по которому производится передача данных. По умолчанию используется порт 5577 **Примечания:** 1. При задании адреса службы вручную, в случае установки флага **Использование SSL** значение поля <FQDN_хоста> должно совпадать с именем хоста, на который выпущен выбранный в окне сертификат. 2. Адрес службы каталога, указанный в поле **Задать вручную** следует использовать в параметрах настройки внешней ресурсной системы в серверном агенте JMS (приложение *Сервер JMS*).

Примечание. Для обеспечения защищенного канала связи со службой JDS в случае ее установки как приложения IIS, необходимо выполнить установку и привязку сертификата SSL на сервер IIS в соответствии с документацией Microsoft.

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

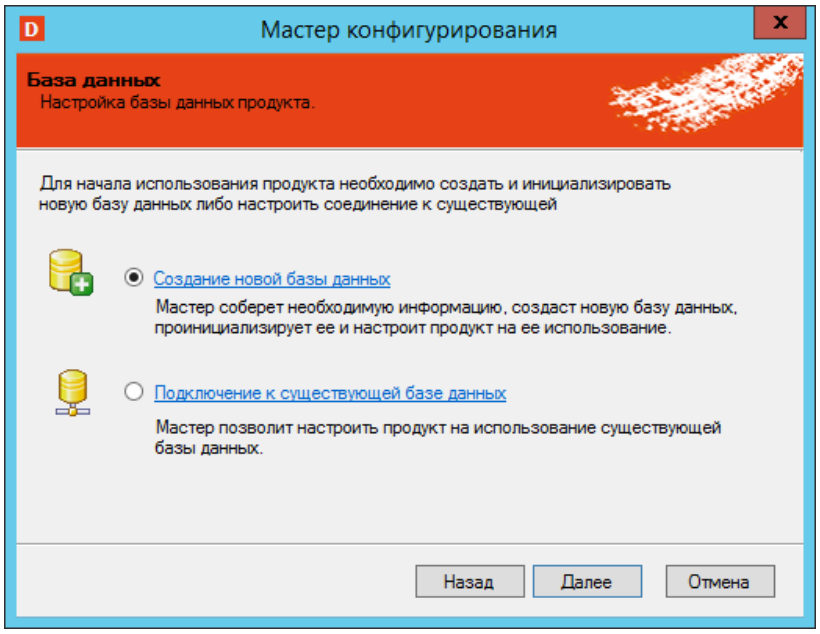


Рис. 479 – Окно выбора подключения к серверу СУБД

8. В случае обновления или восстановления JDS выберите опцию **Подключение к существующей базе данных**.

Примечание. База данных JDS предназначена для хранения служебных данных самого компонента JDS и устанавливается и работает независимо от базы данных JMS.

9. Нажмите **Далее**.
Отобразится следующее окно.

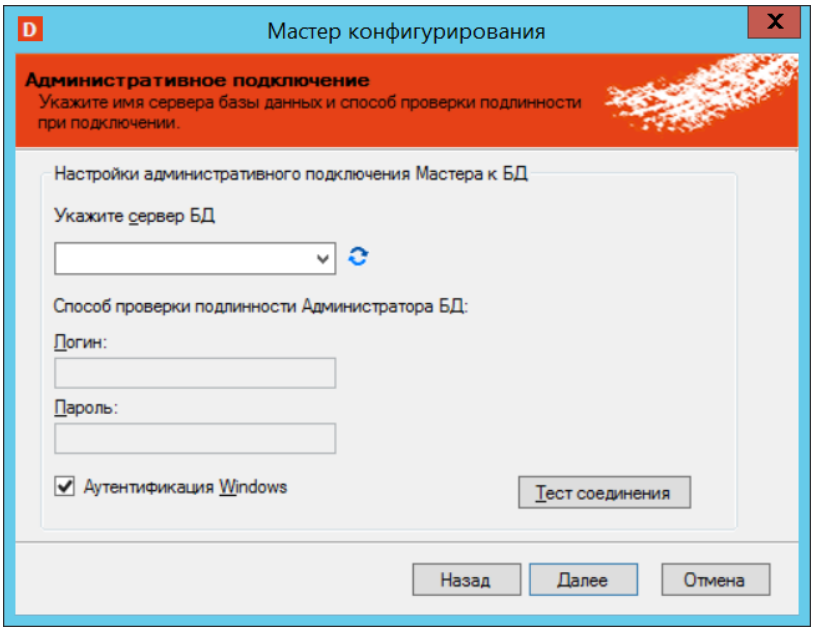


Рис. 480 – Окно выбора сервера СУБД

10. Выполните настройки подключения к серверу СУБД, руководствуясь Табл. 124.

Табл. 124 – Настройки подключения к серверу БД JDS

Настройка	Описание
Укажите сервер БД	Выберите из списка имя сервера базы данных. В списке серверов могут отображаться не все удаленные экземпляры служб MS SQL Server. Если нужный экземпляр MS SQL Server не отображается в списке, полное имя этого экземпляра следует ввести вручную.
Аутентификация Windows	Выберите этот пункт для подключения к базе данных с использованием проверки подлинности Windows, в противном случае (если пункт не указан) в полях **Логин** и **Пароль** необходимо указать соответственно имя и пароль учетной записи для подключения к серверу Microsoft SQL. **Примечания:** 1. При выборе пункта **Аутентификация Windows** (проверка подлинности Windows) убедитесь, что доменному пользователю, от имени которого выполняется мастер настройки, предоставлены права на администрирование SQL-сервера. 2. В случае если JDS устанавливалась как приложение IIS и при этом запускается от имени системной учетной записи (встроенной учетной записи IIS), рекомендуется не использовать опцию **Windows Аутентификация** из-за сложности предоставления такой учетной записи необходимых полномочий по работе с сервером SQL

11. Нажмите **Далее**.
Отобразится следующее окно.

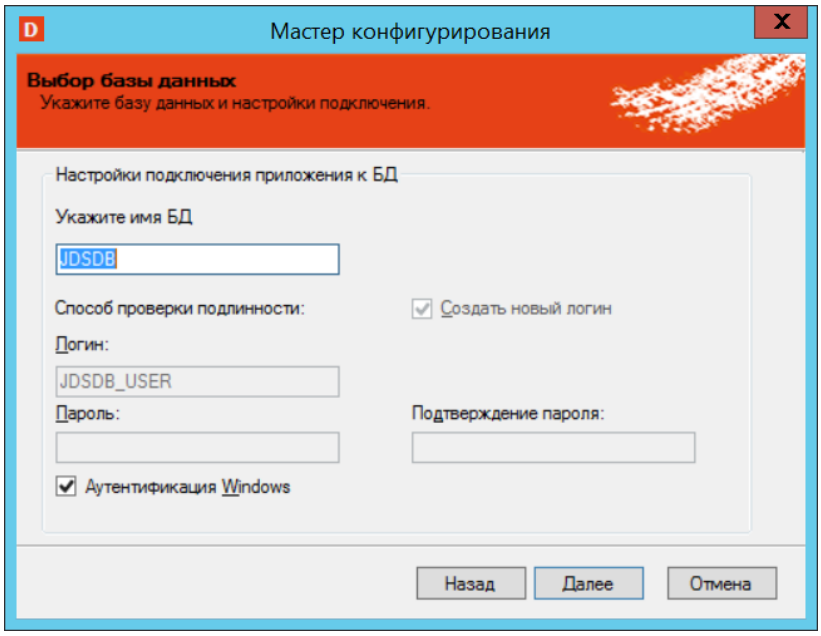


Рис. 481 – Окно создания базы данных

12. Выполните настройки в соответствии с Табл. 125.

Табл. 125 – Настройки подключения к базе данных JDS

Настройка	Описание
Укажите имя БД	Укажите имя новой базы данных (или оставьте значение по умолчанию), которая будет создана в процессе настройки JDS
Аутентификация Windows	При установке флага **Аутентификация Windows** (проверка подлинности Windows) в создаваемой базе данных будет создано специализированное имя входа, позволяющее обращаться к БД от имени доменной учетной записи рабочей станции (Local System), т.е. имя хоста, на котором функционирует служба JDS. Если предполагается запуск службы под доменной учетной записью пользователя (т.е. не Local System), то по окончании работы мастера настройки необходимо убедиться, что права на создаваемую базу данных предоставлены этой учетной записи, в противном случе их необходимо выдать вручную В случае если флаг **Аутентификация Widows** сброшен, обращение к создаваемой базе данных будет производиться либо от вновь созданного имени входа (флаг **Создать новый логин** установлен), либо от ранее созданного на SQL-сервере имени входа (флаг **Создать новый логин** сброшен). **Примечание.** В случае если JDS была установлена в качестве IIS-приложения и ее запуск осуществляется от имени системной учетной записи (встроенной учетной записи IIS), для обеспечиния Windows-аутентификации следует предоставить учетной записи IIS права на доступ к созданной базе данных на SQL-сервере вручную. Для выполнения такой настройки обратитесь к документации Microsoft.

13. Нажмите **Далее**.

Отобразится следующее окно.

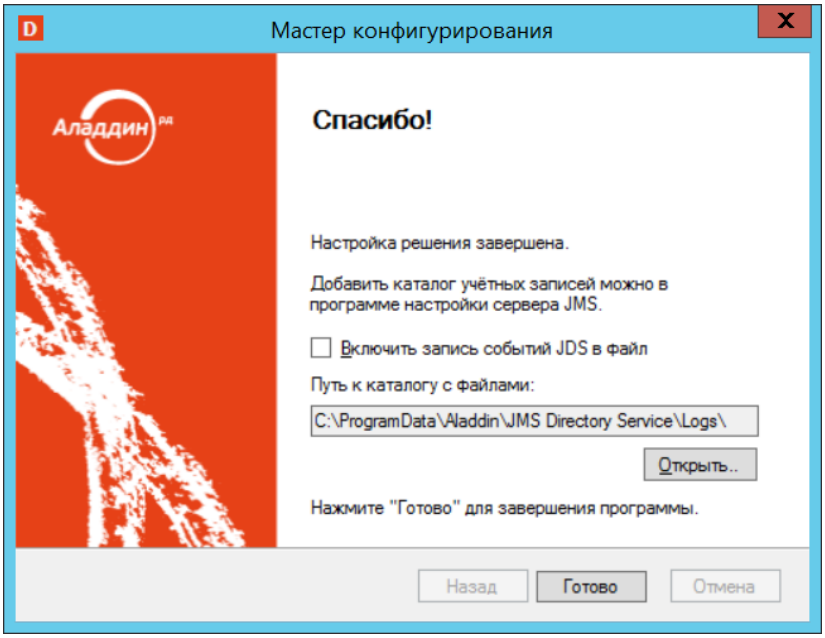


Рис. 482 – Окно завершения работы мастера настройки JDS

14. Чтобы включить журналирование работы JDS установите флаг **Включить запись событий JDS в файл**.

Примечание. Файлы журналов располагаются в папке *%ProgramData%\Aladdin\JMS Directory Service\Logs* (можно также воспользоваться подсказкой мастера настройки, Рис. 482).

15. Нажмите **Готово** для окончания процедуры.

Важно! Если перезагрузка сервера и консоли JMS не была выполнена в ходе установки JDS, то для получения доступа к службе каталога JMS необходимо вручную выполнить перезагрузку службы JMS, приложений Сервер JMS и Консоль управления JMS

Для обеспечения корректной работы службы JDS необходимо также выполнить настройки серверного агента JMS (приложение Сервер JMS), см. раздел «Регистрация каталога учетных записей JDS на сервере JMS», ниже.

15.6 Регистрация каталога учетных записей JDS на сервере JMS

Чтобы зарегистрировать каталог учетных записей JDS, выполните следующие действия.

1. Нажмите правой кнопкой на значке (Сервер JMS) в области уведомлений и выберите **Открыть**.
2. В отобразившемся окне перейдите на вкладку **Каталоги учетных записей**.

Окно примет следующий вид.

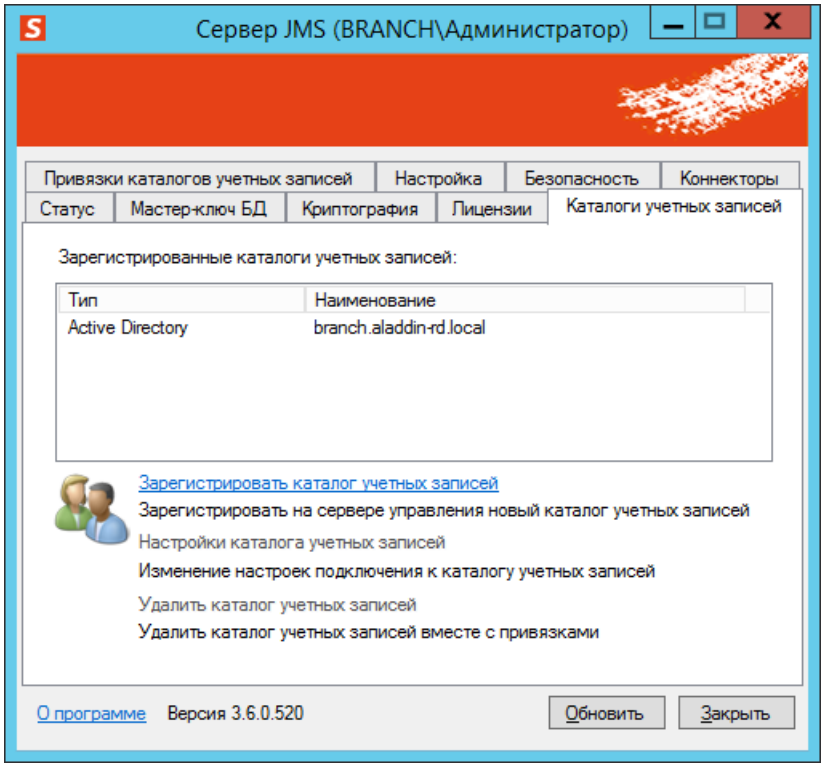


Рис. 483 – Вкладка Каталоги учетных записей

3. Нажмите на ссылке **Зарегистрировать каталог учетных записей**.
Отобразится следующее окно.

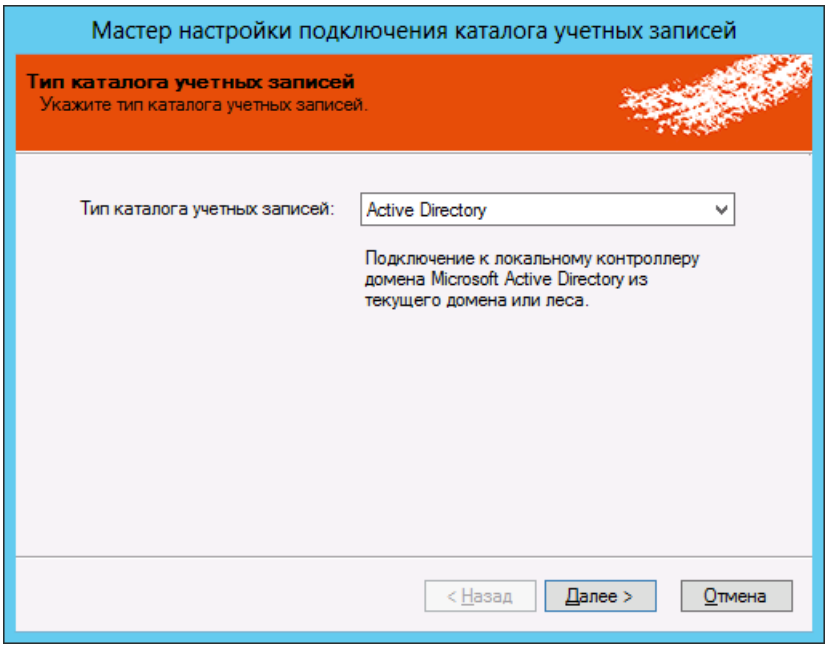


Рис. 484 – Выбор типа каталога учетных записей

4. В **списке Тип каталога учетных записей** выберите **Служба каталога JMS** и нажмите **Далее**.

Отобразится следующее окно.

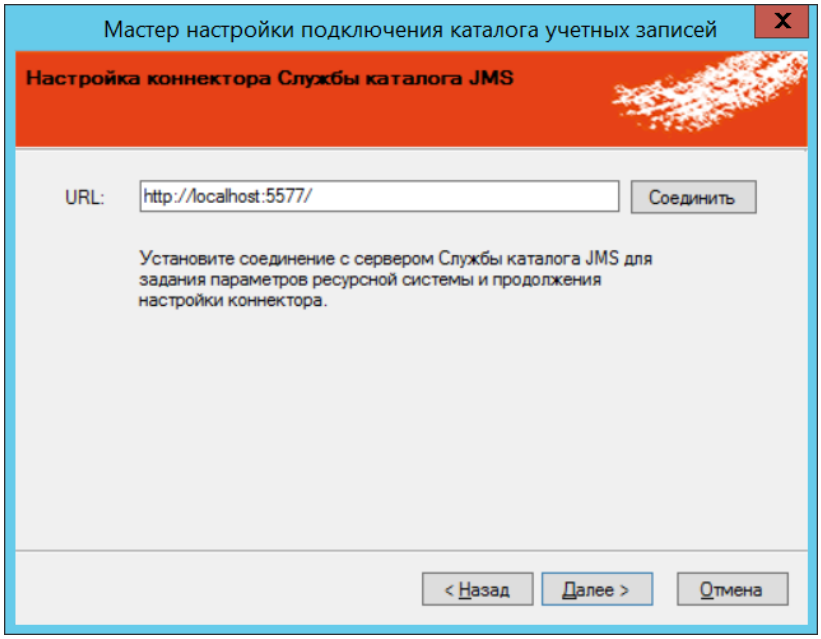


Рис. 485 – Настройка подключения к службе каталога JMS

5. В случае если JDS установлен на хосте отличном от хоста с сервером JMS, в поле URL вместо адреса, указанного по умолчанию (например, *localhost*) введите адрес хоста (имя DNS), на котором установлена служба каталога JMS и нажмите **Соединить**.

Примечания:

1. Если при настройке JDS была выбрана опция **Использовать SSL** (см. раздел «Настройка JDS», Рис. 478, с. 533), убедитесь, что DNS-имя хоста в составе адреса, указываемого в поле **URL** (Рис. 485), совпадает с именем, указанным в сертификате данного хоста (сертификат выбирается также в процессе настройки JDS, см. «Настройка JDS»).
2. Если адрес службы каталога (JDS) при ее настройке задавался вручную (см. раздел «Настройка JDS», Рис. 478, с. 533), то в поле URL следует указать данный адрес (включая порт).
3. Если JDS была установлена как приложение IIS, в поле **URL** адрес JDS следует указать в следующем формате:

   `<протокол>://<FQDN IIS>/<виртуальная директория>/`, где

   - <протокол> — http или https, в зависимости от значения опции **Использовать SSL** при установке JDS и настроек IIS;
   - <FQDN IIS> — полное доменное имя хоста, на котором функционирует IIS с приложением JDS;
   - <виртуальная директория> — имя виртуального каталога (псевдоним) приложения JDS на сервере IIS (задается на шаге 6 процедуры установки JDS, с. 527)

   Например:

   `https://JMS31.jasdomain.aladdin-rd.local/JDS/`

Отобразится следующее окно.

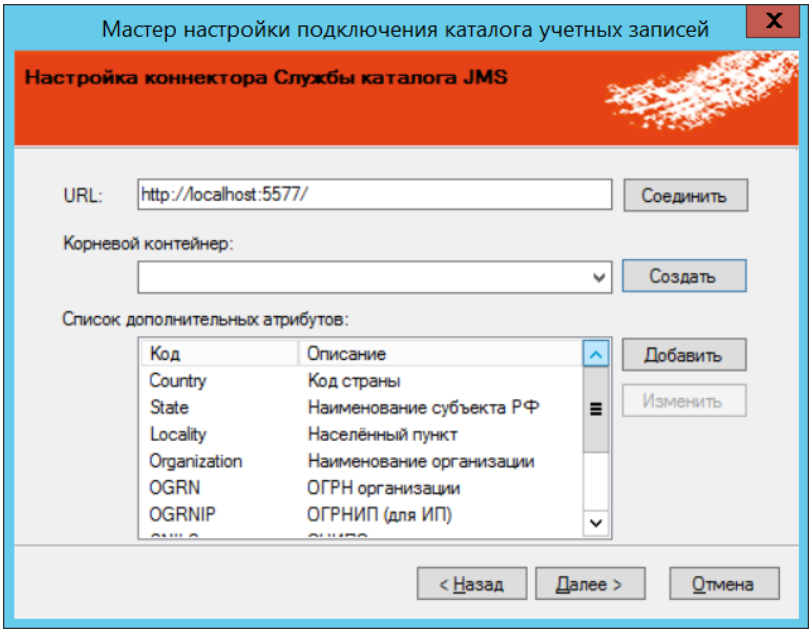


Рис. 486 – Настройка подключения к службе каталога JMS

6. Нажмите **Создать** и в диалоговом окне (Рис. 487) введите имя корневого контейнера службы JDS в формате Distinguished Name LDAP (например *DC=jds, DC=aladdin-rd, DC=local*) и нажмите **OK**.

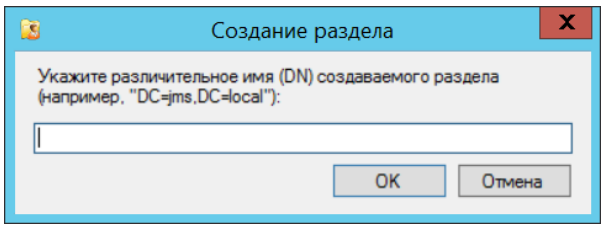


Рис. 487 – Настройка подключения к службе каталога JMS

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

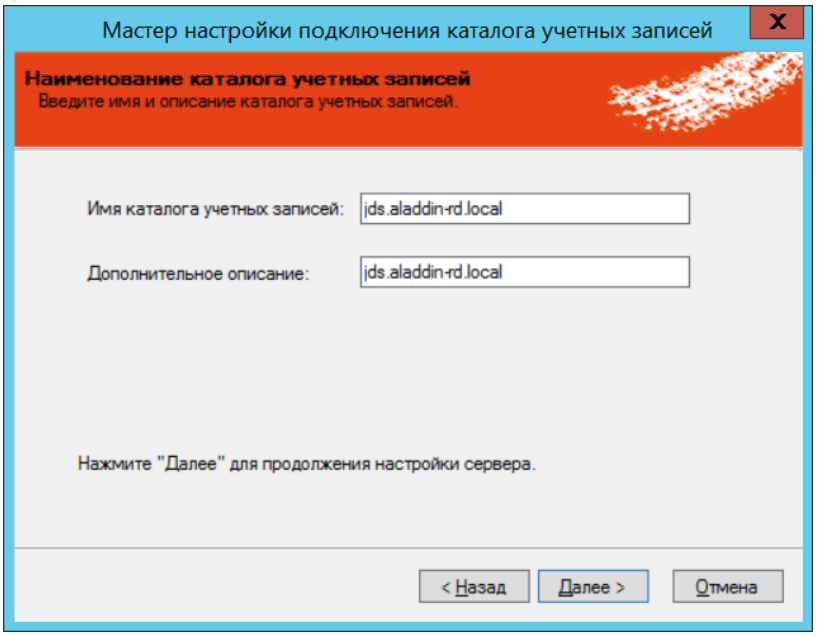


Рис. 488 – Настройка подключения к службе каталога JMS

8. Измените значения полей на нужные или оставьте значения по умолчанию, после чего нажмите **Далее**.
   Отобразится следующее окно.

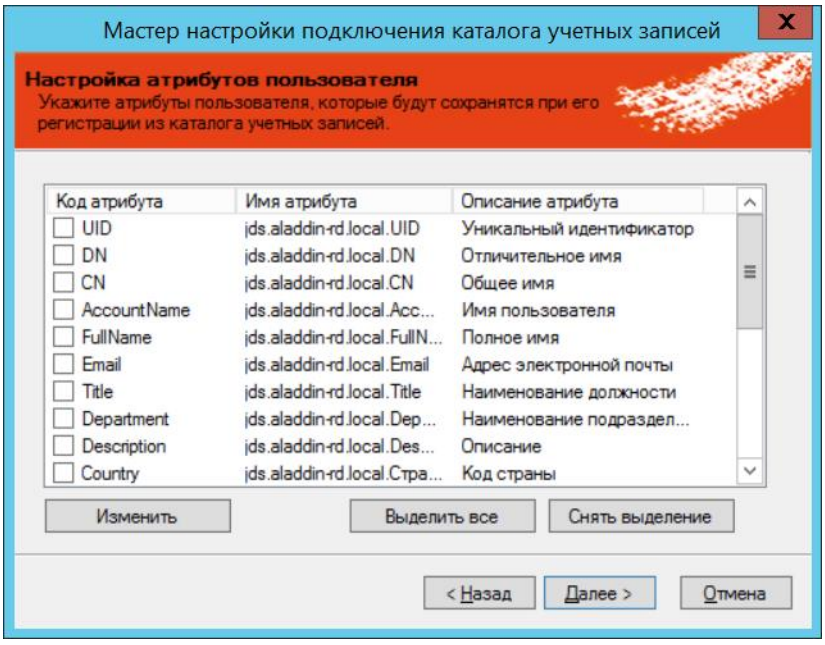


Рис. 489 – Настройка атрибутов пользователей

9. Укажите атрибуты пользователя, которые будут сохранены в базе данных JMS при регистрации из каталога учетных записей JDS, после чего нажмите **Далее**.
10. В диалоговом окне запроса на добавление нового каталога учетных записей и перезапуска сервера управления JMS нажмите **Да**.

После этого произойдет перезапуск сервера управления JMS.

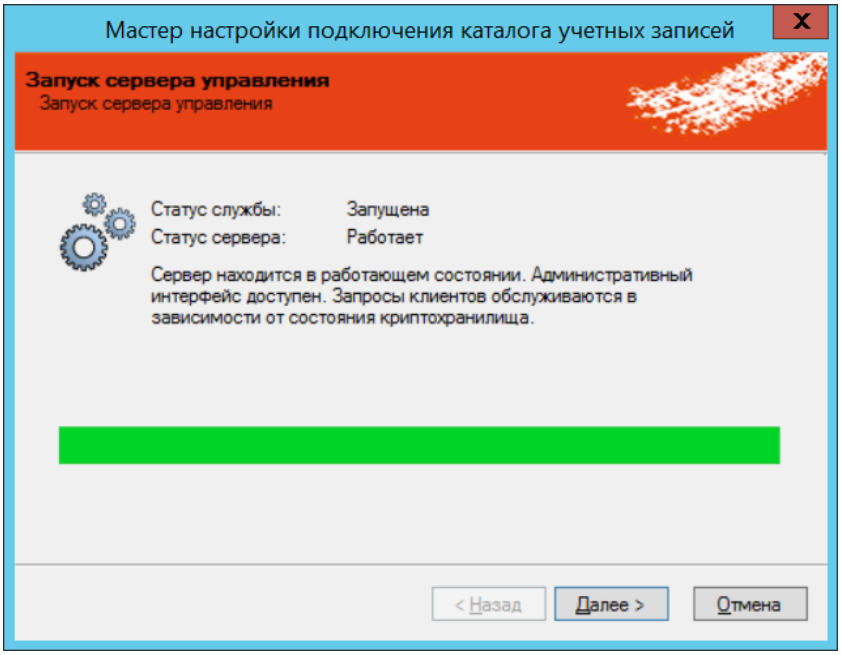


Рис. 490 – Перезапуск сервера управления JMS

11. Нажмите **Далее**.
Отобразится следующее окно.

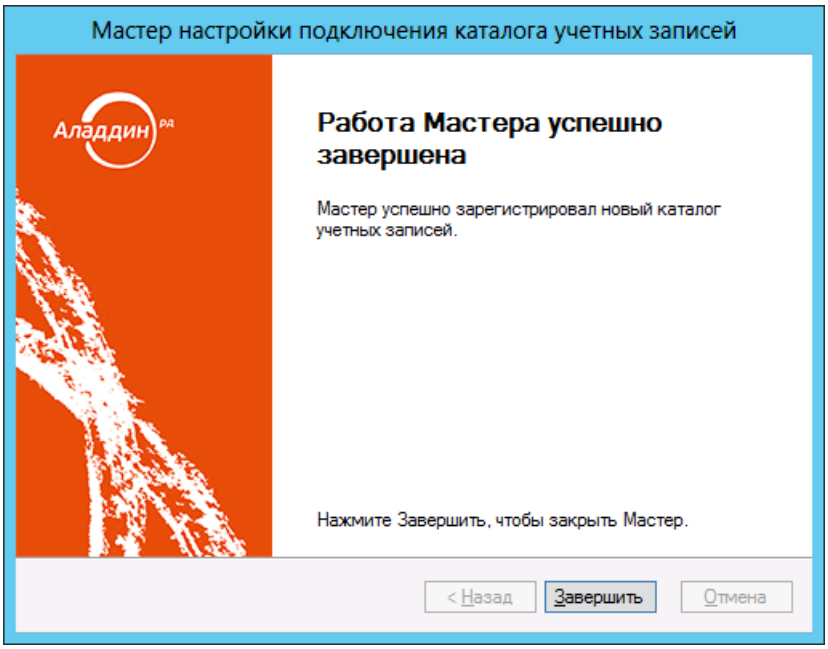


Рис. 491 – Окно завершения работы мастера подключения каталога учетных записей

12. Нажмите **Завершить**.

Новый корневой каталог учетных записей JDS отобразится на вкладке **Каталоги учетных записей** окна управления сервером JMS.

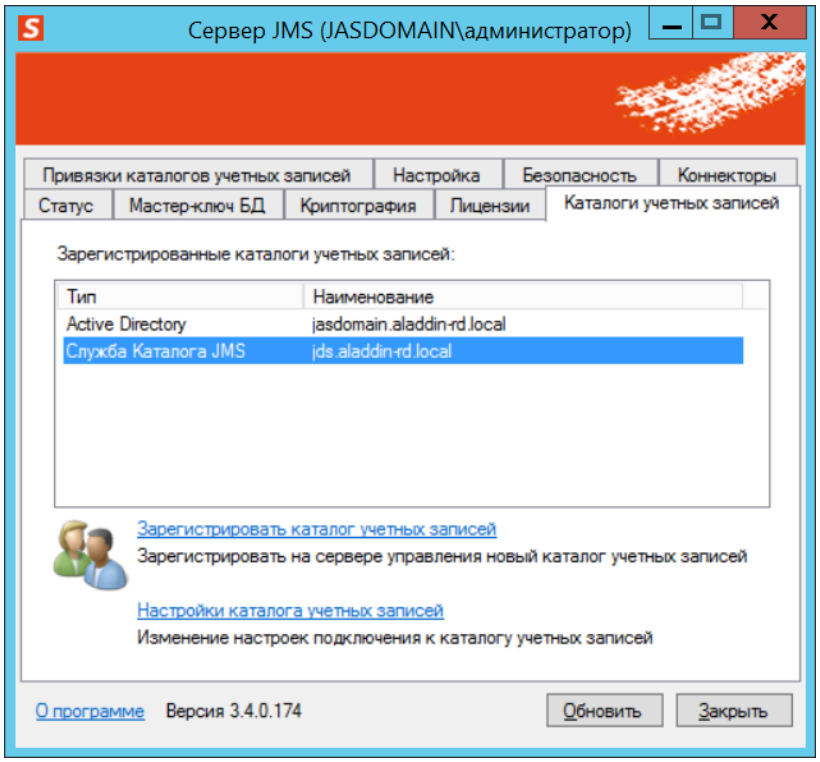


Рис. 492 – Каталог учетных записей JDS зарегистрирован

Корневой каталог учетных записей также будет отображаться в окне консоли управления JMS (для этого консоль необходимо перезагрузить).

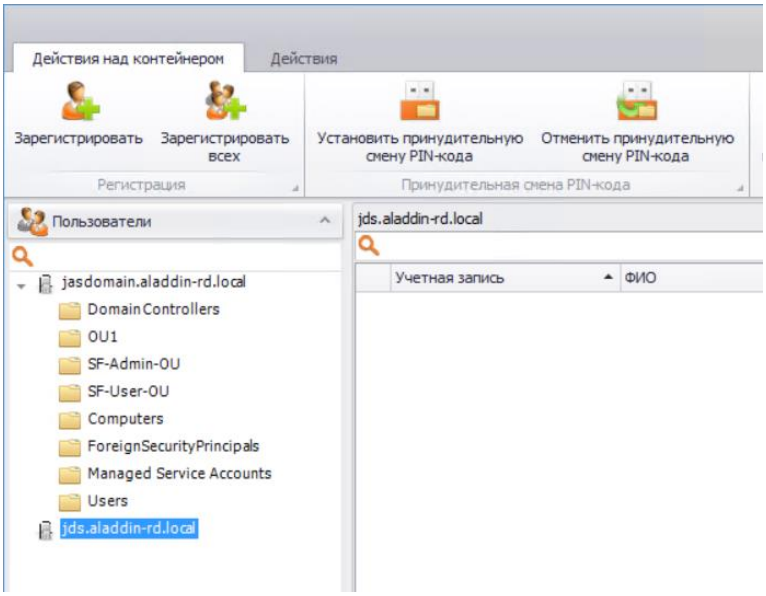


Рис. 493 – Каталог учетных записей JDS отображается в консоли управления JMS

По окончании регистрации JDS в административной консоли JMS становятся доступны новые операции (см. раздел «Управление объектами в JDS», ниже).

15.7 Управление объектами в JDS

После установки расширения JDS для консоли управления JMS, в ней добавляется новые секции **Служба Каталога** на вкладках **Действие над контейнерами** (Рис. 494) и **Действия** (Рис. 495).

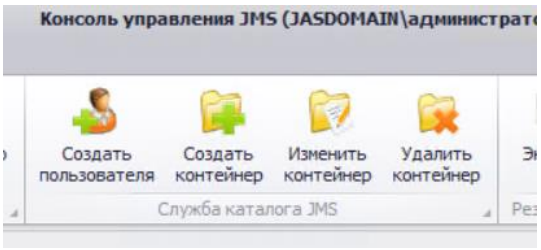


*Рис. 494 – Новая секция в разделе **Пользователи** на вкладке **Действия над контейнером***

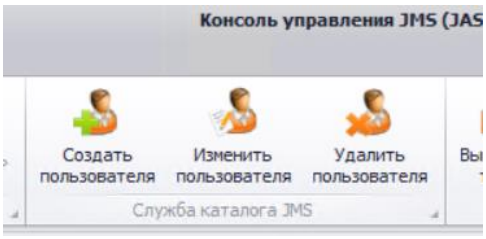


*Рис. 495 – Новая секция в разделе **Пользователи** на вкладке **Действия***

В новых секциях становятся доступны следующие операции:

- **Создать контейнер** (см. раздел «Создание контейнера в JDS», с. 544);
- **Изменить контейнер** (см. раздел «Изменение контейнера в JDS» , с. 545);
- **Удалить контейнер** (см. раздел «Удаление контейнера в JDS» , с. 547);
- **Создать пользователя** (см. раздел «Создание пользователя в JDS» , с. 547);
- **Изменить пользователя** (см. раздел «Изменение учетной записи пользователя в JDS» , с. 550);
- **Удалить пользователя** (см. раздел «Удаление учетной записи пользователя из JDS» , с. 552).

Обратите внимание на особенности регистрации пользователей JDS в JMS (см. раздел «Регистрация пользователя в JMS», с. 553), а также на особенность удаления пользователей JDS из JMS (см. раздел «Удаление учетной записи пользователя», с. 552).

15.7.1 Создание контейнера в JDS

Чтобы создать новый контейнер в службе каталога JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Пользователи**. На вкладке **Действия над контейнером** выберите необходимый корневой контейнер службы каталога JMS. (При необходимости выберите вложенный в него контейнер).

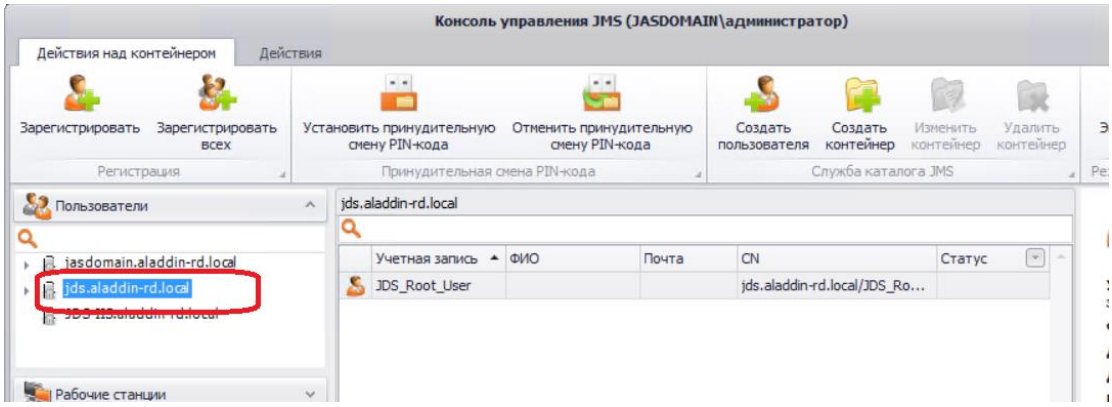


Рис. 496 – Создание контейнера службы каталога JMS

2. В секции **Служба каталога JMS** нажмите **Создать контейнер.**
Отобразится следующее окно.

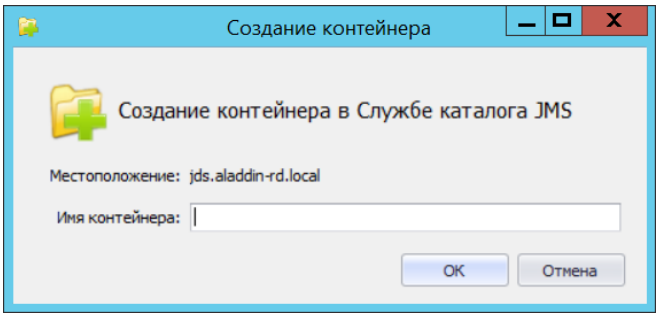


Рис. 497 – Диалог ввода имени контейнера

3. Введите имя контейнера и нажмите **OK**. Добавленный контейнер отобразится в дереве контейнеров (Рис. 498)

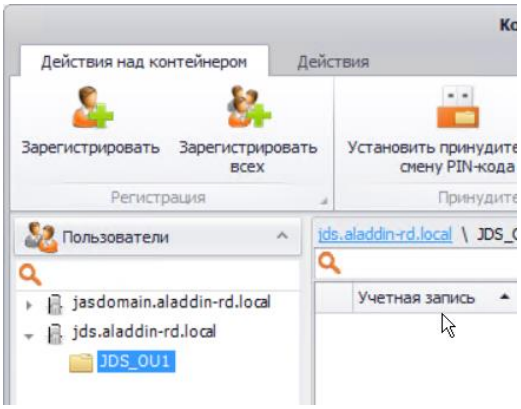


Рис. 498 – Отображение добавленного контейнера

15.7.2 Изменение контейнера в JDS

Чтобы внести изменение в имя или расположение контейнера в дереве службы каталога JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Пользователи**. На вкладке **Действия над контейнером** выберите необходимый корневой контейнер службы каталога JMS. (При необходимости выберите вложенный в него контейнер).

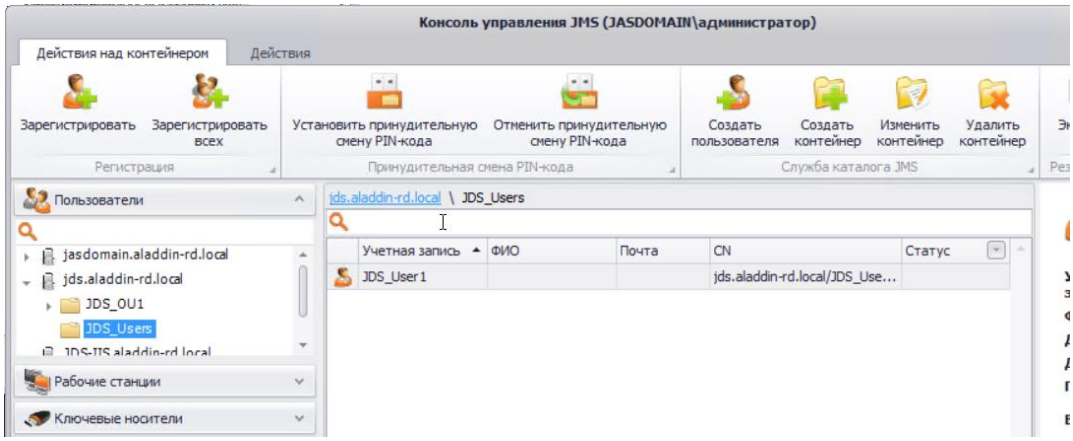


Рис. 499 – Выбор контейнера в JDS для изменения

2. В секции **Служба каталога JMS** нажмите **Изменить Контейнер.**
   Отобразится следующее окно.

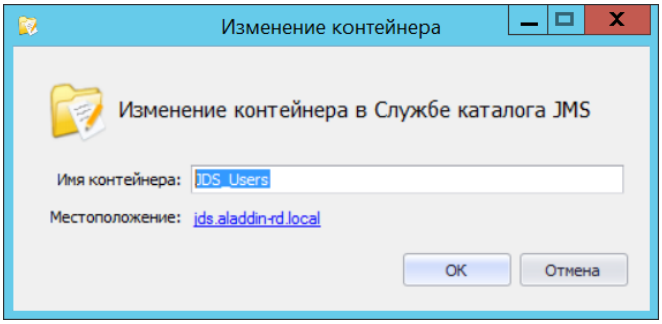


Рис. 500 – Диалог внесения изменений в контейнер

3. При необходимости отредактируйте имя контейнера.
4. При необходимости измените размещение контейнера в дереве службы каталога, нажав на ссылку **Местоположение** (Рис. 501).

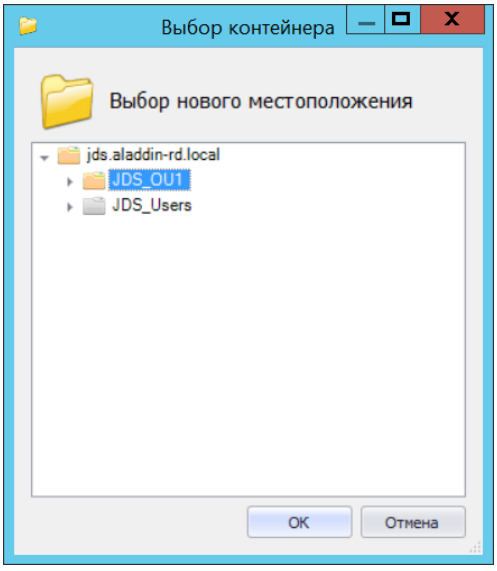


Рис. 501 – Диалог изменения расположения контейнера

   После чего выберите контейнер, в который необходимо переместить изменяемый контейнер и нажмите **OK**.
5. Для завершения редактирования нажмите **OK**.

15.7.3 Удаление контейнера в JDS

Важно! При удалении контейнера службы каталога JMS будут удалены все вложенные объекты (контейнеры и пользователи) данного контейнера без возможности их дальнейшего восстановления.

Чтобы удалить контейнер из дерева службы каталога JMS, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Пользователи**. На вкладке **Действия над контейнером** выберите необходимый корневой контейнер службы каталога JMS, в нем – контейнер, который необходимо удалить, и в секции **Служба каталога JMS** нажмите **Удалить контейнер**.
2. В окне подтверждения нажмите **ОК**.

Примечание. В случае если контейнер содержит вложенные объекты (пользователей) или другие контейнеры в диалоговом окне удаления контейнера будет отображено соответствующее предупреждение.

15.7.4 Создание пользователя в JDS

Для создания пользователя в службе каталога JMS (JDS) выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Пользователи**, на вкладку **Действия над контейнером (**Рис. 502**)**, в левой панели выберите корневой контейнер JDS и при необходимости выберите в нем контейнер, в котором необходимо создать пользователя.

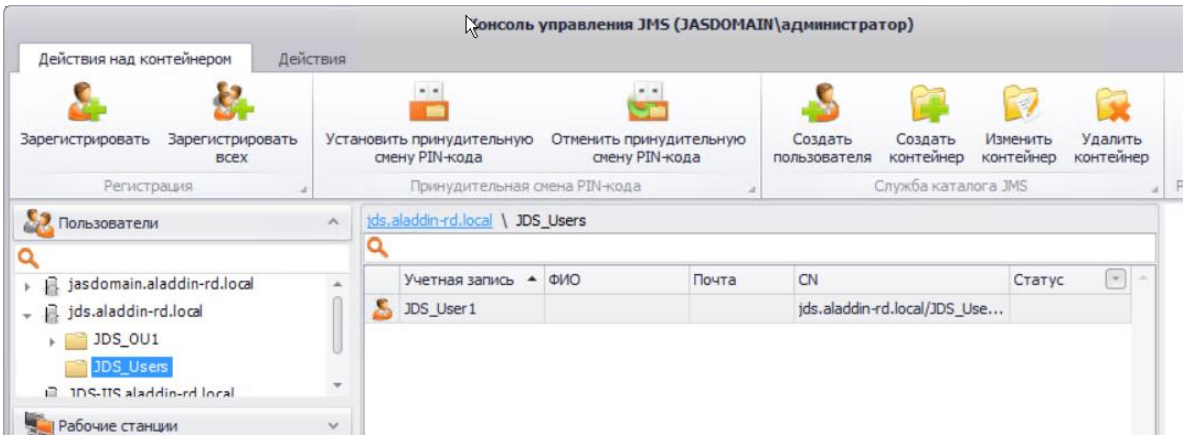


Рис. 502 – Выбор контейнера JDS для создания пользователя

2. Нажмите **Создать пользователя**.

Отобразится следующее окно.

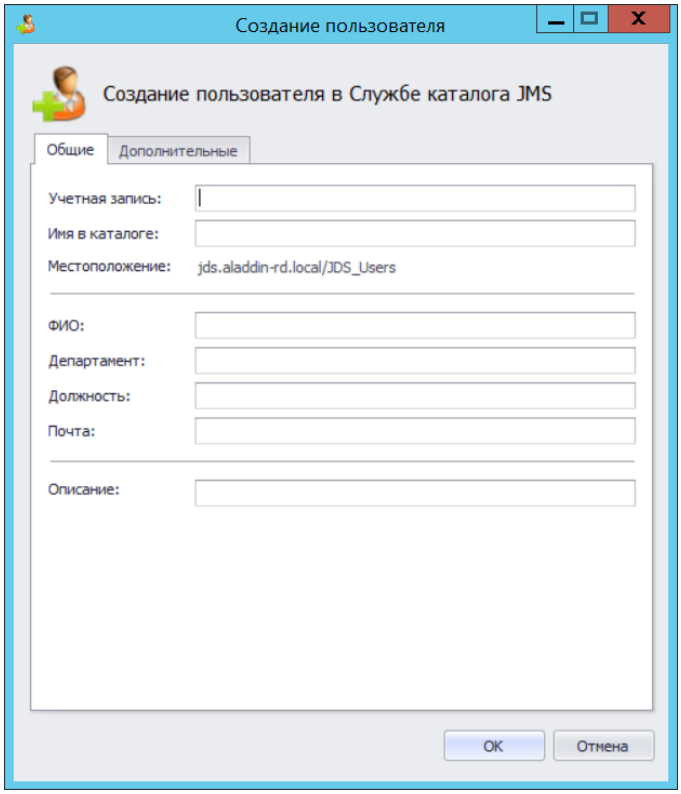


Рис. 503 – Окно создания пользователя в JDS

3. Выполните настройки на вкладке **Общие**, руководствуясь Табл. 126.

Табл. 126 – Создание пользователя в JDS

Настройка	Описание
Учетная запись	Введите имя учетной записи пользователя в JMS. (Имя учетной записи используется при аутентификации пользователя в JMS.) Поле обязательно для заполнения Максимальная длина поля: 200 символов **Примечания:** 1. Вводимое значение должно быть уникальным в JDS. 2. Значение не может состоять из одних пробелов
Имя в каталоге	Введите имя пользователя для службы каталога JMS (JDS) (Поле регистрируется в службе каталога JMS как имя Common Name (CN) согласно стандарту X.500. Значение поля **Имя в каталоге** может совпадать со значением поля **Учетная запись**.) Поле обязательно для заполнения Максимальная длина поля: 200 символов **Примечания:** 1. Вводимое значение должно быть уникальным в JDS. 2. Значение не может состоять из одних пробелов.

Настройка	Описание
	3. В случае если отличительное имя (DN), формируемое на основе имени каталога JDS и имени пользователя (**Имя в каталоге**), превысит 450 символов, будет отображено соответствующее сообщение об ошибке.
Местоположение	Нередактируемое поле. Отражает путь расположения пользователя в дереве службы каталога
ФИО	Введите полное имя пользователя Максимальная длина поля: 400 символов
Департамент **Должность**	Заполните поля при необходимости Максимальная длина каждого поля: 400 символов
Почта	Введите адрес электронной почты при необходимости Максимальная длина поля: 50 символов
Описание	Заполните поле при необходимости Максимальная длина поля: 400 символов

Примечания:

1. Во вводимых полях допускается использовать любые символьные значения, включая символы запятой, точки с запятой, одинарных и двойных кавычек, обратного слеша.
2. Концевые пробелы в строках отбрасываются.

4. Выберите вкладку **Дополнительные (**Рис. 504**).**

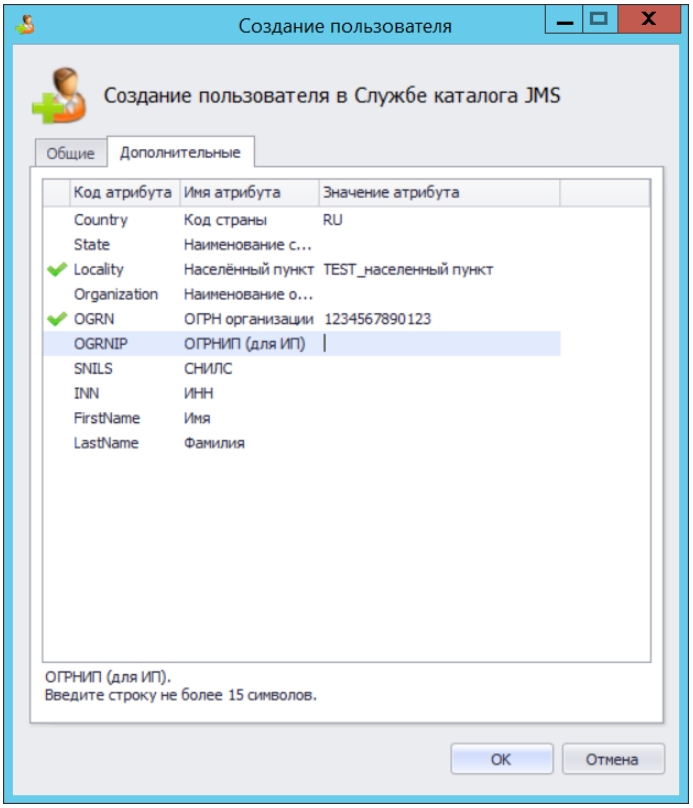


Рис. 504 – Вкладка дополнительных атрибутов пользователя в JDS

5. Выберите атрибут (отметьте левой кнопкой мыши строку атрибута) и введите его текстовое значение в столбце **Значение атрибута**.

Примечания:

1. Длина значения любого из атрибутов на вкладке **Дополнительные** не должна превышать 400 символов.
2. Во вводимых полях допускается использовать любые символьные значения, включая символы запятой, точки с запятой, одинарных и двойных кавычек, обратного слеша.
3. Концевые пробелы в строках отбрасываются.

6. Повторите шаг 0 для всех необходимых атрибутов пользователя. Отредактированные атрибуты будут помечены значком ✔.
7. Нажмите **ОК**, чтобы сохранить учетную запись пользователя.

15.7.5 Изменение учетной записи пользователя в JDS

Для внесения изменений в учетную запись пользователя в JDS выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Пользователи**, на вкладку **Действия над контейнером**, в левой панели выберите корневой контейнер службы каталога JMS (JDS) и в соответствующем контейнере выберите необходимого пользователя.
2. На вкладке **Действия (**Рис. 505**)**, в секции **Служба каталога JMS** нажмите **Изменить пользователя**.

