УТВЕРЖДЕН
RU.АЛДЕ.03.16.001-04 32 01-1-ЛУ

# JaCarta Management System v3.7

## Руководство администратора. Часть 1

## Установка и настройка

## RU.АЛДЕ.03.16.001-04 32 01-1

| | |
|---|---|
| Версия продукта | 3.7.1 |
| Версия документа | 1.00 |
| Статус | Публичный |
| Дата | 4 мая 2023 г. |
| Листов | 259 |

2023

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

# Оглавление

# 1. О документе

## 1.1 Назначение документа

Настоящий документ является частью руководства администратора и представляет собой описание операций по установке и настройке 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*

| | |
|---|---|
| **JMS CA Edition** | Версия поставки продукта, предназначенная для заказчиков, которые не используют компонент JMS Client |
| **JMS Enterprise Edition** | Полнофункциональная версия поставки продукта, обеспечивающая автоматизацию администрирования электронных ключей на предприятии с использованием компонента JMS Client на рабочих станциях |
| **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 |
| **