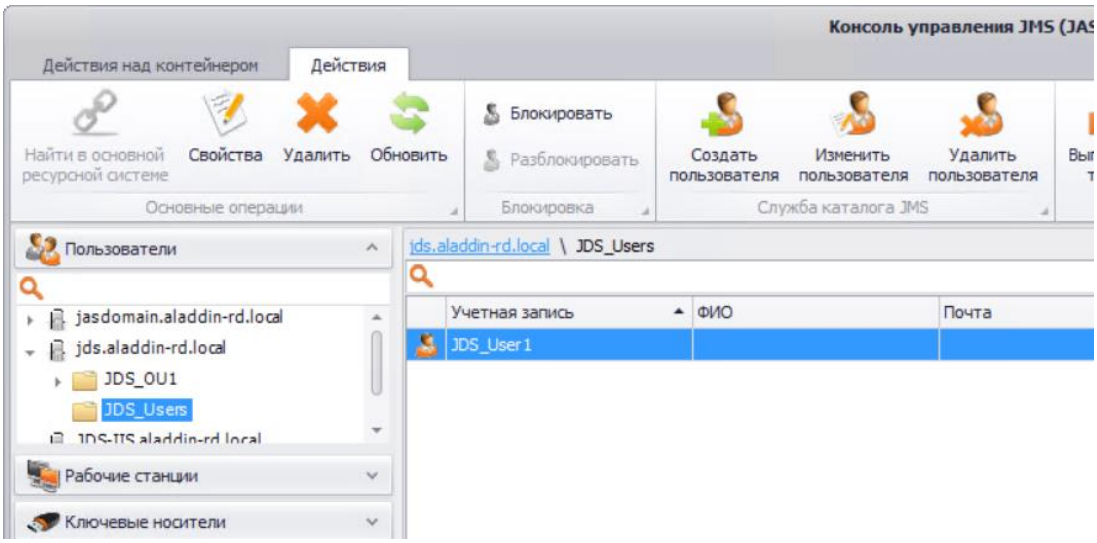


Рис. 505 – Выбор пользователя в контейнере JDS

3. В окне **Свойства пользователя** (Рис. 506) при необходимости измените значения соответствующих полей.

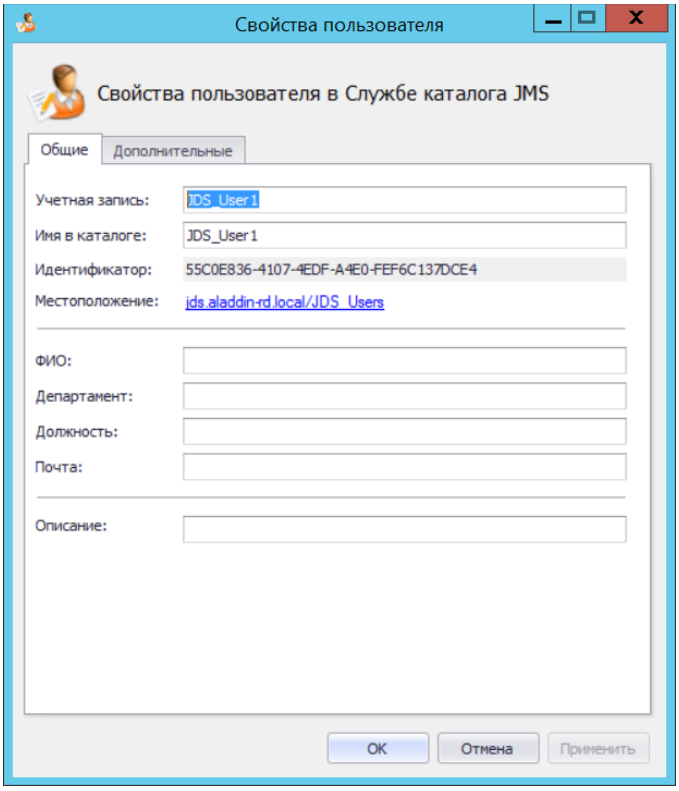


Рис. 506 – Окно редактирования свойств пользователя в JDS

4. При необходимости измените размещение пользователя в дереве контейнеров JDS, нажав на ссылку **Местоположение** (Рис. 506).
   Отобразится следующее окно

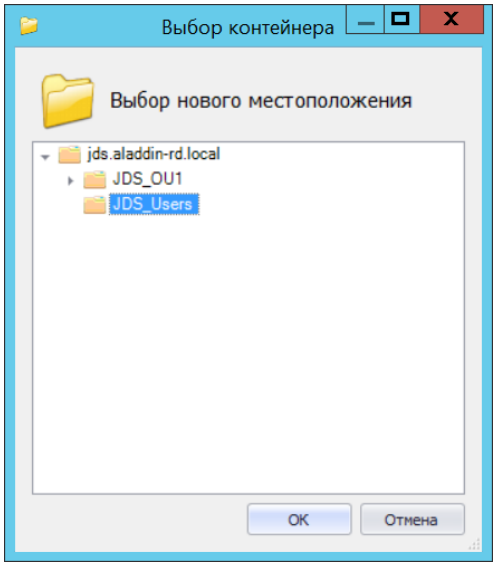


Рис. 507 – Диалог изменения расположения пользователя в иерархии контейнеров JDS

   Выберите контейнер, в который необходимо переместить пользователя и нажмите **OK**.
5. Для сохранения внесенных изменений нажмите **OK**.

15.7.6 Удаление учетной записи пользователя

15.7.6.1 Удаление учетной записи пользователя из JMS

Поскольку служба каталога JMS (JDS) используется в JMS наряду с другими ресурсными системами (такими как служба каталога Active Directory или удостоверяющие центры КриптоПро УЦ), учетная запись пользователя, зарегистрированного в JDS, может быть удалена из JMS так же, как из JMS удаляются учетные записи, относящиеся к другим ресурсным системам (см. «Удаление пользователей из JMS», с. 47). При этом удаленная из JMS учетная запись пользователя сохраняется службе каталога JDS.

Пользователь, удаленный из JMS, может быть в последующем восстановлен путем процедуры регистрации (см. раздел «Регистрация пользователей в JMS», с. 36).

Для удаления учетной записи из JDS (т.е. полного удаления без возмжоности восстановления) необходимо выполнить действия, описанные в разделе «Удаление учетной записи пользователя из JDS», ниже.

15.7.6.2 Удаление учетной записи пользователя из JDS

Важно! При удалении пользователя из службы каталога JMS (JDS) учетная запись пользователя будет удалена из JMS без возможности ее дальнейшего восстановления.

Чтобы удалить учетную запись пользователя из JDS выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Пользователи**, на вкладку **Действия над контейнером**, в левой панели выберите корневой контейнер службы каталога JMS (JDS) и в соответствующем контейнере выберите пользователя, которого необходимо удалить.
2. На вкладке **Действия (**Рис. 508**)**, в секции **Служба каталога JMS** нажмите **Удалить пользователя**.

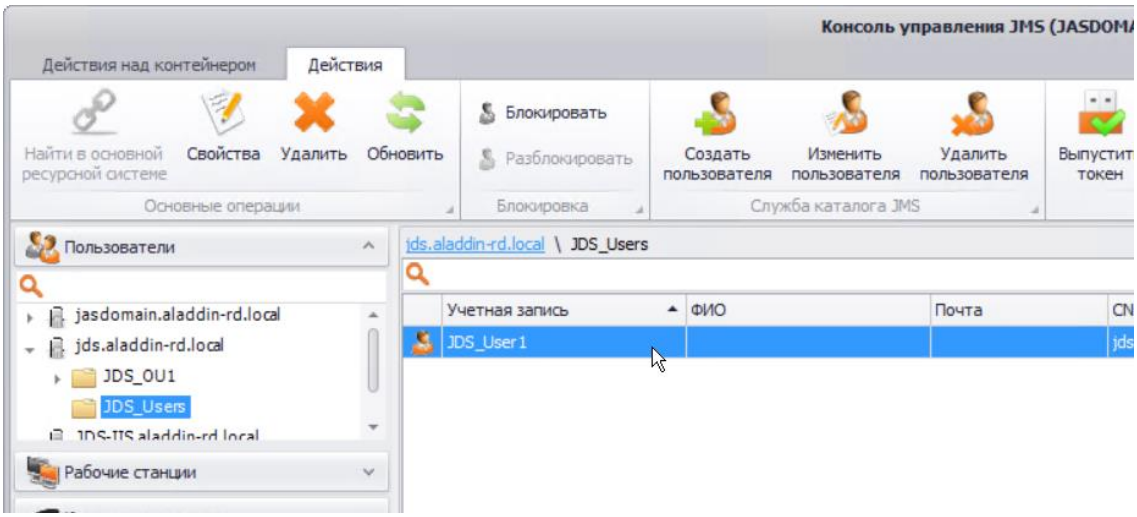


Рис. 508 – Выбор контейнера JDS для удаления пользователя

3. В окне подтверждения (Рис. 509) нажмите **OK**.

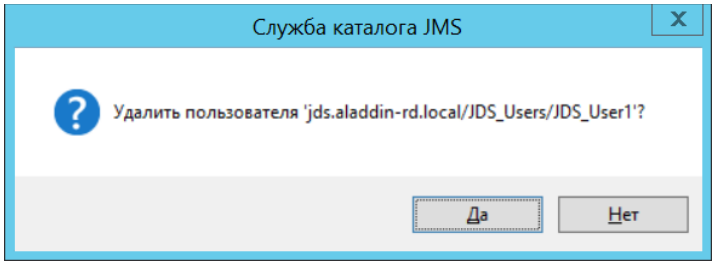


Рис. 509 – Окно удаления пользователя из JDS

15.7.7 Регистрация пользователя в JMS

При создании пользователя в службе каталога JMS (см. «Создание пользователя в JDS», с. 547) происходит автоматическая его регистрация также в системе JMS (т.е. никаких специальных действий по регистрации пользователя в JMS производить не надо).

В случае если учетная запись пользователя, созданного в JDS, была удалена из базы данных JMS (см. «Удаление учетной записи пользователя из JMS», с. 552), данного пользователя можно восстановить с помощью стандартной процедуры регистрации (см. «Регистрация пользователей в JMS», с. 36).

16. 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 (и/или сертификатов, выпущенных в хранилище пользователя) пользовательская лицензия высвобождается и может быть задействована вновь.

По факту исчерпания всех приобретенных заказчиком пользовательских лицензий 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. Подробную актуальную информацию о схеме лицензирования следует запросить у производителя.

16.1 Процедура учета (блокировки) пользовательской лицензии

При выполнении с электронным ключом операции **Назначить пользователю**, см. раздел «Жизненный цикл электронного ключа», с. 55 (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).

«Блокирование» 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. 46).

16.2 Процедура освобождения пользовательской лицензии

При выполнении с электронным ключом операций **Вернуть в эксплуатацию** или **Удалить** (см. раздел «Жизненный цикл электронного ключа», с. 55) происходит «освобождение» одной

пользовательской лицензии (при условии, что пользователю не назначены в JMS другие электронные ключи/сертификаты).

«Разблокирование» 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. 46).

17. Коннектор SecurLogon

17.1 Дистрибутив

В поставку коннектора SecurLogon входят следующие файлы (табл. 127).

Табл. 127 – Дистрибутив коннектора SecurLogon

Файл	Описание
Aladdin.JMS.SecurLogon.Connector.Server.x.x.x.x-x86.ru.msi **Aladdin.JMS.SecurLogon.Connector.Server.x.x.x.x-x64.ru.msi**	Серверный компонент коннектора для установки на сервер JMS. 32- и 64-битная версия соответственно.
Aladdin.JMS.SecurLogon.Connector.Admin.x.x.x.x-x86.ru.msi **Aladdin.JMS.SecurLogon.Connector.Admin.x.x.x.x-x64.ru.msi**	Административный компонент коннектора для установки на компьютер, на котором установлена консоль управления JMS. 32- и 64-битная версия соответственно.

17.2 Установка и настройка серверной части

Чтобы установить и настроить серверный компонент SecurLogon, выполните следующие действия.

1. На сервере JMS запустите файл установки серверного компонента коннектора SecurLogon (см. табл. 127 выше).
   Отобразится следующее окно.

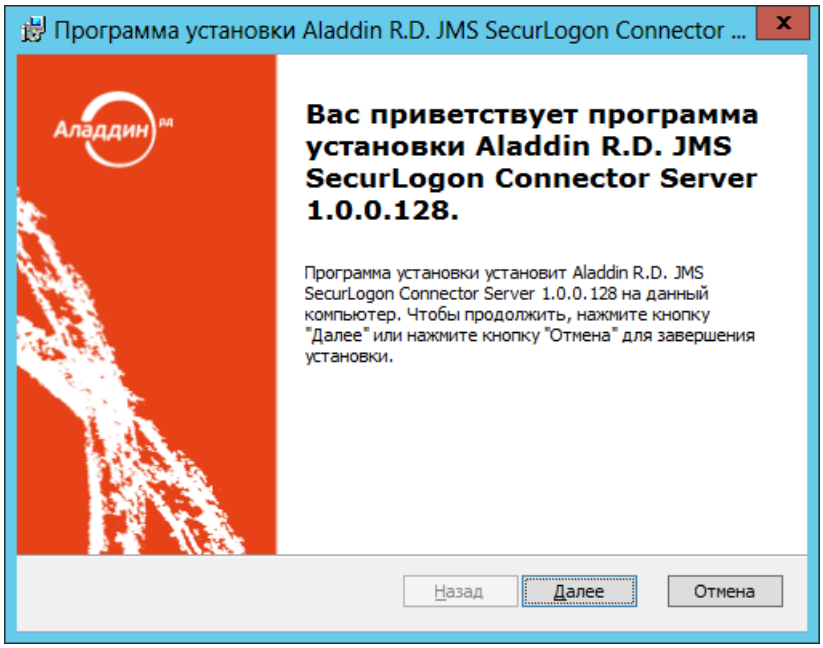


Рис. 510 – Окно приветствия мастера установки серверного компонента коннектора SecurLogon

2. Нажмите **Далее**.

Отобразится следующее окно.

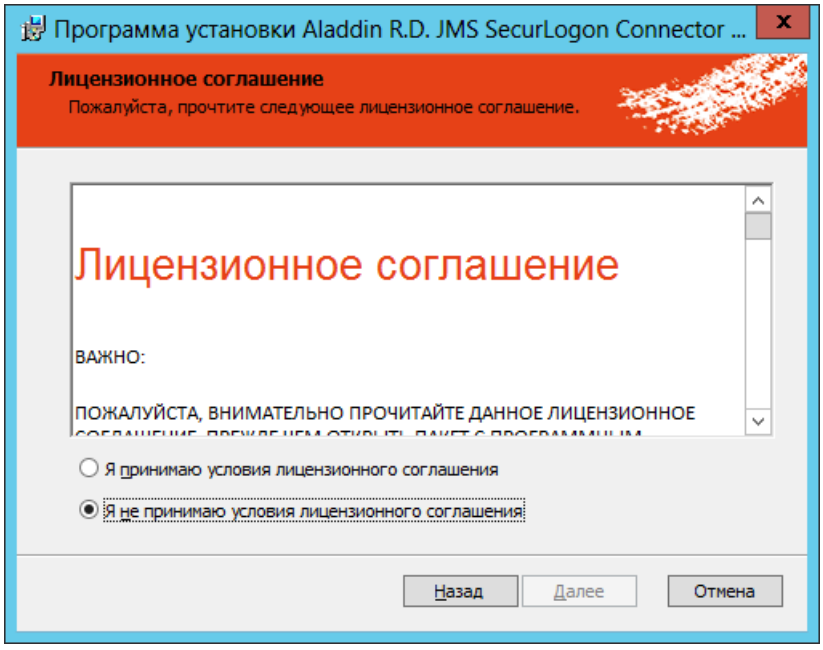


Рис. 511 – Окно лицензионного соглашения

3. Выберите пункт **Я принимаю условия лицензионного соглашения**, после чего нажмите **Далее**. Отобразится следующее окно.

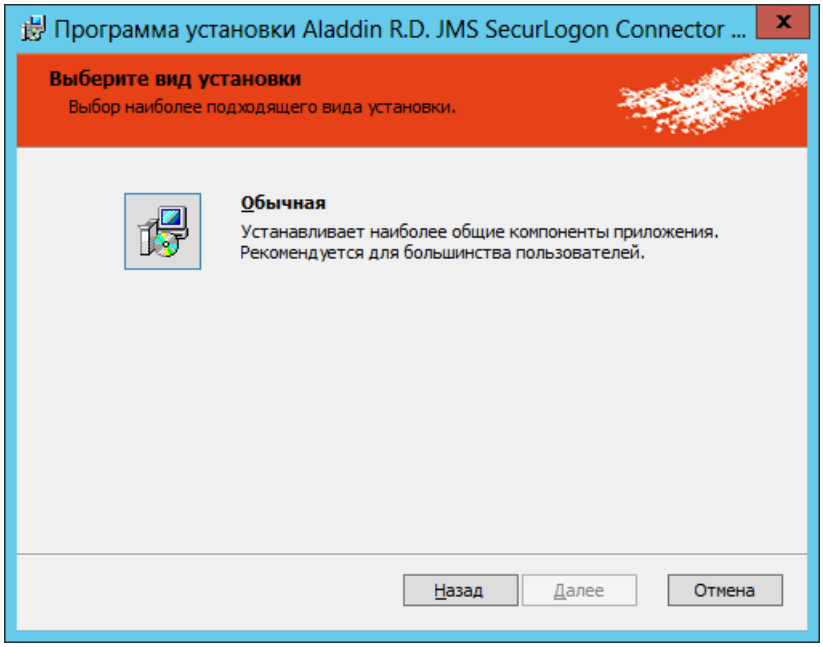


Рис. 512 – Выбор варианта установки

4. Выберите **Обычная**.

Отобразится следующее окно.

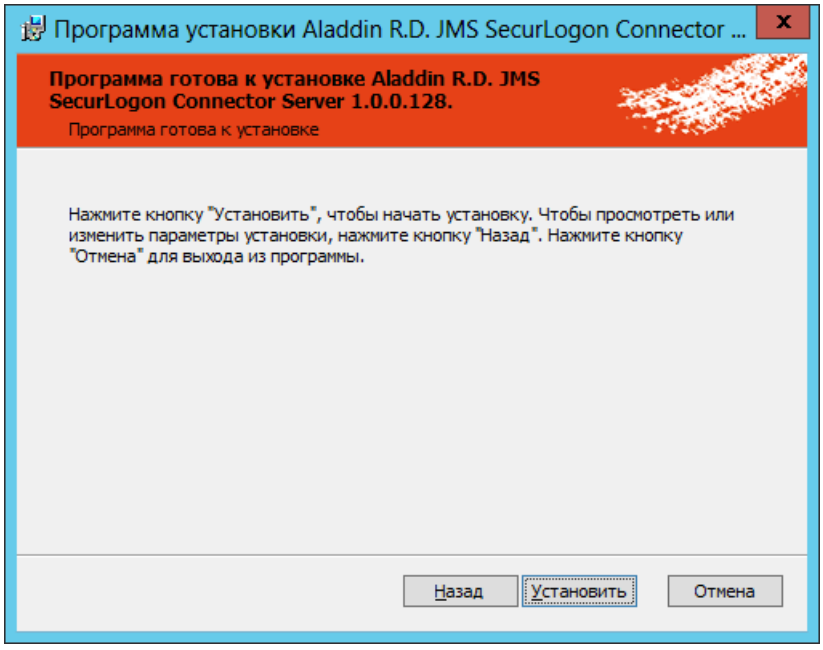


Рис. 513 – Подготовка к установке

5. Нажмите **Установить**.
   Отобразится следующее окно.

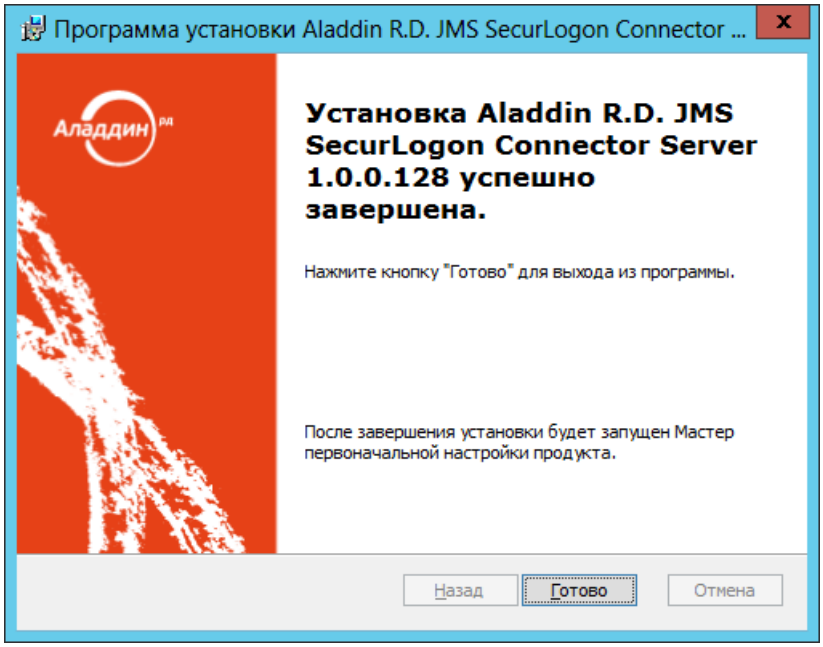


Рис. 514 – Окно завершения работы мастера установки серверного компонента коннектора SecurLogon

6. Нажмите **Готово** для завершения установки.

Отобразится следующее окно.

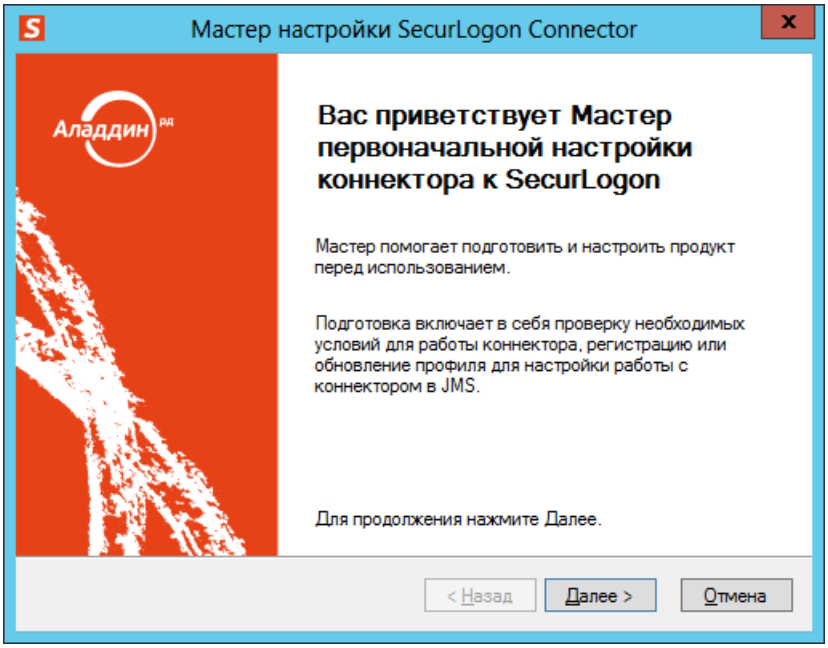


Рис. 515 – Окно приветствия мастера первоначальной настройки коннектора SecurLogon

7. Нажмите **Далее**.
   Отобразится следующее предупреждение.

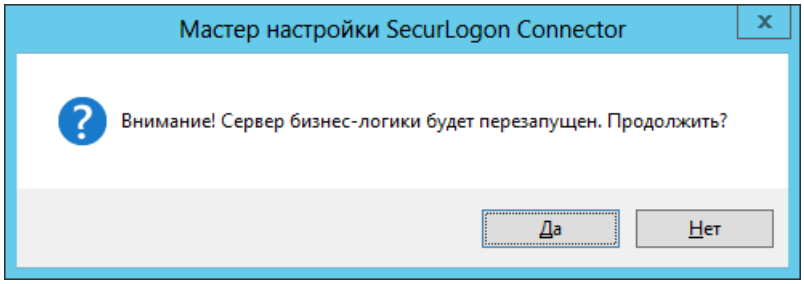


Рис. 516 – Предупреждение о перезапуске сервера JMS

8. Нажмите **Да**, чтобы подтвердить действия.

Отобразится следующее окно.

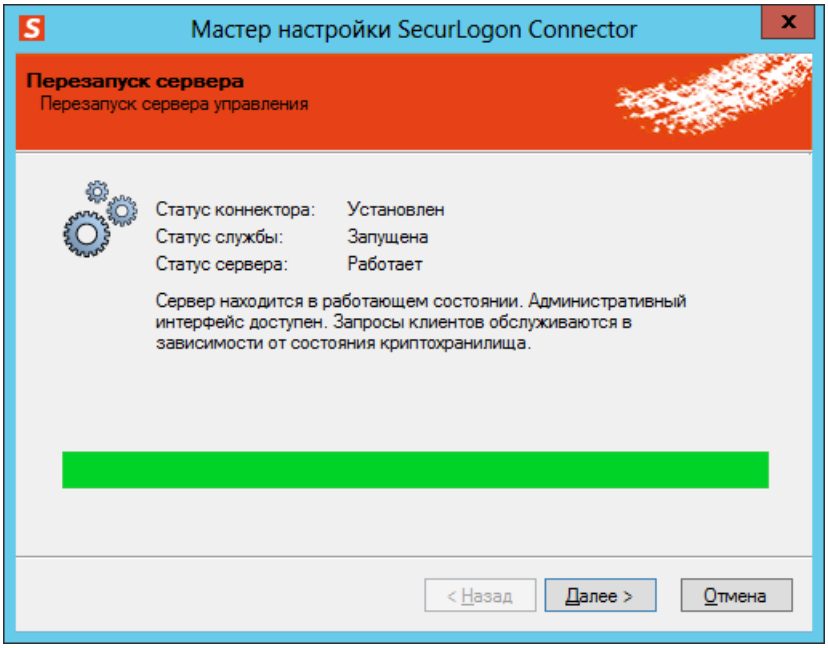


Рис. 517 – Перезапуск сервера JMS

9. Нажмите **Далее**.
   Отобразится следующее окно.

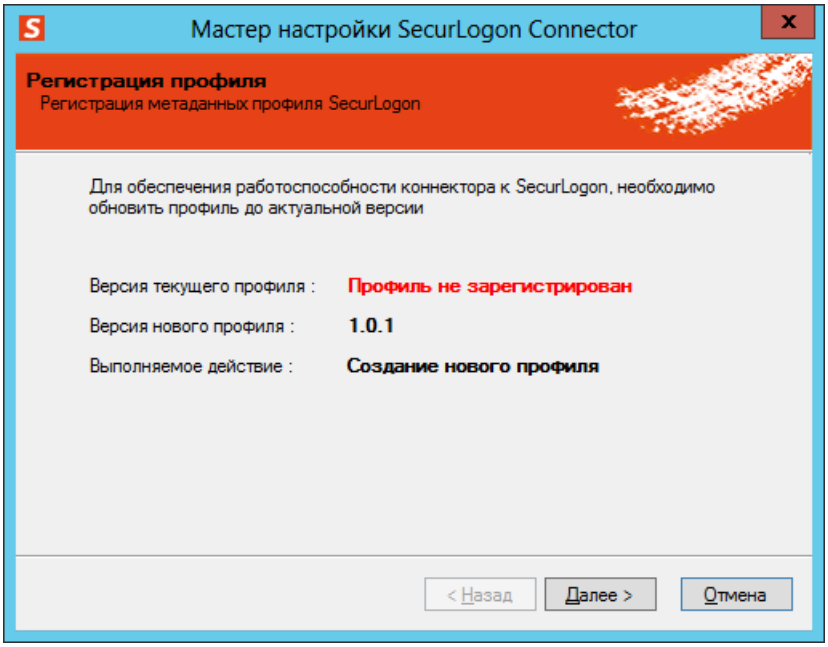


Рис. 518 – Регистрация профиля SecurLogon

10. Нажмите **Далее**.

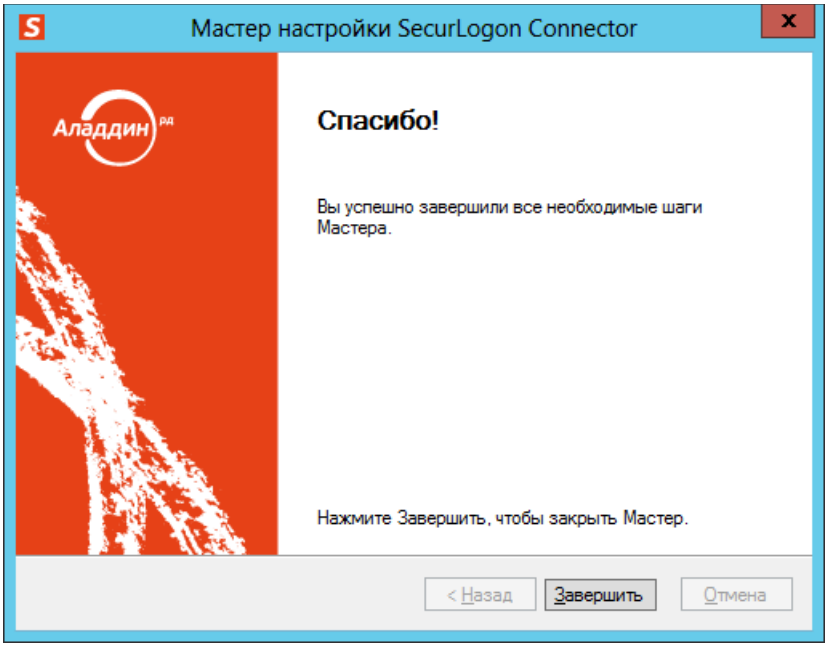


Рис. 519 – Окно завершения работы мастера первоначальной настройки SecurLogon

11. Нажмите **Завершить**.
12. Воспользовавшись окном управления сервером JMS, добавьте лицензию на коннектор SecurLogon (подробнее см. «Руководство администратора. Часть 1» [2], раздел «Окно управления сервером JMS (серверный агент)» -> «Лицензии»).

17.3 Установка дополнения для консоли управления JMS

Чтобы установить административный компонент коннектора SecurLogon, выполните следующие действия.

1. На компьютере, на котором установлена консоль управления JMS, запустите файл установки административного компонента SecurLogon (см. табл. 127, с. 554).
   Отобразится следующее окно.

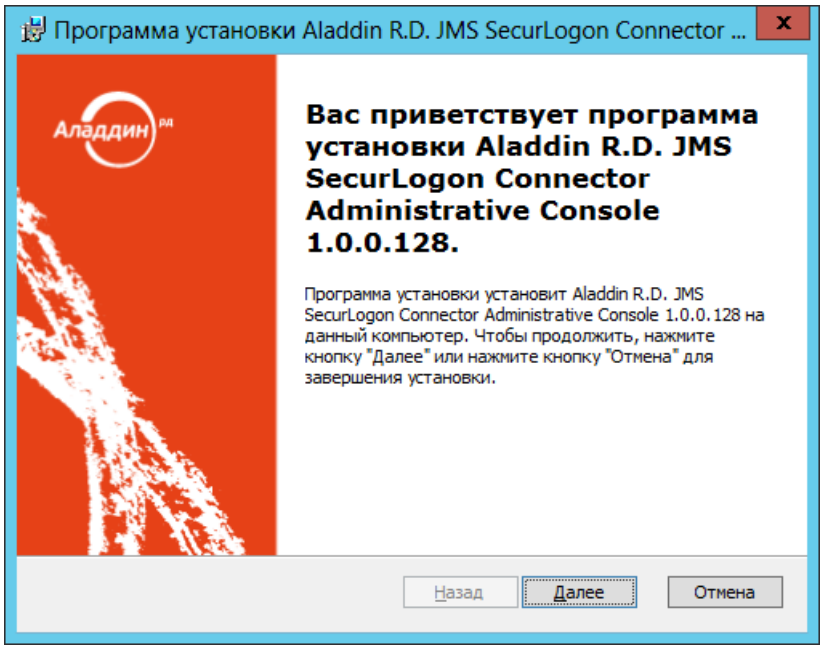


Рис. 520 – Окно приветствия мастера установки административного компонента SecurLogon

2. Нажмите **Далее**.
   Отобразится следующее окно.

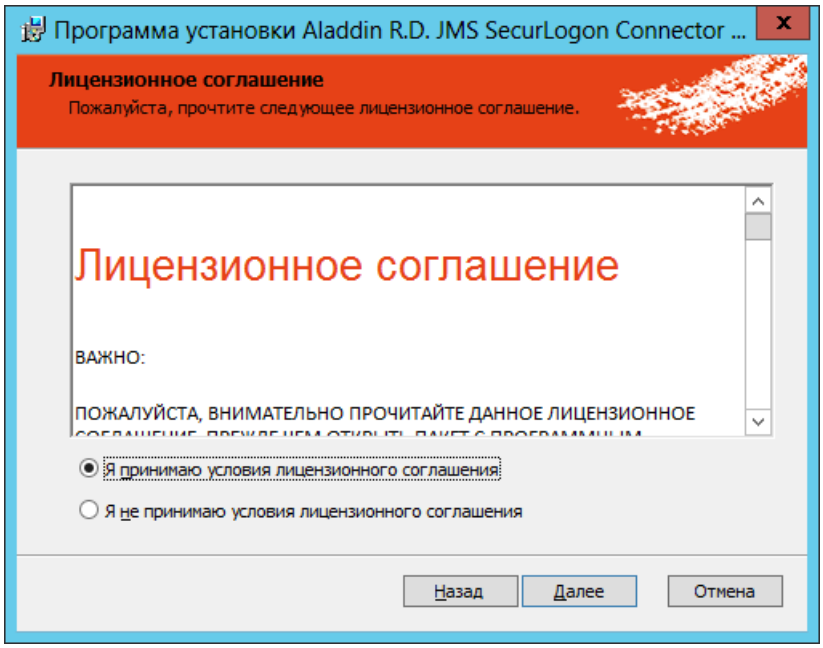


Рис. 521 – Окно лицензионного соглашения

3. Выберите пункт **Я принимаю условия лицензионного соглашения**, после чего нажмите **Далее**.
   Отобразится следующее окно.

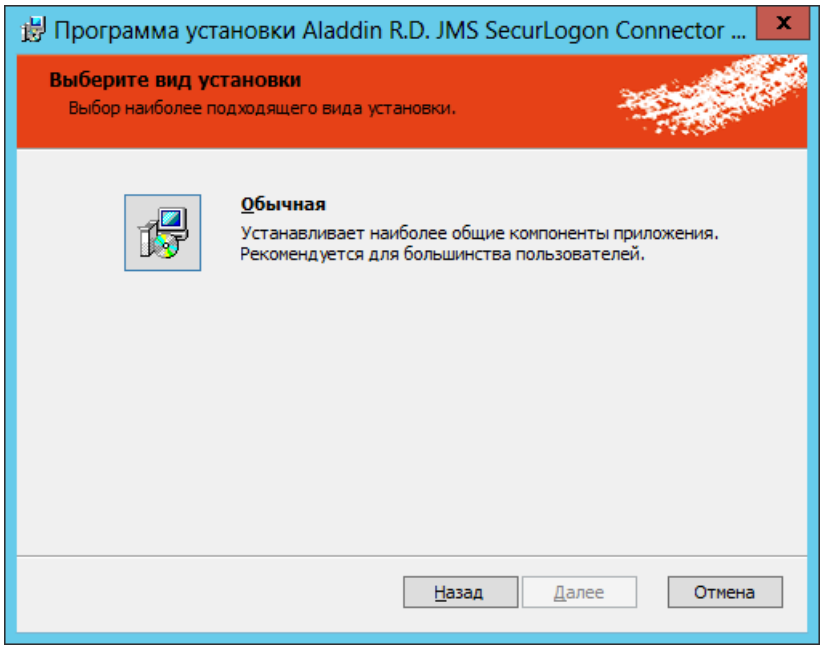


Рис. 522 – Окно выбора варианта установки

4. Выберите пункт **Обычная**.

Отобразится следующее окно.

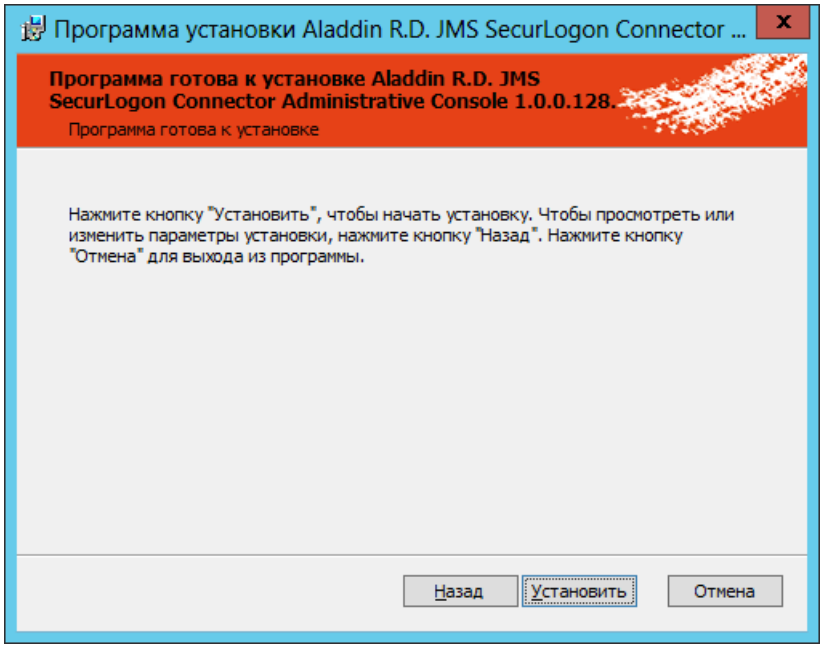


Рис. 523 – Подготовка к установке

5. Нажмите **Установить**.
   Отобразится следующее окно.

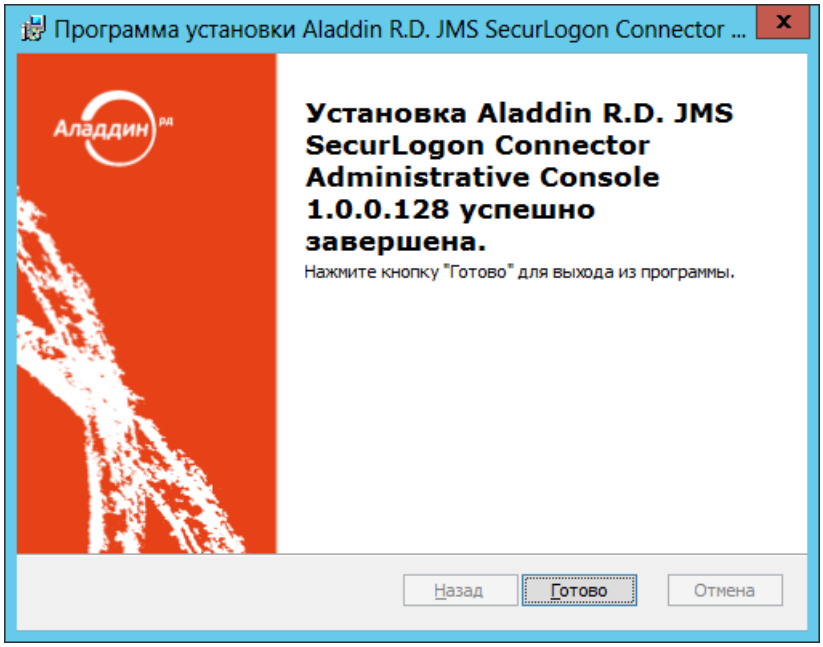


Рис. 524 – Окно завершения работы мастера установки коннектора SecurLogon

6. Нажмите **Готово** для завершения процедуры.

17.4 Создание и настройка профиля SecurLogon

Чтобы настроить профиль выпуска электронных ключей для использования с SecurLogon, выполните следующие действия.

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

2. В центральной части окна выберите пункт **Выпуск КН для использования в SecurLogon**.
3. В верхней панели нажмите **Создать**.
   Отобразится следующее окно.

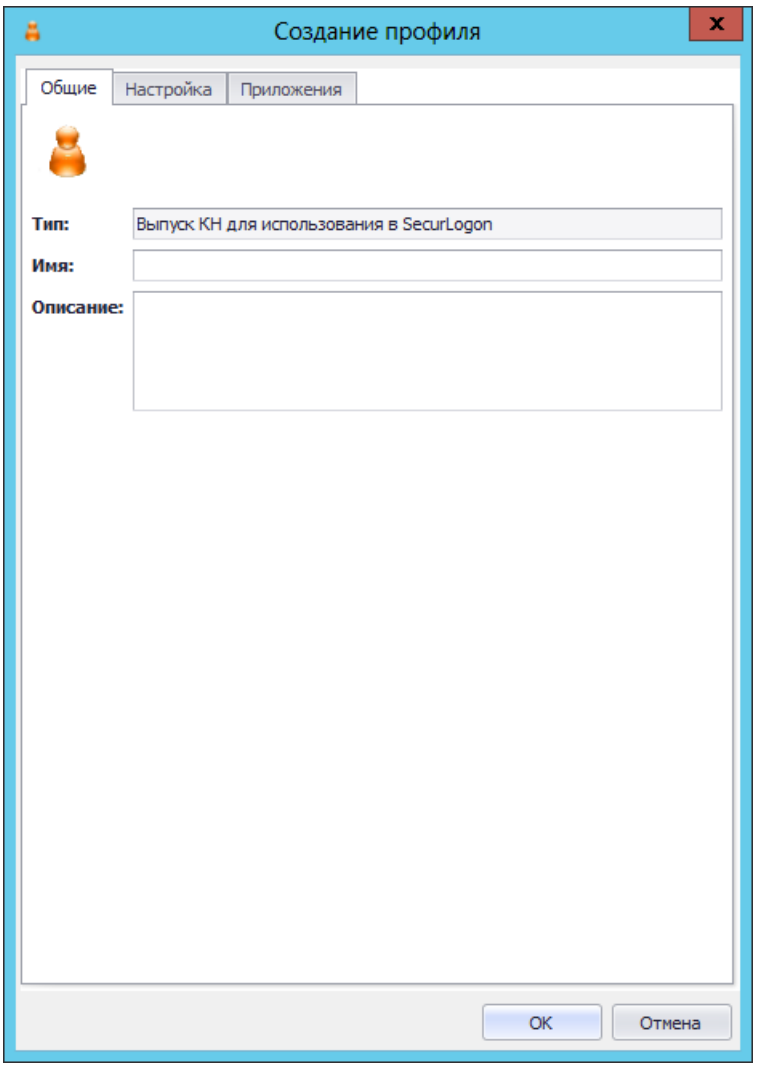


*Рис. 525 – Вкладка **Общие** профиля SecurLogon*

4. В поля **Имя** и **Описание** введите соответственно название и описание профиля, после чего перейдите на вкладку **Настройка**.

Окно примет следующий вид.

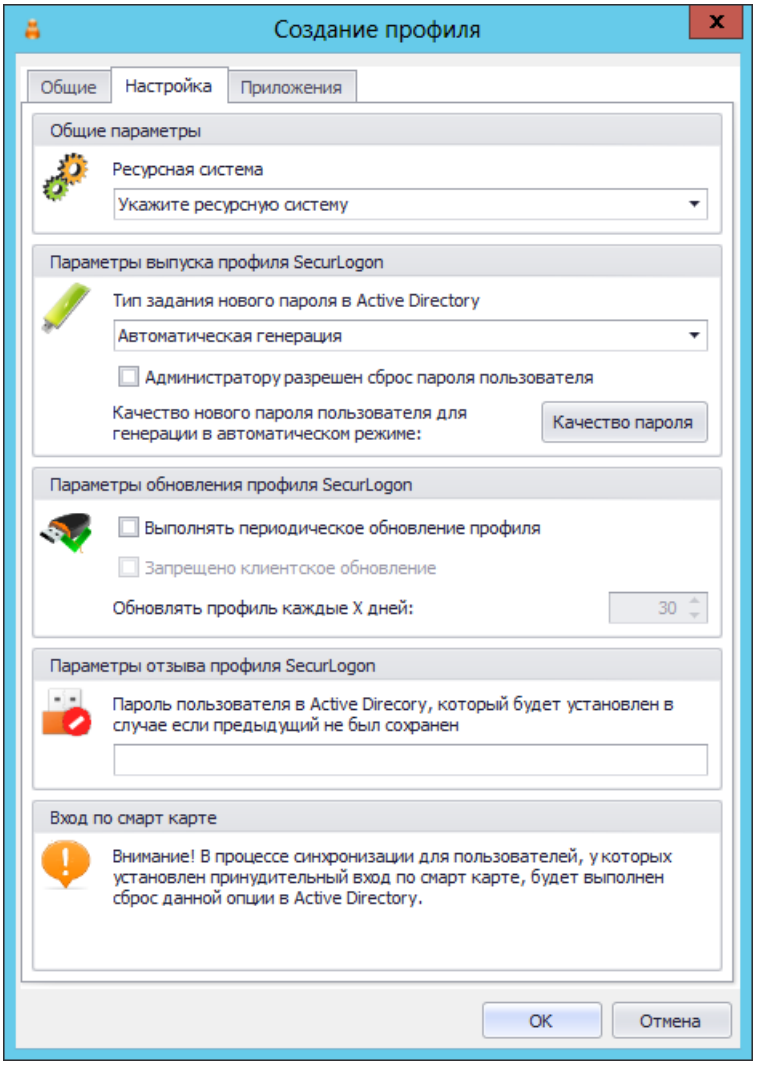


Рис. 526 – Настройки профиля SecurLogon

5. Выполните настройку, руководствуясь табл. 128.

Табл. 128 – Настройки профиля SecurLogon

Секция	Настройка	Описание
Общие параметры	**Ресурсная система**	Выберите из списка ресурсную систему, для пользователей которой настраивается объект (профиль) SecurLogon в электронном ключе.
Параметры выпуска профиля SecurLogon	**Тип задания нового пароля в Active Directory**	Позволяет выбрать метод формирования пароля пользователя, который будет записываться в объект (профиль) SecurLogon на электронном ключе. Доступны следующие варианты: • **Автоматическая генерация** – пароль будет сформирован автоматически, в этому случае следует задать критерии качества пароля, воспользовавшись соответствующей кнопкой; • **Указывается вручную** – пароль будет указан вручную при выпуске электронного ключа, эта настройка не позволяет задать качество пароля.

Секция	Настройка	Описание
	Администратору разрешен сброс пароля пользователя	Если настройка включена, при выпуске электронного ключа администратором станет доступна возможность сброса пароля. Это позволит администратору сбросить пароль пользователя, не зная его. ⚠ При сбросе пароля пользователя могут быть утеряны данные пользователя, зашифрованные на предыдущем пароле.
	Качество пароля	Нажатие на кнопку отображает окно, позволяющее задать параметры сложности пароля. Доступны следующие настройки: • **Минимальная длина** – позволяет задать минимальную длину пароля; • **Максимальная длина** – позволяет задать максимальную длину пароля; • **Символы алфавита** – позволяет задать минимальное число символов алфавита в пароле; • **Символы в верхнем регистре** – позволяет задать минимальное число символов алфавита в верхнем регистре; • **Символы в нижнем регистре** – позволяет задать минимальное число символов алфавита в нижнем регистре; • **Числовые символы** – позволяет задать минимальное число цифр в пароле; • **Специальные символы** – позволяет задать минимальное число символов, не входящих в алфавитно-цифровой набор, в пароле; • **Максимальное количество повторений символов** – позволяет задать максимальное число идущих подряд повторений символов в пароле.
Параметры обновления профиля SecurLogon	**Выполнять периодическое обновление профиля**	Включение настройки позволяет выполнять автоматическое пересоздание объекта (профиля) SecurLogon в электронном ключе и автоматическую замену пароля пользователя в Active Directory каждых X дней, где значение X равно значению, указанному в параметре **Обновлять профиль каждые X дней**. Обновление профиля выполняется коннектором SecurLogon в рамках процесса синхронизации JMS.
	Запрещено клиентское обновление	Если настройка включена, объект (профиль) SecurLogon в электронном ключе невозможно обновить, используя Клиент JMS. Обновление объекта (профиля) в электронном ключе возможно только в консоли управления JMS. Настройка становится доступной, только если включена настройка **Выполнять периодическое обновление профиля**.
	Обновлять профиль каждые X дней	Значение параметра используется для определения необходимости повторного выпуска объекта (профиля) SecurLogon в электронных ключах и замены пароля пользователя в Active Directory. Параметр становится доступным для выбора только если выбран параметр **Выполнять периодическое обновление профиля**.
Параметры отзыва профиля SecurLogon	**Пароль пользователя в Active Directory, который будет установлен в случае если предыдущий не был сохранен**	Позволяет задать пароль пользователя в Active Directory, который будет использоваться, если предыдущий пароль не был сохранен. Это обязательный параметр. ⚠ Если в выбранной ресурсной системе настроены и действуют политики с требованиями к качеству пароля пользователя, то в данном поле необходимо указывать пароль соответствующий действующим политикам.

6. Перейдите на вкладку **Приложения** и отметьте приложения, соответствующие электронным ключам, на которые будут записываться данные настраиваемого объекта (профиля) SecurLogon.
7. Нажмите **OK**, чтобы сохранить сделанные изменения.

18. Работа с ViPNet УЦ

Чтобы выпускать электронные ключи с сертификатами ViPNet УЦ средствами JMS, выполните следующие действия:

1. Выполните инструкции, приведенные в подразделе «Подготовительные действия».
2. Настройте соответствующий профиль JMS (см. «Настройка профиля для выпуска сертификатов в ViPNet УЦ», с. 585).
3. Настройте остальные необходимые профили, после чего выполните привязку профилей к нужным организационным единицам в Active Directory (см. «Настройка профилей JMS», с. 155) и переходите к выпуску электронных ключей.

18.1 Подготовительные действия

1. Убедитесь, что JMS сервер имеет доступ к УЦ Инфотекс по DNS имени (в случае отсутствия связи пропишите DNS пути или внесите изменения в файл **hosts**).
2. Убедитесь что компонент **ViPNet CA Web Service** настроен, а служба **ViPNet CA Web Service** запущена и работает.

Примечание. Чтобы проверить настройки компонента **ViPNet CA Web Service** и статус службы **ViPNet CA Web Service** рекомендуется использовать утилиту **ViPNet CA Web Service – Консоль администрирования**.

3. Запустите утилиту **ViPNet Удостоверяющий и ключевой центр**. Выполните следующие действия:

а) Создайте шаблон для установки TLS соединения, для чего выполните следующее:

– в верхней панели инструментов перейдите **Сервис -> Настройка...** (см. рис. 527) и в появившемся окне выберите **Шаблоны сертификатов** и нажмите **Добавить** (см. рис. 528);

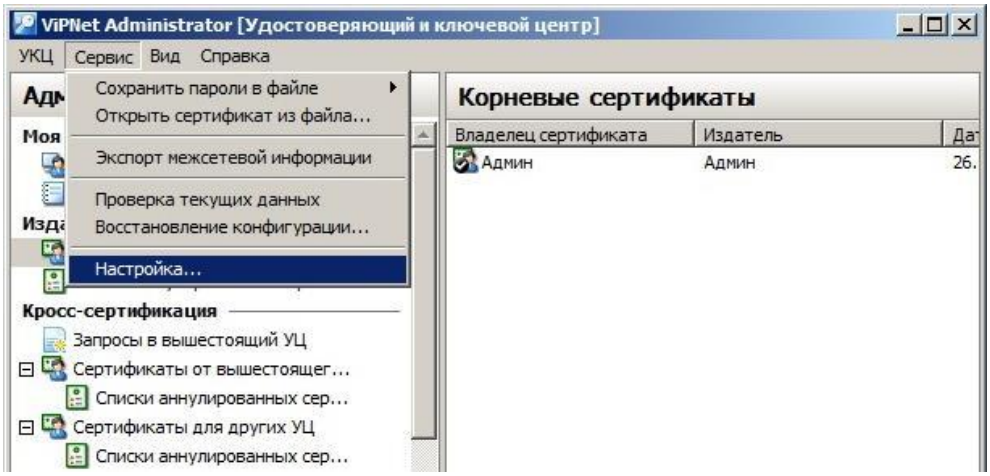


*Рис. 527 – Окно **ViPNet Удостоверяющий и ключевой центр:** Сервис – Настройка...*

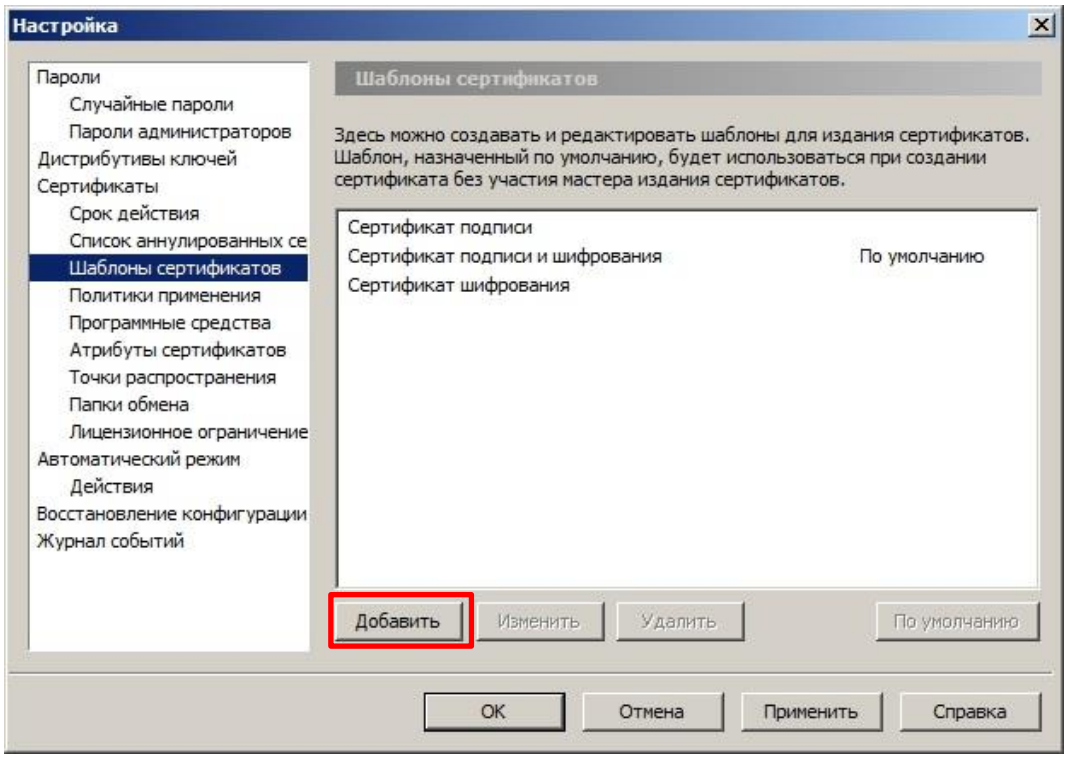


Рис. 528 – Окно Настройка – Шаблоны сертификатов

– в появившемся окне **Шаблон сертификата** введите имя шаблона сертификата (например: Проверка подлинности клиента) и нажмите **Далее**;

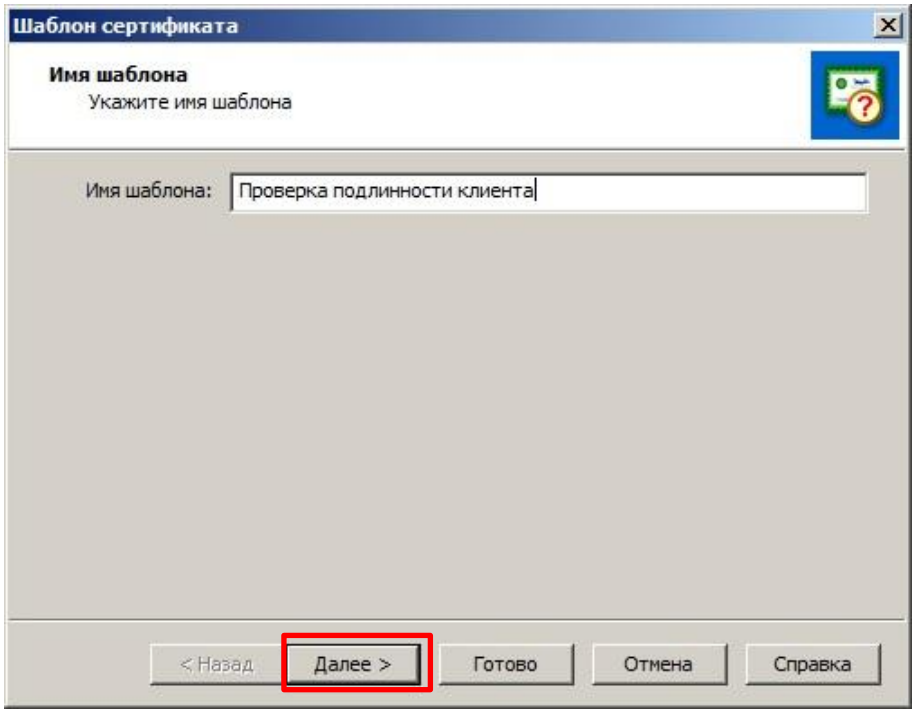


Рис. 529 – Окно Шаблон сертификата – Ввод имени шаблона

– в появившемся окне нажмите **Далее**;

– в появившемся окне нажмите **Далее**;

– в появившемся окне (см. рис. 530) нажмите **Добавить** и в появившемся окне **Допустимые разрешения** (см. рис. 531) выберите опцию **Расширенное использование ключа** и нажмите **ОК**;

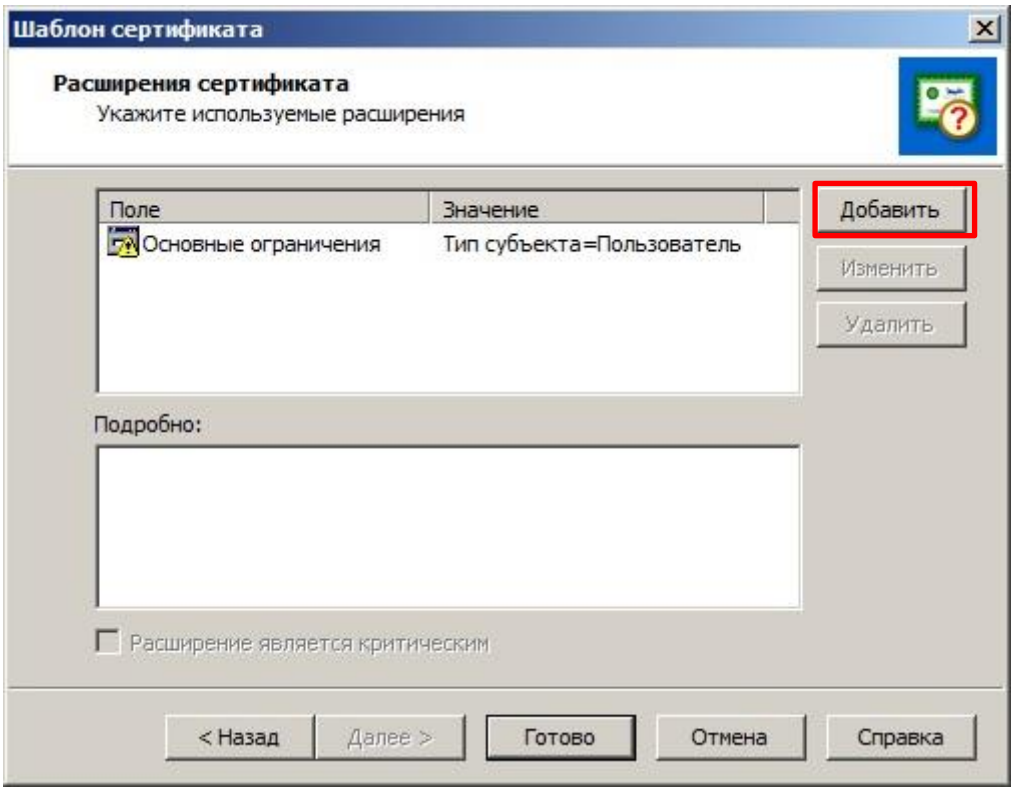


Рис. 530 – Окно Шаблон сертификата – Расширения сертификата

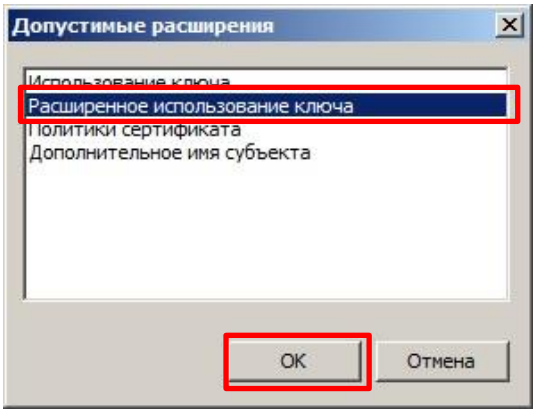


Рис. 531 – Окно Допустимые расширения

– в появившемся окне **Расширенное использование ключа** (см. рис. 532) выберите опцию **Проверка подлинности клиента** и нажмите **Добавить ->** после чего нажмите **ОК**;

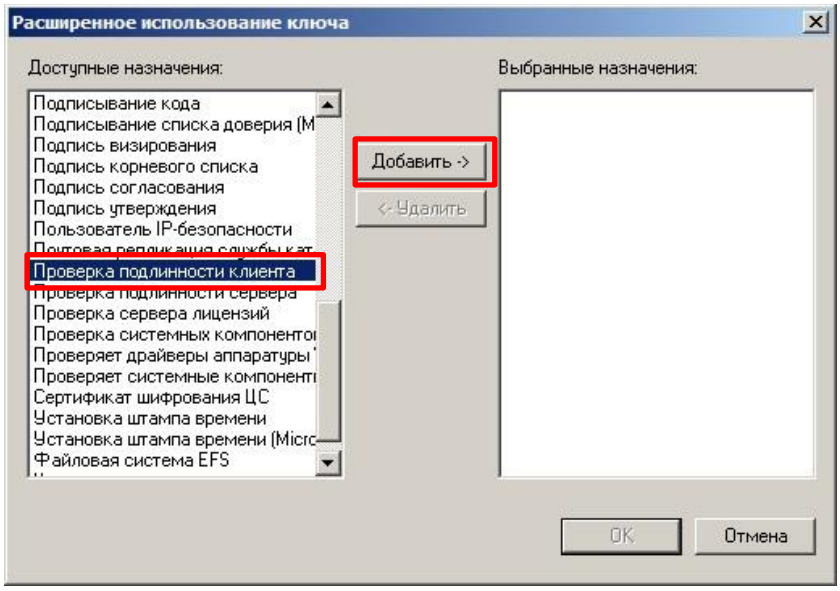


Рис. 532 – Окно Расширенное использование ключа

– в окне **Шаблон сертификата** нажмите **Готово**.

– в окне **Сервис -> Настройка...** нажмите **ОК**.

б) Создайте шаблон для подписи запросов на сертификаты, для чего выполните следующее:

– в верхней панели инструментов перейдите **Сервис -> Настройка...** (см. рис. 527) и в появившемся окне выберите **Шаблоны сертификатов** и нажмите **Добавить** (см. рис. 528);

– в появившемся окне **Шаблон сертификата** (см. рис. 533) введите имя шаблона сертификата (например: Агент запроса сертификатов) и нажмите **Далее**;

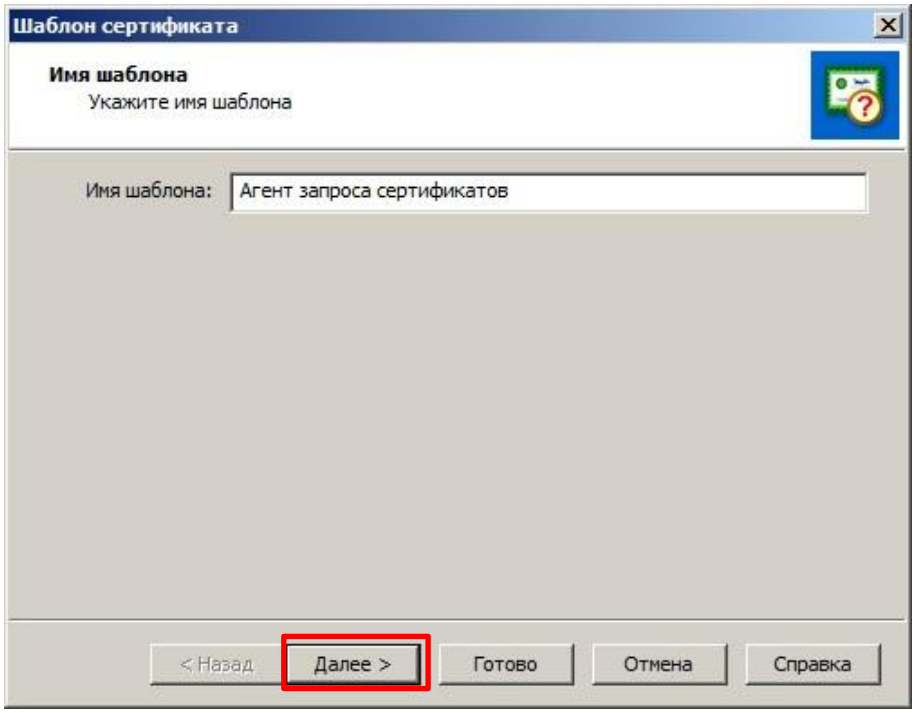


Рис. 533 – Окно Шаблон сертификата – Ввод имени шаблона

– в появившемся окне нажмите **Далее**;

– в появившемся окне нажмите **Далее**;

– в появившемся окне нажмите **Добавить** и в появившемся окне **Допустимые разрешения** выберите опцию **Расширенное использование ключа** и нажмите **ОК**;

– в появившемся окне **Расширенное использование ключа** (см. рис. 534) выберите опцию **Агент запроса сертификата** и нажмите **Добавить ->** после чего нажмите **ОК**.

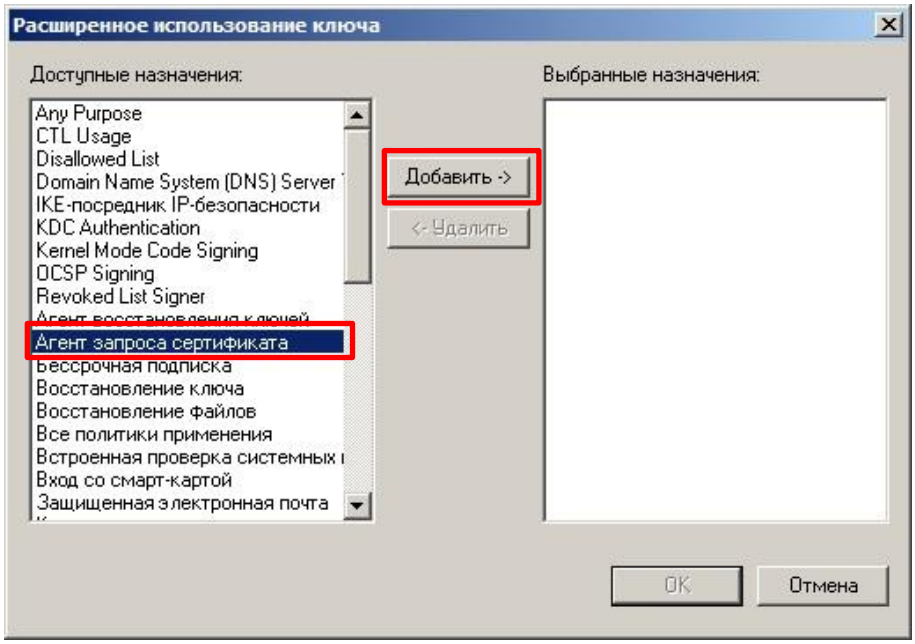


Рис. 534 – Окно Расширенное использование ключа

– в окне **Шаблон сертификата** нажмите **Готово**.

– в окне **Сервис -> Настройка...** нажмите **ОК**.

4. Запустите утилиту **Создание запроса на сертификат**, входящую в состав **ViPNet CSP**. Выполните следующие действия:

Примечание. В данном описании для создания запроса на сертификат используется утилита **Создание запроса на сертификат**, входящая в состав **ViPNet CSP**. Использование этой утилиты не обязательно. Допускается производить данную операцию с помощью других CSP. Главное, чтобы сертификаты были выпущены с правильными политиками применения.

а) Создайте запрос на сертификат для установки TLS соединения, для чего выполните следующее:

– в появившемся окне создания запроса на сертификат перейдите в секцию **Данные о владельце сертификата** и в поле **Имя (ФИО)** (см. рис. 535) введите имя (например: TLS Client) и нажмите кнопку **Сформировать запрос**;

Примечание. При необходимости дополнительно заполнить другие поля данных о владельце сертификата (адрес электронной почты, организация, подразделение и т.д.) заполните эти поля данных.

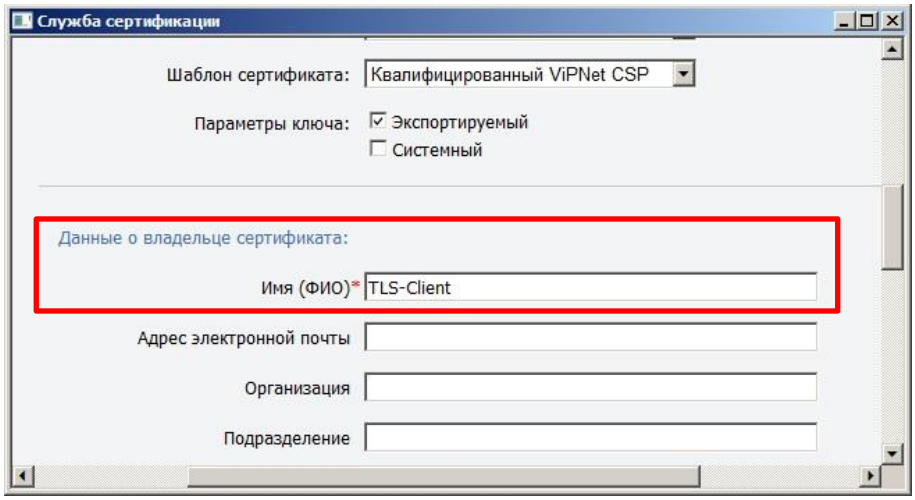


Рис. 535 – Окно Служба сертификации – Данные о владельце сертификата

– в появившемся окне **ViPNet CSP – инициализация контейнера ключей** (см. рис. 536) в поле **Имя контейнера** введите имя (либо оставьте поле со случайносгенерированным именем) и нажмите **OK**;

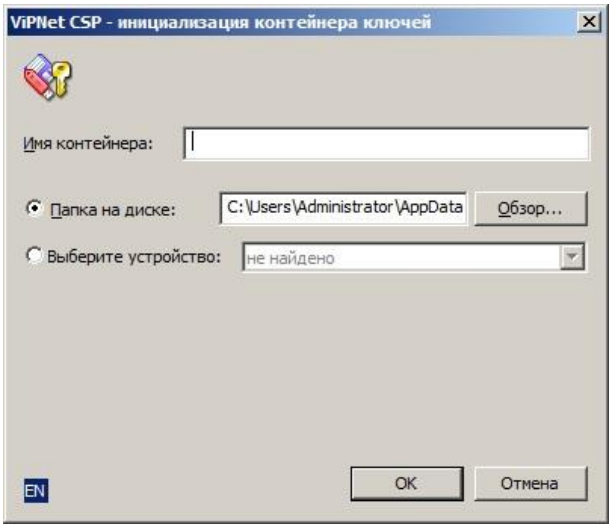


*Рис. 536 – Окно **ViPNet CSP – инициализация контейнера ключей***

– в появившемся окне **ViPNet CSP – пароль контейнера ключей** введите пароль и его подтверждение, выберите опцию **Сохранить пароль** (см. рис. 537), после чего нажмите кнопку **OK**.

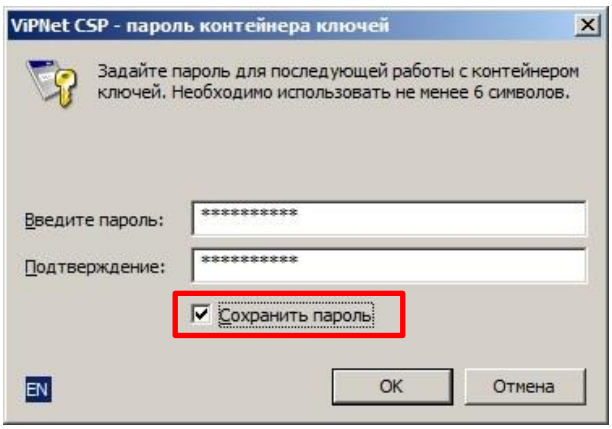


Рис. 537 – Окно ViPNet CSP – пароль контейнера ключей

– в появившемся окне **Электронная рулетка** выполните действия, описанные в окне;

– в появившемся сообщении об успешном создании запроса нажмите **OK**.

б) Создайте запрос на сертификат для подписи запросов на сертификаты, для чего выполните следующее:

– в появившемся окне создания запроса на сертификат перейдите в секцию **Данные о владельце сертификата** и в поле **Имя (ФИО)** (см. рис. 538) введите имя (например: Enrollment Agent) и нажмите кнопку **Сформировать запрос**;

Примечание. При необходимости дополнительно заполнить другие поля данных о владельце сертификата (адрес электронной почты, организация, подразделение и т.д.) заполните эти поля данных.

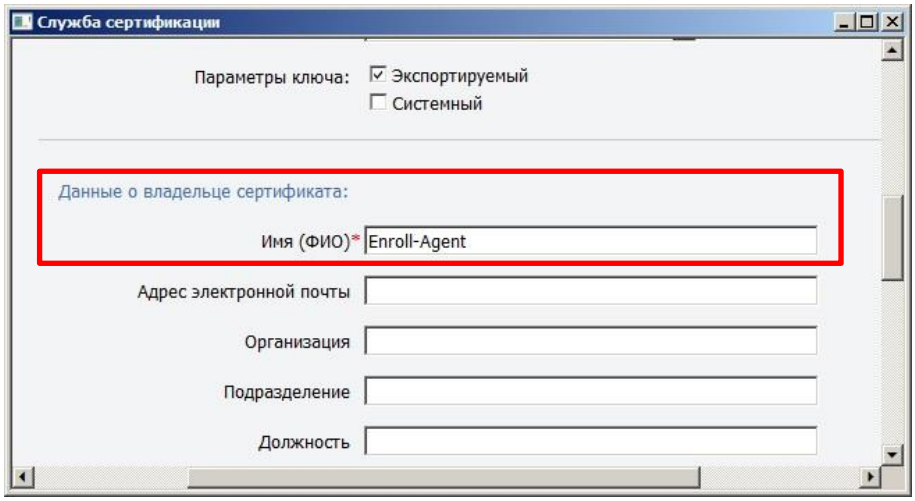


Рис. 538 – Окно Служба сертификации – Данные о владельце сертификата

– в появившемся окне **ViPNet CSP – инициализация контейнера ключей** в поле **Имя контейнера** введите имя (либо оставьте поле, как есть) и нажмите **OK**;

– в появившемся окне **ViPNet CSP – пароль контейнера ключей** введите пароль и его подтверждение, выберите опцию **Сохранить пароль** (см. рис. 539), после чего нажмите кнопку **OK**;

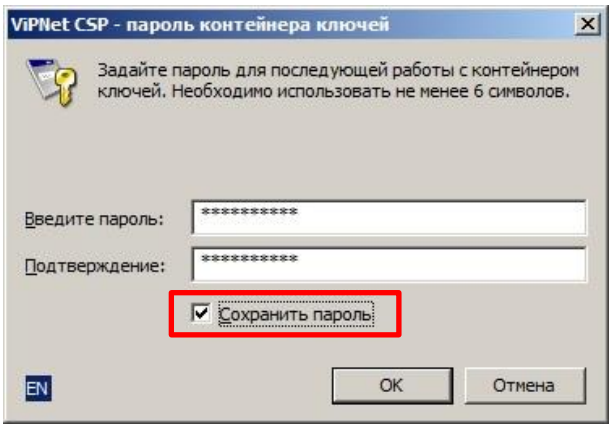


Рис. 539 – Окно ViPNet CSP – пароль контейнера ключей

– в появившемся окне **Электронная рулетка** (см. рис. 540) выполните действия, описанные в окне;

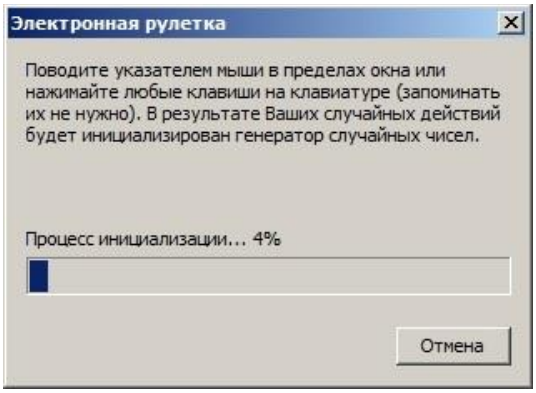


Рис. 540 – Окно Электронная рулетка

– в появившемся сообщении об успешном создании запроса нажмите **OK**.

5. Запустите утилиту **ViPNet Удостоверяющий и ключевой центр**. Выполните следующие действия:

а) Загрузите сформированный запрос на сертификат для установки TLS соединения и выпустите сертификат, для чего выполните следующее:

– перейдите на вкладку **Удостоверяющий центр** и в разделе **Изданные сертификаты** выберите опцию **Внешние пользователи**, затем нажмите на кнопку **Загрузить и обработать запрос...** (см. рис. 541);

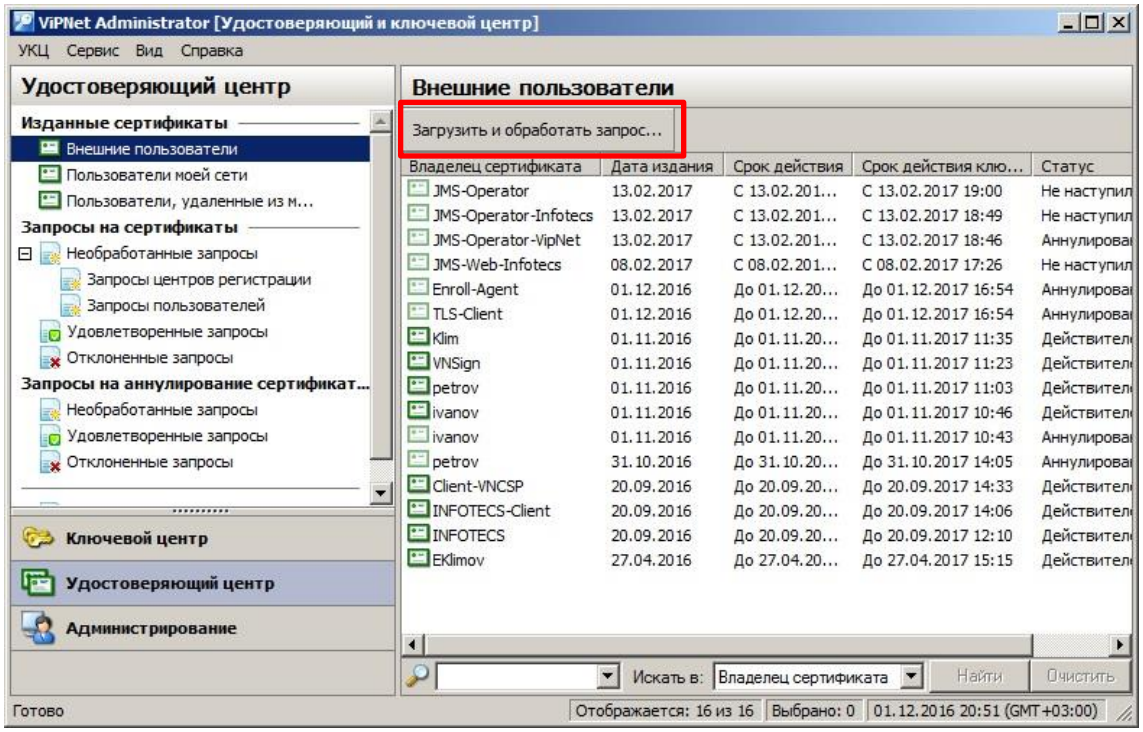


*Рис. 541 – Окно **ViPNet Удостоверяющий и ключевой центр** – Загрузить и обработать запрос*

– в появившемся окне **Open** выберите файл запроса на сертификат и нажмите **Открыть**;

– в появившемся окне **Издание сертификатов пользователей** (см. рис. 542) выделите файл запроса и нажмите **Издать сертификат...**;

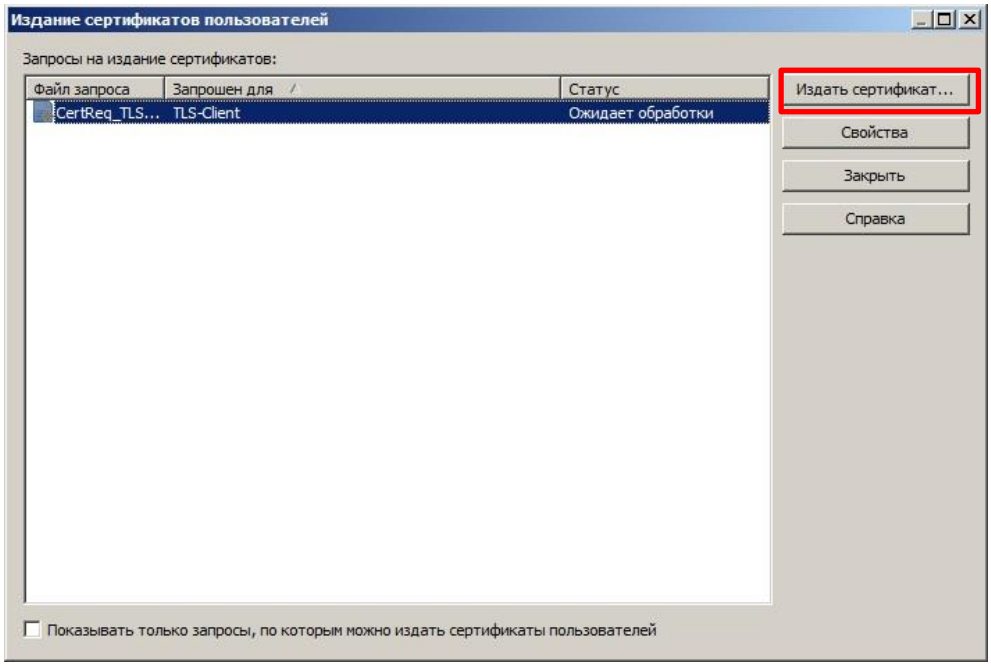


Рис. 542 – Окно Издание сертификатов пользователей

– в появившемся окне **Редактирование полей сертификата** нажмите **Далее**;

– в появившемся окне нажмите **Далее**;

– в появившемся окне нажмите **Далее**;

– в появившемся окне нажмите **Далее**;

– в появившемся окне **Источник параметров сертификата** выберите опцию **Из шаблона сертификата** (см. рис. 543) и из раскрывающегося списка выберите имя созданного ранее шаблона сертификата (Проверка подлинности клиента), после чего нажмите **Далее**;

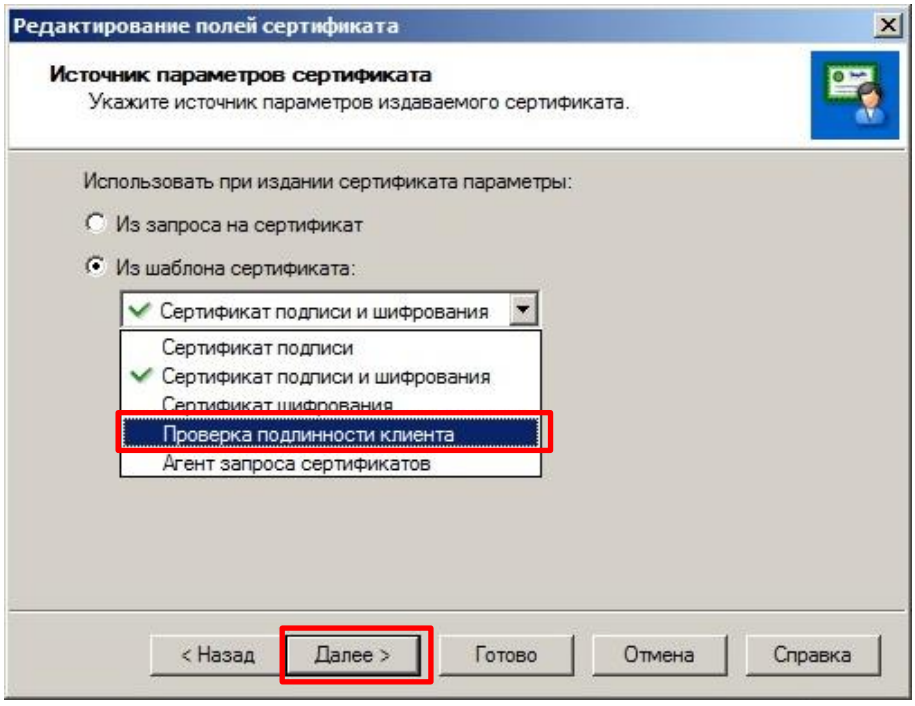


Рис. 543 – Окно Источник параметров сертификата

– в появившемся окне нажмите **Далее**;

– в появившемся окне нажмите **Далее**;

– в появившемся окне нажмите **Готово**;

– в появившемся сообщении об успешном издании сертификата нажмите **ОК**;

– в окне **Издание сертификатов пользователей** нажмите **Закрыть**. Изданный сертификат отобразится в списке сертификатов;

– выделите изданный сертификат правой кнопкой мыши и в появившемся контекстном меню выберите опцию **Экспорт** (см. рис. 544);

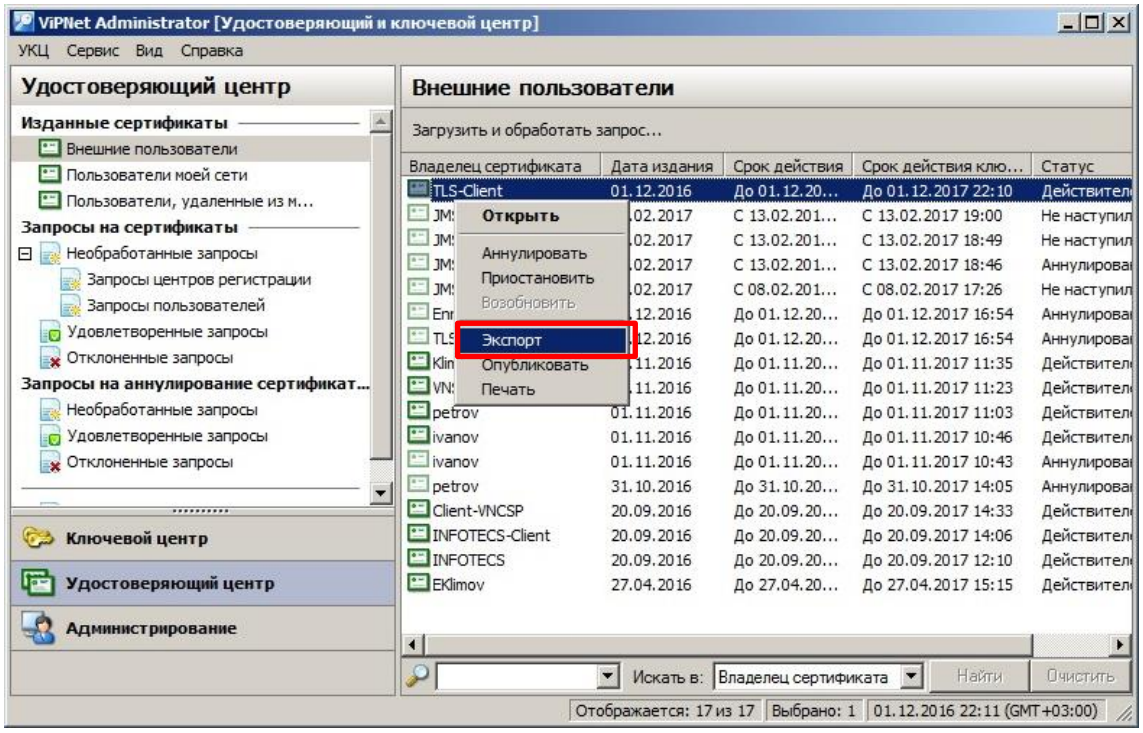


Рис. 544 – Окно Экспорт сертификата

– в появившемся окне Мастера экспорта сертификатов нажмите **Next**;

– в появившемся окне нажмите **Next**;

– в появившемся окне нажмите **Finish**;

– в появившемся сообщении об успешном экспорте сертификата нажмите **ОК**.

б) Загрузите сформированный запрос на сертификат для подписи запросов на сертификаты и выпустите сертификат, для чего выполните следующее:

– перейдите на вкладку **Удостоверяющий центр** и в разделе **Изданные сертификаты** выберите опцию **Внешние пользователи**, затем нажмите на кнопку **Загрузить и обработать запрос...** (см. рис. 541);

– в появившемся окне **Open** выберите файл запроса на сертификат и нажмите **Открыть**;

– в появившемся окне **Издание сертификатов пользователей** (см. рис. 545) выделите файл запроса и нажмите **Издать сертификат...**;

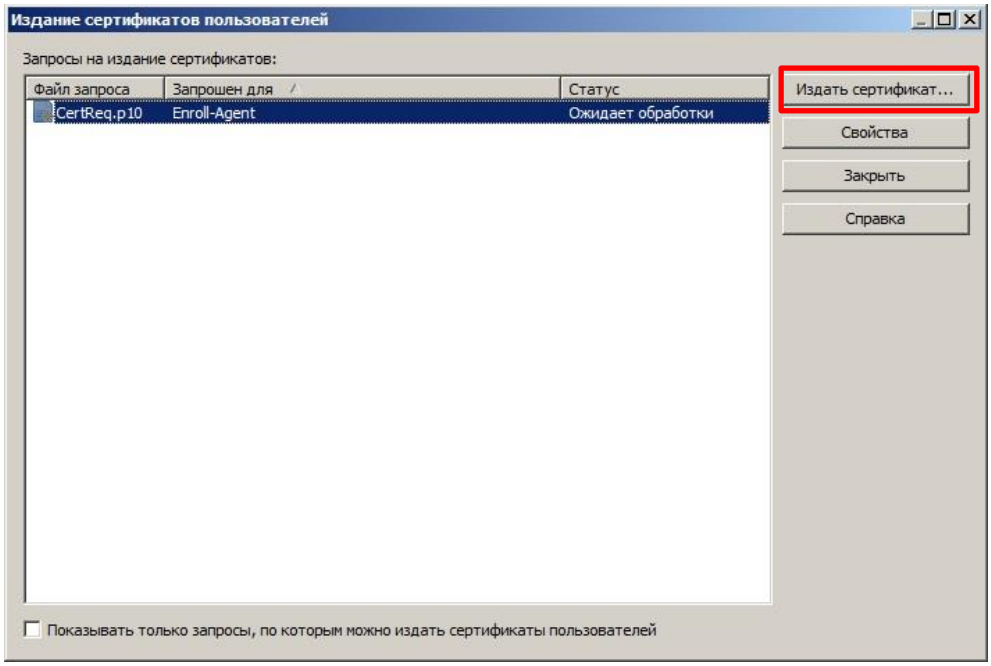


Рис. 545 – Окно Издание сертификатов пользователей

– в появившемся окне **Редактирование полей сертификата** нажмите **Далее**;

– в появившемся окне нажмите **Далее**;

– в появившемся окне нажмите **Далее**;

– в появившемся окне **Источник параметров сертификата** выберите опцию **Из шаблона сертификата** (см. рис. 546) и из раскрывающегося списка выберите имя созданного ранее шаблона сертификата (Агент запроса сертификатов), после чего нажмите **Далее**;

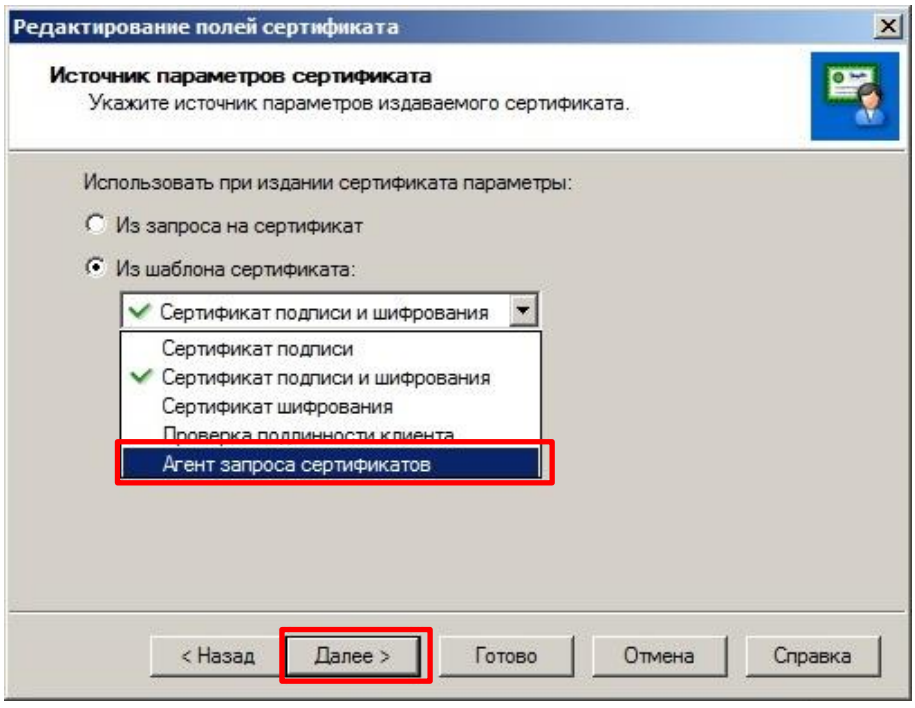


Рис. 546 – Окно Источник параметров сертификата

– в появившемся окне нажмите **Далее**;

– в появившемся окне нажмите **Далее**;

– в появившемся окне нажмите **Готово**;

– в появившемся сообщении об успешном издании сертификата нажмите **OK**;

– в окне **Издание сертификатов пользователей** нажмите **Закрыть**. Изданный сертификат отобразится в списке сертификатов;

– выделите изданный сертификат правой кнопкой мыши и в появившемся контекстном меню выберите опцию **Экспорт** (см. рис. 544);

– в появившемся окне Мастера экспорта сертификатов нажмите **Next**;

– в появившемся окне нажмите **Next**;

– в появившемся окне нажмите **Finish**;

– в появившемся сообщении об успешном экспорте сертификата нажмите **OK**.

6. Запустите утилиту **ViPNet CA Web Service – Консоль администрирования**. Выполните следующие действия:

– перейдите на вкладку **Клиенты** и нажмите **+Добавить** (см. рис. 547);

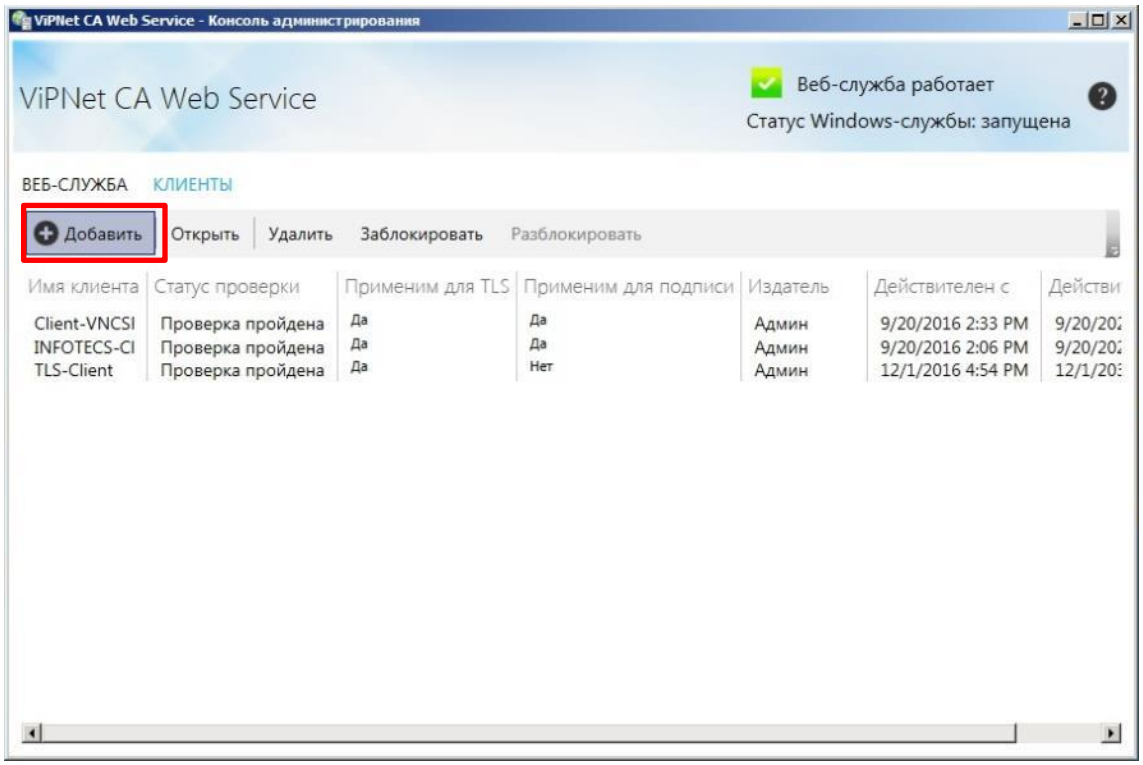


Рис. 547 – Окно ViPNet CA Web Service – Консоль администрирования

– в появившемся окне **Установка сертификата клиента** нажмите на кнопку **...** ;

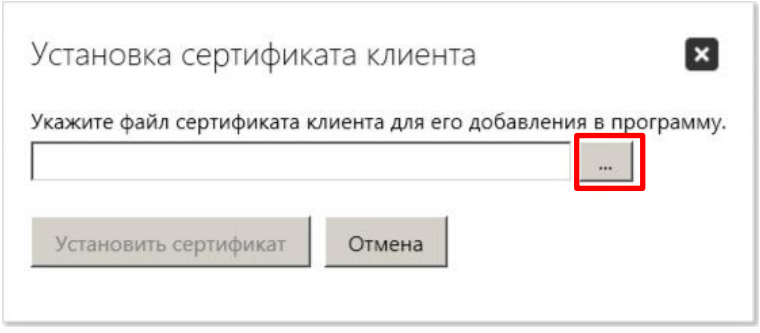


Рис. 548 – Окно ViPNet CA Web Service – Консоль администрирования

– в появившемся окне **Open** выберите изданный сертификат (TLS Client) и нажать **Открыть**;

– в окне **Установка сертификата клиента** нажмите на кнопку **Установить сертификат**

В списке клиентов появится добавленный сертификат.

7. Переведите **ViPNet Удостоверяющий и ключевой центр** в автоматический режим работы, для чего выполните следующее:

– запустите утилиту **ViPNet Удостоверяющий и ключевой центр**;

– в появившемся окне в панели инструментов перейдите: **УКЦ** -> **Перейти в автоматический режим...** (см. рис. 549).

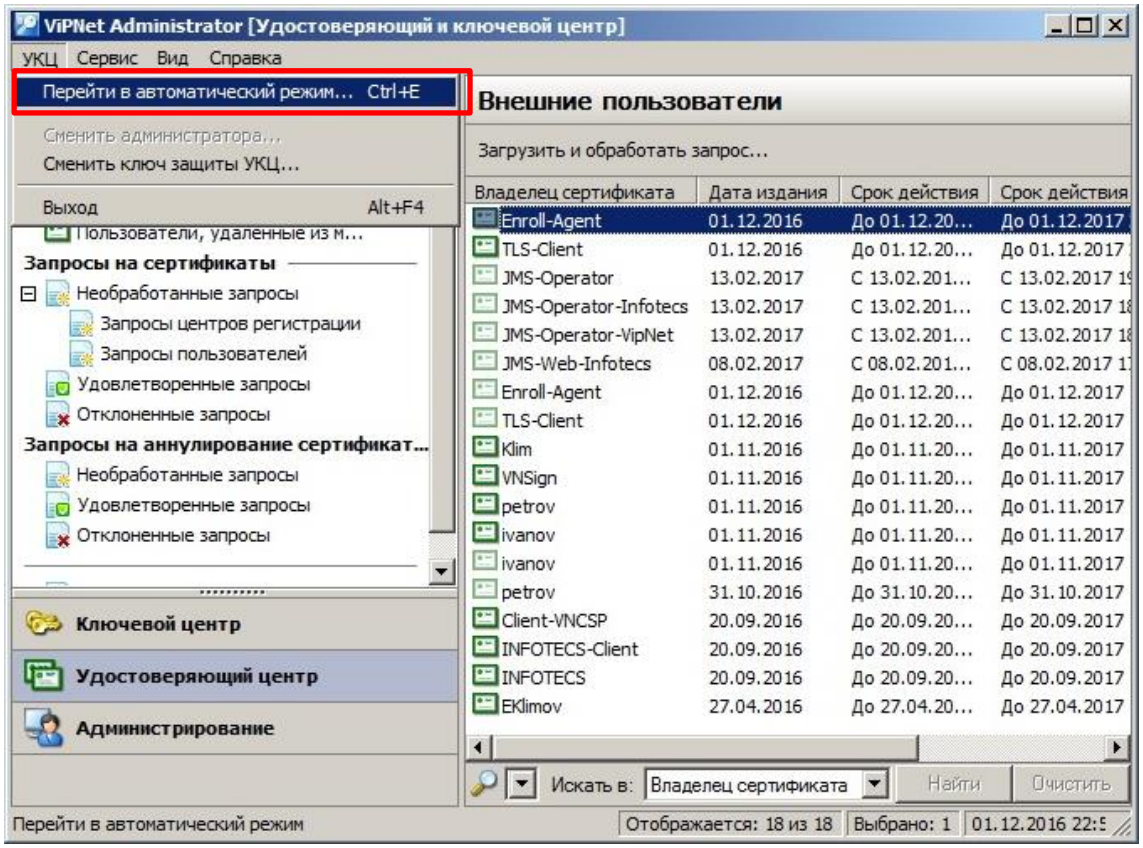


Рис. 549 – Окно ViPNet Удостоверяющий и ключевой центр

– в появившемся окне **Электронная рулетка** (см. рис. 550) выполните действия, описанные в окне.

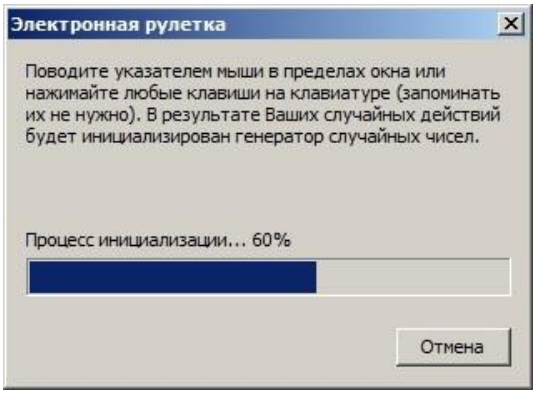


Рис. 550 – Окно Электронная рулетка

После завершения работы Электронной рулетки **ViPNet Удостоверяющий и ключевой центр** будет переведен в автоматический режим работы.

8. Скопируйте корневой сертификат ViPNet УЦ и 2 сертификата (TLS Client и Enrollment Agent) с закрытыми ключами на JMS сервер.

Примечание. По умолчанию закрытые ключи находятся в папке C:\Users\UserName\AppData\Local\Infotecs\Containers

9. Установите скопированный корневой сертификат ViPNet УЦ в доверенные корневые сертификаты локального ПК и проверьте корректность установки, для чего выполните следующие действия:

– откройте файл корневого сертификата ViPNet УЦ;

– в появившемся окне (см. рис. 551) нажмите **Установить сертификат...** ;

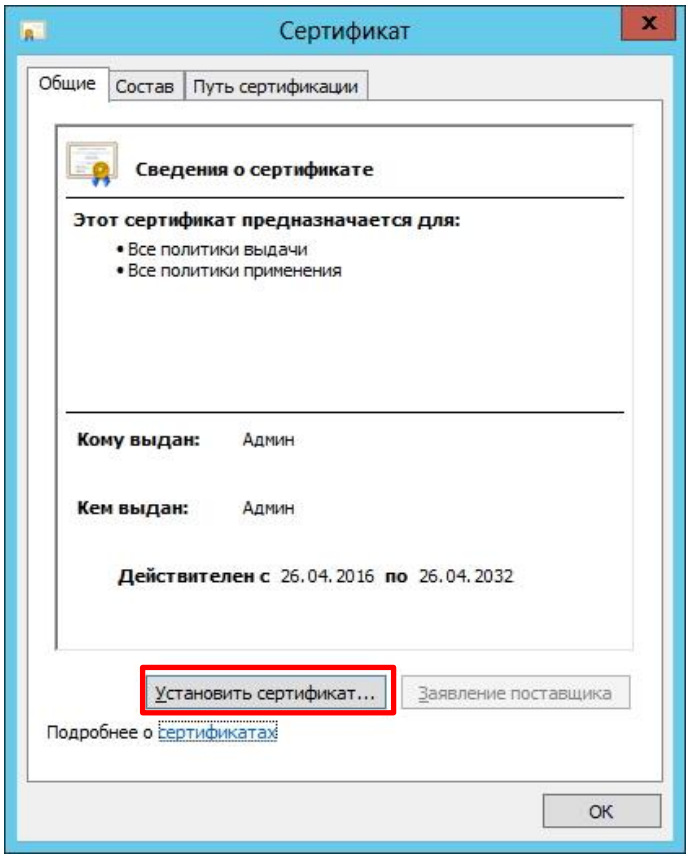


Рис. 551 – Вкладка Общие в окне корневого сертификата

– в появившемся окне Мастера импорта сертификатов (см. рис. 552) выберите опцию **Локальный компьютер** и нажмите **Далее**;

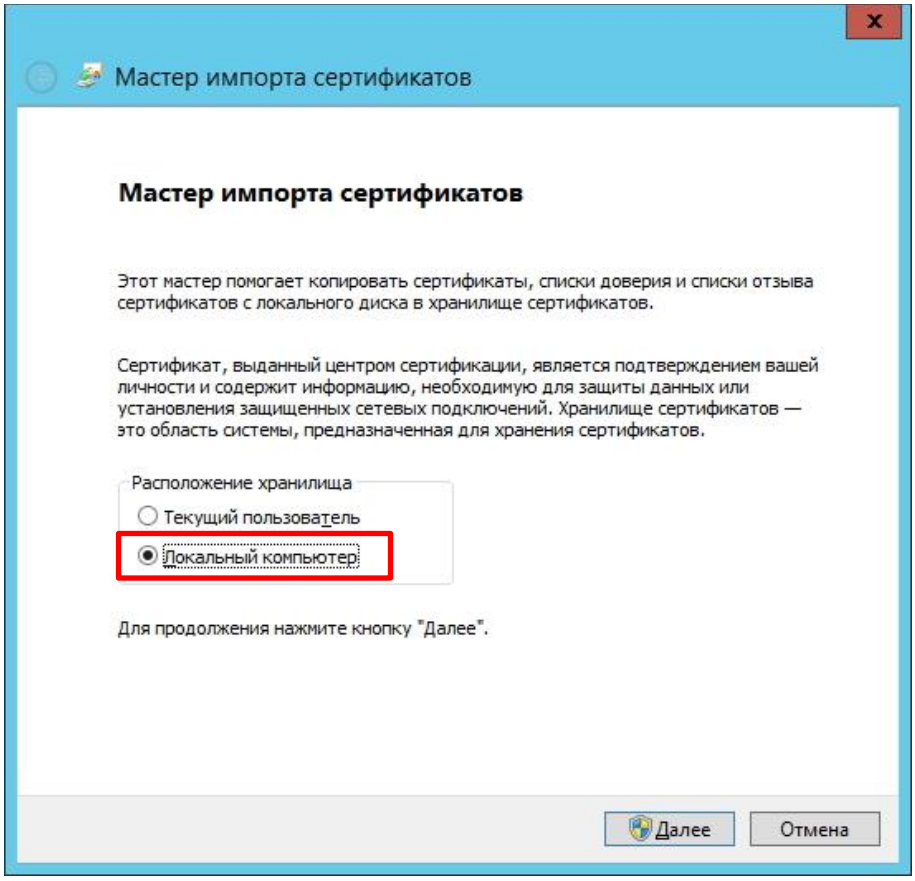


Рис. 552 – Окно Мастера импорта сертификатов

– в появившемся окне (см. рис. 553) выберите опцию **Поместить все сертификаты в следующее хранилище** и нажмите кнопку **Обзор...** ;

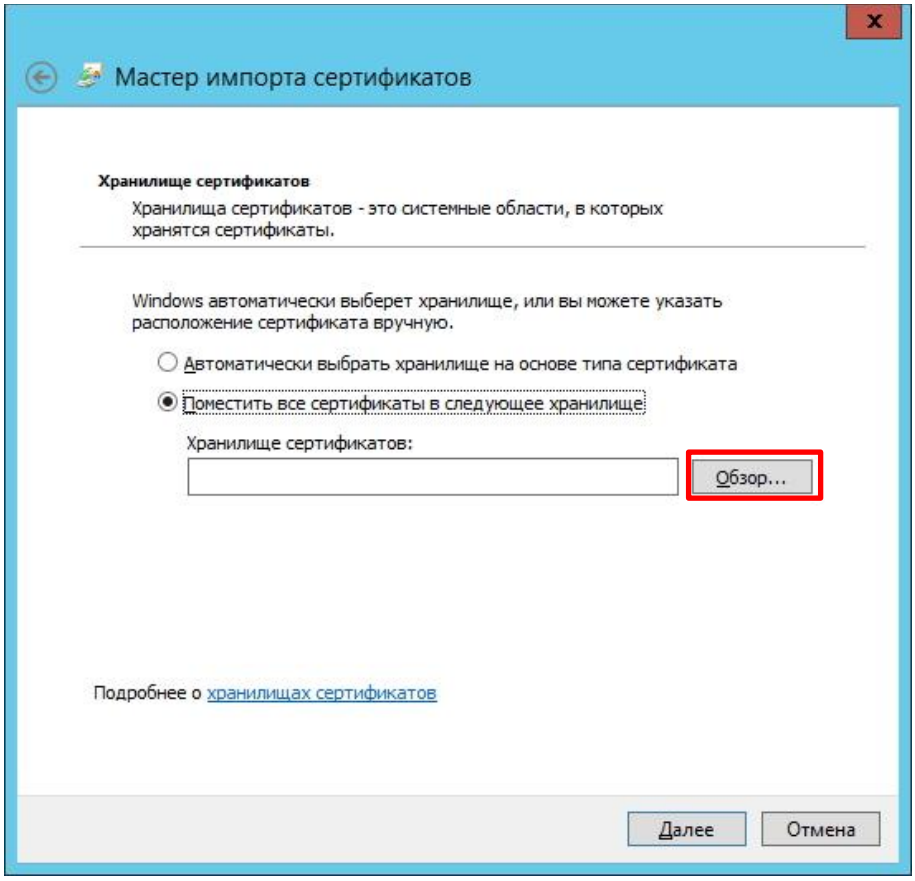


Рис. 553 – Окно Мастера импорта сертификатов. Выбор хранилища сертификатов

– в появившемся окне (см. рис. 554) выберите папку **Доверенные корневые центры сертификации** и нажмите **ОК**;

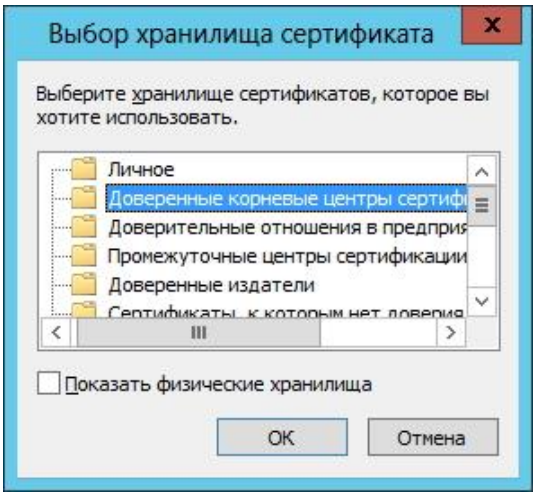


Рис. 554 – Окно выбора хранилища сертификата

– в окне Мастера импорта сертификатов (см. рис. 555) нажмите **Далее**;

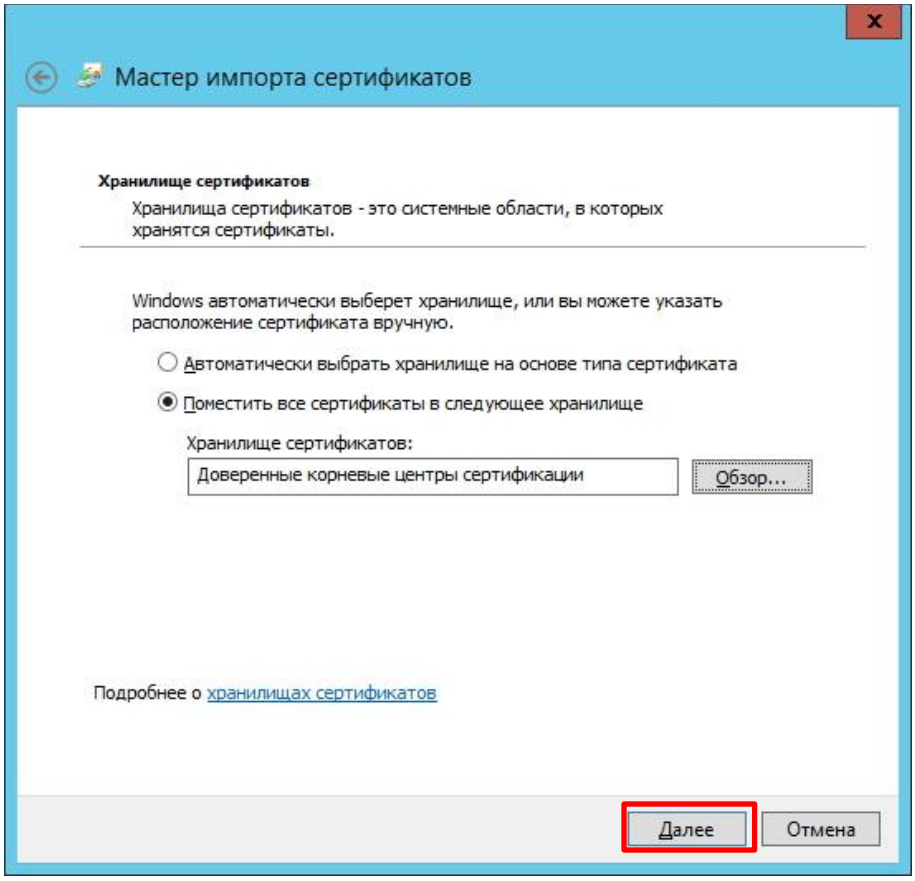


Рис. 555 – Окно Мастера импорта сертификатов

– в появившемся окне (см. рис. 556) нажмите **Готово**;

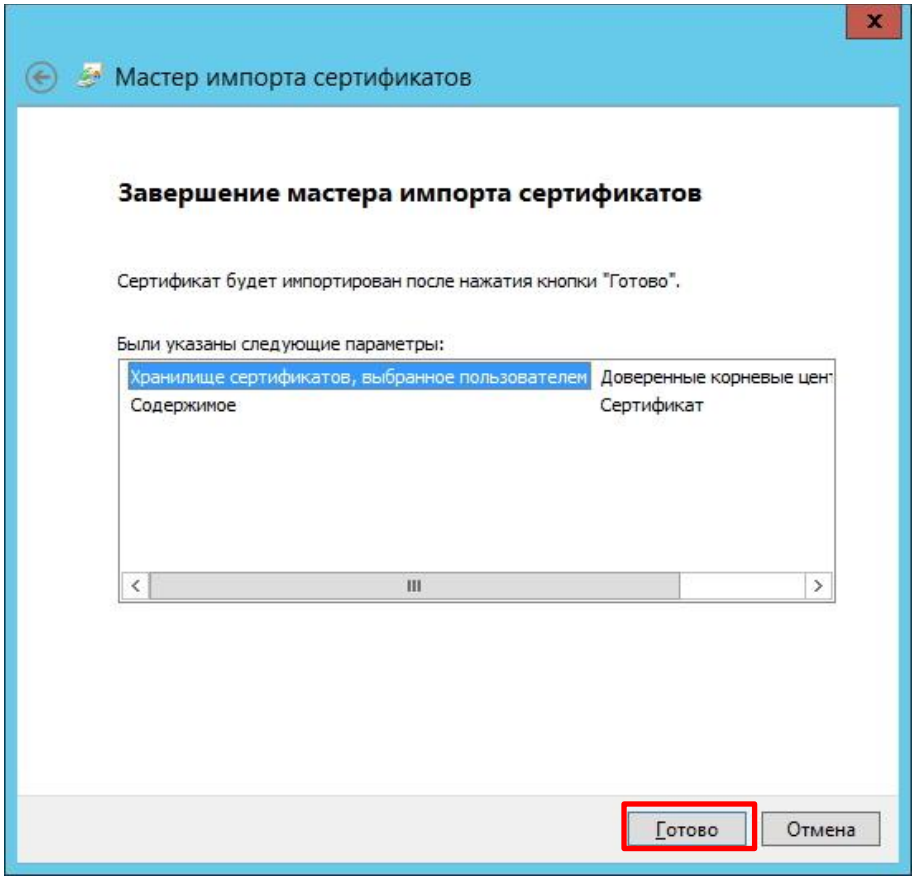


Рис. 556 – Окно Мастера импорта сертификатов

– в появившемся сообщении об успешном импорте сертификата нажмите **ОК**;

– откройте файл сертификата и убедитесь в отсутствии сообщений об ошибках и некорректной работе.

10. Установите закрытые ключи (TLS Client и Enrollment Agent) в хранилище, для чего выполните следующие действия:

Примечание. Если служба JMS запущена от имени пользователя, то устанавливать закрытые ключи следует в хранилище Пользователя, если служба JMS запущена от имени компьютера – устанавливать закрытые ключи следует в хранилище ПК.

– в случае, если служба JMS запущена от имени пользователя – скопируйте закрытые ключи в папку C:\Users\UserName\AppData\Local\Infotecs\Containers;

– в случае, если служба JMS запущена от имени компьютера – скопируйте закрытые ключи в папку C:\ProgramData\InfoTeCS\Containers.

11. Установите сертификаты (TLS Client и Enrollment Agent) с помощью утилиты ViPNet CSP и привяжите их к контейнерам с закрытыми ключами, для чего выполните следующие действия:

– запустите утилиту ViPNet CSP;

Примечание. В данном примере для установки сертификата с закрытым ключом используется утилита ViPNet CSP, однако для этой же цели может быть использована и другая утилита, например, КриптоПро CSP.

– в появившемся окне (см. рис. 557) в разделе **Контейнеры ключей** выберите опцию **Ключи пользователя** и выделите устанавливаемый сертификат (TLS Client), после чего нажмите **Установить сертификат**;

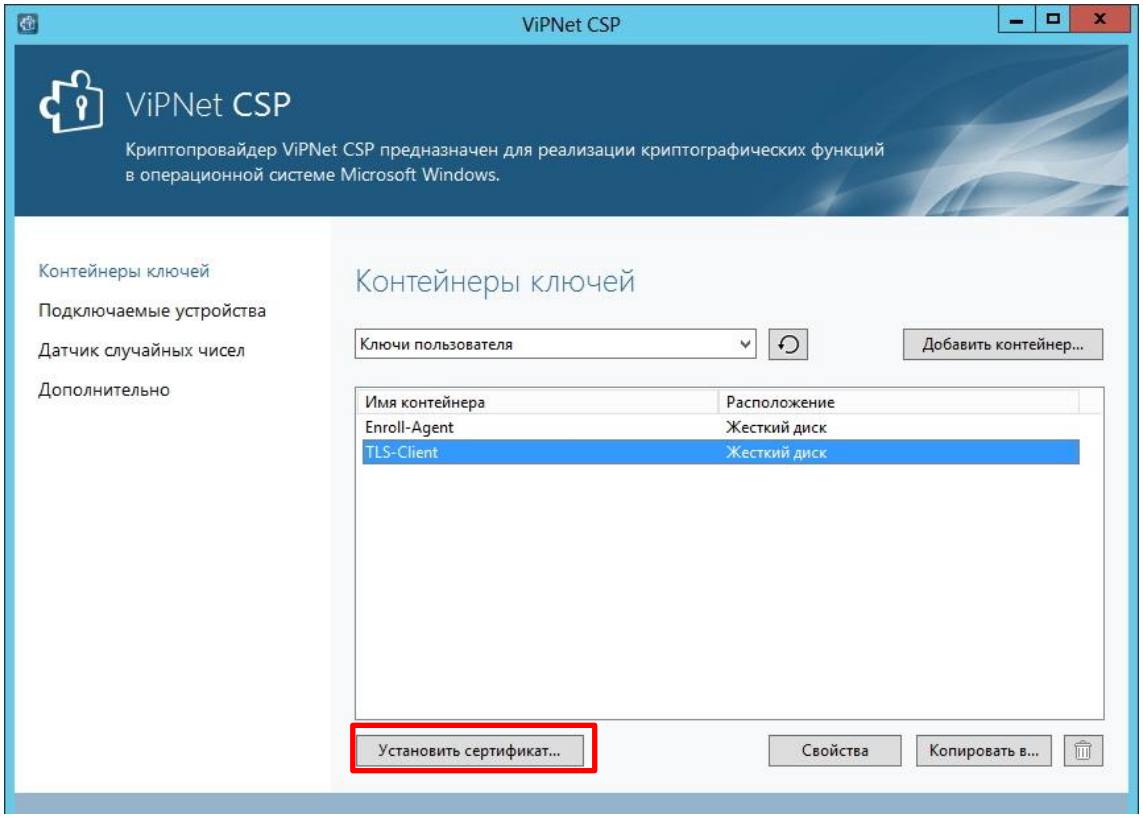


Рис. 557 – Окно ViPNet CSP. Установка сертификата TLS Client

– в появившемся окне укажите на скопированный файл сертификата и нажмите **Открыть**;

– в появившемся окне Мастера установки сертификатов нажмите **Далее**;

– в появившемся окне взавистмости от того, куда необходмио установить сертификат выберите соответствующую опцию и нажмите **Далее**;

– в появившемся окне (см. рис. 558) из раскрывающегося списка выберите опцию **Найти контейнер с закрытым ключом** и нажмите **Далее**;

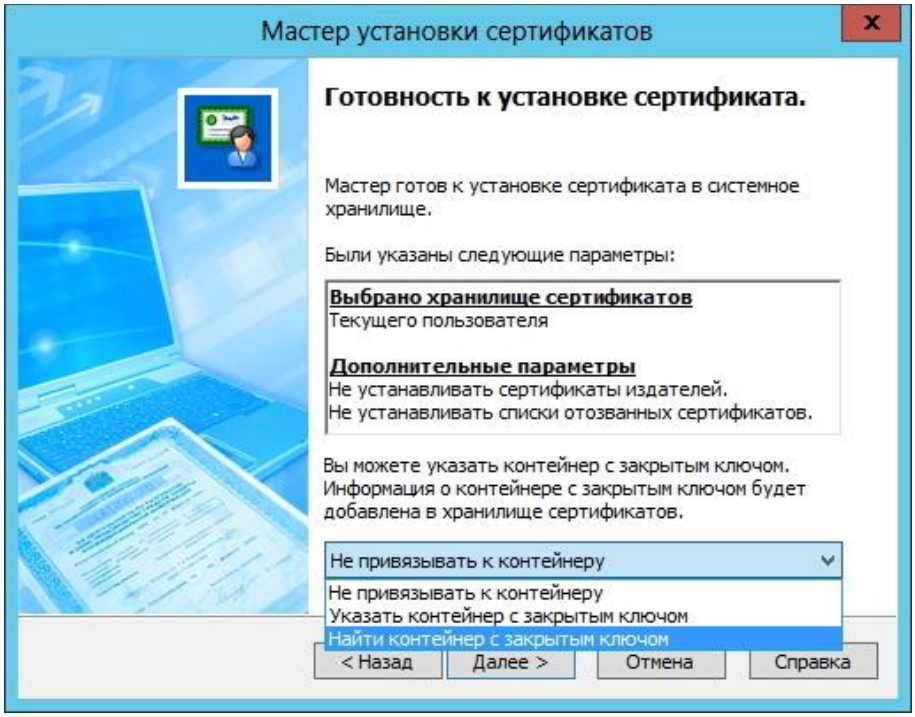


Рис. 558 – Окно Мастера установки сертификатов

– в появившемся окне нажмите **ОК**;

– в появившемся окне (см. рис. 559) подтвердите сохранение сертификата в контейнере с закрытым ключом, нажав **Да**;

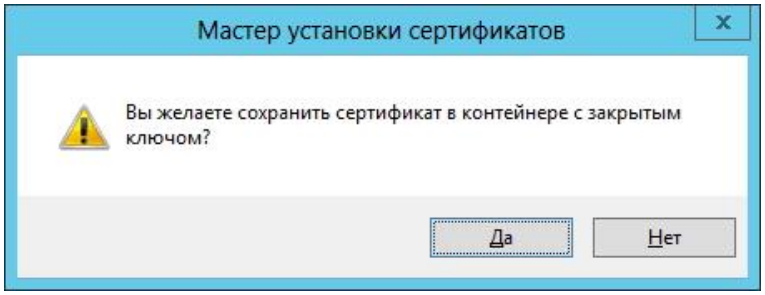


Рис. 559 – Окно подтверждения сохранения сертификата

– в появившемся окне (см. рис. 560) введите пароль контейнера ключей, выберите опцию **Сохранить пароль** и нажмите **ОК**;

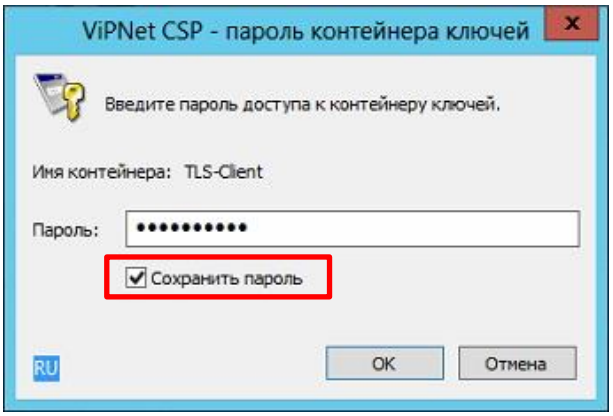


Рис. 560 – Окно ввода пароля контейнера ключей

ВНИМАНИЕ! Обязательно выберите опцию **Сохранить пароль** для сохранения пароля от контейнера.

– в окне мастера сертификатов нажмите **Готово**;

– выполните вышеперечисленные действия п.11 для второго сертификата (Enrollment Agent).

18.2 Настройка профиля для выпуска сертификатов в ViPNet УЦ

Чтобы настроить профиль выпуска сертификатов средствами ViPNet УЦ, выполните следующие действия:

1. В консоли управления JMS перейдите в раздел **Профили -> Профили**.
2. В центральной части окна выберите пункт **Выпуск сертификатов – ViPNet УЦ** и в верхней панели нажмите **Создать**.
   Отобразится следующее окно.

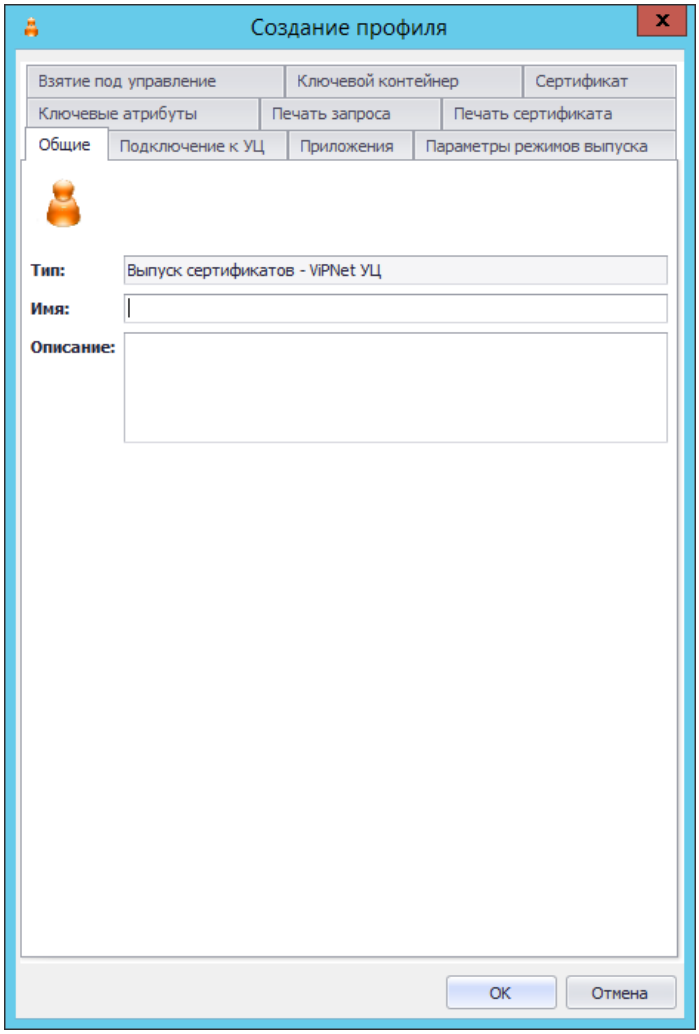


Рис. 561 – Вкладке Общие в окне создания профиля ViPNet УЦ

3. В полях **Имя** и **Описание** соответственно задайте название и описание создаваемого профиля, после чего перейдите на вкладку **Подключение к УЦ**.

Окно примет следующий вид (Рис. 562).

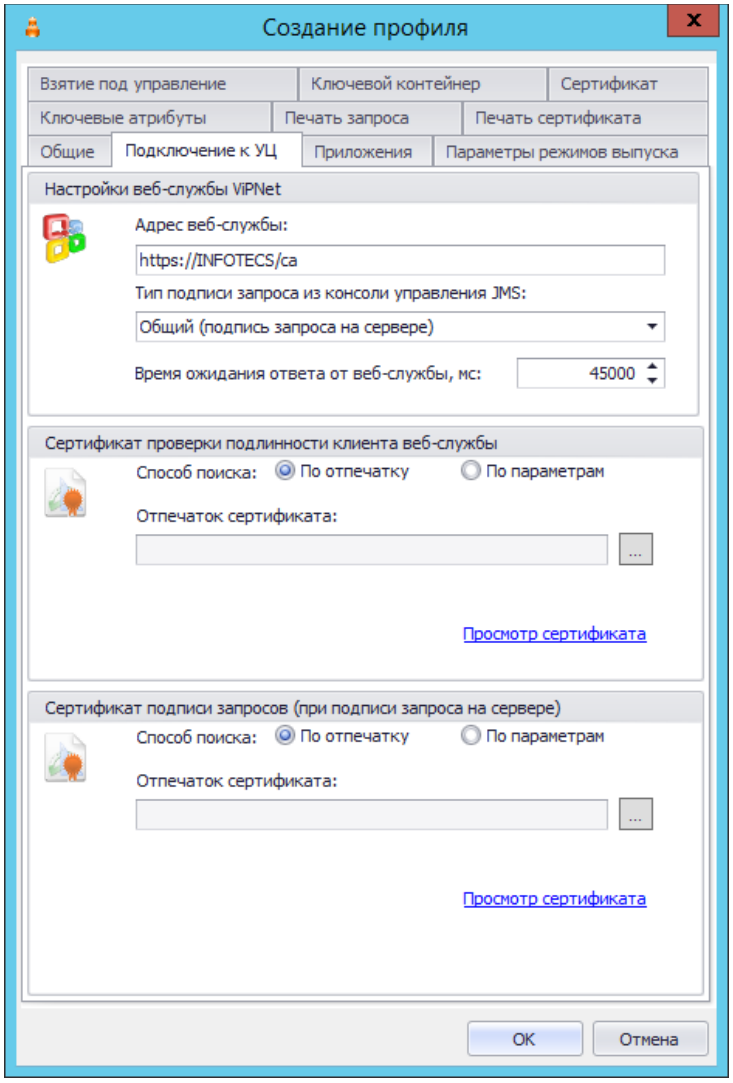


Рис. 562 – Вкладка Подключение к УЦ в окне создания профиля ViPNet УЦ

4. В поле **Адрес веб-службы** введите адрес подключения к ViPNet УЦ в следующем формате: **https:\\<Имя хоста ViPNet УЦ>\ca**.
5. Установите **Сертификат проверки подлинности клиента веб-службы** (TLS Client), для чего выполните следующее:

– нажмите на кнопку [...] ;

– появившемся окне (см. Рис. 563) выделите требуемый сертификат и нажмите **OK**.

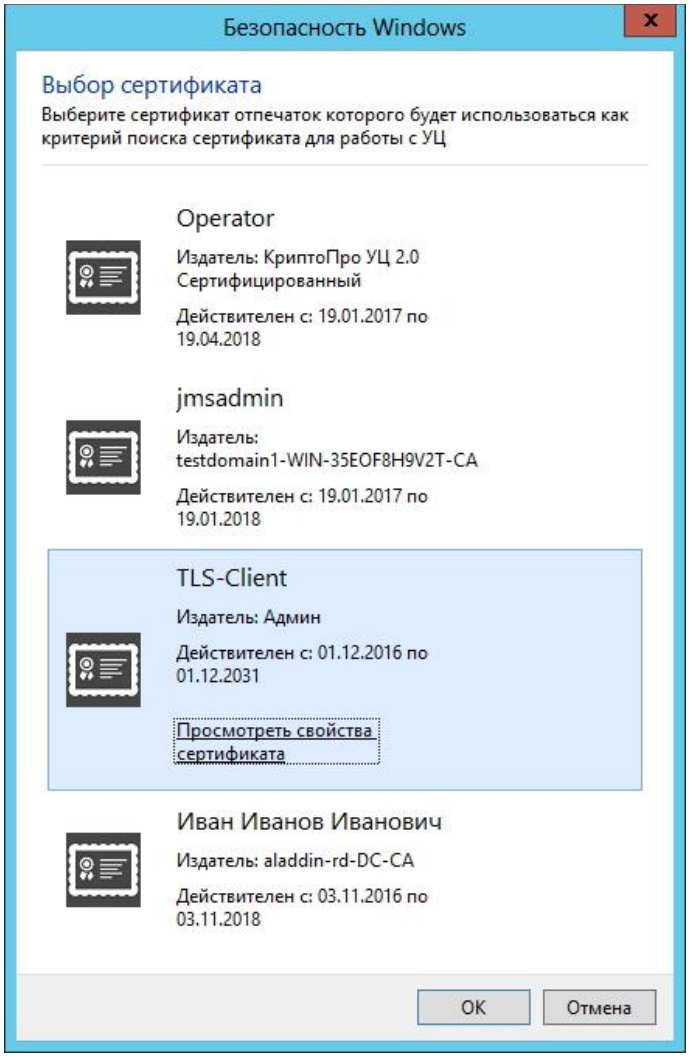


Рис. 563 – Окно выбора сертификата

6. В поле **Сертификат подписи запросов (при подписи запроса на сервере)** установите сертификат подписи запросов (Enrollment Agent), для чего выполните следующее:

– нажмите на кнопку [...] ;

– появившемся окне (см. Рис. 564) выделите требуемый сертификат и нажмите **OK**.

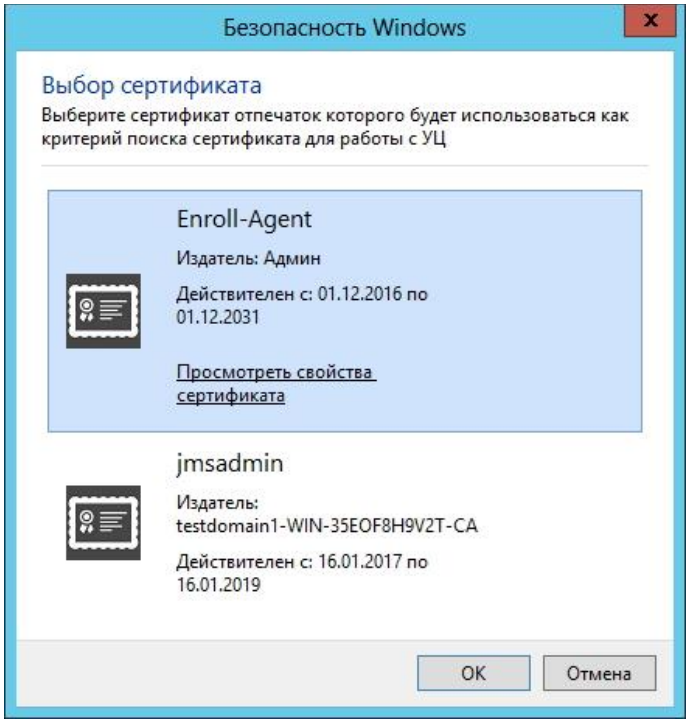


Рис. 564 – Окно выбора сертификата

7. Перейдите на вкладку **Приложения** (см. Рис. 565) и укажите требуемые приложения, к которым будет применен данный профиль.

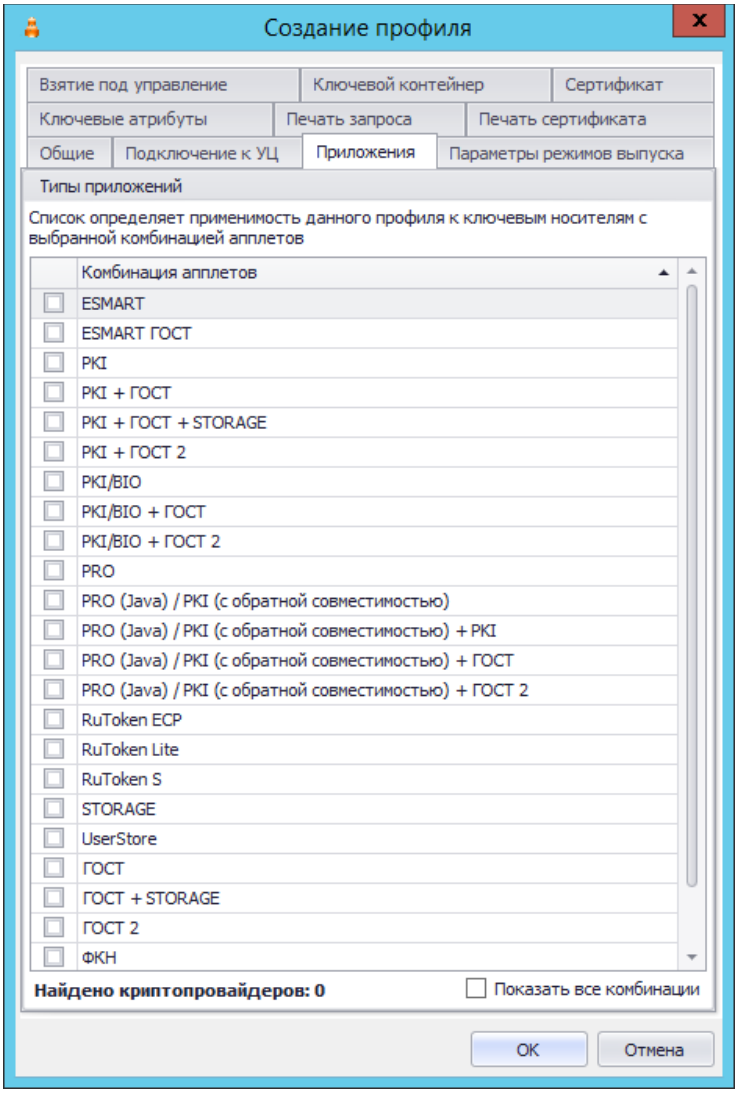


*Рис. 565 – Вкладка **Приложения** в окне создания профиля*

8. Перейдите на вкладку **Параметры режимов выпуска** (рис. 566) и укажите необходимые параметры выпуска, руководствуясь Табл. 33, с. 215.

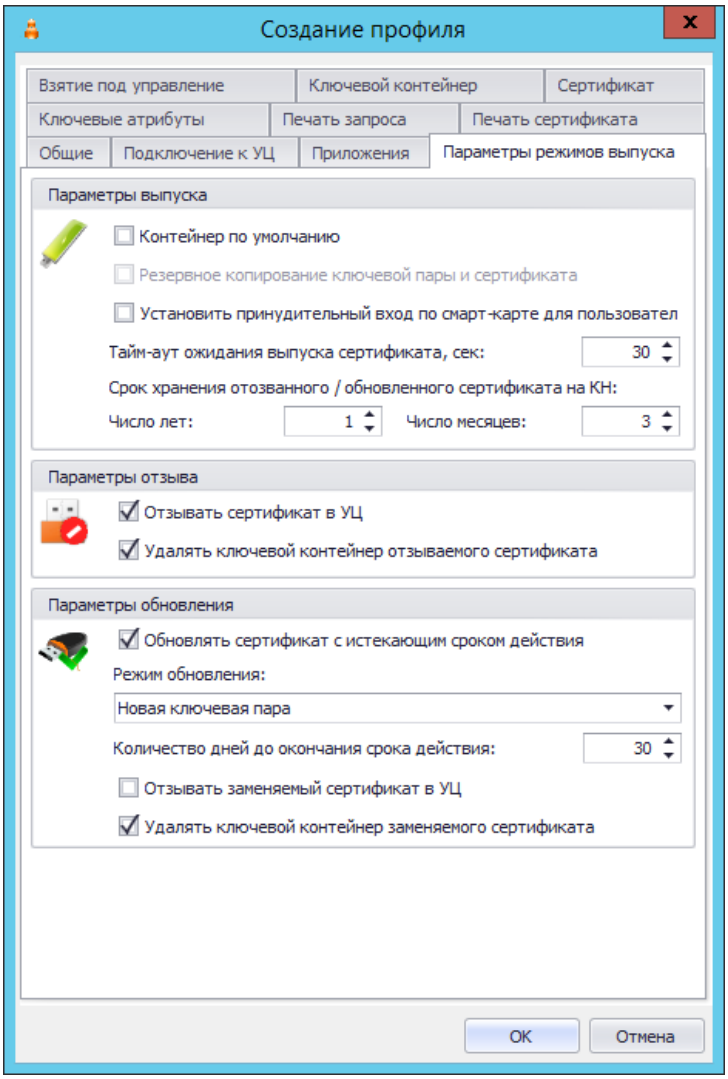


*Рис. 566 – Вкладка **Параметры режимов выпуска** в окне создания профиля*

9. Перейдите на вкладку **Ключевой контейнер** и выполните настройки аналогично настройкам профиля выпуска сертификатов MSCA (см. Табл. 34, с. 218).
10. Перейдите на вкладку **Сертификат** и выполните настройки аналогично настройкам одноименной вкладки в профиле выпуска сертификатов КриптоПро УЦ 1.5 (см раздел «Настройка профиля для выпуска сертификатов в КриптоПро УЦ 1.5», с. 620).
11. Перейдите на вкладку **Ключевые атрибуты** и выполните настройки аналогично настройкам одноименной вкладки в профиле выпуска сертификатов MSCA (см. «Настройки на вкладке Ключевые атрибуты», с. 222).
12. При необходимости, выполните настройку печати документов (вкладки **Печать запроса** на сертификат и **Печать сертификата**) при выпуске электронного ключа (подробнее о настройке шаблона печатной формы см. «Настройка параметров печати при выпуске объектов JMS», с. 304).
13. После завершения всех настроек нажмите **OK** для сохранения профиля.

19. Работа с КриптоПро УЦ 1.5

Чтобы выпускать электронные ключи с сертификатами КриптоПро УЦ средствами JMS, выполните следующие действия.

1. В Active Directory создайте учетную запись, предназначенную для связывания КриптоПро УЦ и JMS. В настоящем документе такая учетная запись будет называться **учетной записью JMS** – для такой учетной записи достаточно быть членом группы **Пользователи домена**.
2. Выполните инструкции, приведенные в подразделе «Подготовительные действия».
3. Настройте соответствующий профиль JMS (см. «Настройка профиля для выпуска сертификатов в КриптоПро УЦ 1.5», с. 620).
4. Настройте остальные необходимые профили, после чего выполните привязку профилей к нужным организационным единицам в Active Directory (см. «Настройка профилей JMS», с. 155) и переходите к выпуску электронных ключей.

19.1 Подготовительные действия

19.1.1 Создание объектного идентификатора

Чтобы создать новый объектный идентификатор, выполните следующие действия.

В разделе, посвященном КриптоПро УЦ 1.5, действия приведены на примере операционной системы Microsoft Windows 2008 R2.

1. На сервере КриптоПро УЦ 1.5 запустите оснастку центра сертификации.
2. В отобразившемся окне щелкните правой кнопкой на центре сертификации и выберите **Свойства**, как показано на изображении ниже.

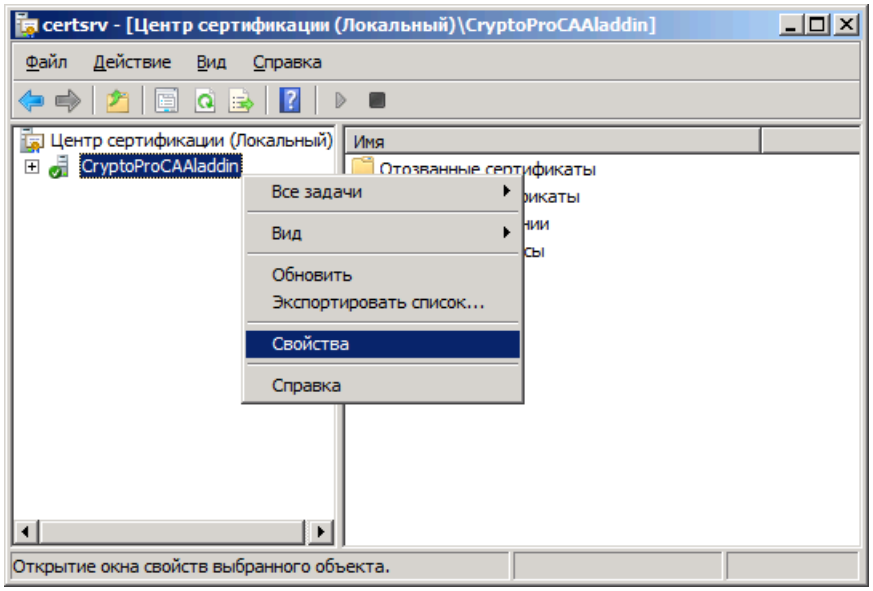


Рис. 567 – Открытие окна свойств центра сертификации

3. В отобразившемся окне выберите вкладку **Модуль политики**.

Окно примет следующий вид.

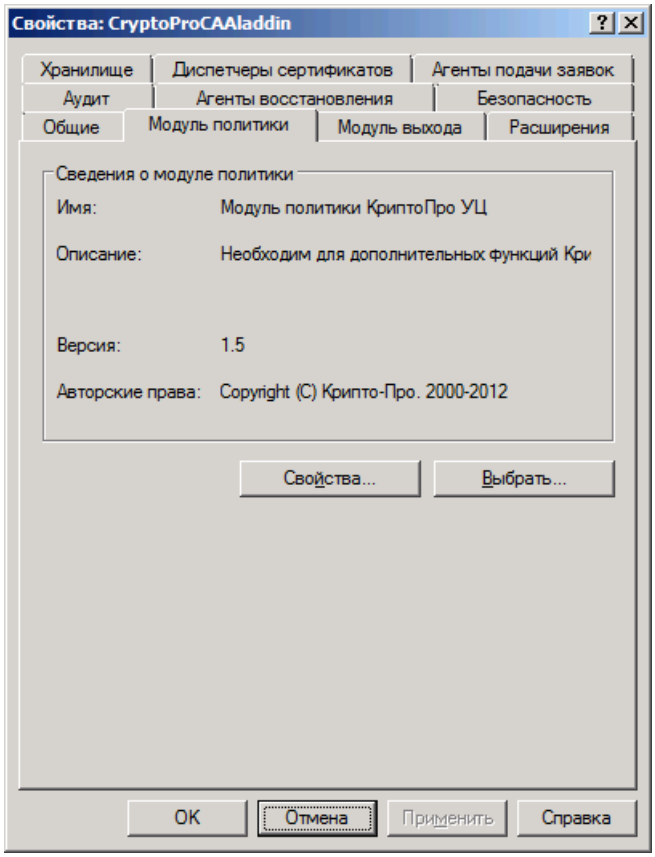


Рис. 568 – Вкладка Модуль политики

4. Нажмите **Свойства** и в отобразившемся окне выберите вкладку **Использование ключа**.

Окно примет следующий вид.

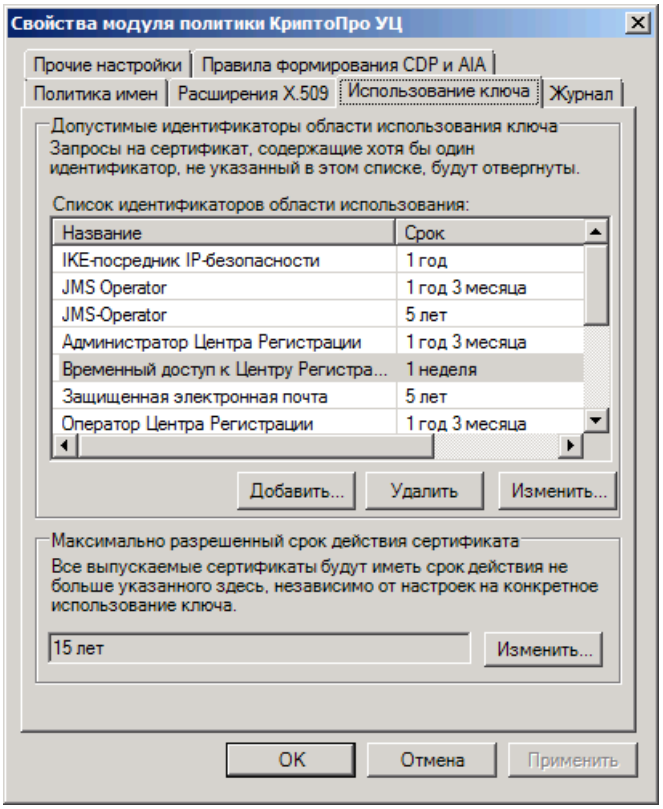


*Рис. 569 – Вкладка **Использование ключа***

5. Нажмите **Добавить**.

Отобразится следующее окно.

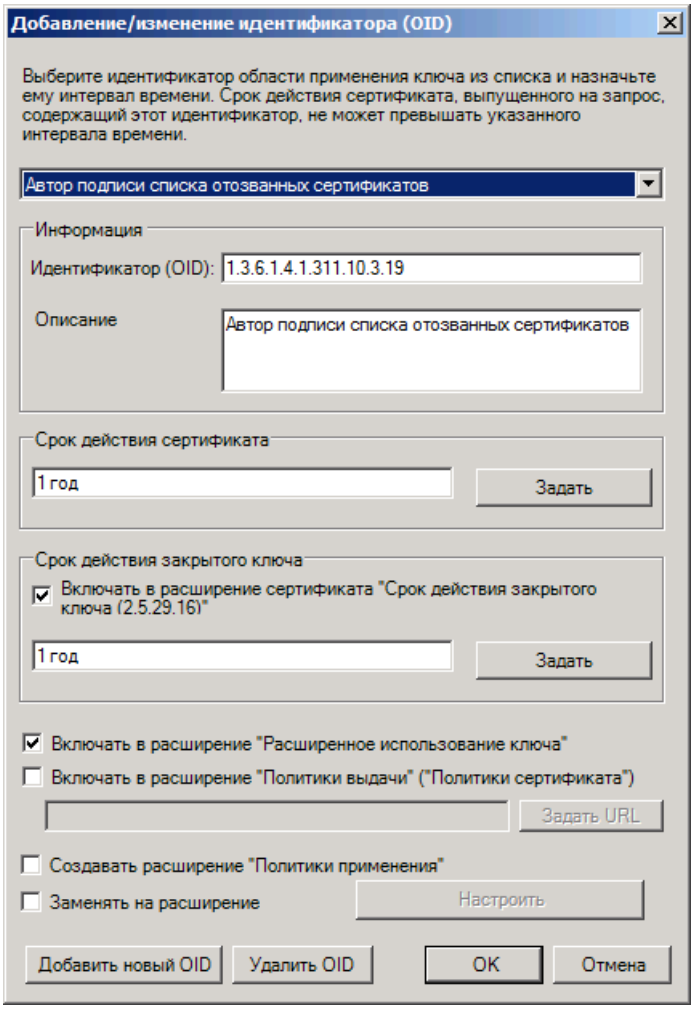


Рис. 570 – Окно добавления объектного идентификатора

6. Нажмите **Добавить новый OID**.
   Отобразится следующее окно.

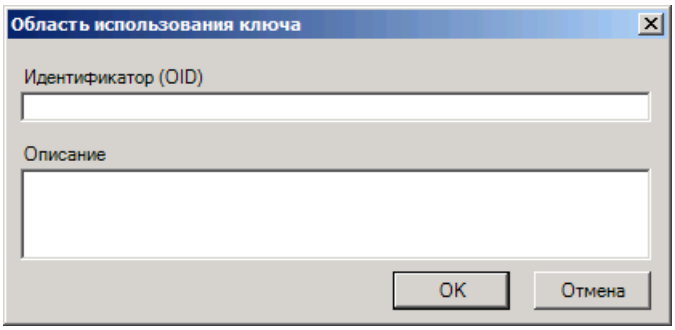


Рис. 571 – Ввод нового объектного идентификатора

7. Введите новый объектный идентификатор (например, **1.2.643.25.100.1.1**) и его описание (например, **JMS-Оператор**), после чего нажмите **OK**.
8. В окне отобразившегося предупреждения нажмите **OK**.
9. Последовательно нажмите **OK**, чтобы закрыть окно добавления объектного идентификатора, окно свойств модуля политики и окно свойств центра сертификации.

Созданный объектный идентификатор появится в следующем разделе реестра:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType
0\CryptDllFindOIDInfo\
```

Значение объектного идентификатора будет состоять из введенного цифрового значения (например, **1.2.643.25.100.1.1**) и суффикса **!7**. То есть, целиком соответствующий раздел реестра будет выглядеть следующим образом: **1.2.643.25.100.1.1!7**.

10. Перезагрузите компьютер, после чего снова запустите оснастку центра сертификации, затем щелкните правой кнопкой на центре сертификации и выберите вкладку **Свойства**.
11. В отобразившемся окне выберите вкладку **Модуль политики** и нажмите **Свойства**.
12. В отобразившемся окне выберите вкладку **Использование ключа** и нажмите **Добавить**.
13. В раскрывающемся списке выберите созданный идентификатор (**JMS-Оператор**).
14. Нажмите **OK**.
    Добавленный объектный идентификатор появится в списке идентификаторов области использования.

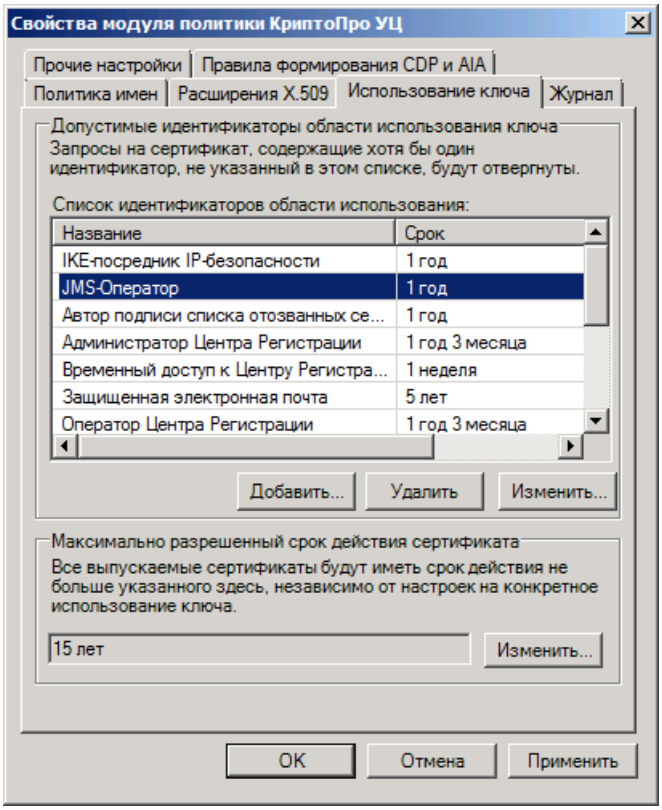


Рис. 572 – Добавленный объектный идентификатор появился в списке идентификаторов области использования.

Если в этом списке отсутствует пункт **Установка отметки времени**, нажмите **Добавить**, в отобразившемся окне из раскрывающегося списка выберите **Установка отметки времени** (идентификатор: 1.3.6.1.5.5.7.3.8) и нажмите **OK**.

15. Нажмите **OK**, чтобы закрыть окно свойств модуля политики КриптоПро УЦ.
16. В окне предупреждения о необходимости перезапуска службы центра сертификации нажмите **OK**.
17. Перезапустите службу центра сертификации.

19.1.2 Создание системной роли для учетной записи JMS

Чтобы создать системную роль, выполните следующие действия.

1. Экспортируйте созданный объектный идентификатор из реестра и установите его на следующие компьютеры:

   - компьютер, на котором установлен Центр регистрации КриптоПро УЦ;
   - компьютер, на котором установлено Автоматизированное рабочее место Центра регистрации КриптоПро УЦ;
   - Сервер JMS.

2. В каждом случае после внесения изменений в реестр перезагрузите компьютер.
3. Запустите приложение Параметры центра регистрации (**Пуск -> Все программы -> КриптоПро -> Параметры центра регистрации**).
   Отобразится следующее окно.

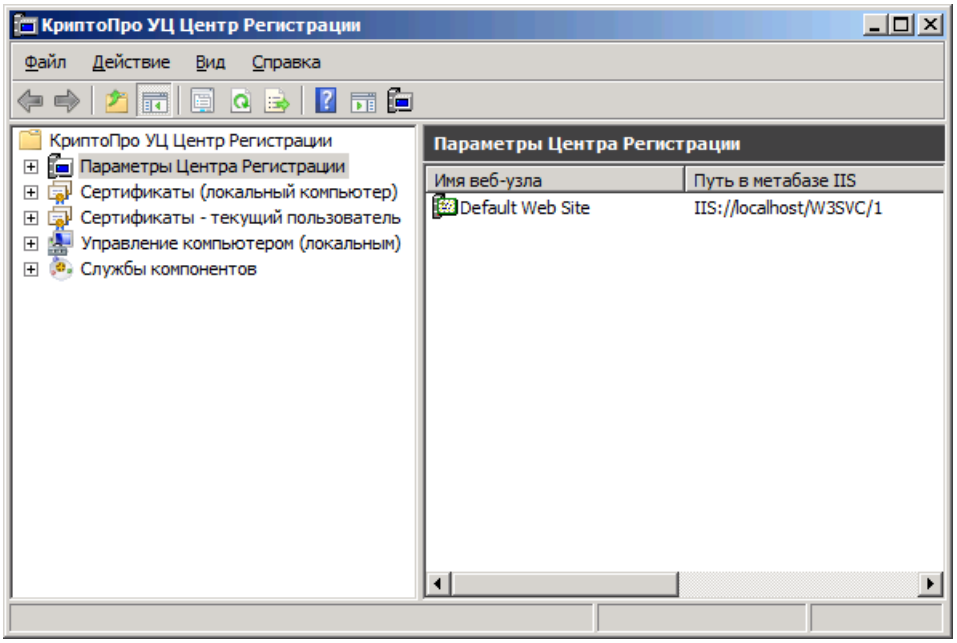


Рис. 573 – Окно приложения Параметры центра регистрации

4. В левой части окна разверните узел **Параметры центра регистрации**, щелкните правой кнопкой на центре регистрации и выберите **Свойства**.
5. В отобразившемся окне выберите вкладку **Политики**.

Окно примет следующий вид.

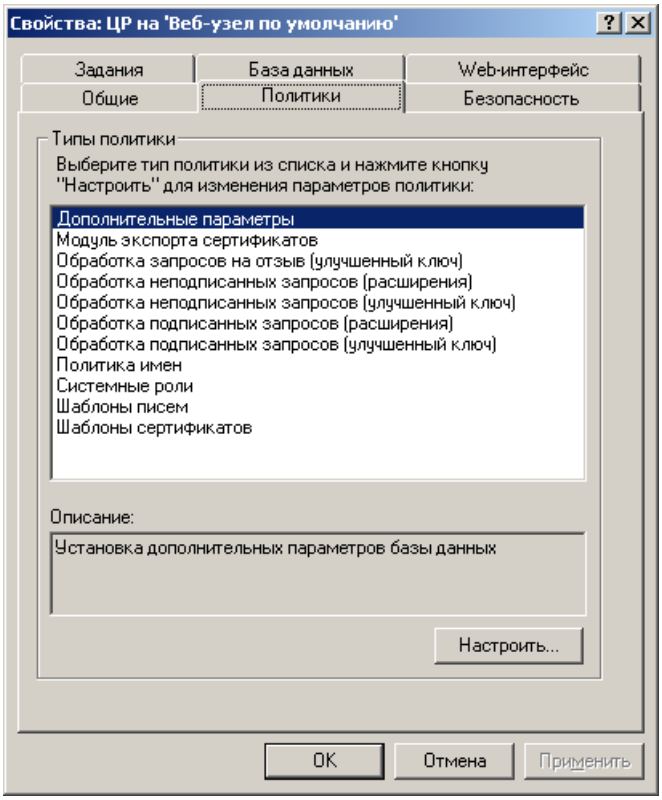


*Рис. 574 – Вкладка **Политики***

6. Выберите пункт **Системные роли** и нажмите **Настроить**.
Отобразится следующее окно.

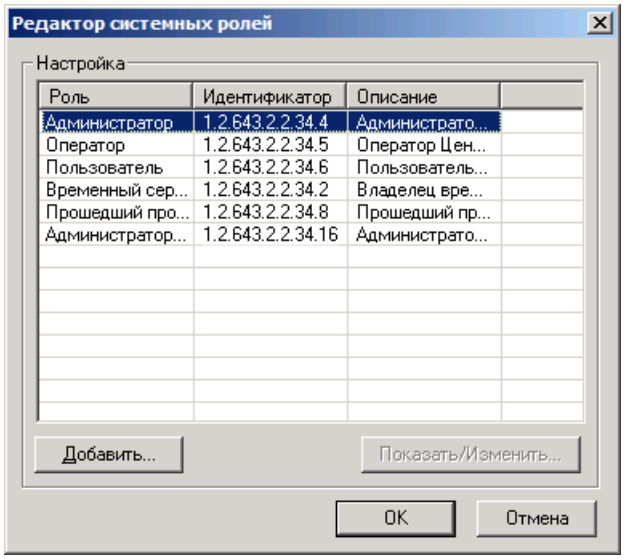


Рис. 575 – Окно Редактор системный ролей

7. Нажмите **Добавить**.

- Если в отобразившемся в списке **Идентификатор** отсутствует созданный объектный идентификатор, нажмите **Добавить** и переходите к следующему шагу процедуры.
- Если созданный идентификатор объекта отображается в списке Идентификатор, переходите к шагу 13 настоящей процедуры.

Отобразится следующее окно.

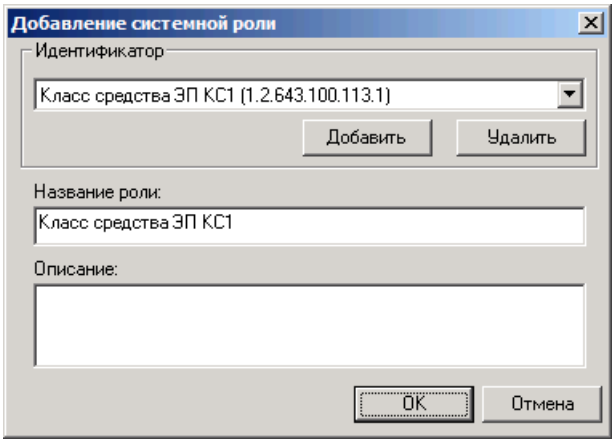


Рис. 576 – Окно добавления системной роли

8. Нажмите **Добавить**.
   Отобразится следующее окно.

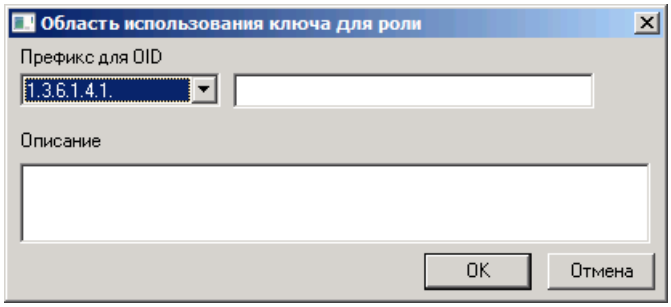


Рис. 577 – Окно Область использования ключа для роли

9. В списке **Префикс для OID** выберете префикс **1.2.643** и в поле справа введите остальную часть объектного идентификатора (в нашем примере - **25.100.1.1**).
10. В поле **Описание** введите **JMS-Оператор**.
11. Нажмите **OK** и перезапустите приложение **Параметры центра регистрации**.
12. После перезапуска приложения **Параметры центра регистрации** повторите пункты 1-7 настоящей процедуры.
13. В отобразившемся окне в списке **Идентификатор** выберите **JMS-Оператор**.
14. При необходимости в поле **Описание** введите описание роли, после чего нажмите **OK**.
15. Последовательно нажмите **OK**, чтобы закрыть окно редактора системных ролей и окно свойств центра регистрации КриптоПро УЦ 1.5.

19.1.3 Разрешения на выпуск и отзыв сертификатов для созданной системной роли

Чтобы установить необходимые разрешения на выпуск/отзыв сертификата для созданной системной роли, выполните следующие действия.

1. Запустите приложение Параметры центра регистрации (**Пуск -> Все программы -> Крипто-Про -> Параметры центра регистрации**).
2. В отобразившемся окне разверните ветвь **Параметры Центра Регистрации**, щелкните правой кнопкой на центре регистрации и выберите **Свойства**.
3. В отобразившемся окне выберите вкладку **Политики**.

4. Настройте политики, руководствуясь табл. 129.

Табл. 129 - Настройки системной роли, необходимые для выпуска и отзыва сертификатов

Тип политики	Системная роль	Использование сертификата
Обработка неподписанных запросов (улучшенный ключ)	Администратор Оператор	JMS-Оператор
	JMS-Оператор	• JMS-Оператор • Все (область применения отсутствует в запросе) • Защищенная электронная подпись • Пользователь Центра Регистрации • Проверка подлинности клиента
Обработка запросов на отзыв (улучшенный ключ)	Администратор Оператор	JMS-Оператор
	JMS-Оператор	• JMS-Оператор • Все (область применения отсутствует в запросе) • Защищенная электронная подпись • Пользователь Центра Регистрации • Проверка подлинности клиента • HTTP • TLS клиент
Обработка неподписанных запросов (расширения)	JMS-Оператор	• Улучшенный ключ • Использование ключа • Возможности SMIME
Обработка подписанных запросов (расширения)		

Продолжение процедуры представлено на примере политики **Обработка неподписанных запросов (улучшенный ключ)** и системной роли JMS-Оператор. После настройки этой политики настройте оставшиеся политики в соответствии с табл. 129.

5. Выберите **Обработка неподписанных запросов (улучшенный ключ)** и нажмите **Настроить**. Отобразится следующее окно.

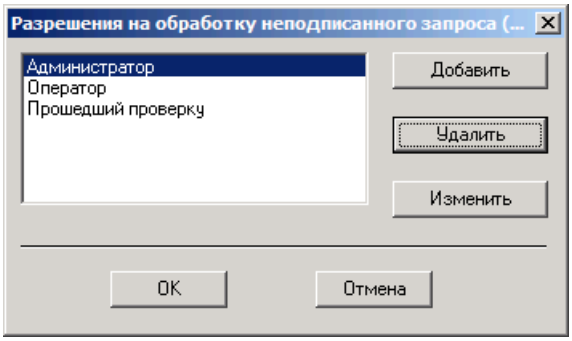


Рис. 578 – Список системных ролей

6. Выберите нужную роль (в нашем примере **JMS-Оператор**) и нажмите **Изменить**.

Чтобы роль **JMS-Оператор** появилась в списке, нажмите **Добавить**, выберите эту роль в отобразившемся окне и нажмите **OK**.

Отобразится следующее окно.

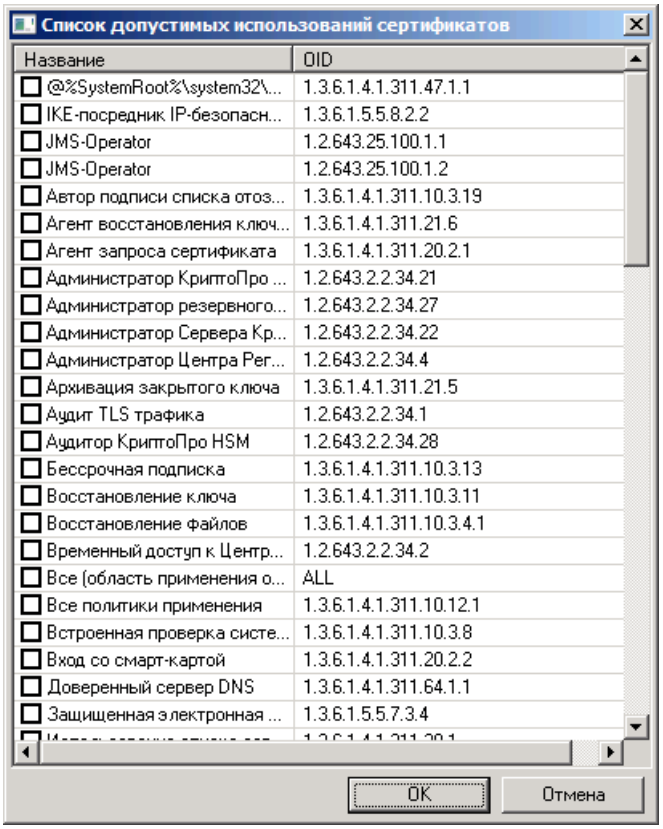


Рис. 579 – Окно Список допустимых использований сертификатов

7. Установите флаг **JMS-Оператор** и **Все (область применения отсутствует в запросе)**, после чего нажмите **OK**.
8. Повторите необходимые действия для системных ролей и политик, указанных в табл. 129, с. 599.

19.1.4 Создание шаблона сертификата для учетной записи JMS

Чтобы создать шаблон сертификата для учетной записи, которой будет назначена созданная системная роль (учетная запись JMS), выполните следующие действия.

1. Запустите приложение Параметры центра регистрации (**Пуск -> Все программы -> Крипто-Про -> Параметры центра регистрации**).
2. В отобразившемся окне разверните ветвь **Параметры Центра Регистрации**, щелкните правой кнопкой на центре регистрации и выберите **Свойства**.
3. В отобразившемся окне выберите вкладку **Политики**.

Отобразится следующее окно.

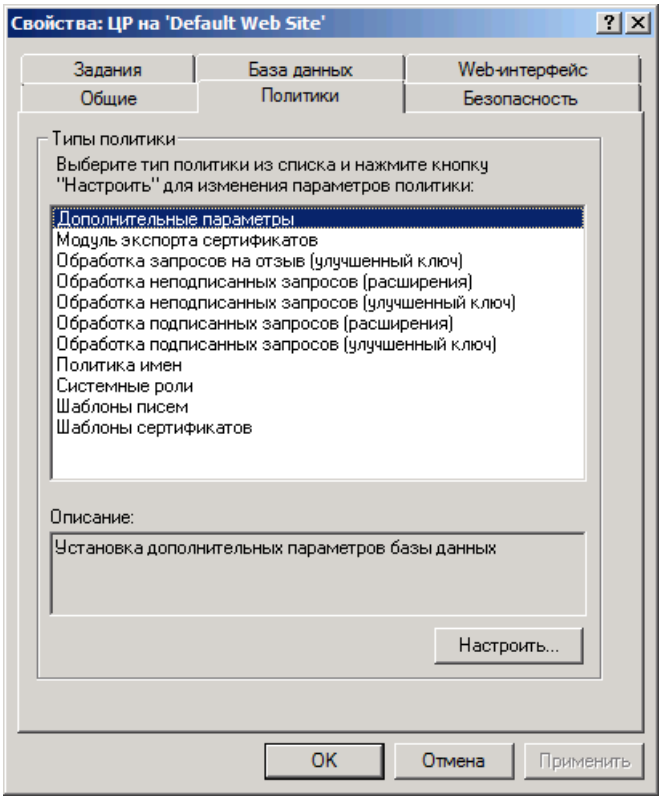


Рис. 580 – Вкладка Политики

4. В отобразившемся окне выберите пункт **Шаблоны сертификатов** и нажмите **Настроить**. Отобразится следующее окно.

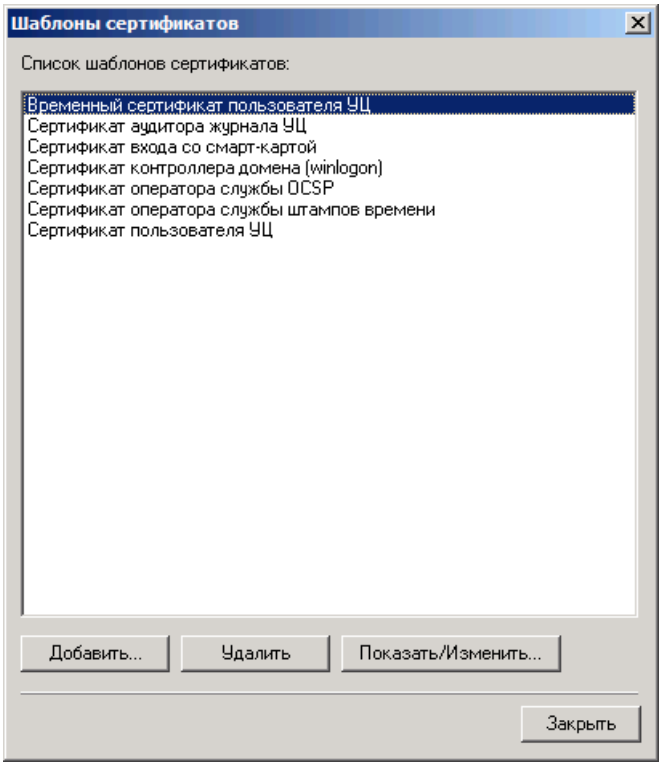


Рис. 581 – Список шаблонов сертификатов

5. Нажмите **Добавить**.
   Отобразится следующее окно.

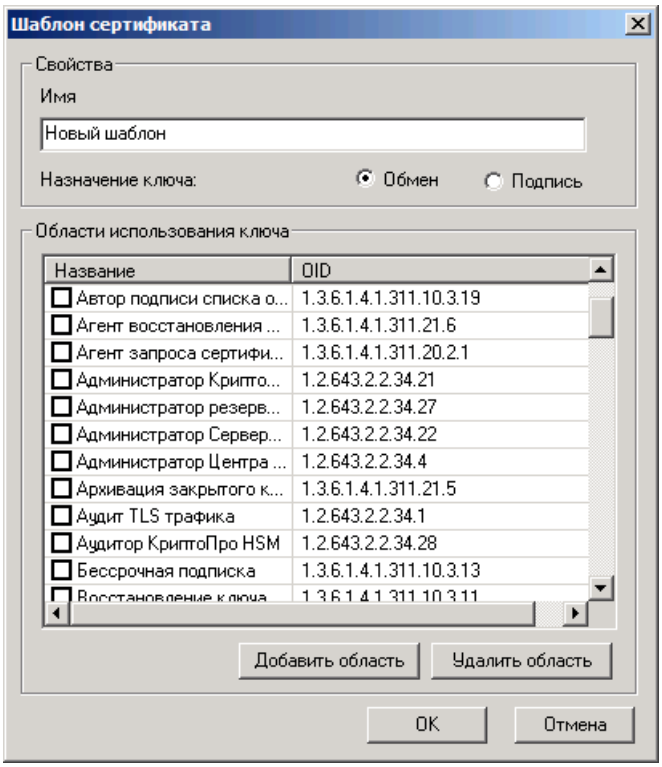


Рис. 582 – Свойства создаваемого шаблона сертификатов

6. В поле **Имя** введите имя нового шаблона, укажите назначение ключа и в списке **Области использования ключа** отметьте области использования ключа, которые будут включены в сертификаты, выдаваемые пользователям.
   Необходимо отметить следующие области:

   - **JMS-Оператор**;
   - **Проверка подлинности клиента**.

7. Нажмите **OK**.

19.1.5 Создание сертификата для учетной записи JMS

Чтобы запросить сертификат для учетной записи JMS, выполните следующие действия.

1. В **АРМ администратора Центра Регистрации** выберите **Operator**, щелкните правой кнопкой на пункте **Пользователи** и выберите **Создать -> Нового пользователя**, как показано на рис. 583.

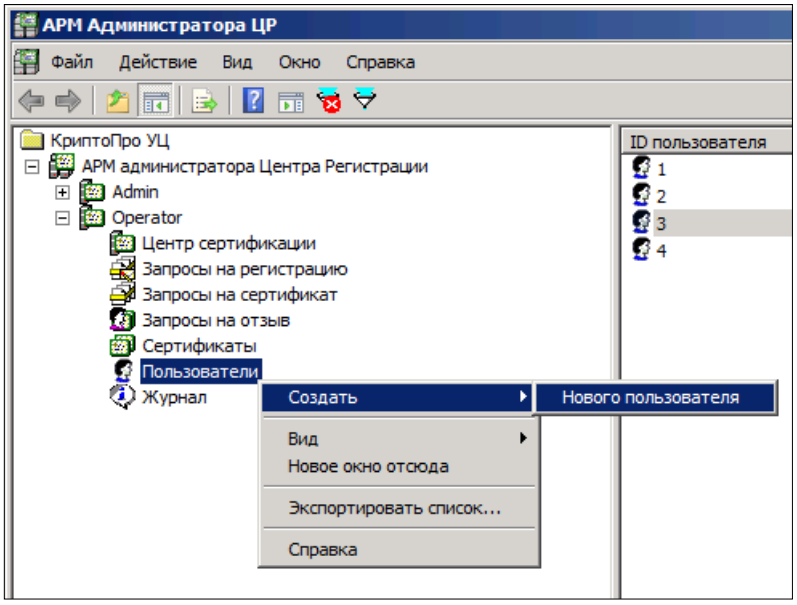


Рис. 583 – АРМ Администратора ЦР

Отобразится следующее окно.

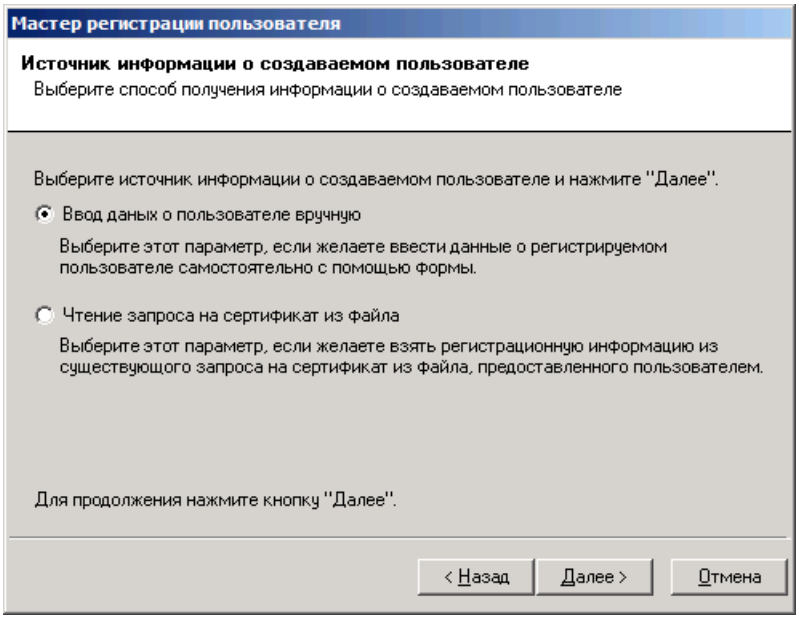


Рис. 584 – Выбор способа получения информации о создаваемом пользователе

2. Выберите пункт **Ввод данных о пользователе вручную** и нажмите **Далее**.

Отобразится следующее окно.

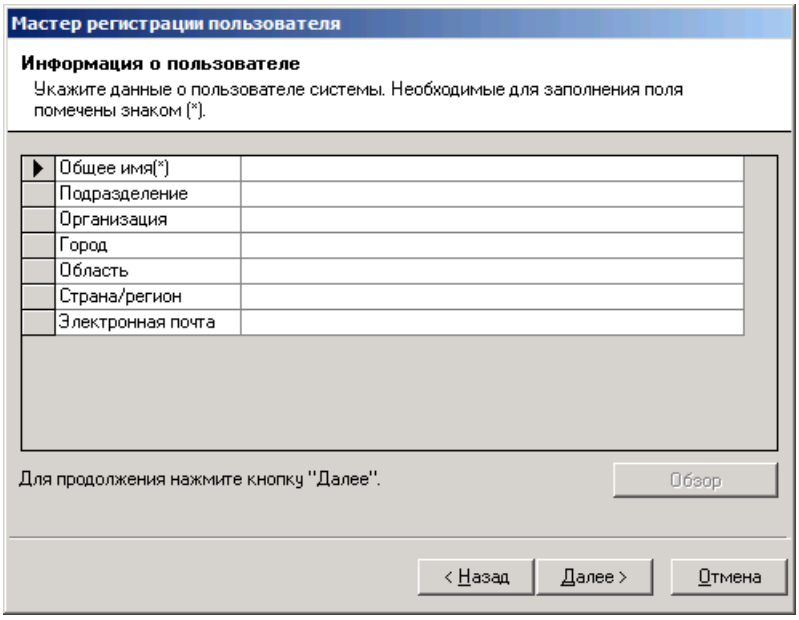


Рис. 585 – Окно данных о пользователе

3. В поле **Общее имя** укажите имя пользователя учетной записи JMS, после чего нажмите **Далее**.

Если КриптоПро УЦ находится в одном домене с JMS, то для выбора имени вы можете воспользоваться кнопкой Обзор. В противном случае введите имя вручную.

Отобразится следующее окно.

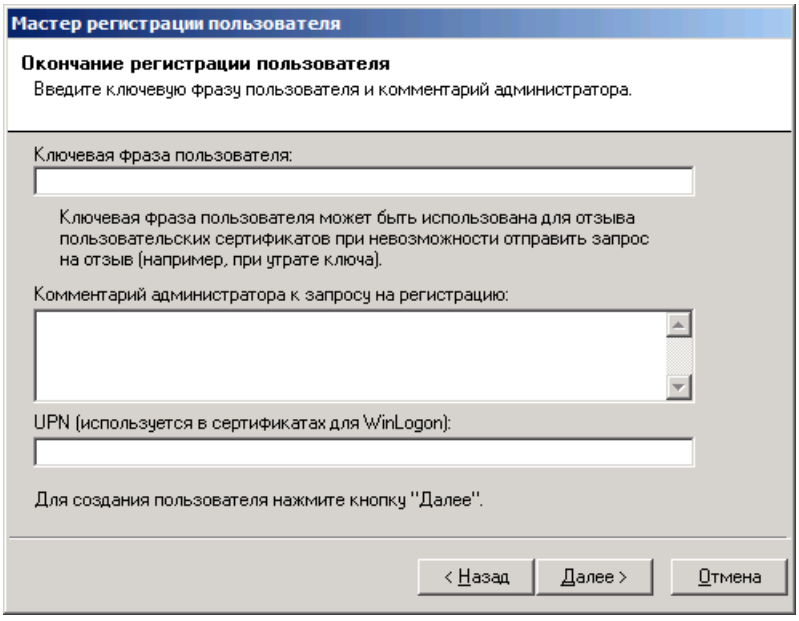


Рис. 586 – Окно окончания регистрации пользователя

4. Заполните поле **UPN**.

Если КриптоПро УЦ находится в одном домене с JMS, поле будет заполнено автоматически. В противном случае в этом поле вы должны ввести имя входа учетной записи JMS.

5. При необходимости заполните остальные поля и нажмите **Далее**.

Отобразится следующее окно.

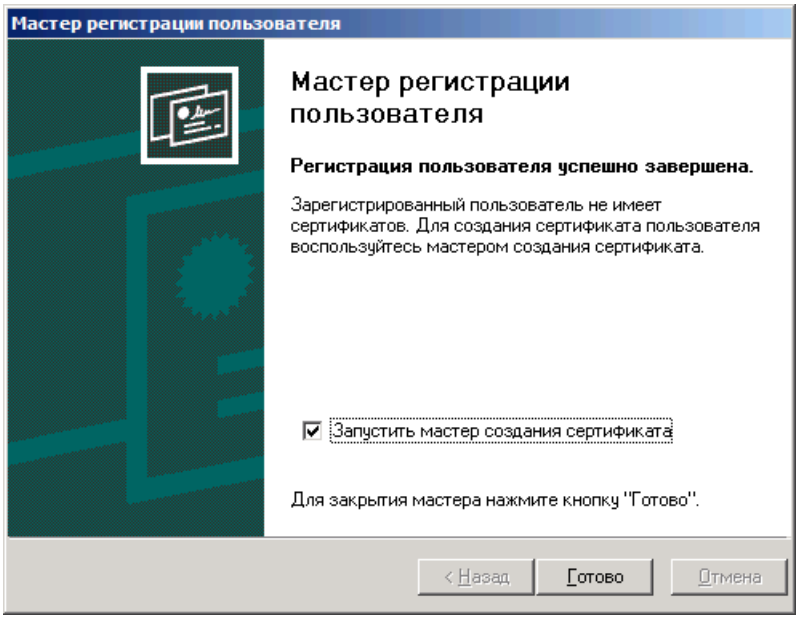


Рис. 587 – Регистрация пользователя завершена

6. Оставьте отмеченным флаг **Запустить мастер создания сертификата** и нажмите **Готово**. Отобразится следующее окно.

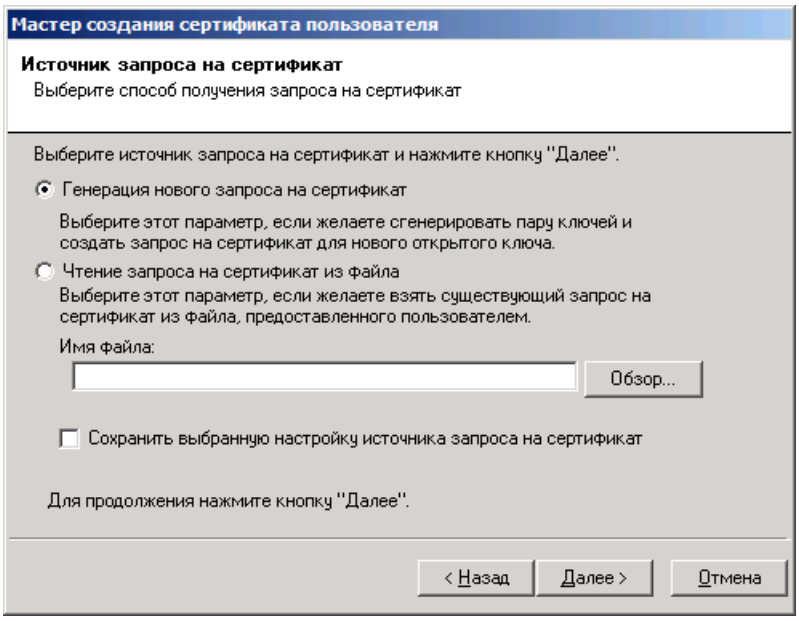


Рис. 588 – Выбор способа получения запроса не сертификат

7. Выберите **Генерация нового запроса на сертификат** и нажмите **Далее**.

Отобразится следующее окно.

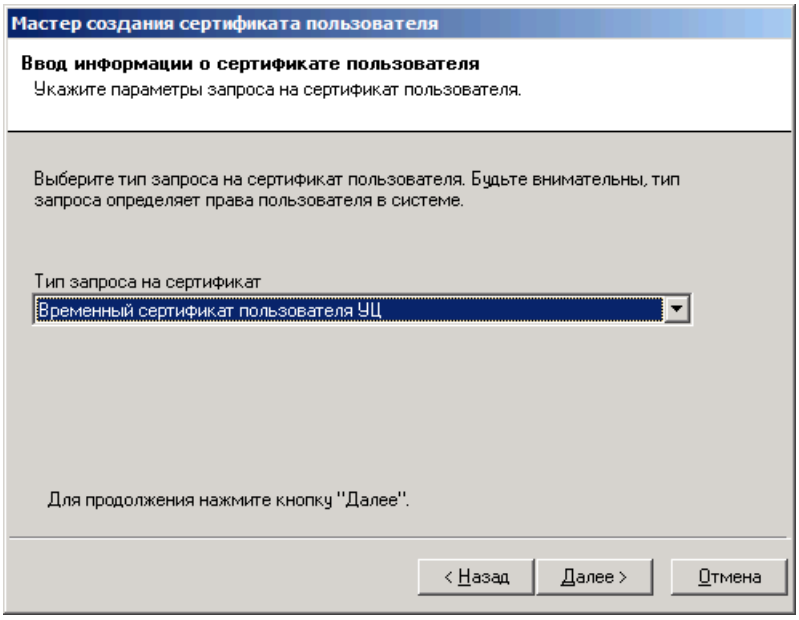


Рис. 589 – Выбор шаблона сертификата

8. В раскрывающемся списке **Тип запроса на сертификат** выберите подготовленный шаблон сертификата (подробнее см. «Создание шаблона сертификата для учетной записи JMS», с. 600), после чего нажмите **Далее**.
   Отобразится следующее окно.

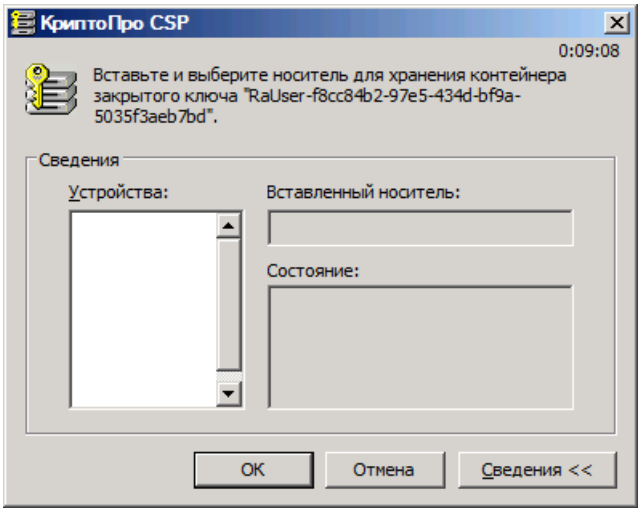


Рис. 590 – Выбор носителя для хранения ключевого контейнера

9. Сохраните имя ключевого контейнера (RaUser-xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx) - Оно потребуется на следующем этапе настройки системной роли.
10. В списке **Устройства** выберите **Реестр** и нажмите **ОК**.

11. Отобразится окно датчика случайных чисел. Следуйте приведенным в нем указаниям. По выполнении необходимых действий отобразится следующее окно.

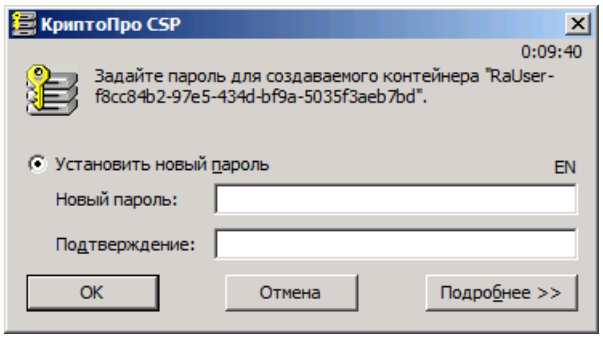


Рис. 591 – Окно задания пароля для создаваемого ключевого контейнера

12. При необходимости установите пароль для ключевого контейнера (это необязательно) и нажмите **OK**.
Отобразится следующее окно.

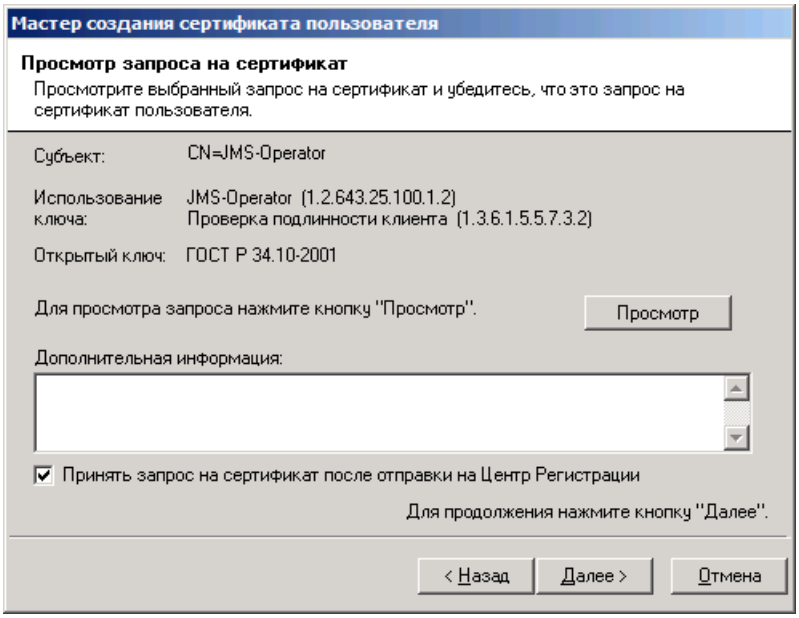


Рис. 592 – Окно просмотра параметров запроса на сертификат

13. При необходимости заполните поле **Дополнительная информация** и нажмите **Далее**.

Отобразится следующее окно.

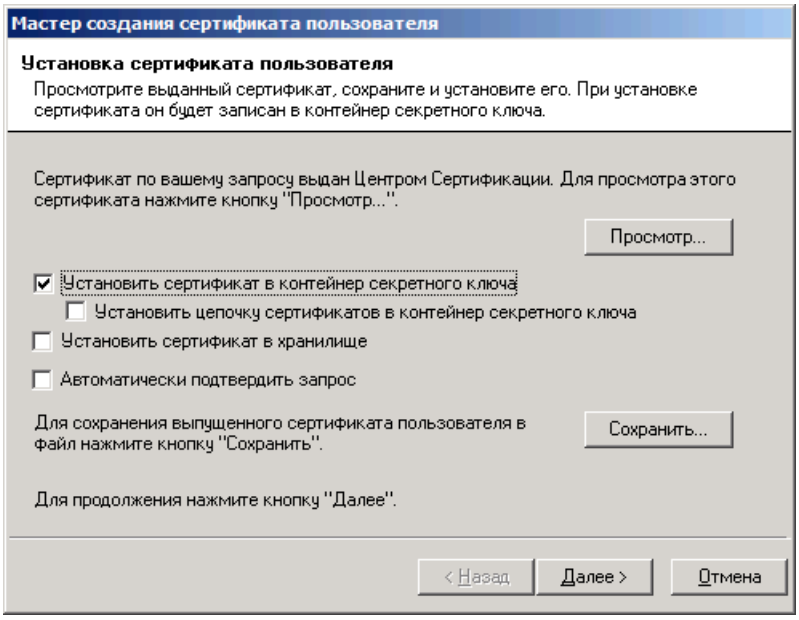


Рис. 593 – Установка сертификата пользователя

14. Оставьте отмеченным флаг **Установить сертификат в контейнер секретного ключа** и нажмите **Далее**.
    Отобразится следующее окно.

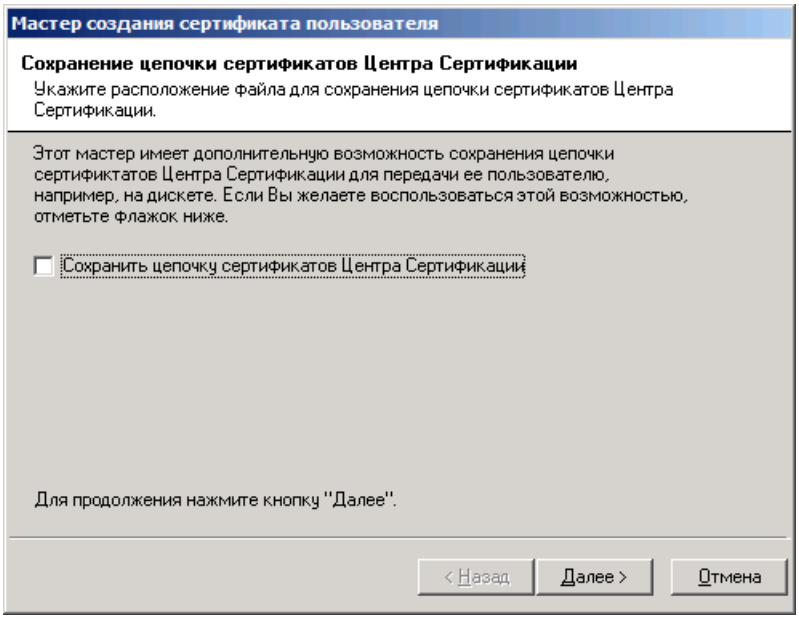


Рис. 594 – Окно установки сертификатов центра регистрации

15. Нажмите **Далее**.

Отобразится следующее окно.

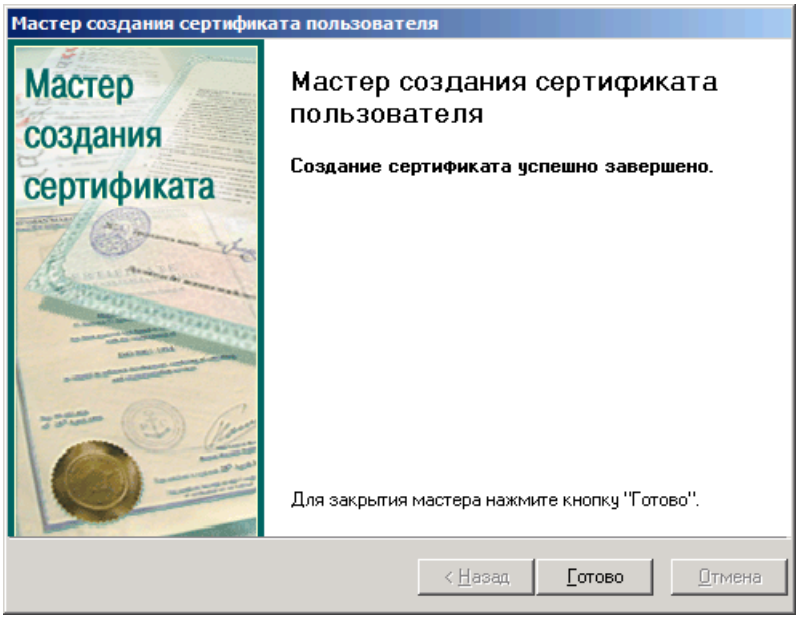


Рис. 595 – Окно завершения создания сертификата

16. Нажмите **Готово** для завершения процедуры.

19.1.6 Перенос ключевого контейнера

Чтобы перенести ключевой контейнер, созданный для учетной записи JMS, в хранилище локального компьютера на сервере JMS, выполните следующие действия.

1. На сервере КриптоПро УЦ запустите КриптоПро CSP (**Выберите Пуск -> Панель управления -> КриптоПро CSP**).
2. В отобразившемся окне выберите вкладку **Сервис**.

Окно примет следующий вид.

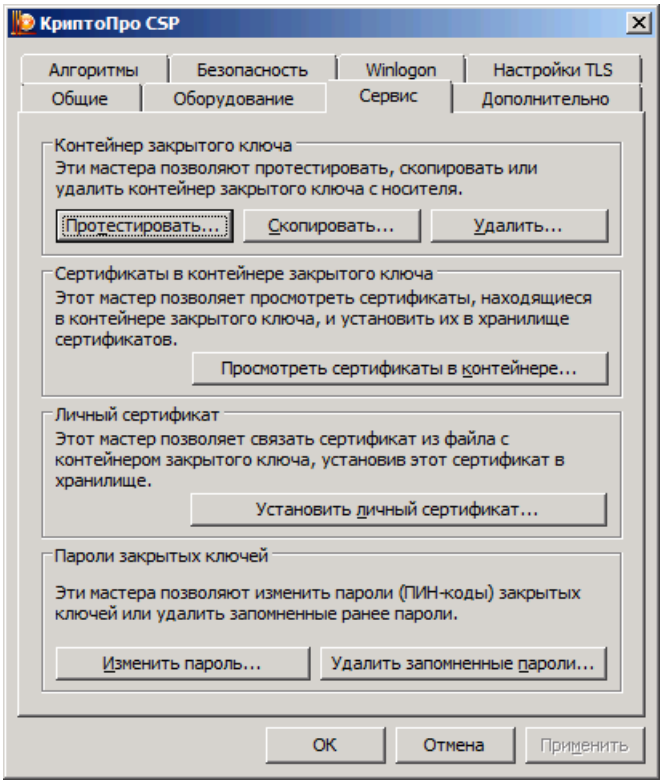


Рис. 596 – Вкладка Сервис окна свойств КриптоПро CSP

3. Нажмите **Скопировать контейнер**.
   Отобразится следующее окно.

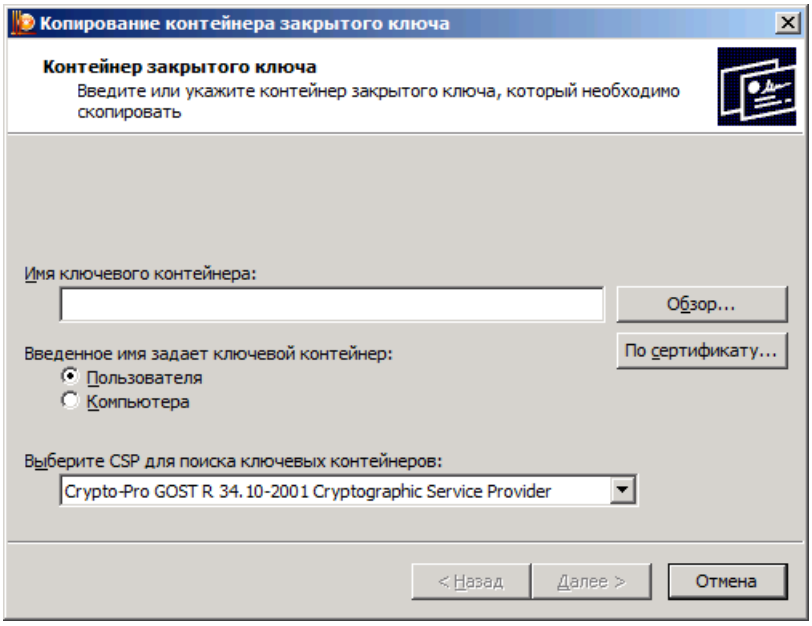


Рис. 597 – Окно для указания контейнера закрытого ключа, который надо скопировать

4. Оставьте отмеченным пункт **Пользователя** и нажмите **Обзор**.

Отобразится следующее окно.

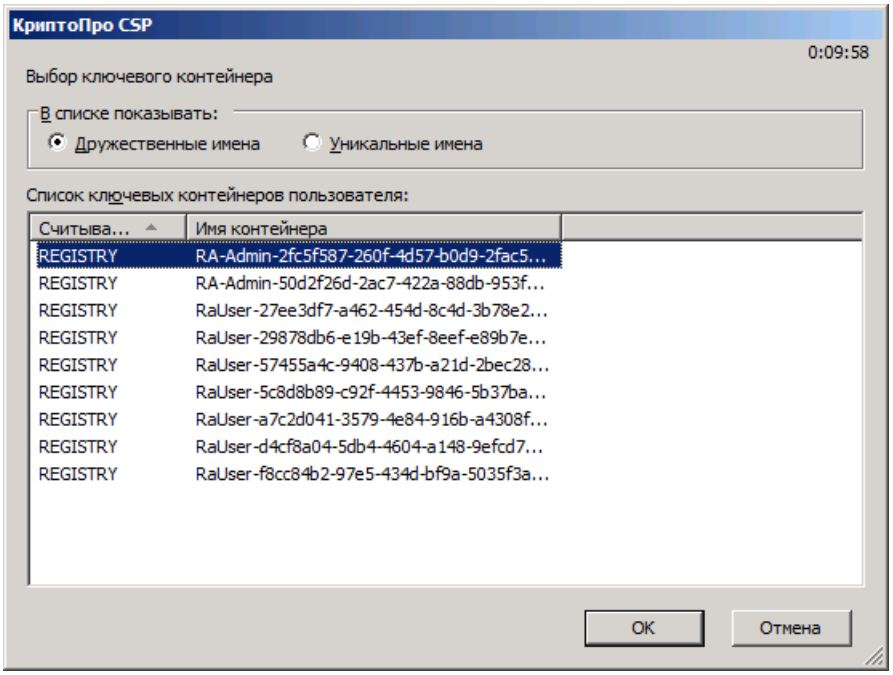


Рис. 598 – Выбор копируемого ключевого контейнера

5. Выберите имя контейнера, созданного при выпуске сертификата для учетной записи JMS (подробнее см. «Создание сертификата для учетной записи JMS», с. 603).и нажмите **OK**.
6. В основном окне мастера копирования контейнера нажмите **Далее**.
   Отобразится следующее окно.

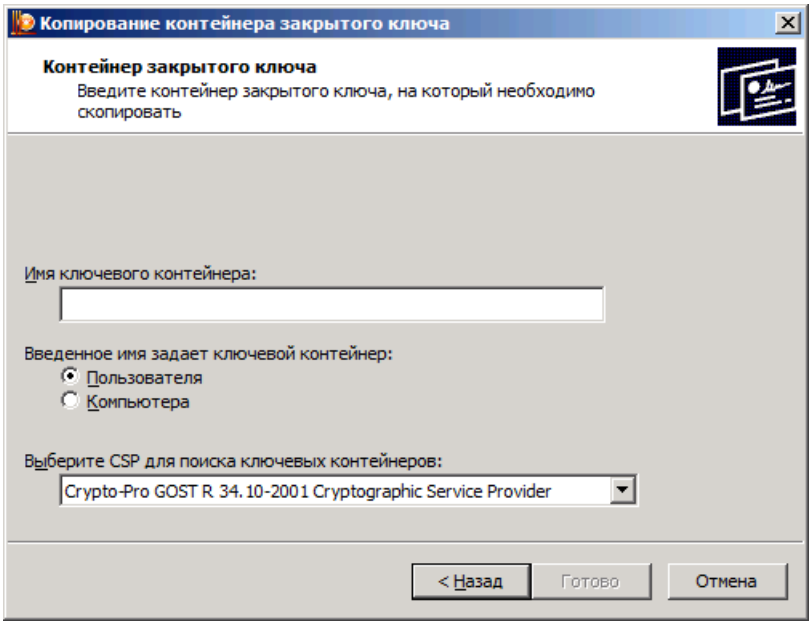


Рис. 599 – Выбор места копирования целевого контейнера

7. Выберите пункт **Компьютера**, в поле **Имя ключевого контейнера** введите имя для нового контейнера (например, **JMS**).
8. Запомните или запишите введенное имя. Оно потребуется на одном из следующих этапов настройки системной роли.
9. Нажмите **Готово**.

Отобразится следующее окно.

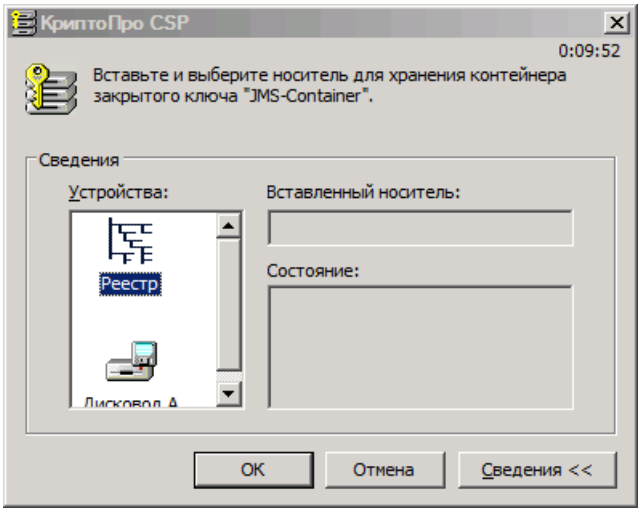


Рис. 600 – Выбор ключевого носителя

10. В зависимости от того, на каком компьютере расположен сервер JMS, выполните следующие действия.

    – Если сервер JMS расположен на том же компьютере, что и КриптоПро УЦ, в списке **Устройства** выберите **Реестр** и нажмите **OK**.
    – Если сервер JMS расположен на другом компьютере, нежели КриптоПро УЦ, подсоедините съемный носитель, например, устройство флеш-памяти, выберите его в списке **Устройства** и нажмите **OK**.

    Отобразится следующее окно.

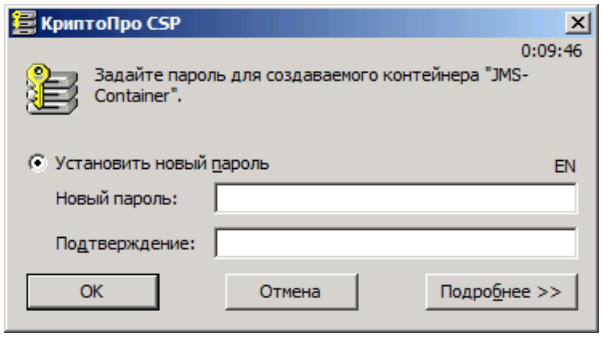


Рис. 601 – Задание пароля для ключевого контейнера

11. Нажмите **OK**, не устанавливая новый пароль.

⚠ Если сервер JMS находится на другом компьютере, нежели КриптоПро УЦ, воспользуйтесь КриптоПро CSP, чтобы со съемного носителя установить ключевой контейнер учетной записи JMS в хранилище локального компьютера на сервере JMS.

19.1.7 Редактирование разрешений реестра

Чтобы осуществлять выпуск электронных ключей с сертификатами КриптоПро УЦ, требуется установить необходимые разрешения на чтение определенных разделов реестра на сервере JMS.

1. Запустите редактор реестра. Для этого выберите **Пуск -> Выполнить**, в отобразившемся окне введите `regedit` и нажмите **OK**.

2. В отобразившемся окне щелкните правой кнопкой на нужном разделе реестра (см. табл. 130) и выберите **Разрешения**, как показано на рис. 602.

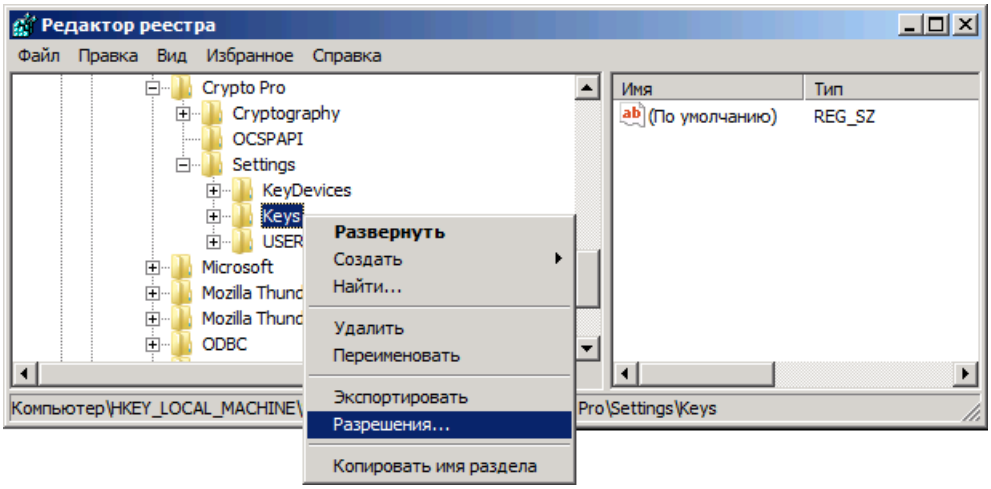


Рис. 602 – Редактор реестра

Отобразится следующее окно.

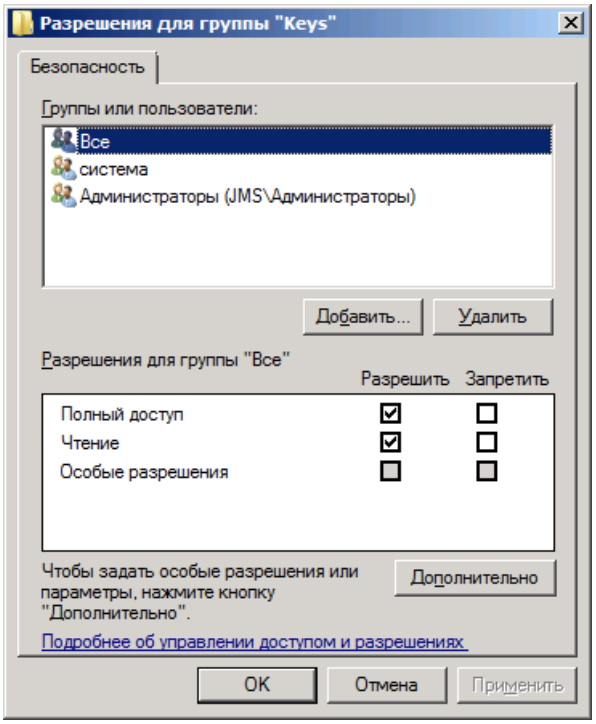


Рис. 603 – Редактирование разрешений

3. Отредактируйте разрешения в соответствии с табл. 130.

Табл. 130 - Редактирование разрешений реестра

Разрядность операционной системы	Раздел реестра	Группы или пользователи	Разрешения
32	HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings\Keys	**Все**	

Разрядность операционной системы	Раздел реестра	Группы или пользователи	Разрешения
	HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings\KeyDevices	**NETWORK SERVICE**	**Полный доступ**
		Учетная запись JMS	
64	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Crypto Pro\Settings\Keys	**Все**	
	HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Crypto Pro\Settings\KeyDevices	**NETWORK SERVICE**	
		Учетная запись JMS	

19.1.8 Редактирование разрешений безопасности

Для обеспечения взаимодействия между коннектором и центром регистрации КриптоПро УЦ необходимо предоставить системной роли, которая была назначена учетной записи JMS, определенные разрешения безопасности. Для этого выполните следующие действия.

1. Запустите приложение Параметры Центра Регистрации (**Пуск -> Все программы -> Крипто-Про -> Параметры Центра Регистрации**).
2. В отобразившемся окне раскройте узел **Параметры Центра Регистрации**, щелкните правой кнопкой на нужном центре регистрации и выберите **Свойства**.
3. В отобразившемся окне выберите вкладку **Безопасность**.

Окно примет следующий вид.

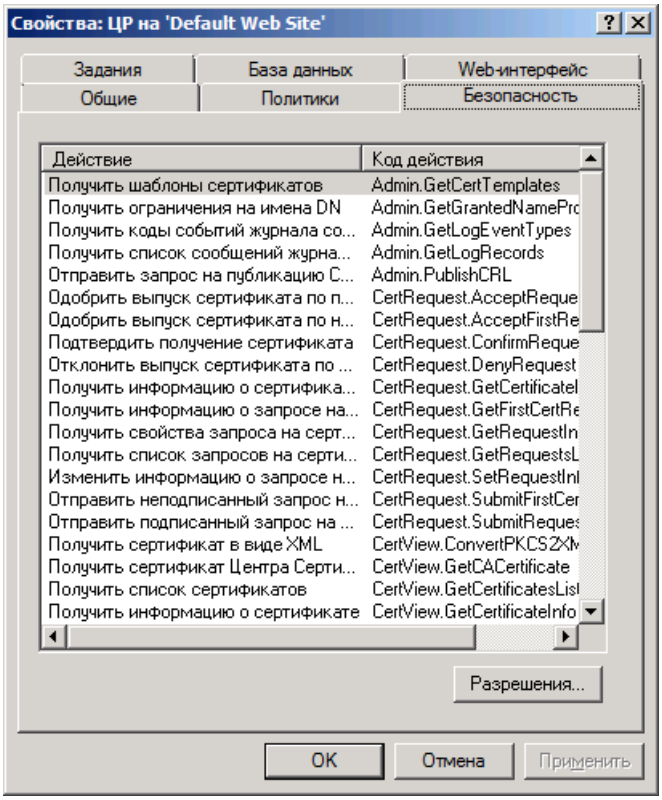


Рис. 604 – Список параметров безопасности

4. Добавьте необходимые разрешения в соответствии с табл. 131, с. 616.

Продолжение процедуры представлено на примере объекта **Admin.GetCertTemplates**.

5. Выберите в списке **Admin.GetCertTemplates** и нажмите **Разрешения**. Отобразится следующее окно.

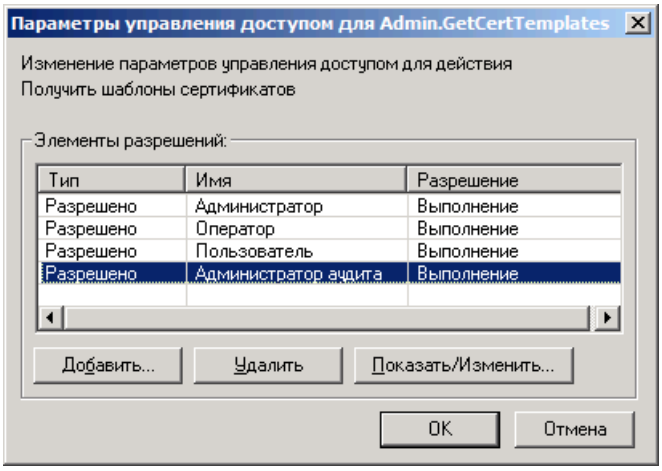


Рис. 605 – Окно Параметры управления доступом

6. Нажмите **Добавить**.

Отобразится следующее окно.

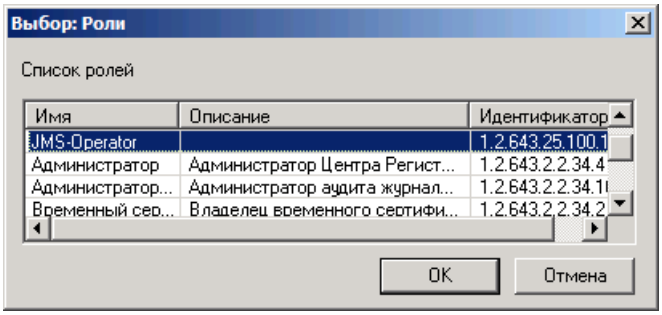


Рис. 606 – Список доступных ролей

7. Выберите **JMS-Оператор** и нажмите **OK**.
   Отобразится следующее окно.

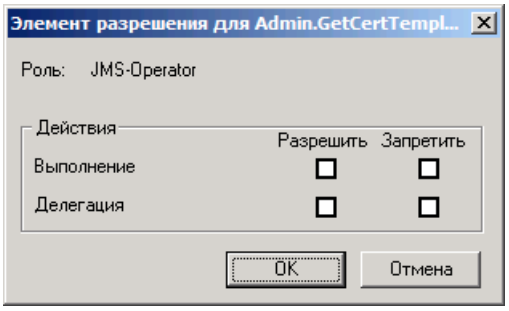


Рис. 607 – Выбор разрешений действий

8. В строке **Выполнение** отметьте пункт **Разрешить** и нажмите **OK**.
9. Повторите необходимые действия для объектов, указанных в табл. 131.

Табл. 131 – Разрешения безопасности

	Код действия	Описание	Разрешение	
			Выполнение	**Делегирование**
1	**Admin.GetCertTemplates**	Получить шаблоны сертификатов	+	
2	**Admin.GetGrantedNameProperties**	Получить ограничения на имена DN	+	
3	**Admin.GetLogEventTypes**	Получить коды событий журнала событий	+	
4	**Admin.GetLogRecords**	Получить список сообщений журнала событий		
5	**Admin.PublishCRL**	Отправить запрос на публикацию COC	+	

	Код действия	Описание	Разрешение	
			Выполнение	Делегирование
6	**CertRequest.AcceptRequest**	Одобрить выпуск сертификата по подписанному запросу на сертификат	+	
~~7~~	**CertRequest.AcceptFirstRequest**	Одобрить выпуск сертификата по неподписанному запросу на сертификат	+	+
8	**CertRequest.ConfirmRequest**	Подтвердить получение сертификата	+	
9	**CertRequest.DenyRequest**	Отклонить выпуск сертификата по запросу		
10	**CertRequest.GetCertificateInfo**	Получить информацию о сертификате по коду запроса на сертификат	+	+
11	**CertRequest.GetFirstCertRequestInfo**	Получить информацию о запросе на сертификат по коду запроса на регистрацию		
12	**CertRequest.GetRequestInfo**	Получить свойства запроса на сертификат	+	+
13	**CertRequest.GetRequestsList**	Получить список запросов на сертификат	+	
14	**CertRequest.SetRequestInfo**	Изменить информацию о запросе на сертификат	+	
15	**CertRequest.SubmitFirstCertRequest**	Отправить неподписанный запрос на сертификат	+	+
16	**CertRequest.SubmitRequest**	Отправить подписанный запрос на сертификат	+	
17	**CertView.ConvertPKCS2XML**	Получить сертификат в виде XML		
18	**CertView.GetCACertificate**	Получить сертификат Центра Сертификации	+	
19	**CertView.GetCertificatesList**	Получить список сертификатов	+	+
20	**CertView.GetCertificateInfo**	Получить информацию о сертификате	+	+

	Код действия	Описание	Разрешение	
			Выполнение	Делегирование
21	**CertView.GetCRL**	Получить список отозванных сертификатов (COC)		
22	**Registration.AcceptRequest**	Одобрить создание пользователя по запросу на регистрацию	+	+
23	**Registration.CreateCertRequest**	Извлечь запрос на сертификат из запроса на регистрацию	+	+
24	**Registration.CreateRequestByAdmin**	Отправить запрос на регистрацию пользователя администратором	+	
25	**Registration.DenyRequest**	Отклонить запрос на регистрацию	+	+
26	**Registration.GetRequestInfo**	Получить информацию о запросе на регистрацию	+	+
27	**Registration.GetRequestsList**	Получить список запросов на регистрацию	+	+
28	**Registration.SetRequestInfo**	Изменить информацию о запросе на регистрацию	+	+
29	**RevokeRequest.AcceptRequest**	Одобрить запрос на отзыв сертификата	+	+
30	**RevokeRequest.DenyRequest**	Отклонить запрос на отзыв сертификата	+	+
31	**RevokeRequest.GetRequestInfo**	Получить информацию о запросе на отзыв сертификата	+	+
32	**RevokeRequest.GetRequestsList**	Получить список запросов на отзыв сертификата	+	+
33	**RevokeRequest.SetRequestInfo**	Изменить информацию о запросе на отзыв сертификата		
34	**RevokeRequest.SubmitRequest**	Отправить запрос на отзыв сертификата	+	+
35	**RevokeRequest.SubmitHoldRequest**	Отправить запрос на приостановление действия сертификата	+	+

	Код действия	Описание	Разрешение	
			Выполнение	Делегирование
36	**RevokeRequest.SubmitUnHoldRequest**	Отправить запрос на возобновление действия сертификата	+	+
37	**UserView.AddDocument**	Добавить документ пользователя		
38	**UserView.GetDocumentInfo**	Получить информацию о документе пользователя		
39	**UserView.GetDocumentsList**	Получить список документов пользователя		
40	**UserView.GetUserByCertificate**	Найти идентификатор пользователя по сертификату	+	
41	**UserView.GetUserInfo**	Получить информацию о пользователе	+	+
42	**UserView.GetUsersList**	Получить список пользователей	+	
43	**UserView.RemoveDocument**	Удалить документ пользователя		
44	**UserView.SetUserInfo**	Изменить информацию о пользователе	+	+
45	**UserView.DeleteUser**	Удалить пользователя		
46	**Admin.CreateTokenForUser**	Создать маркер временного доступа	+	+
47	**Audit.SaveLog**	Сохранить журнал событий ЦР		
48	**Audit.GetSavedLog**	Получить список сохраненных событий журнала ЦР		
49	**Audit.DeleteSavedLog**	Очистить сохраненные события журнала ЦР		
50	**RevokeRequest.AcceptHoldRequest**	Одобрить запрос на приостановление сертификата		
51	**RevokeRequest.AcceptUnholdRequest**	Одобрить запрос на возобновление сертификата		

	Код действия	Описание	Разрешение	
			Выполнение	Делегирование
52	**RevokeRequest.DenyHoldRequest**	Отклонить запрос на приостановление сертификата		
53	**RevokeRequest.DenyUnholdRequest**	Отклонить запрос на возобновление сертификата		

19.2 Настройка профиля для выпуска сертификатов в КриптоПро УЦ 1.5

Чтобы настроить профиль выпуска сертификатов средствами КриптоПро УЦ 1.5, выполните следующие действия.

1. В консоли управления JMS перейдите в раздел **Профили -> Профили**.
2. В центральной части окна выберите пункт **Выпуск сертификатов – КриптоПро УЦ 1.5** и в верхней панели нажмите **Создать**.
   Отобразится следующее окно.

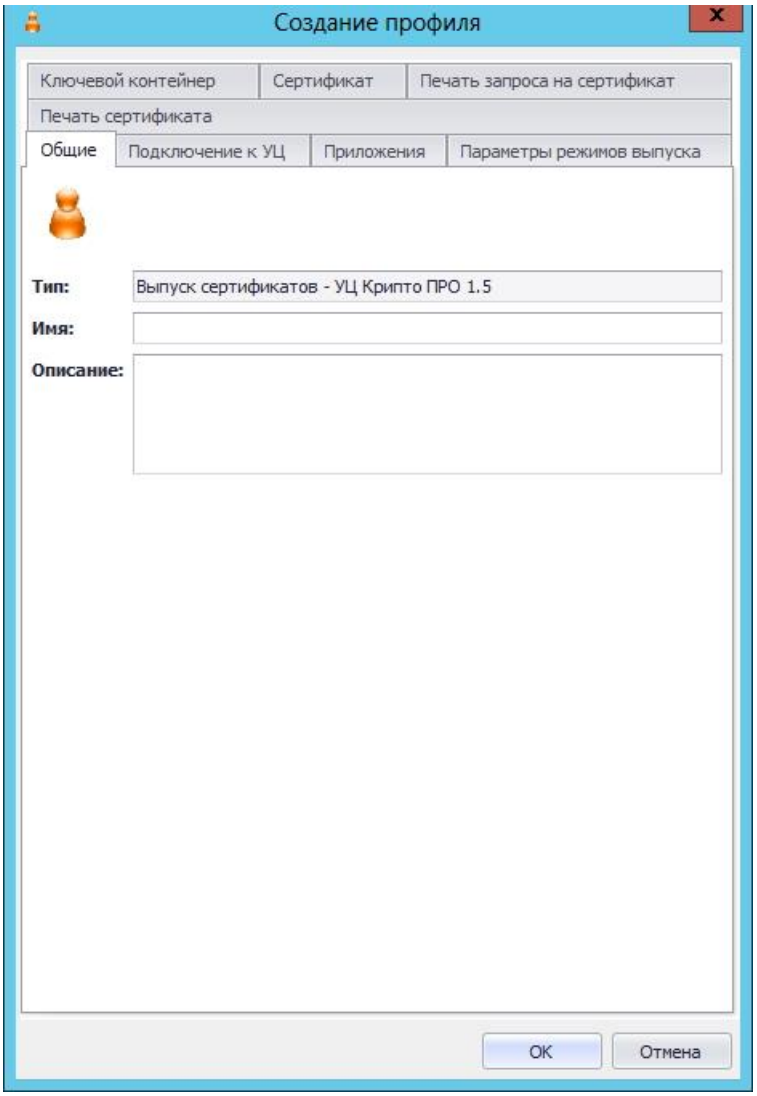


Рис. 608 – Вкладка Общие настроек профиля выпуска сертификатов средствами КриптоПро УЦ 1.5

3. В полях **Имя** и **Описание** соответственно задайте название и описание создаваемого профиля, после чего перейдите на вкладку **Подключение**.
Окно примет следующий вид.

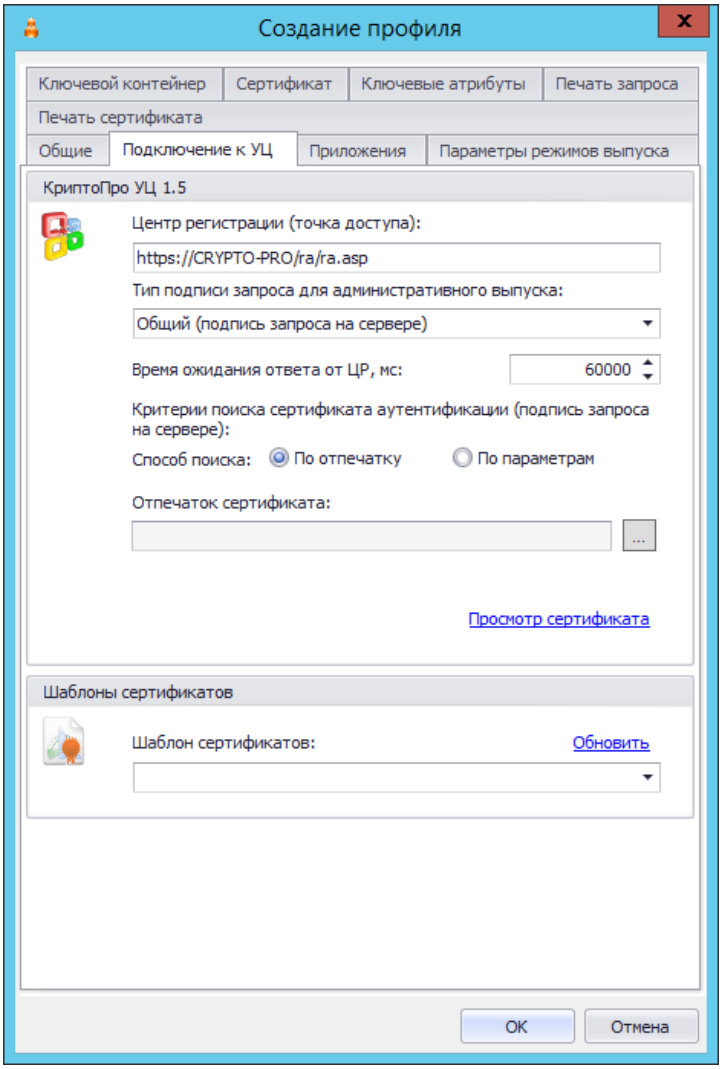


Рис. 609 – Вкладка Подключение настроек профиля выпуска сертификатов средствами КриптоПро УЦ 1.5

4. Выполните настройку, руководствуясь табл. 132.

Табл. 132 – Настройка параметров подключения к КриптоПро УЦ 1.5

Секция	Настройка	Описание
КриптоПро УЦ 1.5	**Центр регистрации (точка доступа)**	Поле для указания строки подключения к центру регистрации.
	Тип подписи запроса для административного выпуска	Список имеет два пункта: • **Общий (подпись запроса на сервере)** – в качестве оператора Центра регистрации КриптоПро выступает сервер JMS, и соответствующий сертификат КриптоПро должен быть установлен в хранилище компьютера на сервере JMS (настройка обязательна); • **Частный (подпись запроса на клиенте)** – в качестве оператора Центра регистрации КриптоПро выступает администратора JMS, использующий консоль

Секция	Настройка	Описание
		управления JMS; в этом случае сертификат оператора Центра регистрации КриптоПро может быть установлен в хранилище пользователя на компьютере, где установлена консоль управления JMS, или записан в память электронного ключа. В настоящем документе подробно рассматривается вариант, где в качестве оператора Центра регистрации КриптоПро выступает сервер JMS.
	Время ожидания ответа от ЦР	Позволяет задать время ожидание ответа от центра регистрации (в миллисекундах).
	Критерии поиска сертификата аутентификации (подпись запроса на сервере)	Позволяет задать критерий поиска сертификата учетной записи JMS, возможны два варианта: • **По отпечатку**; • **По параметрам**. **Примечания:** 3. Независимо от того, настраивается профиль для единичного сервера JMS (т.е. без кластера) или для кластера JMS следует выбрить способ поиска **По отпечатку**, поскольку в кластерной конфигурации на всех узлах для подписи запроса в КриптоПро УЦ устанавливается один и тот же сертификат. Порядок развертывания кластерной конфигурации приведен в соответствующем руководстве [5]. 4. 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 будет предложены на выбор все сертификаты из личного хранилища пользователя, от имени которого запущена консоль управления. 5. При работе JMS с КриптоПро УЦ подпись запроса осуществляется на сертификате аутентификации.
Шаблоны сертификатов	**Шаблон сертификатов**	При успешном соединении с КриптоПро УЦ из данного списка можно выбрать шаблон сертификата, по которому будут выпускаться сертификаты для пользователей JMS. 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.

5. Перейдите на вкладку **Приложения** и отметьте комбинации приложений, на которые будет распространяться профиль.
6. Перейдите на вкладку **Параметры режимов выпуска**.

Окно примет следующий вид.

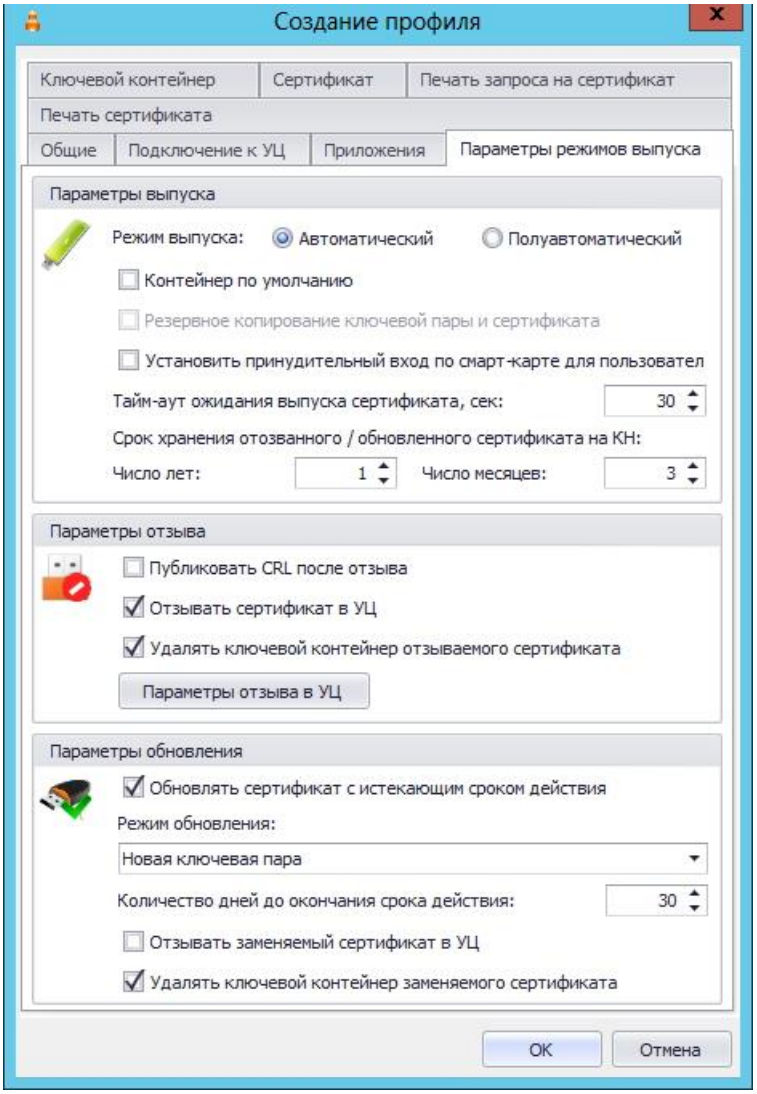


Рис. 610 – Вкладка Выпуск настроек профиля выпуска сертификатов средствами КриптоПро УЦ 1.5

7. Выполните настройку, руководствуясь табл. 133.

Табл. 133 – Настройка параметров выпуска

Секция	Настройка	Описание
Параметры выпуска	**Режим выпуска**	Позволяет выбрать режим выпуска электронных ключей с сертификатами КриптоПро УЦ: **Автоматический** – запись сертификата в память электронного ключа происходит в результате однократного выпуска; **Полуавтоматический** - в полуавтоматическом режиме выпуск электронного ключа происходит в несколько этапов (см. описание ниже). 1. При первичном выпуске в памяти электронного ключа формируется ключевой контейнер; запрос на сертификат поступает на центр регистрации.

Секция	Настройка	Описание
		2. Администратор, используя приложение «АРМ Администратора ЦР», должен подтвердить запрос сертификата. 3. После того как запрос подтвержден, электронный ключ необходимо синхронизировать с JMS. 4. Если в настройках профиля для ключевых контейнеров задано одинаковое имя, перед выпуском нового электронного ключа необходимо удалить запомненные пароли пользователя. Если подряд выполнить первичный выпуск нескольких электронных ключей с одноименными контейнерами, повторный выпуск (запись сертификата) будет невозможен. Для каждого отдельного электронного ключа с одноименным контейнером процедуру необходимо проходить целиком.
	Контейнер по умолчанию	Если данный флаг установлен, созданный в процессе выпуска ключевой контейнер будет помечен как контейнер по умолчанию.
	Резервное копирование ключевой пары и сертификата	Позволяет выполнять резервное копирование ключевой пары и сертификата в процессе выпуска электронного ключа.
	Установить принудительный вход по смарт-карте для пользователя	При выпуске электронного ключа в настройках профиля пользователя будет установлена необходимость использования смарт-карты (электронного ключа) для входа в домен.
	Тайм-аут ожидания выпуска сертификата	Позволяет задать время ожидания при выпуске сертификата (в секундах).
	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 электронного ключа», с. 88); • при отмене привязки *профиля выпуска сертификата*, применявшегося к данному электронному ключу (см. «Привязка профилей», с. 296), в том числе и при удалении профиля; • при отзыве сертификата средствами JMS (см. раздел «Операции с сертификатами», с. 50); • при отзыве сертификата 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

Секция	Настройка	Описание
		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.
	Удалять ключевой контейнер	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 отзыва в УЦ	Нажатие на кнопку отображает окно, в котором можно настроить параметры отзыва сертификата в удостоверяющем центре: • **Создавать запрос на отзыв** - если флаг установлен, при отзыве электронного ключа в удостоверяющий центр будет подаваться запрос на отзыв сертификата соответствующего пользователя; • **Подтверждать запрос на отзыв** - если флаг установлен, при отзыве электронного ключа в удостоверяющем центре будет одобряться запрос на отзыв сертификата соответствующего пользователя. • **Отключать пользователя на ЦР** - Если флаг установлен, при отзыве электронного ключа будет произведена попытка удаления пользователя из центра регистрации КриптоПро. Если у пользователя есть другие запросы на сертификат, пользователь удален не будет. Настройка работает только в том случае, если включены настройки **Создавать запрос на отзыв** и **Подтверждать запрос на отзыв**.
Параметры обновления	**Обновлять сертификат с истекшим сроком действия**	Позволяет обновлять сертификаты в памяти электронных ключей пользователей, срок действия которых подходит к концу. В результате в памяти электронного ключа создается новая ключевая пара.
	Режим обновления	Обновление возможно только в режиме создания новой ключевой пары.
	Количество дней до окончания срока действия	Позволяет задать число дней до окончания срока действия сертификата, в течение которых можно сделать обновление.
	Отзывать заменяемый сертификат в УЦ	Если флаг установлен, заменяемый сертификат будет отозван в удостоверяющем центре КриптоПро.
	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.

Секция	Настройка	Описание
		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**).

8. Перейдите на вкладку **Ключевой контейнер** и **в**ыполните настройки аналогично настройкам профиля выпуска сертификатов MSCA (см. Табл. 34, с. 218).

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

*Рис. 611 – Вкладка **Сертификат***

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

10.1. В секции с названием нужного поля щелкните на кнопке **Редактировать шаблон**;
10.2. Отредактируйте шаблон, руководствуясь сведениями, представленными в табл. 134.
10.3. В окне редактирования шаблона нажмите **OK**, чтобы сохранить изменения.
10.4. В секции с названием нужного поля установите флаг **Формировать с помощью шаблона**.
10.5. При необходимости повторите действия для других полей.

Табл. 134 – 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.

11. Перейдите на вкладку **Ключевые атрибуты** и выполните настройки аналогично настройкам одноименной вкладки в профиле выпуска сертификатов MSCA (см. раздел «Настройки профиля выпуска сертификатов в центре сертификации Microsoft», с. 209).
12. При необходимости, выполните настройку печати документов (вкладки **Печать запроса** на сертификат и **Печать сертификата**) при выпуске электронного ключа (подробнее о настройке Шаблона печатной формы см. «Настройка параметров печати при выпуске объектов JMS», с. 304).
13. Нажмите **OK**, чтобы сохранить изменения.

20. Работа с КриптоПро УЦ 2.0

20.1 Подготовительные действия

Подготовка сервера JMS к работе с КриптоПро УЦ 2.0 состоит в установке в JMS двух сертификатов:

- сертификата КриптоПро УЦ (в хранилище доверенных корневых центров);
- сертификата пользователя (данный сертификат будет использоваться для аутентификации JMS в КриптоПро УЦ).

Для этого выполните следующие действия.

1. Если служба JMS запускается от имени учетной записи пользователя, откройте пользовательский сеанс Windows на сервере JMS от имени данного пользователя; в противном случае откройте пользовательский сеанс Windows от имени администратора сервера JMS.
2. Установите сертификат центра сертификации КриптоПро в хранилище доверенных корневых центров сертификации на сервере JMS.
3. Создайте в КриптоПро УЦ пользователя и добавьте его в группу безопасности КриптоПро УЦ **Операторы** (убедитесь, что у пользователей группы Операторы установлен минимально необходимый набор полномочий, см. документ «Руководство администратора. Часть 1» [2], раздел «Разрешения в КриптоПро УЦ 2.0»).
4. От имени пользователя КриптоПро УЦ, состоящего в группе безопасности **Операторы**, запросите и установите сертификат пользователя КриптоПро УЦ с сервера JMS – сертификат и соответствующий ему ключевой контейнер будут установлены в личное хранилище пользователей КриптоПро на сервере JMS. ***Если служба JMS запускается от имени учетной записи пользователя, то подготовительные действия на этом шаге заканчиваются.***
5. В случае если служба JMS запускается от имени системной учетной записи, выполните следующие шаги.

5.1. На сервере JMS скопируйте ключевой контейнер пользователя КриптоПро УЦ, состоящего в группе безопасности **Операторы**, из хранилища пользователей КриптоПро в хранилище компьютера КриптоПро (см. «Копирование ключевого контейнера из хранилища пользователя в хранилище компьютера», ниже).

5.2. На сервере JMS выполните экспорт сертификата пользователя КриптоПро УЦ, состоящего в группе безопасности Операторы (см. «Экспорт сертификата из хранилища сертификатов пользователя», с. 631).

5.3. На сервере JMS установите экспортированный сертификат пользователя КриптоПро УЦ, состоящего в группе безопасности Операторы, в хранилище сертификатов компьютеров КриптоПро (см. «Установка сертификата оператора КриптоПро УЦ в хранилище компьютера», с. 637).

20.1.1 Копирование ключевого контейнера из хранилища пользователя в хранилище компьютера

1. На сервере JMS запустите КриптоПро CSP от имени администратора и перейдите на вкладку **Сервис**.
   Окно КриптоПро CSP будет выглядеть следующим образом.

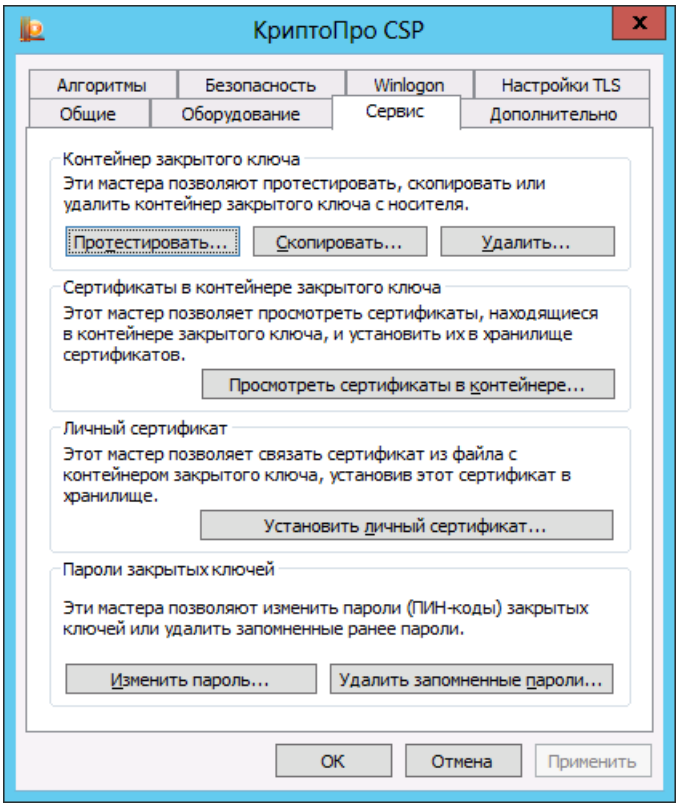


Рис. 612 – Вкладка Сервис окна настроек КриптоПро CSP

2. Нажмите **Скопировать**.

Отобразится следующее окно.

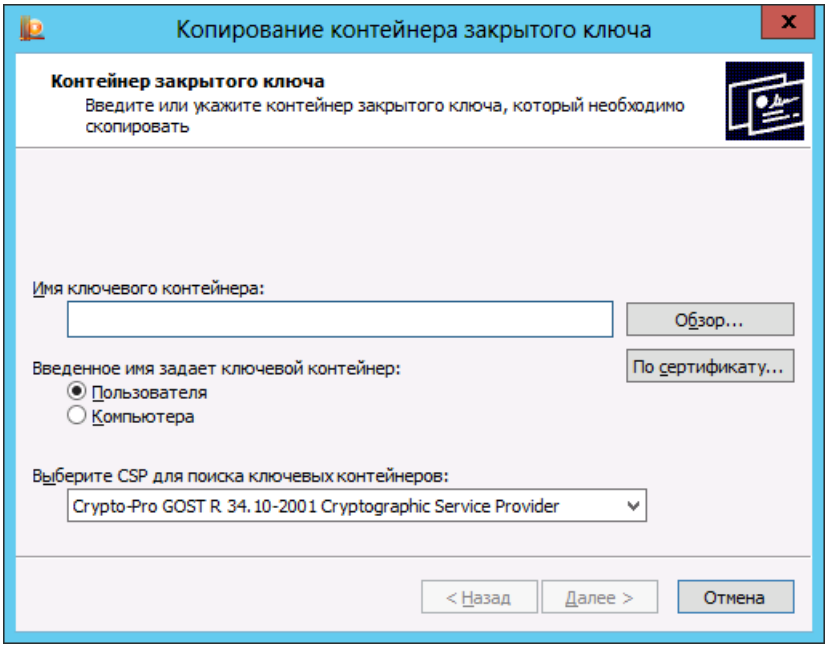


Рис. 613 – Копирование контейнера закрытого ключа

3. Нажмите **Обзор...** (либо нажмите **По сертификату** и выберите нужный сертификат из предложенного списка).
   Отобразится следующее окно.

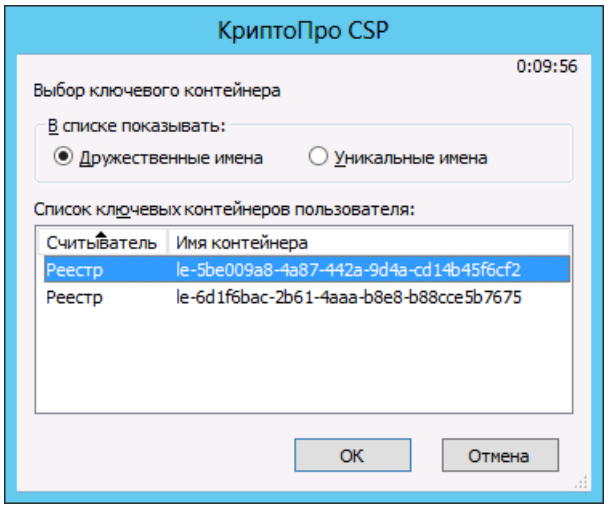


Рис. 614 – Выбор ключевого контейнера

4. Выберите ключевой контейнер, который был создан при выпуске сертификата оператора КриптоПро УЦ для JMS, после чего нажмите **OK**.
5. В окне контейнера копирования закрытого ключа нажмите **Далее**.

Отобразится следующее окно.

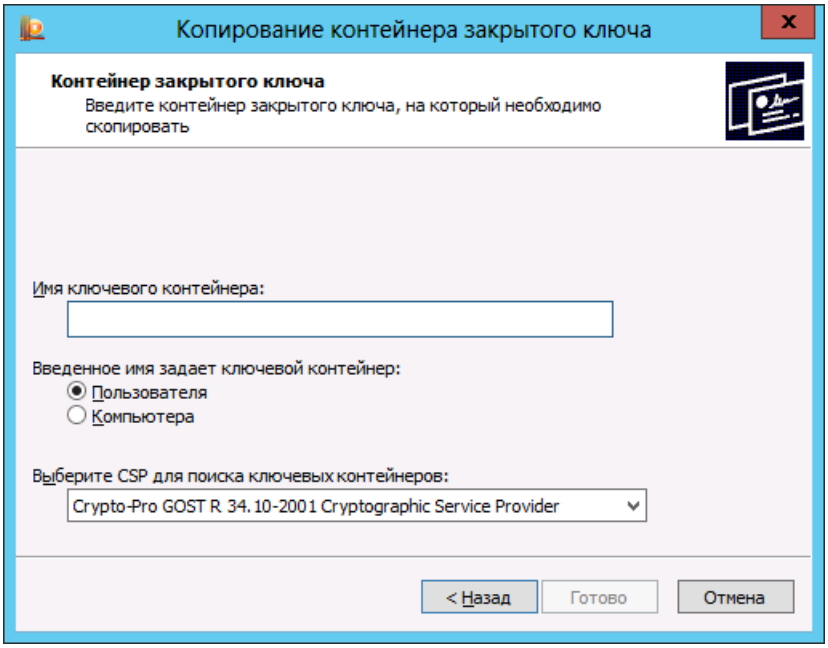


Рис. 615 – Создание контейнера закрытого ключа

6. В поле **Имя ключевого контейнера** задайте имя для ключевого контейнера в хранилище компьютера.
7. В секции **Введенное имя задает ключевой контейнер** выберите **Компьютера**, после чего нажмите **Готово**.
   Отобразится следующее окно.

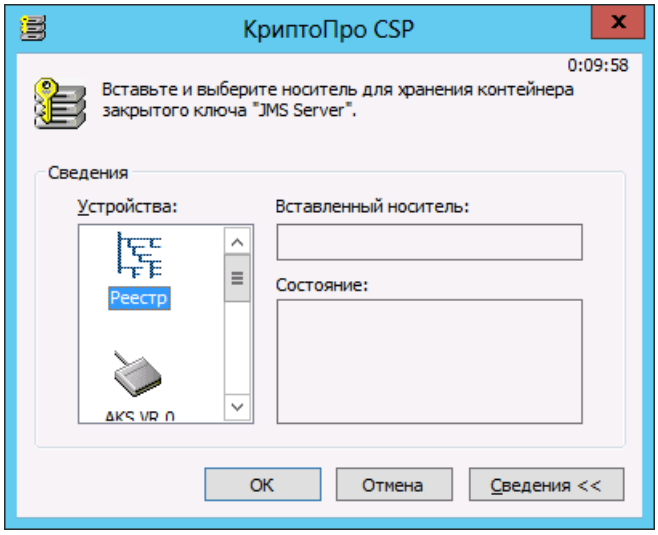


Рис. 616 – Выбор носителя для хранения ключевого контейнера

8. В списке **Устройства** выберите **Реестр** и нажмите **OK**.
9. В отобразившемся окне нажмите **OK**, не устанавливая пароль.
10. В окне настроек КриптоПро CSP нажмите **OK**.

20.1.2 Экспорт сертификата из хранилища сертификатов пользователя

1. В меню **Пуск** выберите **Все программы -> КРИПТО-ПРО -> Сертификаты**.

Отобразится следующее окно.

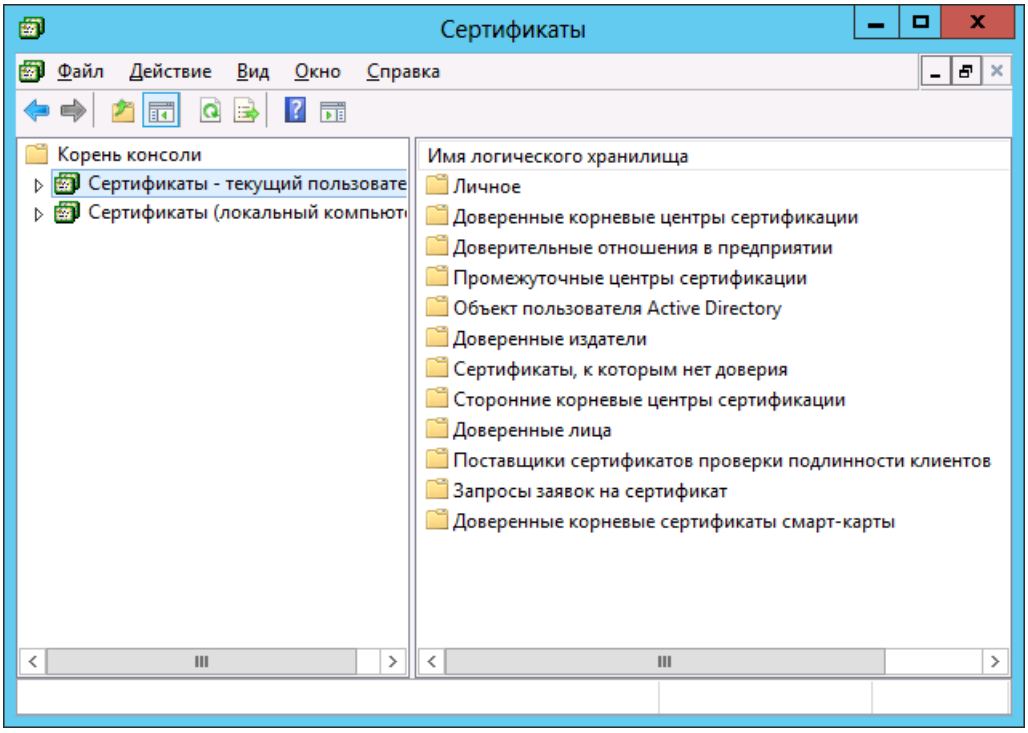


Рис. 617 – Сертификаты КриптоПро УЦ

2. В левой части окна выберите **Сертификаты - текущий пользователь -> Личное -> Реестр -> Сертификаты**.
Окно примет следующий вид.

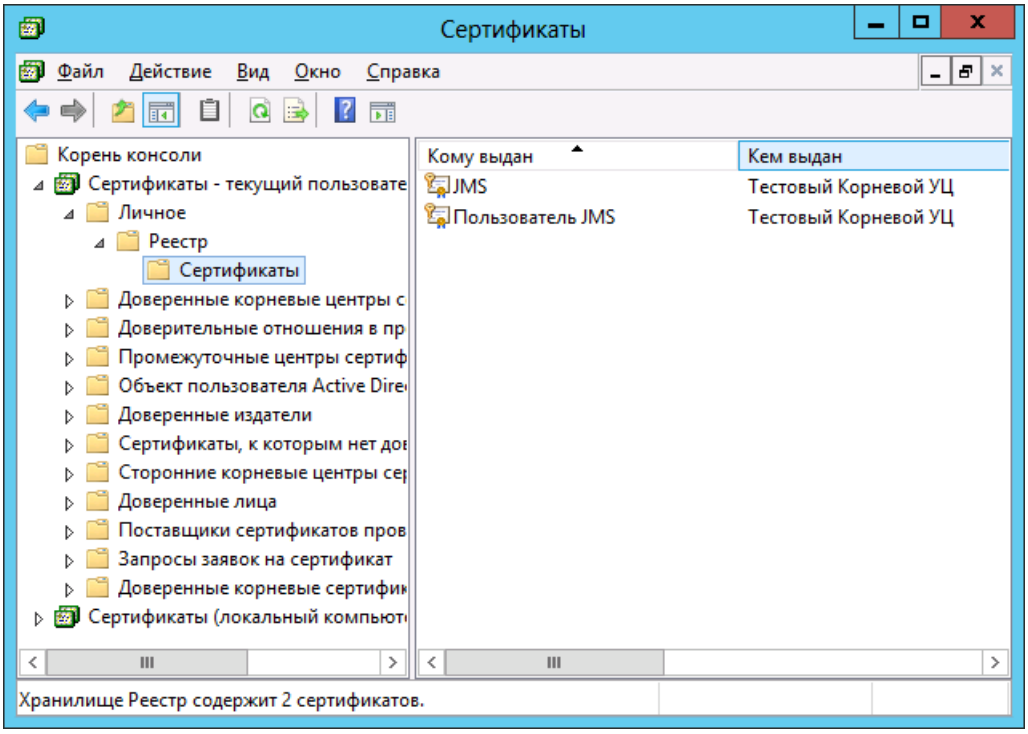


Рис. 618 – Сертификаты КриптоПро УЦ в личном хранилище пользователя

3. В правой части окна нажмите правой кнопкой на сертификате, выпущенном для JMS, и из контекстного меню выберите **Все задачи -> Экспорт**.

Отобразится следующее окно.

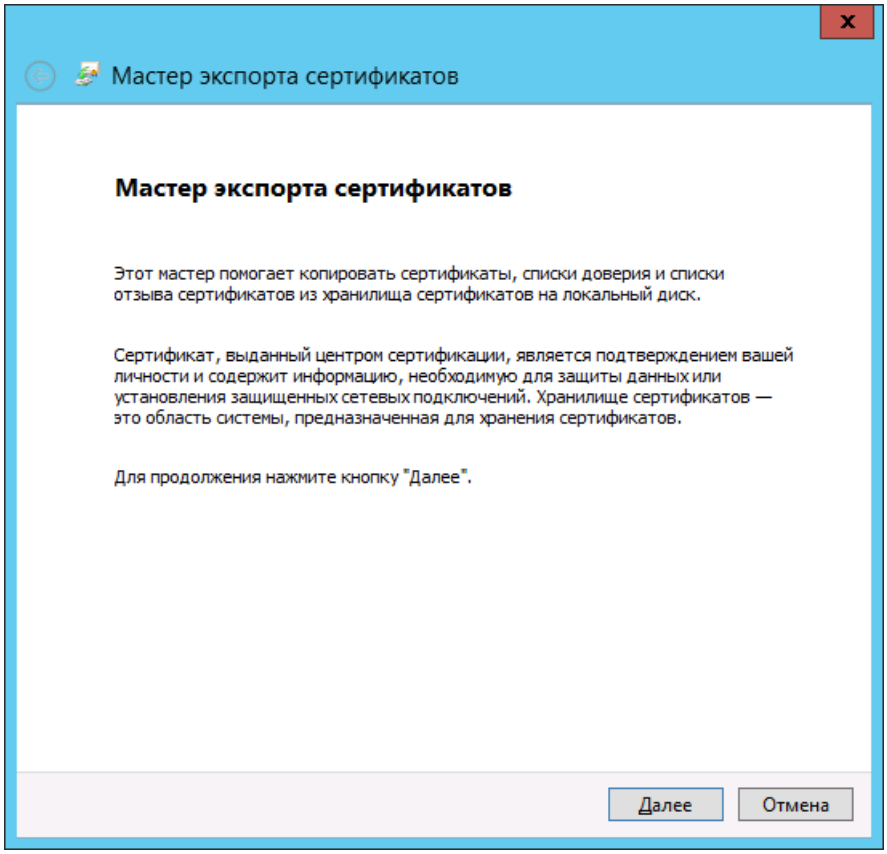


Рис. 619 – Окно приветствия мастера экспорта сертификатов

4. Нажмите **Далее**.

Отобразится следующее окно.

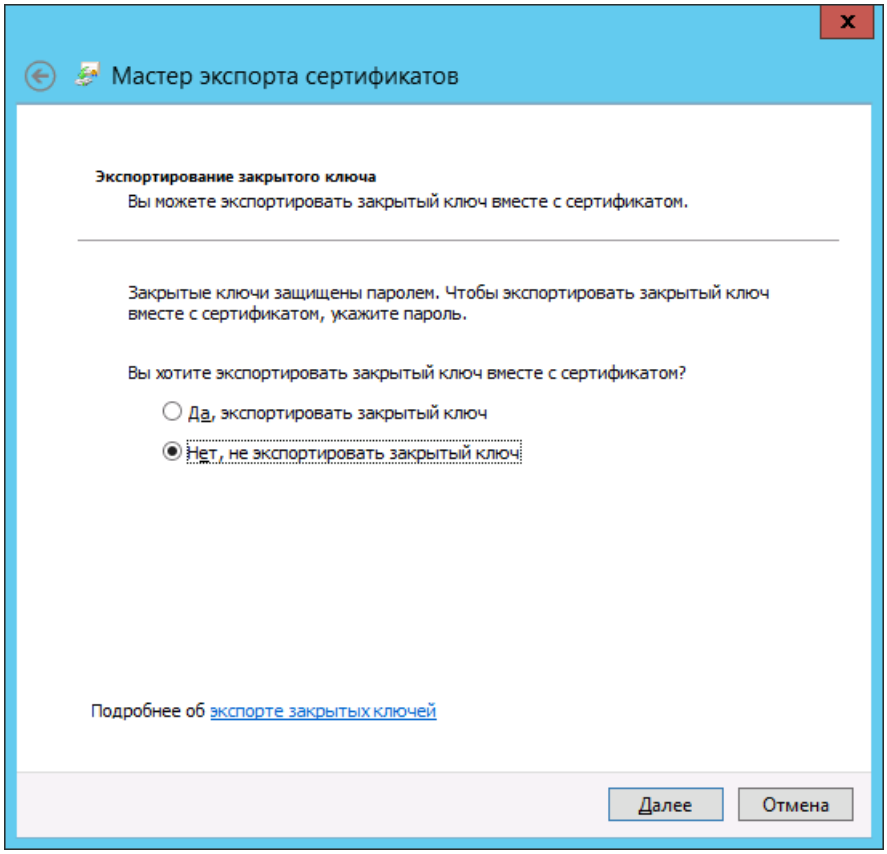


Рис. 620 – Выбор варианта экспорта сертификата

5. Выберите **Нет, не экспортировать закрытый ключ**, после чего нажмите **Далее**.

Отобразится следующее окно.

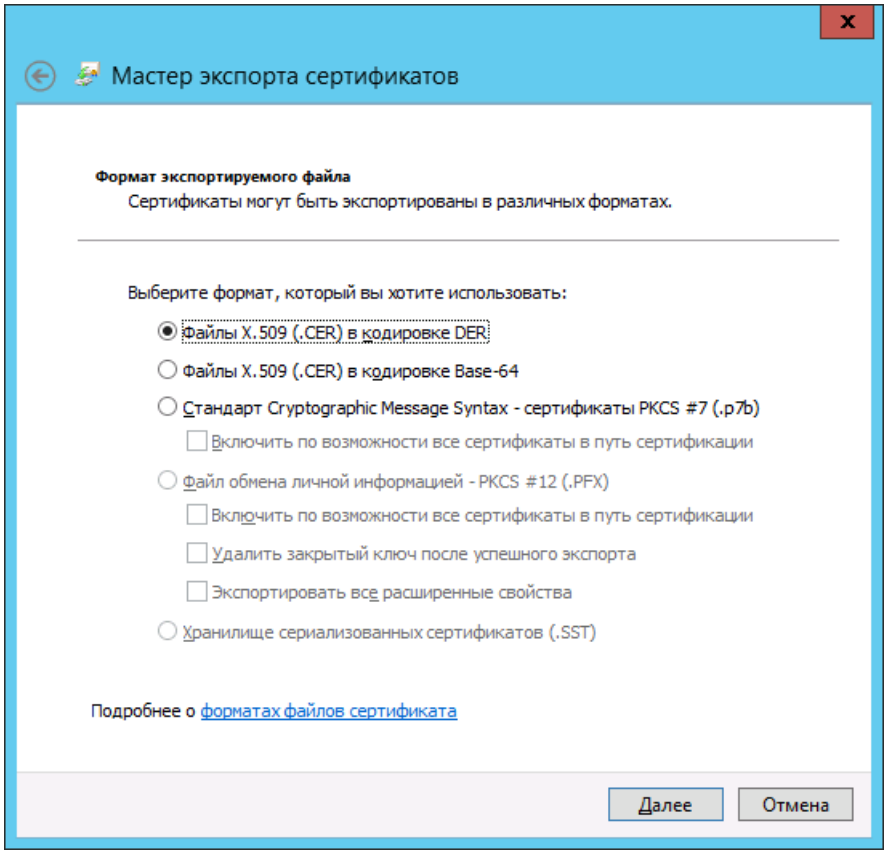


Рис. 621 – Выбор формата экспорта сертификата

6. Выберите пункт **Файлы X.509 (.CER) в кодировке DER**, после чего нажмите **Далее**.

Отобразится следующее окно.

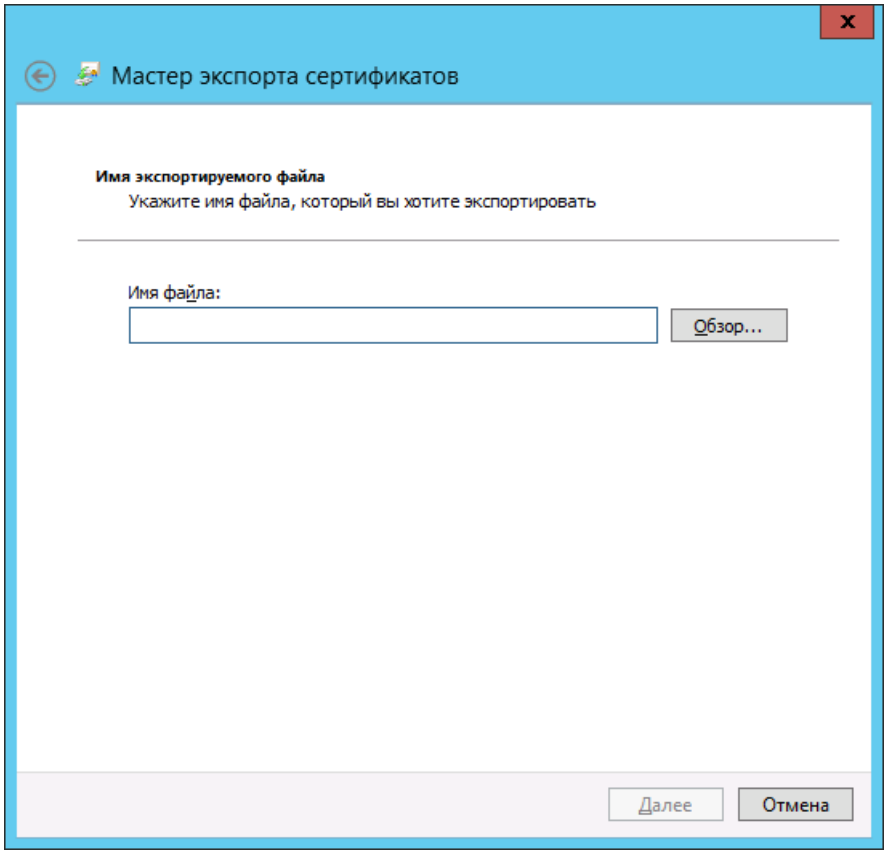


Рис. 622 – Указание пути экспорта сертификата

7. Воспользуйтесь кнопкой **Обзор**, чтобы указать путь, по которому будет сохранен файл сертификата, после чего нажмите **Далее**.

Отобразится следующее окно.

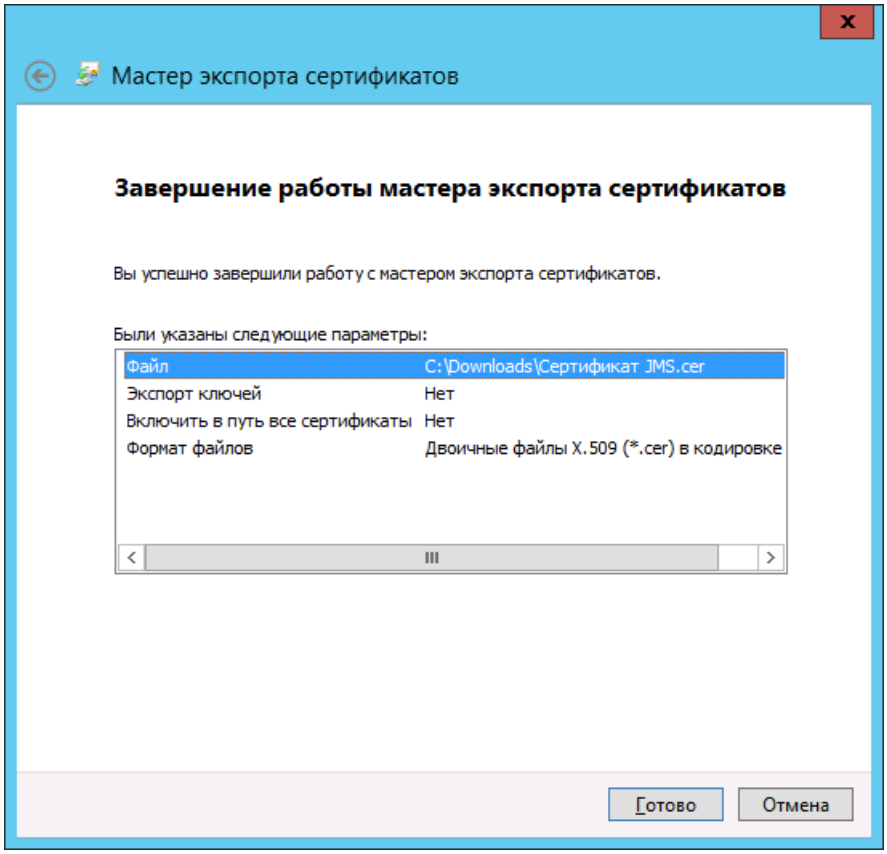


Рис. 623 – Окно завершения работы мастера экспорта сертификатов

8. Нажмите **Готово**.
9. В окне сообщения об успешном экспорте нажмите **ОК**.

20.1.3 Установка сертификата оператора КриптоПро УЦ в хранилище компьютера

Чтобы установить сертификат оператора КриптоПро УЦ в хранилища локального компьютера сервера JMS, выполните следующие действия.

1. Запустите КриптоПро CSP от имени администратора и перейдите на вкладку **Сервис**.
2. В секции **Личный сертификат** нажмите **Установить личный сертификат**.

Отобразится следующее окно.

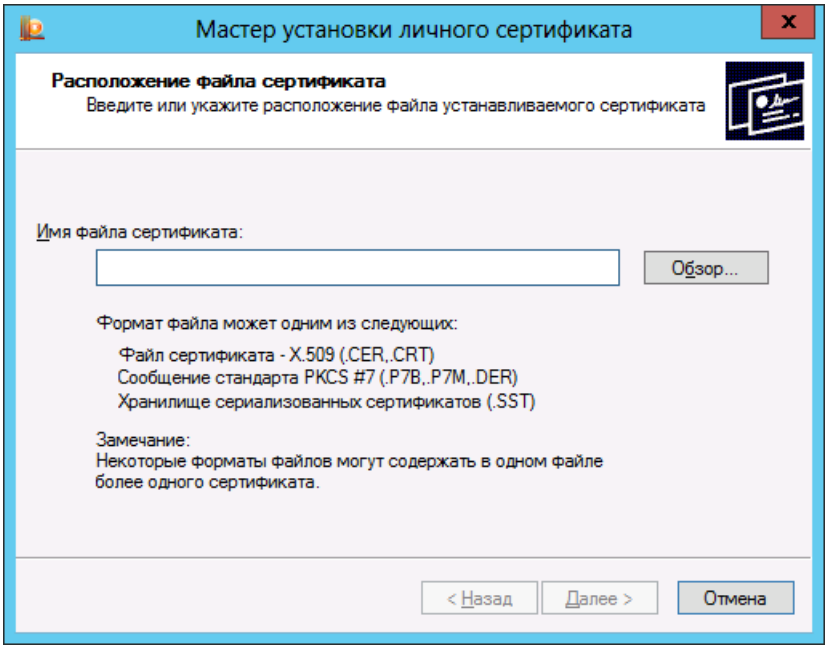


Рис. 624 – Указание пути сохранения экспортируемого сертификата

3. Воспользуйтесь кнопкой **Обзор**, чтобы указать путь к ранее экспортированному сертификату, после чего нажмите **Далее**.
   Отобразится следующее окно.

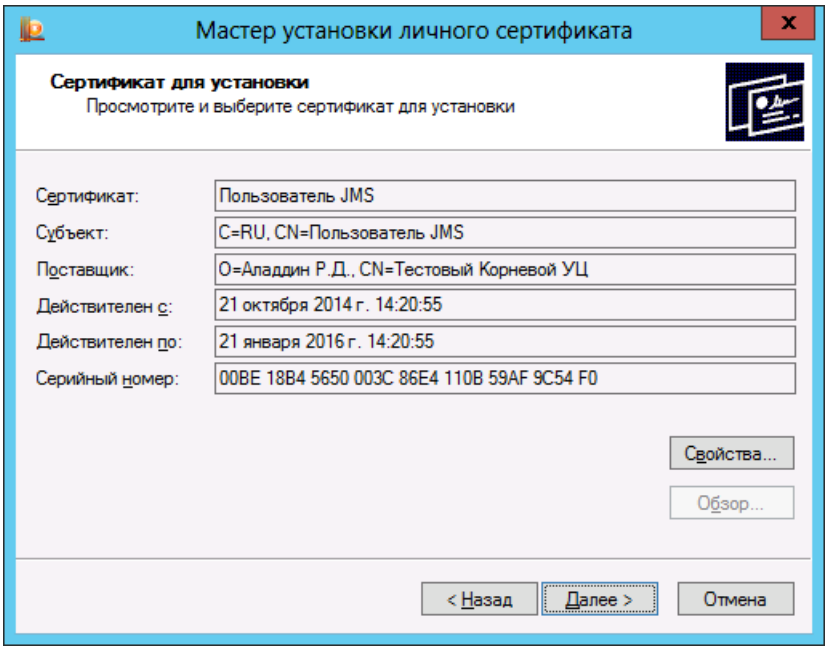


Рис. 625 – Сведения об устанавливаемом сертификате

4. Нажмите **Далее**.

Отобразится следующее окно.

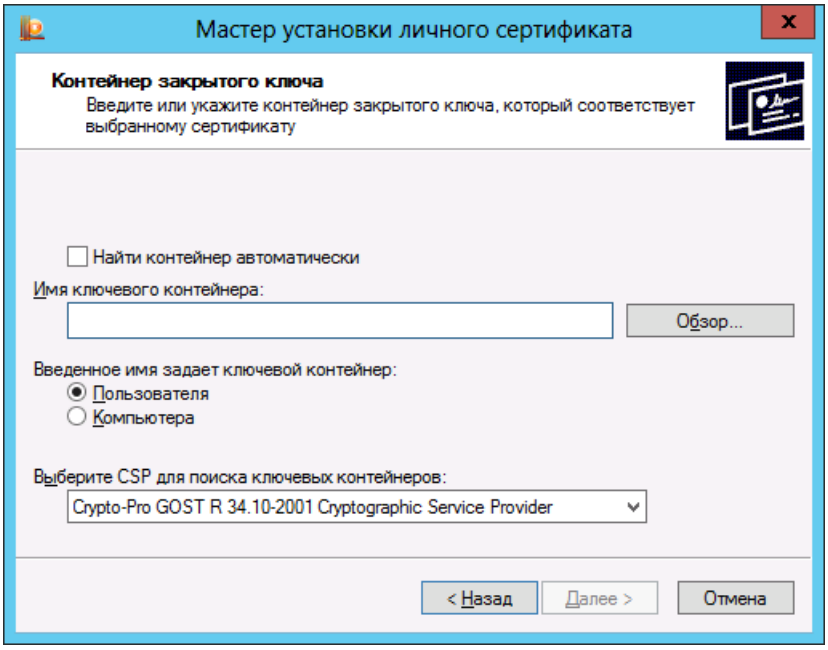


Рис. 626 – Выбор контейнера закрытого ключа, соответствующего импортируемому сертификату

5. Установите флаг **Найти контейнер автоматически**.
6. В секции **Введенное имя задает ключевой контейнер** выберите **Компьютера**, после чего нажмите **Далее**.
   Отобразится следующее окно.

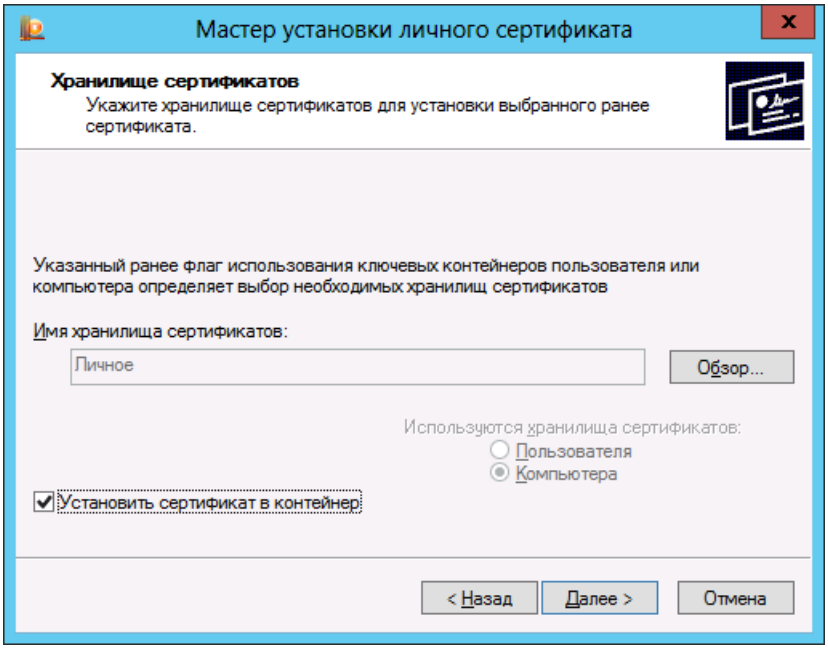


Рис. 627 – Выбор хранилища сертификатов

7. Выполните следующие настройки:

7.1. в поле **Имя хранилища сертификатов** должно значиться **Личное**;
7.2. флаг **Установить сертификат в контейнер** должен быть установлен.
7.3. Нажмите **Далее**.

Отобразится следующее окно.

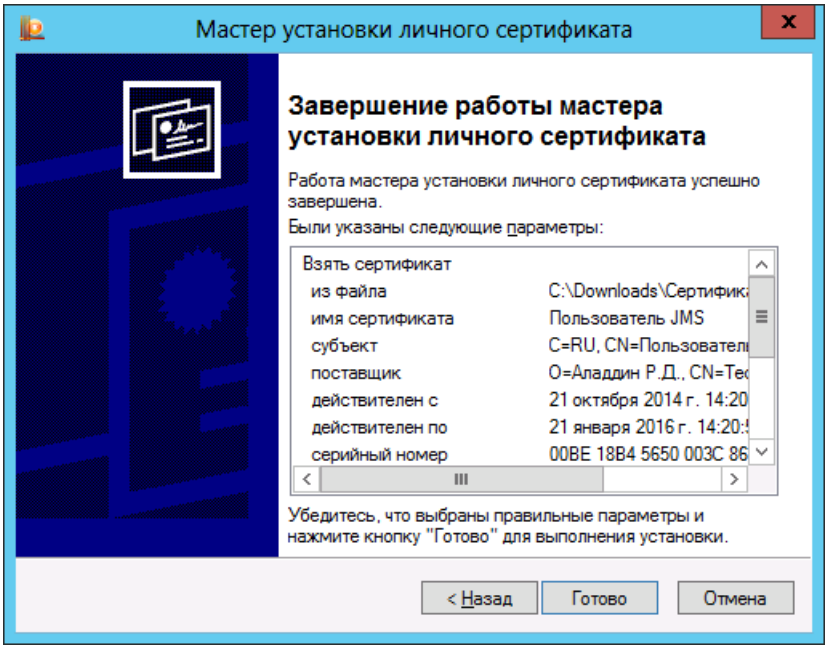


Рис. 628 – Окно завершения работы мастер установки сертификата

8. Нажмите **Готово**.
9. В отобразившемся окне введите заданный пароль для ключевого контейнера, после чего нажмите **ОК**.
10. В окне настроек КриптоПро CSP нажмите **ОК**.

Убедитесь в том, что сертификат установлен в хранилище локального компьютера. Для этого в меню Пуск выберите **Все программы -> КРИПТО-ПРО -> Сертификаты** и в отобразившемся окне выберите **Сертификаты (локальный компьютер) -> Личное -> Реестр -> Сертификаты** - сертификат должен отображаться в правой части окна. Если сертификат не отображается, выберите в панели инструментов **Действие -> Обновить**.

20.1.4 Идентификатор папки пользователей КриптоПро УЦ

1. В консоли управления центра регистрации удостоверяющего центра КриптоПро перейдите в раздел **Пользователи**.

2. В центральной части окна нажмите правой кнопкой мыши на шапке таблицы и в контекстном меню выберите **Выбор колонок** (см. рис. 629).

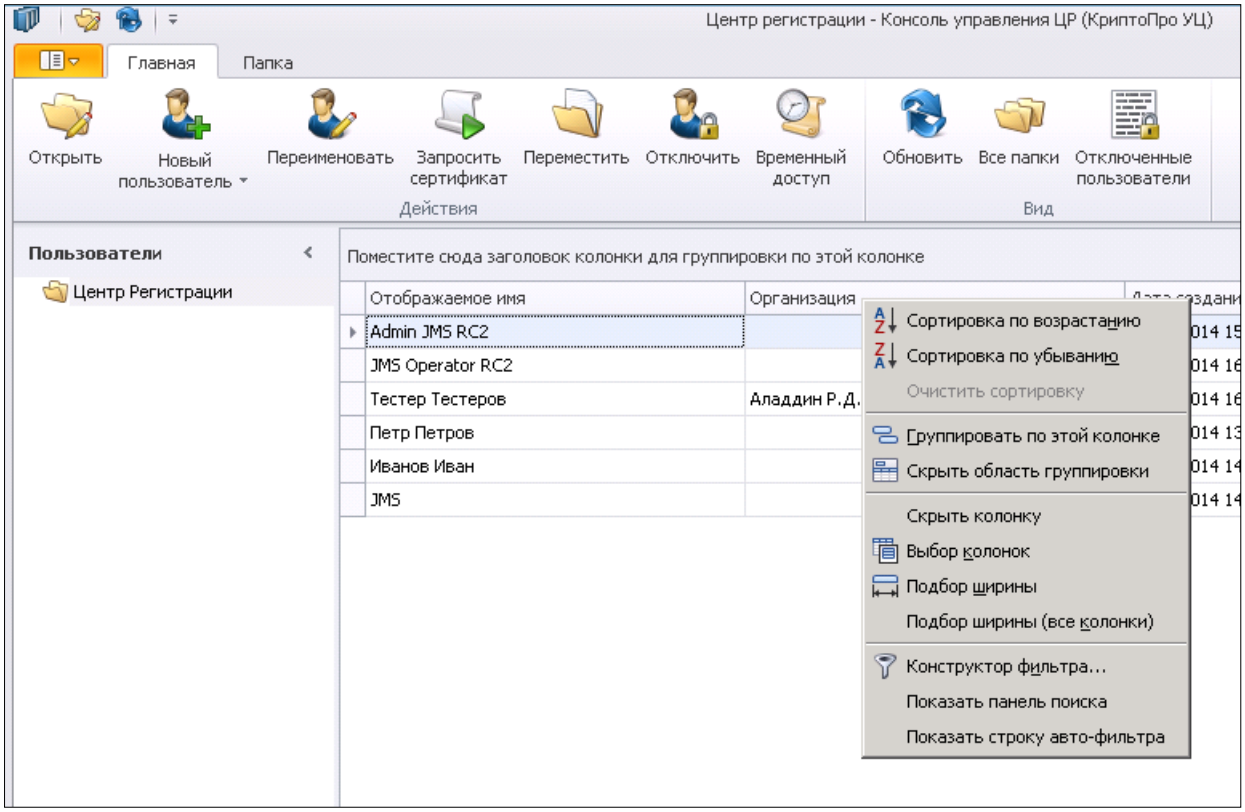


Рис. 629 – Раздел Пользователи консоли управления центра регистрации КриптоПро УЦ

Появится окно, позволяющее выбрать колонки для отображения.

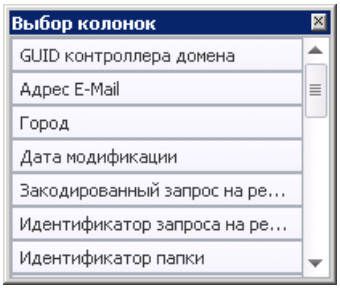


Рис. 630 – Выбор колонок для отображения

3. Выберите **Идентификатор папки** и закройте окно.

В центральной части интерфейса консоли управления центра регистрации КриптоПро УЦ отобразится колонка **Идентификатор папки**.

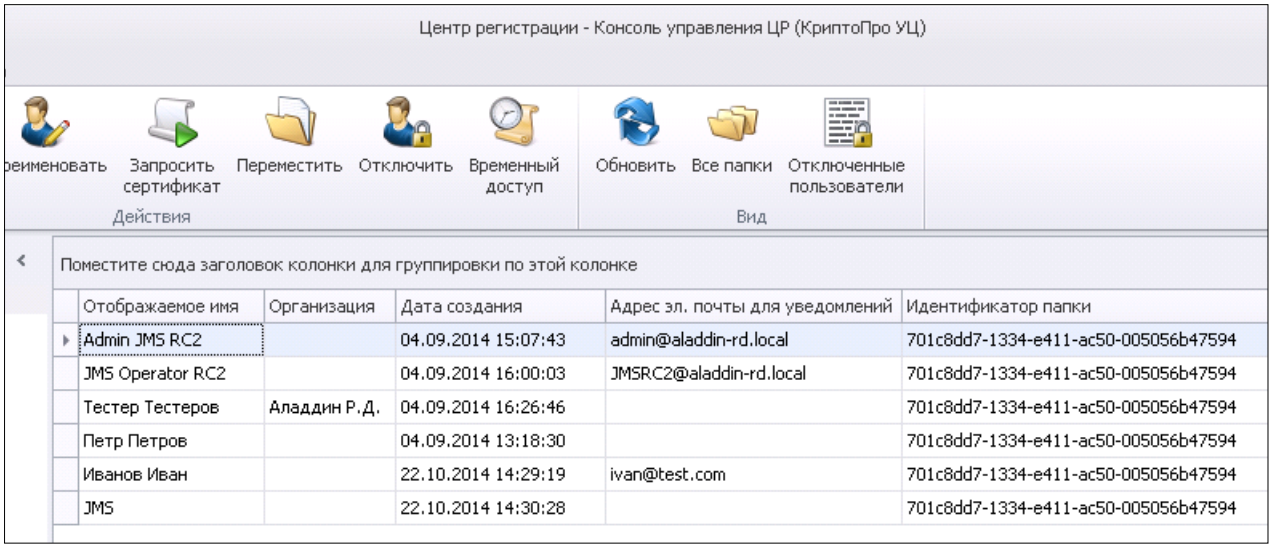


Рис. 631 – Идентификатор папки

Идентификатор папки пользователей отражается соответствующих полях профиля выпуска сертификатов КриптоПро УЦ 2.0. В текущей версии JMS он устанавливается автоматически при выборе соответствующей папки средствами графического пользовательского интерфейса.

20.2 Регистрация каталога учетных записей КриптоПро УЦ на сервере JMS

Чтобы зарегистрировать каталог учетных записей КриптоПро УЦ, выполните следующие действия.

1. Щелкните правой кнопкой на значке (Сервер JMS) в области уведомлений и выберите **Открыть**.
2. В отобразившемся окне перейдите на вкладку **Каталоги учетных записей**.

Окно примет следующий вид.

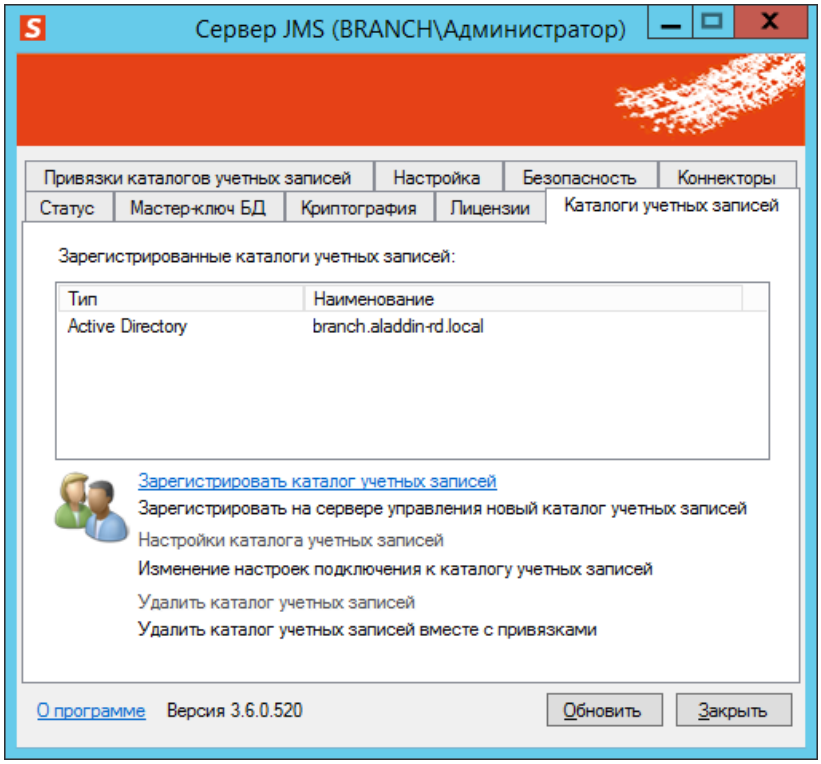


Рис. 632 – Вкладка Каталоги учетных записей

3. Нажмите на ссылке **Зарегистрировать каталог учетных записей**.
Отобразится следующее окно.

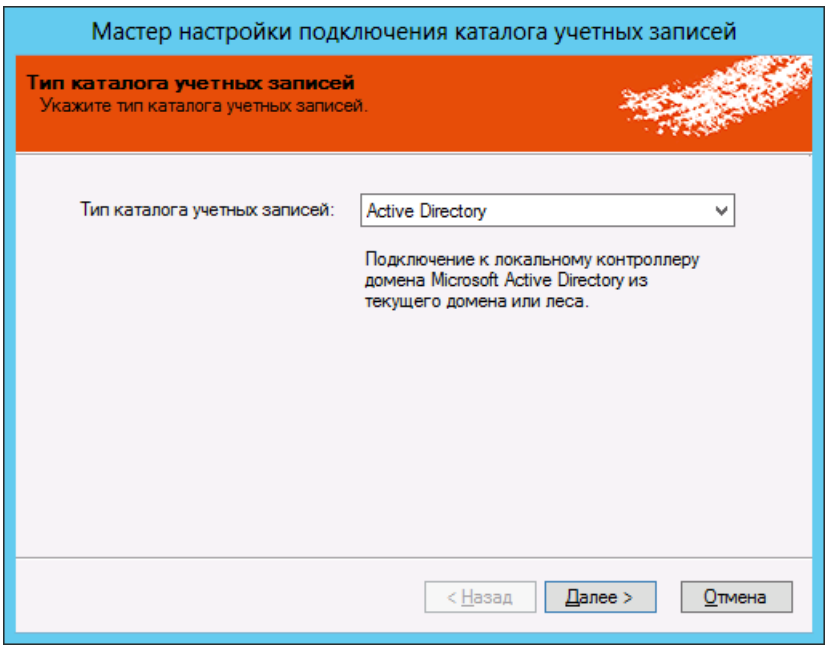


Рис. 633 – Выбор типа каталога учетных записей

4. В списке **Тип каталога учетных записей** выберите **КриптоПро УЦ 2.0** и нажмите **Далее**.

Отобразится следующее окно.

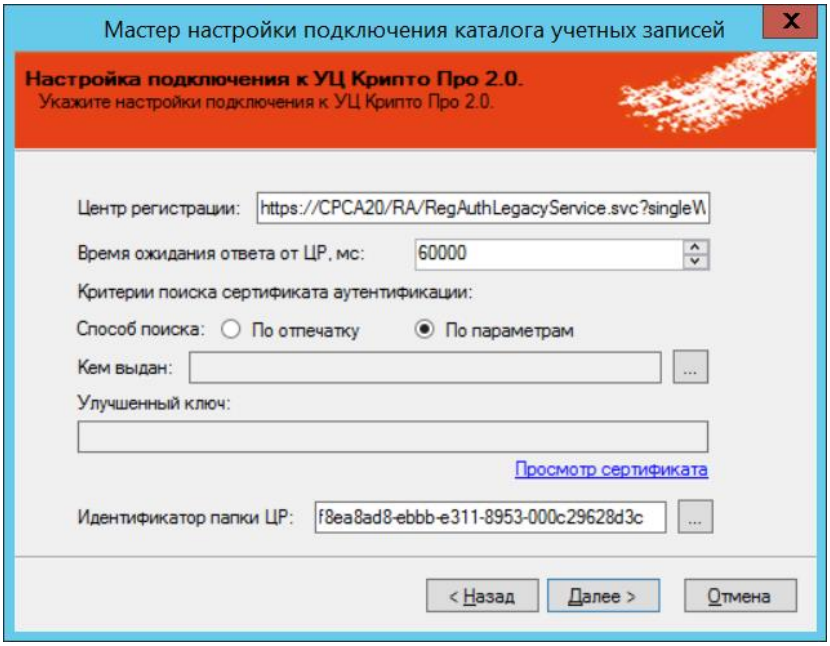


Рис. 634 – Настройка подключения к КриптоПро УЦ 2.0

5. Выполните настройку, руководствуясь табл. 135.

Табл. 135 - Настройка подключения к КриптоПро УЦ 2.0

Настройка	Описание
Центр регистрации	В строке **https://CPCA20/RA/RegAuthLegacyService.svc?singleWsdl** замените **CPCA20** именем компьютера, на котором установлен удостоверяющий центр КриптоПро 2.0.
Время ожидания ответа от ЦР	Установите время (в миллисекундах) ожидания ответа от центра регистрации удостоверяющего центра КриптоПро 2.0 или оставьте значение по умолчанию.
Критерии поиска сертификата аутентификации	В данной секции устанавливается сертификат, используемый для аутентификации сервера JMS при взаимодействии с КриптоПро УЦ.
Способ поиска	Выберите **По отпечатку** и воспользуйтесь кнопкой … (Обзор), чтобы выбрать сертификат оператора КриптоПро, установленный в хранилище компьютера на сервере JMS. (Подробно о выпуске и установке такого сертификата см. в разделе «Подготовительные действия», с. 628)
Идентификатор папки ЦР	Выберите папку центра регистрации КриптоПро УЦ, из которой будут копироваться/синхронизироваться учетные записи пользователей, зарегистрированных в КриптоПро УЦ. Для этого нажмите … (Обзор), выберите необходимую папку и нажмите **OK**. В поле отобразится идентификатор выбранной папки.

1. Нажмите **Далее**.

Отобразится следующее окно.

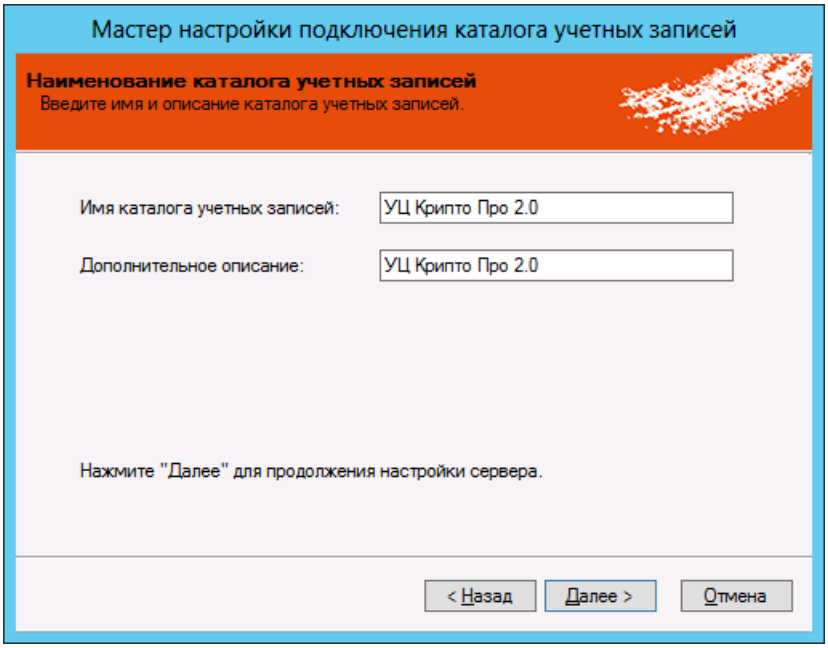


Рис. 635 – Наименование каталога учетных записей

2. Измените значения полей на нужные или оставьте значения по умолчанию, после чего нажмите **Далее**.
   Отобразится следующее окно.

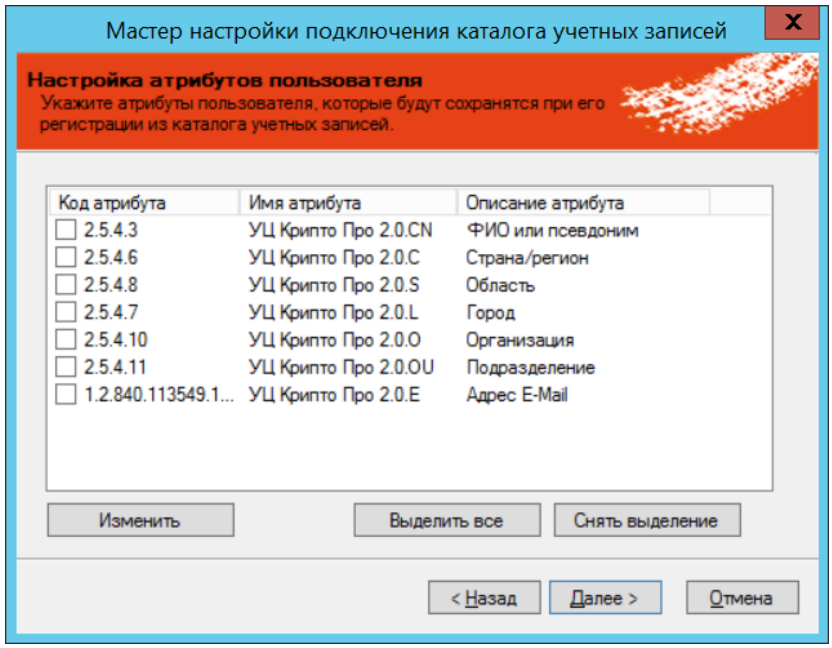


Рис. 636 – Настройка атрибутов пользователя

3. Укажите атрибуты пользователя, которые будут сохранены в базе данных JMS при регистрации из каталога учетных записей КриптоПро УЦ, после чего нажмите **Далее**.

После этого произойдет перезапуск сервера управления JMS.

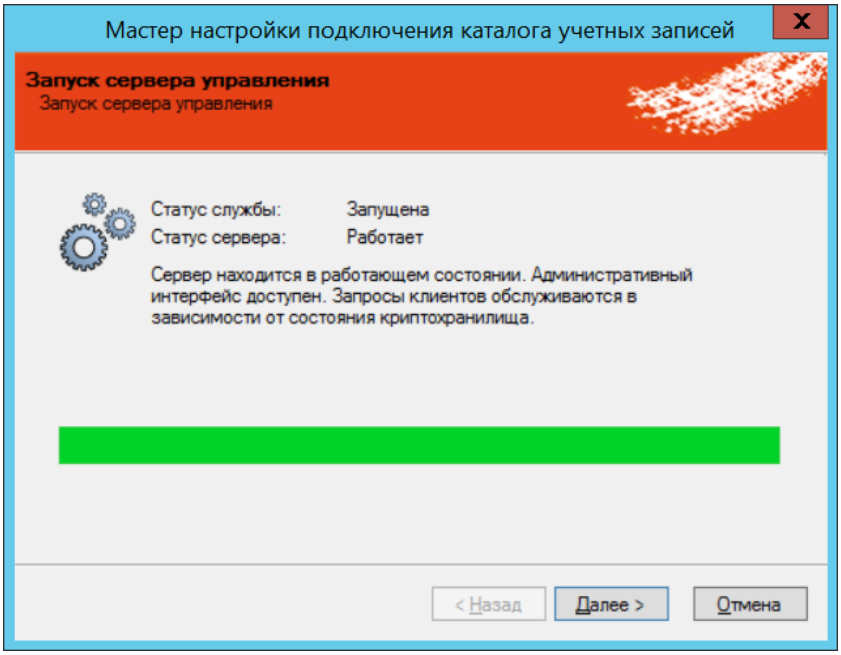


Рис. 637 – Перезапуск сервера управления JMS

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

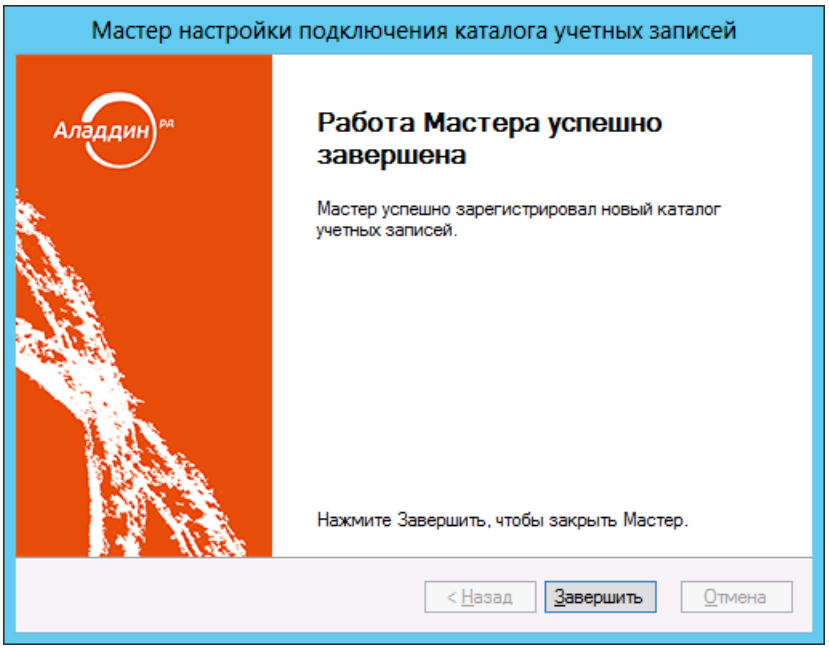


Рис. 638 – Окно завершения работы мастера подключения каталога учетных записей

5. Нажмите **Завершить**.

Новый каталог учетных записей отобразится на вкладке **Каталоги учетных записей** окна управления сервером JMS.

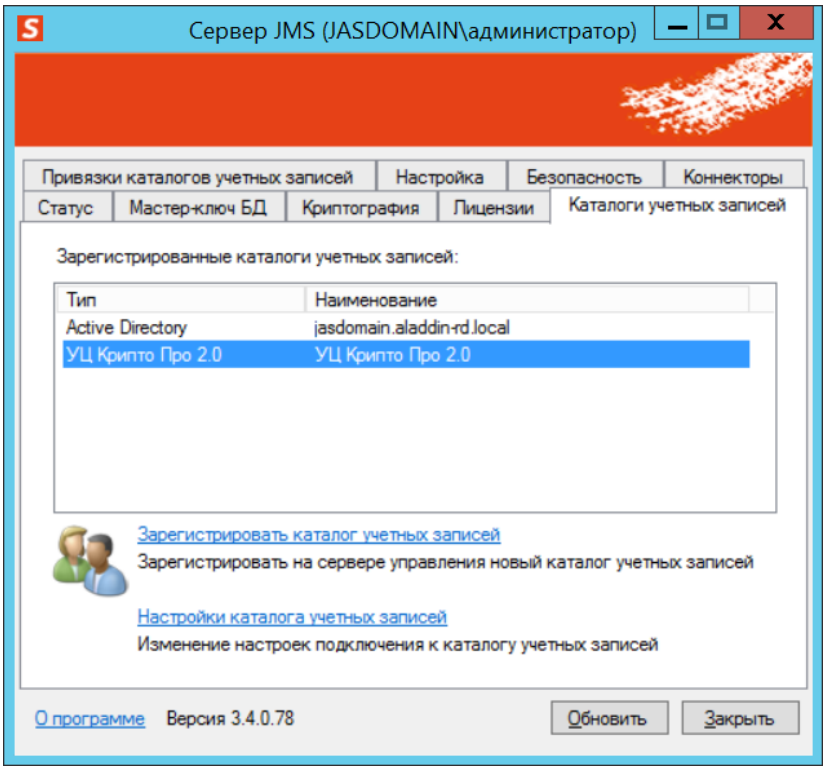


Рис. 639 – Каталог учетных записей КриптоПро УЦ 2.0 зарегистрирован

Каталог учетных записей также будет отображаться в окне консоли управления JMS (для этого консоль необходимо перезагрузить).

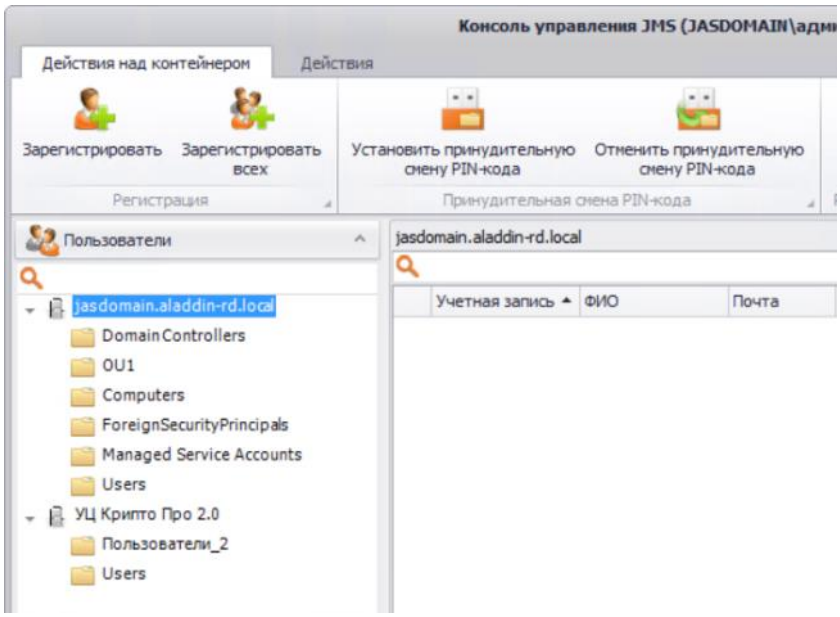


Рис. 640 – Каталог учетных записей КриптоПро УЦ 2.0 отображается в консоли управления JMS

Процедура регистрации пользователей в JMS аналогична процедуре, представленной в подразделе «Регистрация пользователей в JMS», с. 36.

20.3 Настройка профиля для выпуска сертификатов в КриптоПро УЦ 2.0

1. В консоли управления JMS перейдите в раздел **Профили -> Профили**.
   Окно примет следующий вид.

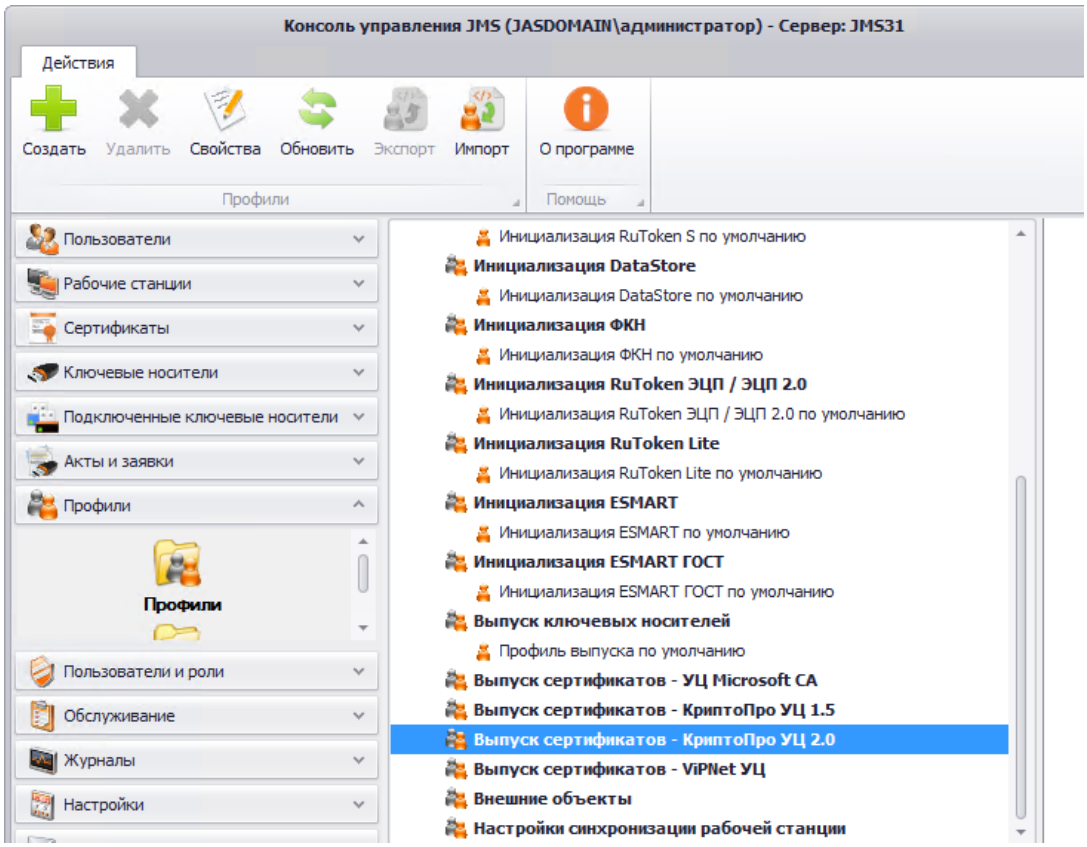


Рис. 641 – Список профилей JMS

2. В центральной части окна выберите **Выпуск сертификатов – КриптоПро УЦ 2.0**, после чего в верхней панели выберите **Создать**.

Отобразится следующее окно.

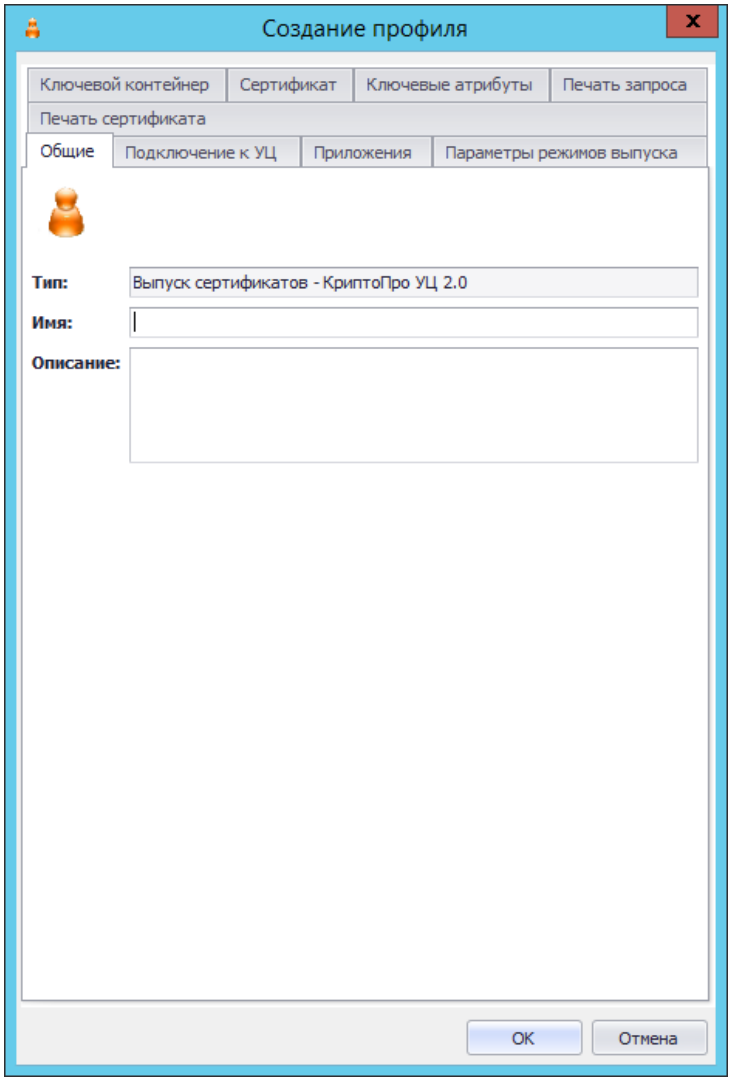
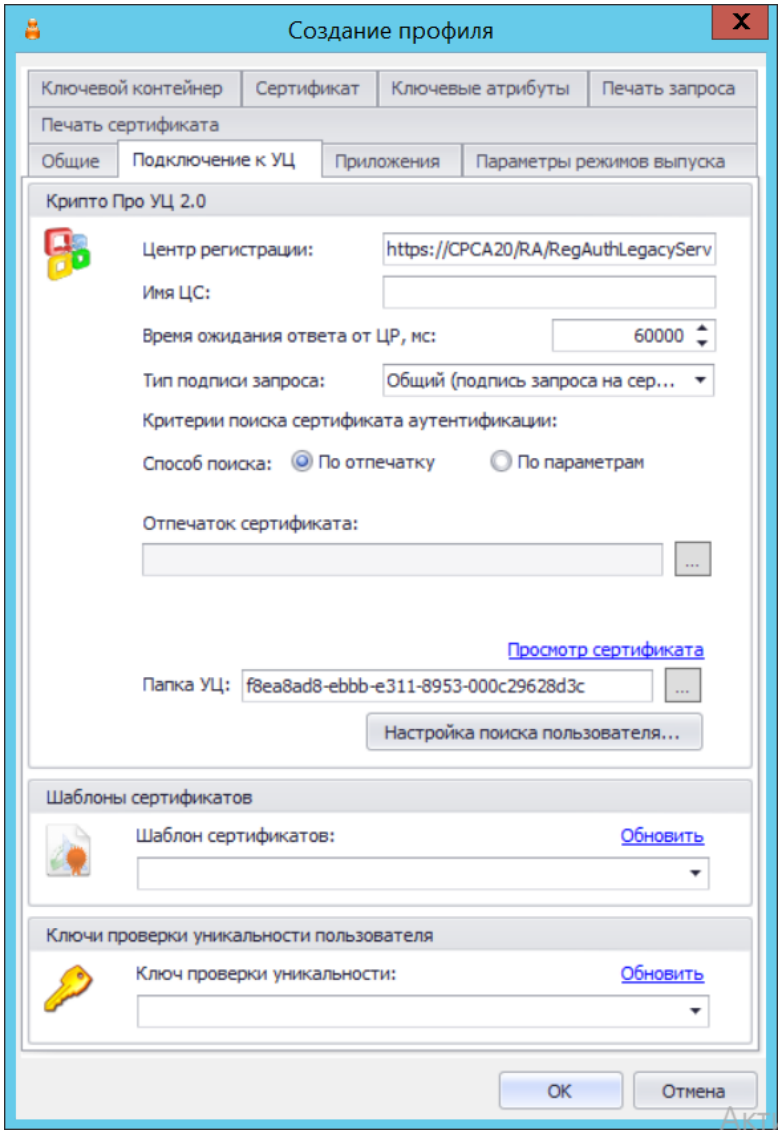


Рис. 642 - Вкладка Общие профиля выпуска сертификатов КриптоПро УЦ

3. Заполните необходимые поля и переходите на вкладку **Подключение**.

Окно примет следующий вид.



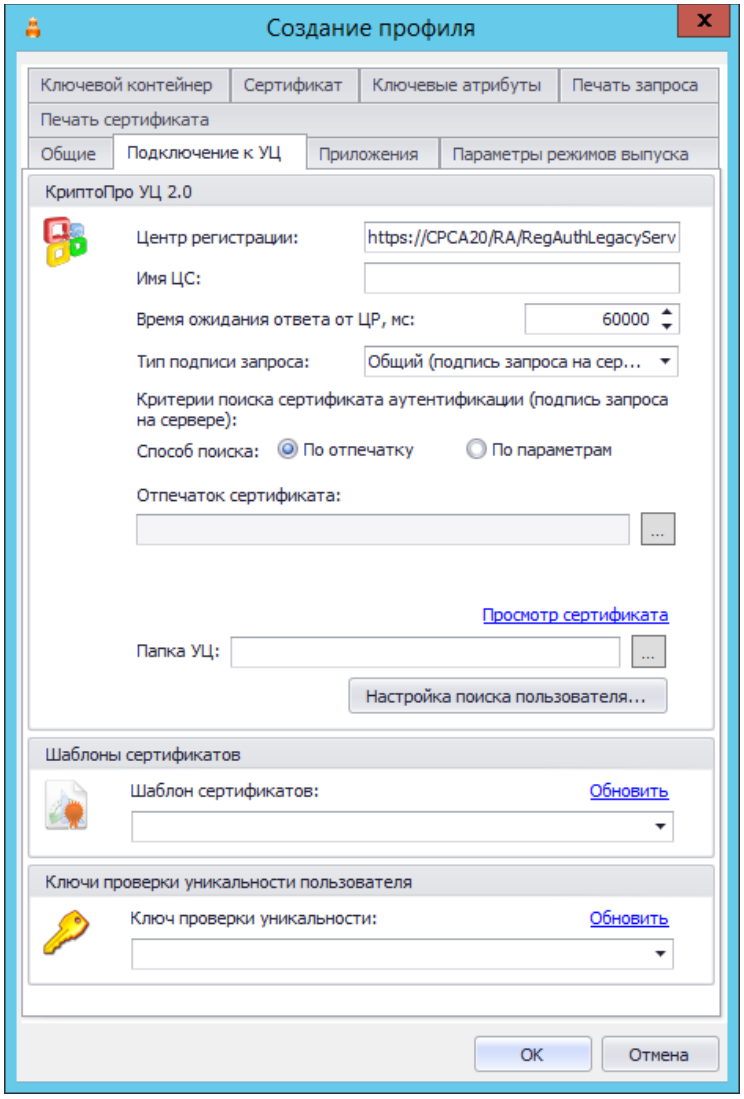


Рис. 643 – Вкладка Подключение профиля выпуска сертификатов КриптоПро УЦ

4. Выполните настройку, руководствуясь табл. 136.

Табл. 136 – Настройка параметров подключения к КриптоПро УЦ

Настройка	Описание
Центр регистрации	В строке **https://CPCA20/RA/RegAuthLegacyService.svc?singleWsdl** замените **CPCA20** именем компьютера, на котором установлен удостоверяющий центр КриптоПро 2.0.
Имя ЦС	Введите желаемое отображаемое имя центра сертификации
Время ожидания ответа от ЦР	Установите время (в миллисекундах) ожидания ответа от центра регистрации удостоверяющего центра КриптоПро 2.0 или оставьте значение по умолчанию.

Настройка	Описание
Тип подписи запроса	Выберите тип подписи запрос на сертификат: • **Общий (подпись запроса на сервере)** – в качестве оператора Центра регистрации КриптоПро выступает сервер JMS, и соответствующий сертификат КриптоПро должен быть установлен в хранилище компьютера на сервере JMS (настройка обязательна). При выборе этой опции закрытый ключ, соответствующий данному сертификату, всегда будет использоваться для подписи запроса на сертификат, независимо от того выпускается ли ключевого носитель из JMS-клиента или из консоли управления JMS; • **Частный (подпись запроса на клиенте)** – в качестве оператора Центра регистрации КриптоПро выступает администратор JMS, использующий консоль управления JMS; в этом случае сертификат оператора Центра регистрации КриптоПро может быть установлен в хранилище пользователя на компьютере, где установлена консоль управления JMS, или записан в память электронного ключа. При выборе этой опции закрытый ключ, соответствующий данному сертификату, будет использоваться только выпуске ключевого носителя из консоли управления JMS. В настоящем документе подробно рассматривается вариант, где в качестве оператора Центра регистрации КриптоПро выступает сервер JMS.
Критерии поиска сертификата аутентификации (подпись запроса на сервере)	В данной секции устанавливается сертификат, используемый для подписи запроса на сертификат, выполняемой на сервере JMS, а также для аутентификации сервера JMS при данном взаимодействии с КриптоПро УЦ. **Примечание.** В общем случае данный сертификат может отличаться от сертификата, установленного в мастере настройки подключения каталога КриптоПро УЦ (см. раздел «Регистрация каталога учетных записей КриптоПро УЦ на сервере JMS», Рис. 634, с. 644).
Способ поиска	Позволяет задать критерий поиска сертификата учетной записи JMS, возможны два варианта: • **По отпечатку**; • **По параметрам**. **Примечания:** 1. Независимо от того, настраивается профиль для единичного сервера JMS (т.е. без кластера) или для кластера JMS следует выбрить способ поиска **По отпечатку**, поскольку в кластерной конфигурации на всех узлах для подписи запроса в КриптоПро УЦ устанавливается один и тот же сертификат. Порядок развертывания кластерной конфигурации приведен в соответствующем руководстве [5]. 2. 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 будет предложены на выбор все сертификаты из личного хранилища пользователя, от имени которого запущена консоль управления. 3. При работе JMS с КриптоПро УЦ подпись запроса осуществляется на сертификате аутентификации
Папка УЦ	Выберите папку центра регистрации КриптоПро УЦ, из которой будут загружаться шаблоны сертификатов КриптоПро УЦ. Для этого нажмите … (Обзор), выберите необходимую папку и нажмите **ОК**. В поле отобразится идентификатор выбранной папки.

Настройка	Описание
Кнопка **Настройка поиска пользователя...**	Кнопка служит для детализации метода поиска пользователя в папках УЦ. При нажатии на кнопу предлагаются дополнительные параметры: • **Искать во вложенных папках** – установите флаг в случае, если поиск пользователя следует осуществлять в папках, являющихся вложенными по отношению к папке, идентификатор которой указан либо в поле **Папка УЦ** (выше), либо в поле **Папка поиска** (если задана, см. ниже) • **Использовать отдельную папку для поиска пользователей** – включите флаг в случае, если папка для поиска пользователей доложна отличаться от папки, указанной в поле **Папка УЦ** (выше); • **Папка поиска** – указывается идентификатор папки для поиска пользователей (в случае если искомый пользователь в указанной папке не будет найден, в данном УЦ будет создан новый пользователь).  **Примечание.** Поиск пользователя в РЦ КриптоПро УЦ осуществляется перед выпуском сертификата с целью принятия решения – выпускать сертификат для уже зарегистрированного в КриптоПро УЦ пользователя, либо данного пользователя необходимо предварительно создать в РЦ КриптоПро УЦ. Поиск пользователя осуществляется по уникальному идентификатору его учетной записи. В случае КриптоПро УЦ 2.0 такой уникальный идентификатор создается на основе параметра **Ключ проверки уникальности пользователя** (см. ниже).
Шаблон сертификатов	Нажмите на ссылке **Обновить** - если данные подключения были введены верно, в списке Шаблон сертификатов можно будет выбрать шаблон КриптоПро УЦ, по которому будут выпускаться сертификаты для пользователей JMS.  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.
Ключ проверки уникальности пользователя	Выберите идентификатор *ключа проверки уникальности пользователя* (идентификатор набора атрибутов пользователя в ЦР КриптоПро УЦ, используемых в качестве ключа проверки уникальности пользователя. По умолчанию – *Все атрибуты*, подробнее см. Руководство по эксплуатации КриптоПро УЦ). Для этого в раскрывающемся списке выберите необходимый ключ

5. Перейдите на вкладку **Приложения** и отметьте комбинации приложений, на которые будет распространяться профиль.
6. Перейдите на вкладку **Параметры режимов выпуска**.

Окно примет следующий вид.

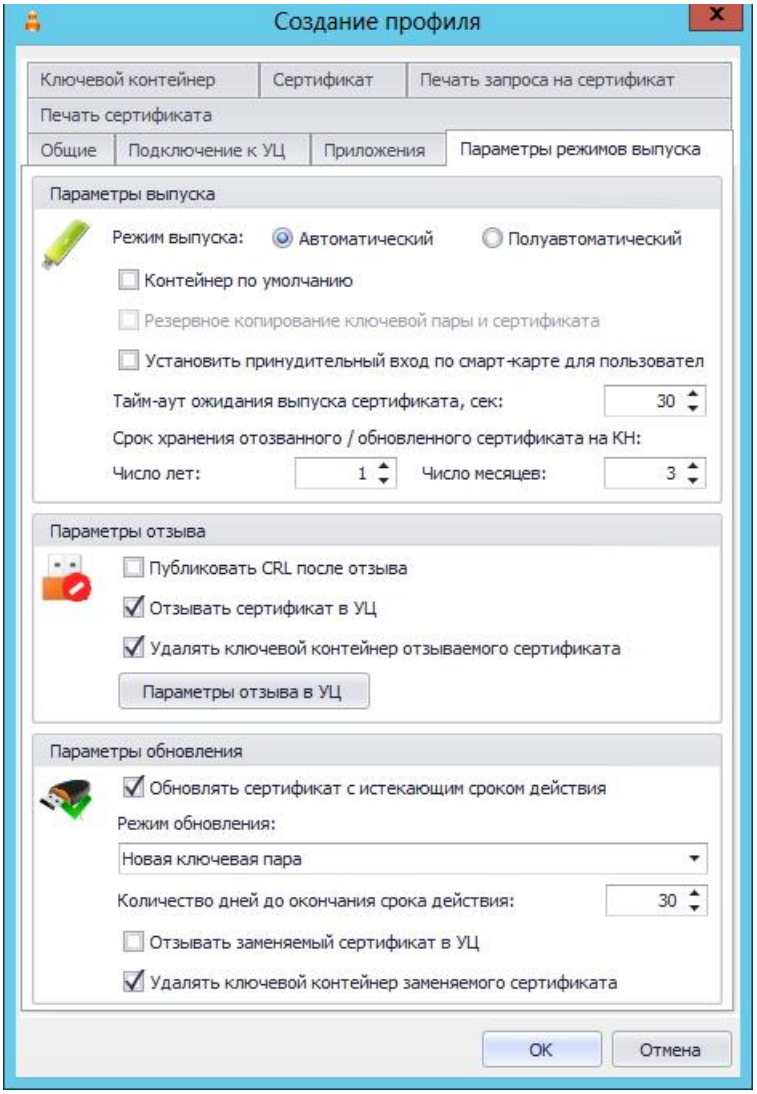


Рис. 644 – Вкладка Выпуск профиля выпуска сертификатов КриптоПро УЦ

7. Выполните настройку, руководствуясь табл. 137.

Табл. 137 – Настройка выпуска сертификатов

Секция	Настройка	Описание
Параметры выпуска	**Режим выпуска**	Позволяет выбрать из двух режимов: • **Автоматический** - этот режим следует использовать, если в удостоверяющем центре включена настройка автоматического одобрения запросов на сертификат - выпуск сертификата посредством JMS происходит в один этап; • **Полуавтоматический** - этот режим следует использовать, если в удостоверяющем центре включена настройка ручного одобрения запросов на сертификат - в этом случае сначала необходимо выпустить электронный ключ, одобрить запрос в удостоверяющем центре, после чего произвести синхронизацию электронного ключа.

Секция	Настройка	Описание
	Контейнер по умолчанию	Если данный флаг установлен, созданный в процессе выпуска электронного ключа ключевой контейнер будет помечен как контейнер по умолчанию.
	Резервное копирование ключевой пары и сертификата	Эта настройка позволяет при выпуске электронного ключа создавать резервную копию ключей и сертификатов, которая будет храниться в базе данных JMS.
	Установить принудительный вход по смарт-карте для пользователя	При выпуске электронного ключа в настройках профиля пользователя будет установлена необходимость использования смарт-карты (электронного ключа) для входа в домен.
	Тайм-аут ожидания выпуска сертификата	Время ожидания при выпуске сертификата (в секундах).
	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 электронного ключа», с. 88); • при отмене привязки *профиля выпуска сертификата*, применявшегося к данному электронному ключу (см. «Привязка профилей», с. 296), в том числе и при удалении профиля; • при отзыве сертификата средствами JMS (см. раздел «Операции с сертификатами», с. 50); • при отзыве сертификата 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.
	Удалять ключевой контейнер	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

Секция	Настройка	Описание
		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 отзыва в УЦ	Нажатие на кнопку отображает окно, в котором можно настроить параметры отзыва сертификата в удостоверяющем центре: • **Создавать запрос на отзыв** - если флаг установлен, при отзыве электронного ключа в удостоверяющий центр будет подаваться запрос на отзыв сертификата соответствующего пользователя; • **Подтверждать запрос на отзыв** - если флаг установлен, при отзыве электронного ключа в удостоверяющем центре будет одобряться запрос на отзыв сертификата соответствующего пользователя.
Параметры обновления	**Обновлять сертификат с истекшим сроком действия**	Если эта настройка включена, сертификат пользователя с истекающим сроком действия будет обновляться по выполнении процедуры синхронизации электронного ключа. Период, когда необходимо обновление задается настройкой **Количество дней до окончания срока действия**.
	Режим обновления	Обновление возможно только в режиме создания новой ключевой пары.
	Количество дней до окончания срока действия	Эта настройка позволяет установить, за сколько дней до истечения срока действия сертификата необходимо выполнить его обновление. Обновление происходит по выполнении процедуры синхронизации электронного ключа.
	Отзывать заменяемый сертификат в УЦ	Если флаг установлен, заменяемый сертификат будет отозван в удостоверяющем центре КриптоПро.
	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**).

8. Перейдите на вкладку **Ключевой контейнер** и **в**ыполните настройки аналогично настройкам профиля выпуска сертификатов MSCA (см. Табл. 34, с. 218).

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

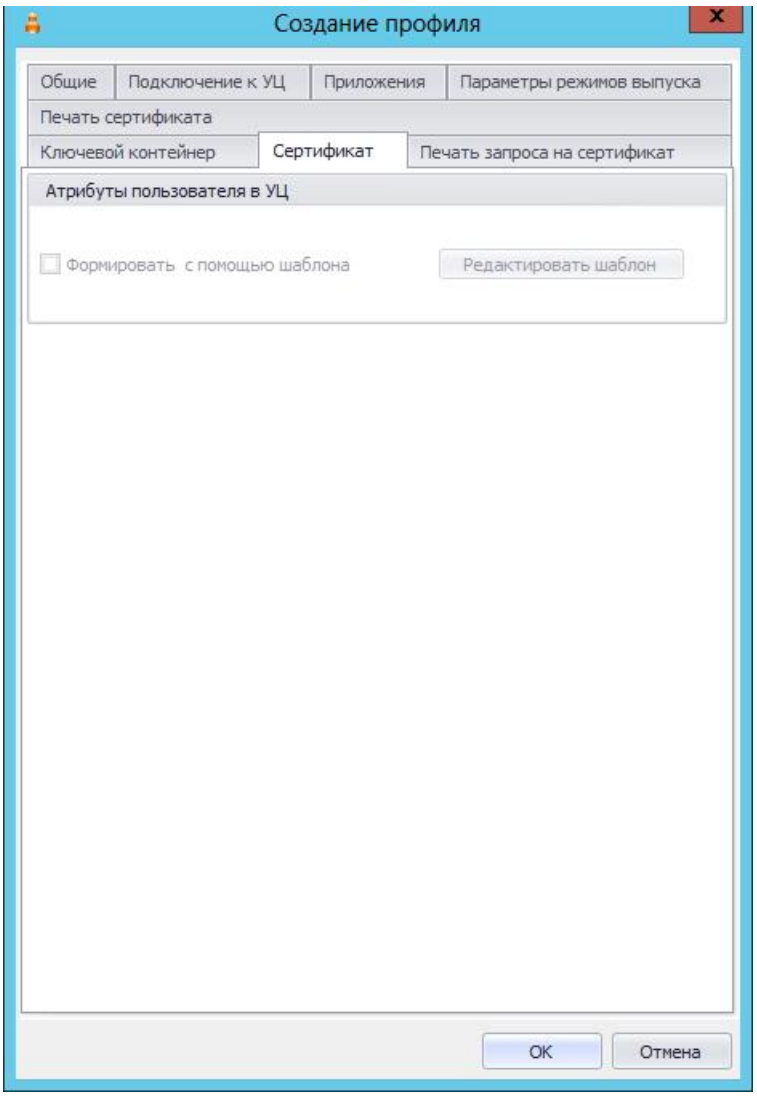


*Рис. 645 – Вкладка **Сертификат***

10. Если вы хотите отредактировать шаблон атрибутов пользователя, щелкните на кнопке **Редактировать шаблон**. (В противном случае нажмите **OK** для завершения настройки профиля.)

Отобразится следующее окно.

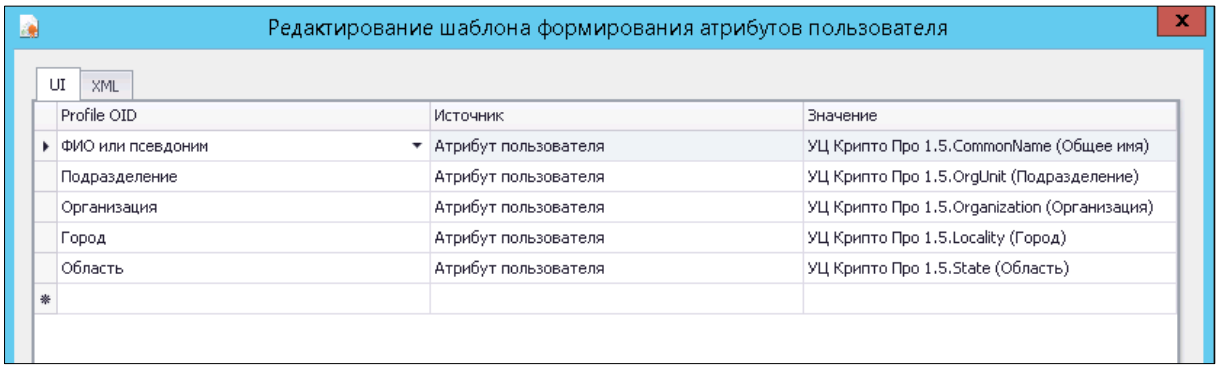


Рис. 646 – Редактирования шаблона формирования атрибутов пользователя

11. Выполните настройку, руководствуясь табл. 138.

Табл. 138 – Шаблон формирования атрибутов пользователя

Столбец	Описание
Profile OID	Позволяет выбрать OID атрибута пользователя.
Источник	Список содержит два пункта: • **Атрибут пользователя** – в имени субъекта будут использоваться значения из КриптоПро УЦ, выбранные в столбцах **OID** и **Значение**; • **Константа** – позволяет вручную ввести значение в столбце **Значение**.
Значение	Позволяет указать значение атрибута, которое будет использоваться в качестве значения атрибута пользователя.

12. Перейдите на вкладку **Ключевые атрибуты** и выполните настройки аналогично настройкам одноименной вкладки в профиле выпуска сертификатов MSCA (см. раздел «Настройки профиля выпуска сертификатов в центре сертификации Microsoft», с. 209).
13. При необходимости, выполните настройку печати документов (вкладки **Печать запроса** на сертификат и **Печать сертификата**) при выпуске электронного ключа (подробнее о настройке Шаблона печатной формы см. «Настройка параметров печати при выпуске объектов JMS», с. 304).
14. Последовательно нажмите **ОК**, чтобы закрыть окно шаблона атрибутов пользователя и окно настройки профиля для выпуска сертификатов в КриптоПро УЦ 2.0.

Приложения

Приложение 1. Миграция из SafeNet Authentication Manager

JMS позволяет импортировать данные о пользователях и электронных ключах из системы учета аппаратных и программных средств аутентификации SafeNet Authentication Manager (SAM) версий 8.0, 8.0 SP2, 8.0 SP3, 8.2. Это возможно, если SAM и JMS расположены в одном домене Windows.

Процедура миграции выполняется в несколько этапов. Сначала необходимо экспортировать данные о пользователях и электронных ключах из SAM, после чего выполнить процедуру импорта в JMS. Для этих целей используются специальные утилиты экспорта-импорта, которые вы можете получить, обратившись в техническую поддержку АО «Аладдин Р. Д.».

В таблице ниже представлено описание этих утилит.

Табл. 139 – Утилиты миграции данных из SAM

Тип утилиты	Файлы утилиты	Описание
Утилита экспорта из SAM	AladdinJMS.SamTokenExport.exe	Исполняемый файл утилиты.
	AladdinJMS.SamTokenExport.exe.config	Файл конфигурации утилиты.
Утилита импорта в JMS	AladdinJMS.ImportTool.exe	Исполняемый файл утилиты.
	AladdinJMS.ImportTool.exe.config	Конфигурационный файл утилиты.
	AladdinJMS.ImportLogic.dll	Динамическая библиотека утилиты.

Экспорт данных из SAM

Чтобы выполнить экспорт данных о пользователях из SAM, выполните следующие действия.

1. Поместите файлы утилиты экспорта из SAM в папку с бинарными файлами на сервере SAM (Bin). В зависимости от разрядности операционной системы эта папка расположена по следующему пути:

   - 32-битные операционные системы: **C:\Program Files\SafeNet\Authentication\SAM\x32\Bin**;
   - 64-битные операционные системы: **C:\Program Files\SafeNet\Authentication\SAM\x64\Bin**.

⚠ Папка не должна быть пустой – там должны находиться бинарные файлы SAM: исполняемые файлы и динамические библиотеки. Путь может отличаться, если на сервере SAM была установлена система Token Management System и/или eToken PKI Client. В этом случае путь по умолчанию:

32-битные системы: C:\Program Files\Aladdin\eToken\SAM\x64\Bin.

64-битные системы: C:\Program Files\Aladdin\eToken\SAM\x64\Bin.

Если стандартные пути размещения бинарных файлов SAM отсутствуют или они ведут к пустой папке, выполните поиск самостоятельно или обратитесь к администратору.

2. Из командной строки в каталоге **Bin** выполните следующую команду.

```
Aladdin.JMS.SamTokenExport.exe –target="C:\Export"
```

Здесь **C:\Export** – каталог, в который будут экспортированы данные об электронных ключах.

3. По успешном выполнении команды в командной строке отобразится строка **Export completed** (Экспорт завершен).
4. Перейдите в каталог, куда были экспортированы данные об электронных ключах (в настоящем примере это **C:\Export**).
5. В каталоге будет размещено два файла: **Tokens.xml** и **HistoryTokens.xml**. Для импорта данных об электронных ключах в JMS потребуется только файл **Tokens.xml** – переместите его на сервер JMS.

Примечание. В случае если в SAM хранятся сертификаты, выпущенные посредством КриптоПро УЦ 1.5, и требуется осуществить экспорт данных сертификатов, в параметрах командной строки при вызове утилите Aladdin.JMS.SamTokenExport.exe необходимо также указать параметр `-cpca`, например:

```
Aladdin.JMS.SamTokenExport.exe -target="C:\Export" -cpca
```

В противном случае сертификаты КриптоПро УЦ 1.5 экспортированы не будут.

Импорт данных в JMS

Чтобы импортировать данные в JMS, выполните следующие действия.

1. Разместите файлы утилиты импорта в папке сервера JMS. По умолчанию папка находится по следующему пути: **C:\Program Files\Enterprise Management System Server**.
2. Запустите утилиту импорта двойным щелчком мыши на файле **Aladdin.JMS.ImportTool.exe**.

Отобразится следующее окно.

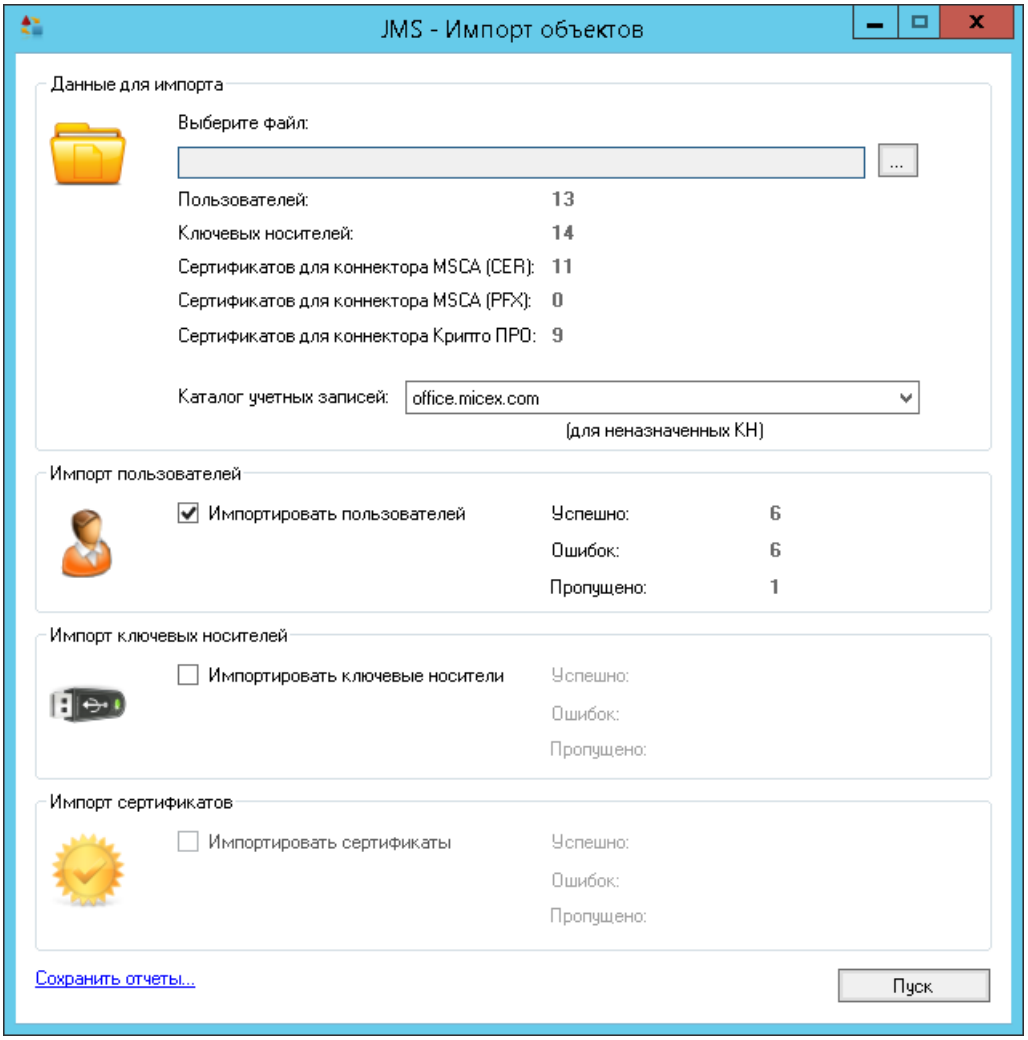


Рис. 647 – Утилита импорта данных JMS

3. В секции **Данные для импорта** выполните следующие действия:

3.1. В поле **Выберите файл** укажите путь к подготовленному файлу **Tokens.xml**, воспользовавшись кнопкой ... (Обзор).

3.2. В списке **Каталог учетных записей** выберите нужную ресурсную систему.

4. В зависимости от того, какие данные вы хотите импортировать, установите один или несколько флагов:

4.1. **Импортировать пользователей**;

4.2. **Импортировать ключевые носители**;

4.3. **Импортировать сертификаты**.

⚠ Последние два профиля должны быть привязаны к организационным единицам, содержащим пользователей, импортированных из SAM. Также, профиль инициализации должен соответствовать используемым моделям электронных ключей (приложениям электронных ключей).

5. Нажмите **Пуск**.
6. Для каждого типа объектов будет последовательно отображаться окно с информацией о ходе импорта. Всякий раз, чтобы перейти к следующему этапу импорта, нажимайте **Далее**.
7. По завершении импорты вы можете сохранить отчеты, щелкнув на ссылке **Сохранить отчеты**, или закрыть окно утилиты.

Приложение 2. Возможные проблемы и способы их решения

Профиль выпуска сертификатов центра сертификации Microsoft

Проблема

При создании профиля выпуска сертификатов MSCA список доступных шаблонов для выпуска может быть пустой, при этом сам центр сертификации доступен и работает.

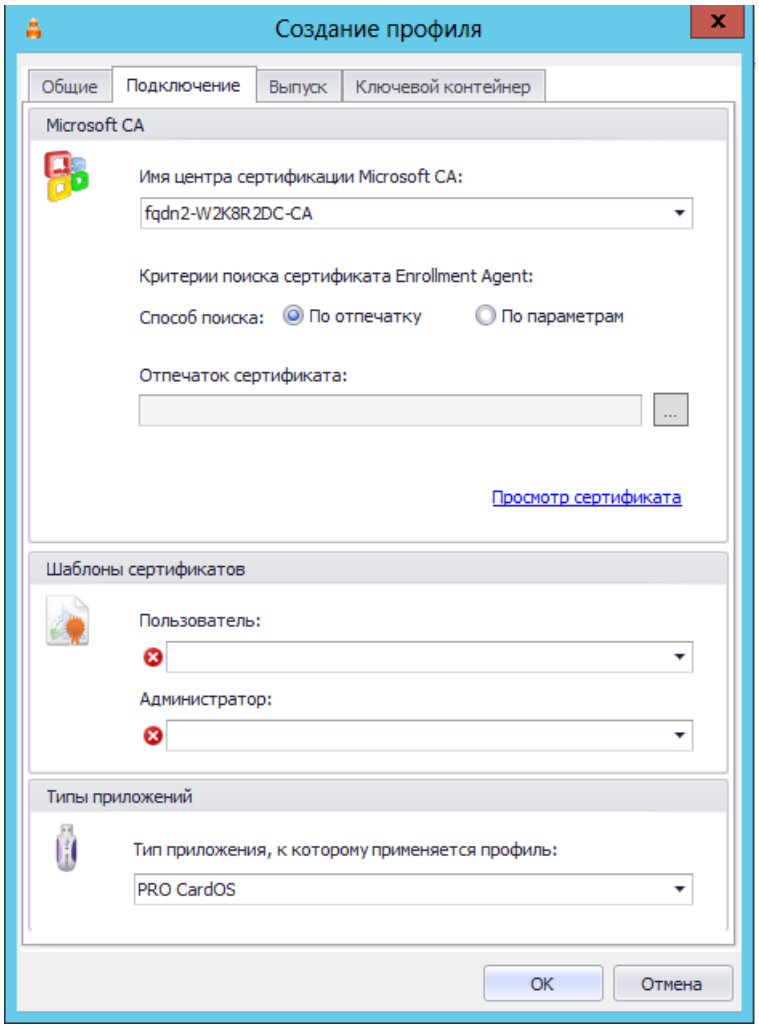


Рис. 648 – Шаблоны сертификатов не отображаются в окне настроек профиля

Эта проблема возникает в очень редких случаях, при определенных настройках инфраструктуры, когда серверная часть продукта установлена на той же станции, что и подчиненный центр сертификации, при выключенном корневом центре и при наличии леса доменов.

Решение

В свойствах подчиненного центра сертификации, на вкладке **Безопасность** для группы локальных администраторов установите флаг **Запросить сертификаты**.

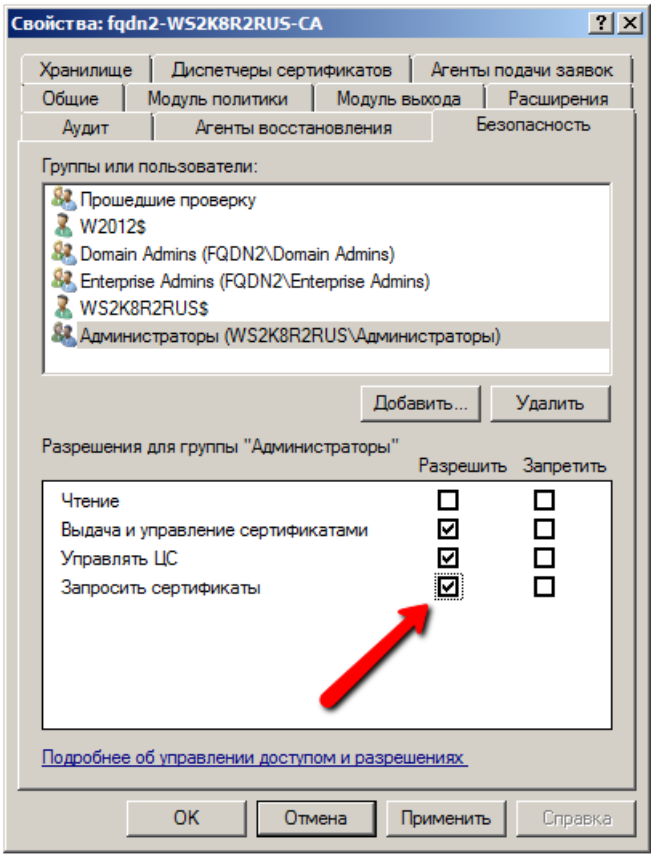
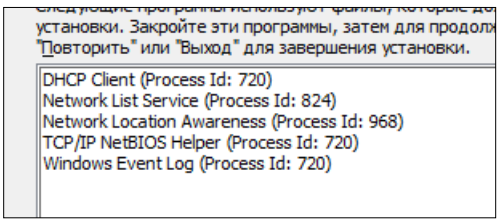


*Рис. 649 – Вкладка **Безопасность** свойств центра сертификации*

Табл. 140 – Другие проблемы

№	Проблема	Решение
1	В процессе установки продукта появляется окно, требующее закрыть несколько программ, так как эти программы используют файлы, которые должны обновиться в ходе установки. Среди предлагаемых к закрытию программ присутствует **Windows Event Log**. 	Отмените установку, нажав **Выход**. Убедитесь, что отсутствуют открытые окна программы **Просмотр событий** (**Event Viewer**), а также другие окна **Консоли управления** (**Microsoft Management Console**). Запустите установку продукта заново.
2	При удалении появляется окно с надписью **Ошибка 1001**, программа удаляется из списка установленных. Служба **EAPEngineSvc_default** не удаляется. При повторной установке продукта	В случае сбоя при удалении - удалите службу **EAPEngineSvc_default** с помощью утилиты **sc.exe** (%systemroot%\system32\sc.exe).

№	Проблема	Решение
	появляется окно с надписью **Ошибка 1001**, при этом продолжение установки невозможно.	Пример запуска: **sc.exe delete EAPEngineSvc_default**
3	При навигации по дереву Active Directory в нем присутствуют элементы, в которых явно нет и не может быть ни компьютеров, ни пользователей.	В таблице настроек БД JMS в параметре **CONTAINER_FILTER_XXX** (XXX – идентификатор ресурсной системы) укажите имена системных контейнеров, которые не нужно выводить: `UPDATE ComponentConfiguration SET [Value] = 'Program Data;System;Application' FROM ComponentConfiguration WHERE [Key]='CONTAINER_FILTER_1'`
4	После критического сбоя выполнения плана обслуживания – например, после принудительной остановки сервера JMS, план обслуживания может некоторое время не запускаться на другом узле кластера (примерно 30 секунд).	Во время работы план обслуживания периодически оповещает все узлы кластера через общую базу данных о своей активности. Если выполнение плана обслуживания на одном из узлов было аварийно прервано, запуск плана на другом узле будет блокироваться некоторое время – за это отвечает параметр **HeartbeatInterval** - по умолчанию он равен 30 секундам. Только по истечении этого интервала план обслуживания будет считаться аварийно прерванным и будет возможен его повторный запуск. [HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Server \Application Name\Default\MaintenanceManager] ;Интервал уведомления об активности выполнения плана обслуживания. **"HeartbeatInterval"=dword:0000001e** Другим временным параметром, отвечающим за выполнение плана обслуживания является: интервал проверки наличия плана обслуживания в очереди на выполнение. **"QueueInterval"=dword:0000000a**
5	В EAP Engine Log пишутся записи следующего вида: Description: **The description for Event ID (1012) in Source (EAP Engine Log) cannot be found.** The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. You may be able to use the /AUXSOURCE= flag to retrieve this description; see Help and Support for details. The following information is part of the event: Engine is started.	В ключе реестра **HKLM\System\CurrentControlset\Services\Eventlog\EAP Engine Log\EAP Engine Log** обновите значения: • CategoryCount=0xA (10) • CategoryMessageFile=%CommonProgramFiles%\Aladdin Shared\Enterprise Application Platform \Eventlog\Aladdin.EAP.EventlogCategories.dll • EventMessageFile=%CommonProgramFiles%\Aladdin Shared\Eventlog\Aladdin.Common.EventlogMessages.dll Изменения вступят в силу после перезапуска **Eventlog Viewer**.
6	При временной потере соединения с сервером базы данных (по умолчанию - более 4 минут), сервер останавливается с ошибкой **Превышен лимит количества сбоев при проверке соединения с БД.**	сервер EAP в процессе работы выполняет периодический мониторинг соединения с сервером базой данных. Число попыток и частота мониторинга настраивается в реестре, при необходимости можно

№	Проблема	Решение
	Сервер EAP будет остановлен. Проверьте настройки соединения с сервером БД.	скорректировать эти правила. За настройки отвечают следующие ключи в разделе: [HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Server *Application Name*\default\DatabaseManager] • Интервал проверки соединения после удачной попытки соединения (в секундах): **"ConnectionSuccessAttemptDelayInterval"=dword:0000003c** • Интервал проверки соединения после неудачной попытки (в секундах): **"ConnectionErrorAttemptDelayInterval"=dword:00000014** • Максимально число *последовательных* неудачных попыток проверки соединения, после которых сервер останавливается: **"MaxConnectionAttempts"=dword:0000000c** Если в рамках мониторинга соединения с сервером БД выявлено, что версия базы данных ниже минимально поддерживаемой, сервер останавливается.
7	При работе с базой данных возникает ошибка превышения времени ожидания выполнения запросов. Необходимо увеличить максимальное время выполнения запроса. ⚠ Данные настройки следует менять только в случае крайней необходимости – для временного решения каких-то критических проблем, для проведения мониторинга и т.п. Само по себе увеличение времени ожидания не может давать повышение производительности. При снижении скорости выполнения запросов к БД в первую очередь необходимо провести анализ производительности средствами MS SQL Server.	JMS позволяет задать максимальное время выполнения одного запроса и максимальную продолжительность одной транзакции. За настройки отвечают следующие ключи в разделе: [HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Server *Application Name*\default\DatabaseManager] • Максимальное время выполнения одного запроса (в секундах). Значение по умолчанию – 30 секунд. **"CommandTimeout"=dword:0000001e** • Максимальная продолжительность транзакции к базе данных (в секундах). Транзакция может состоять из последовательности нескольких команд. Значение по умолчанию – 60 секунд. **"TransactionTimeout"=dword:0000003C** • ;Уровень изоляции транзакции: Serializable = 0, RepeatableRead = 1 (значение по умолчанию), ReadCommited = 2, ReadUncommited = 3. **"TransactionIsolationLevel"=dword:00000001**
8	При перезагрузке компьютера с сервером JMS, настроенного на работу с локальным экземпляром сервера MS SQL Server, серверная служба JMS не стартует с ошибкой **Превышен лимит количества сбоев при проверке соединения с БД. Сервер EAP будет остановлен. Проверьте настройки соединения с сервером БД**.	Проблему можно решить двумя способами. • Увеличьте параметры мониторинга соединения с базой данных – см. параметры **ConnectionErrorAttemptDelayInterval** и **MaxConnectionAttempts**. • Добавьте в зависимости службы **EAPEngineSvc_default** службу MS SQL Server при помощи команды: **sc config "EAPEngineSvc_default" depend= RpcSs/EventLog/MSSQLSERVER** При этом вместо **MSSQLSERVER** необходимо подставить имя экземпляра службы MS SQL Server, например, **MSSQLSERVER** (для экземпляра по умолчанию) или **MSSQL$SQLEXPRESS** (для именованного экземпляра). Имя экземпляра можно посмотреть через оснастку

№	Проблема	Решение
		services.msc в поле **Service name**. В результате должна появиться новая зависимость служб. 
9	При добавлении рабочих станций или пользователей через административный интерфейс появляется сообщение **Ошибка при получении списка рабочих станций из Active Directory** или **Ошибка при получении списка пользователей из Active Directory**. В файле журнала диагностики выводится следующее сообщение: **ERROR ActiveDirectoryManager - System.Runtime.InteropServices.COMException (0x8007202C): Сервер не поддерживает требуемое критическое расширение.** ИЛИ **ERROR ActiveDirectoryManager - System.Runtime.InteropServices.COMException (0x8007202C): The server does not support the requested critical extension.** При этом число объектов в домене близко к 10000 или превышает это значение.	Увеличьте параметр **MaxTempTableSize** – максимальный размер временной таблицы в базе данных для сортировки и выбора промежуточных результатов из Active Directory через протокол LDAP. Для этого последовательно выполните команды: 1. Ntdsutil.exe 2. LDAP policies 3. connections 4. connect to server DC-NAME.your-domain.local *(*указать полное имя контроллера домена*)* 5. q 6. Show Values (должна отобразиться текущая политика LDAP) 7. Set MaxTempTableSize to 50000 (установить требуемое значение – в зависимости от количества хранимых в Active Directory объектов) 8. Commit Changes 9. Show Values (убедиться, что значения применились) После этого перезапустите службы Active Directory Domain Services (NTDS) Дополнительные сведения в сети: • http://support.microsoft.com/kb/315071 • http://support.microsoft.com/kb/315071/ru
10	Поиск пользователей и рабочих станций из Active Directory на странице регистрации выполняется очень долго (до 30 секунд и более) при пустом фильтре и использовании в качестве параметра сортировки поля **Подразделение** (OU). При этом поиск может возвращать не все объекты (не более 1000 – при настройках по умолчанию).	Значение OU не хранится непосредственно в Active Directory, поэтому для выполнения сортировки по этому полю необходимо выгружать все записи из Active Directory в память сервера и сортировать их уже на стороне сервера JMS. Рекомендуется не выполнять сортировку по полю OU, либо ограничивать объем результирующих данных при помощи фильтра поиска или указанием конкретного объекта-контейнера. Максимальное количество возвращаемых объектов можно настроить через политики LDAP – **MaxPageSize** (утилитой **Ntdsutil.exe** – см. описание выше).
11	Открытие клиентского сеанса или получение кэша клиентом выполняется длительное время.	На серверной стороне настроены очень жесткие правила проверки сертификатов. Возможно, используется онлайн-проверка, но удаленный центр сертификации недоступен. Попробуйте задать менее

№	Проблема	Решение
		строгую политику проверки сертификатов или отключить ее.
12	Необходимо увеличить время ожидания (таймаут) соединения с сервером.	За настройку времени ожидания соединения с сервером отвечают следующие элементы файлов конфигурации JMS: <!-- Таймаут попытки установки соединения (сек)--> <add key="OpenTimeout" value="30"/> <!-- Таймаут отправки данных (сек)--> <add key="SendTimeout" value="60"/> <!-- Таймаут получения ответа (сек)--> <add key="ReceiveTimeout" value="60"/>, которые принадлежат элементу <configuration> <appSettings>, например: <?xml version="1.0" encoding="utf-8"?> ... <configuration> ... <appSettings> ... <add key="OpenTimeout" value="30"/> Указанные элементы следует установить как на серверной, так и на клиентской стороне. Настройка вносится в следующие конфигурационные файлы: • для сервера JMS: C:\Program Files\Enterprise Management System Server\Aladdin.EAP.Engine.exe.config • для клиентского сервиса: C:\Program Files\EAP Client\Aladdin.EAP.ClientSTS.Service.exe.config • для клиентского агента: C:\Program Files\EAP Client\Aladdin.EAP.ClientSTS.UI.exe.config • для консоли управления JMS: C:\Program Files\EAP Administrative Client\Aladdin.EAP.Admin.UI.exe.config
13	Если JMS Server установлен на контроллере домена Active Directory, то в некоторых случаях при загрузке операционной системы его служба не запускается автоматически. При этом дальнейший запуск вручную стартует службу без проблем.	Это связано с особенностями работы доменных служб на контроллер домена Active Directory. Если разделить контроллер домена и JMS Server невозможно, то рекомендуется установить запуск службы сервера в **Автоматически (отложенный запуск)**.
14	После настройки режима защиты каналов связи между клиентским или административным агентами и сервером с использованием SSL на клиентской стороне возникает ошибка соединения **Отсутствует связь с сервером. Попробуйте подключиться через**	Настройте систему с помощью команды **netsh**.

№	Проблема	Решение
	некоторое время или обратитесь к администратору системы.	Описание данного подхода http://msdn.microsoft.com/en-us/library/ms733791.aspx. Для манипуляции с сертификатами (удаление, просмотр) можно использовать такой синтаксис вызовов команды: • Для удаления сертификата с порта: **netsh http delete sslcert ipport=0.0.0.0:9010** • Для просмотра сертификатов: **netsh http show sslcert**
15	При работе клиента в режиме кросс-домена: не выполняется аутентификация рабочей станции.	Необходимо настроить доверительные отношения (Domain Trusts) между доменами сервера и клиента. Если это по каким-то причинам сделать невозможно - необходимо через реестр включить режим принудительной внедоменной аутентификации рабочей станции: **HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Client\Default\TransportManager** **"ForceNonDomainAuthentication"=true**
16	При конфигурировании клиентского агента во внедоменной среде возникает ошибка **System.ServiceModel.Security.MessageSecurityException: An unsecured or incorrectly secured fault was received from the other party. See the inner FaultException for the fault code and detail. ---> System.ServiceModel.FaultException: An error occurred when verifying security for the message.** Ошибка может проявляться в журнале диагностики клиентской службы или в клиентском агенте при открытии сеанса.	Вероятная причина – несоответствие времени по UTC на компьютере клиентского агента и сервере JMS. Необходимо убедиться, что время по UTC на всех компьютерах одинаковое.
17	**Ошибка:** `Aladdin.CAPI.CryptographicException: Указаны неправильные флаги.` Возникает в процессе выпуска ключевого носителя модели eToken (на этапе **Создание аутентификатора**), а также выпуске на данный ключевой носитель сертификата при следующих настройках: • На рабочей станции, где выпускается ключевой носитель, установлен программный пакет SafeNet Authentication Client (SAC) версии 10.5 или более поздней; • (в случае выпуска сертификата) использование криптопровайдера **eToken Base Cryptogogaphic Provider** в профиле выпуска сертификата (вкладка **Ключевой контейнер**, поле **Криптопровайдер для генерации ключевой пары**)	Вероятная причина – в настройках криптопровадера **eToken Base Cryptogogaphic Provider** (в составе SAC) установлено ограничение (запрет) на использование ключа RSA длиной менее 2048 бит. Для решения проблемы необходимо снять данное ограничение. **Решение:** На рабочей станции, где выпускается ключевой носитель, следует внести следующие изменения в настройки реестра: • создать (если отсутствует) раздел **`\HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\Crypto`** • создать (если отсутствует) в данном разделе строковый параметр **Disable-Crypto** • Присвоить параметру **Disable-Crypto** значение **None**

№	Проблема	Решение
18	**Ошибка:** `Невозможно смонтировать криптохранилище. Убедитесь, что подключенный электронный ключ содержит действительный сертификат оператора.` Ошибка возникает при попытке в серверном агенте установить поставщик криптографии VipNet CSP с последующей автоматической сменой мастер ключа БД JMS.	**Решение:** В случае возникновения данной ошибки следует прекратить работу мастера подключения поставщика криптографии и выполнить процедуру восстановления мастер-ключа из резервной копии (при этом в качестве нового сертификата на электронном ключе оператора следует выбрать сертификат, ключевая пара которого была сгенерирована с использованием поставщика криптографии ViPNet CSP)

Приложение 3. Права на выполнение операций в JMS

Табл. 141 – 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	
Мастер-ключи		
Чтение информации о Мастер-ключе	Позволяет отображать информацию об используемом мастер-ключе шифрования БД (криптохранилища)	
Отзыв Мастер-ключа	Позволяет отзывать мастер-ключ шифрования БД (криптохранилища)	
Резервное копирование Мастер-ключа	Позволяет выполнять резервное копирование мастер-ключа шифрования БД	

Операция (право на выполнение операции)	Описание	Делегируемая операция
Восстановление Мастер-ключа	Позволяет восстанавливать мастер-ключ шифрования БД из резервной копии	
Смена Мастер-ключа	Позволяет сменить мастер-ключ шифрования БД	
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	+
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**)	+
Чтение сертификатов пользователя	В текущей версии JMS операция не используется	+
Регистрация сертификата пользователя	В текущей версии JMS операция не используется	+
Удаление сертификата пользователя	В текущей версии JMS операция не используется	+
Чтение сертификатов операторов	Право на отображение вкладки **Сертификаты** в свойствах пользователя и показ деталей сертификата оператора	+
Регистрация сертификата оператора	Позволяет зарегистрировать сертификат пользователя (оператора) для обеспечения возможности монтирования криптохранилища пользователем	+
Удаление сертификата оператора	Позволяет удалить сертификат оператора (на вкладке **Сертификаты** в свойствах пользователя)	+
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	+

Операция (право на выполнение операции)	Описание	Делегируемая операция
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 (см. раздел «Установка в БД PIN-кода администратора для приложения электронного ключа», с. 109), 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	+
Замена	Позволяет производить замену ключевых носителей	+
Возврат в эксплуатацию	Позволяет выполнять возврат в эксплуатацию отозванных ключевых носителей	+
Разблокировка Запрос-Ответ	Позволяет выполнять удаленную разблокировку ключевых носителей с использованием механизма Запрос-Ответ	+
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	+
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 (SecurLogon, Indeed и др.) в свойствах пользователя, электронного ключа и в разделе **Сертификаты**	

Операция (право на выполнение операции)	Описание	Делегируемая операция
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)	+
Удаление резервных копий сертификатов	Позволяет удалять резервную копию объектов, выпущенных на КН (экран «Сертификаты»)	+
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.	+
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.	+
Выпуск с восстановлением объектов	Позволяет выполнять выпуск ключевых носителей с возможностью восстановления объектов из резервной копии	+
Очистка	Позволяет выполнять удаление всех объектов из приложений на электронном ключе, путем инициализации данных приложений	+
Роли		
Чтение	Позволяет отображать информацию о созданных ролях	
Создание	Позволяет создавать новые роли	
Удаление	Позволяет удалять ранее созданные роли	
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	
Приложения		
Чтение	В текущей версии JMS операция не используется	

Операция (право на выполнение операции)	Описание	Делегируемая операция
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	

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 JaCarta Management System. Руководство пользователя [Текст]. — «Аладдин Р.Д.». — Файл JMS_x.x_UserGuide_RU.docx

2 JaCarta Management System. Руководство администратора. Часть 1. Установка и настройка [Текст]. — «Аладдин Р.Д.». — Файл JMS_x.x_AdminGuide_(Part1)_Installation_RU.docx

3 JaCarta Management System. Руководство администратора. Часть 3. Установка и настройка сервера аутентификации (JAS) [Текст]. — «Аладдин Р.Д.». — Файл JMS_x.x_AdminGuide_(Part3)_JAS_RU.docx

4 JaCarta Management System. Подготовка и выпуск сертификатов MSCA для JMS [Текст]. — «Аладдин Р.Д.». — Файл JMS_Cert_Guide.docx

5 JaCarta Management System. Развертывание кластерной конфигурации [Текст]. — «Аладдин Р.Д.». — Файл JMS_ClusteringGuide.docx

6 Комплект документации ПАКМ «КРИПТОПРО HSM»:

- ЖТЯИ.00096-02 90 02. Сервер Электронной Подписи. «КриптоПро DSS». КОМПОНЕНТ ПАКМ «КРИПТОПРО HSM». Общее описание [Текст];
- Сервер Электронной Подписи «КриптоПро DSS». КОМПОНЕНТ ПАКМ «КРИПТОПРО HSM». Быстрый старт [Текст];
- ЖТЯИ.00096-02 95 01. Средство криптографической защиты информации КриптоПро HSM. Версия 2.0. Комплектация 3. Правила пользования [Текст]
- ЖТЯИ.00082-01 90 03 06. ПАК «КриптоПро DSS». Инструкция Оператора тестового СЭП [Текст]

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
1.00	Исходная версия документа для JMS версии 3.7.1.

Коротко о компании

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

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

Основные направления

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

Лицензии

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

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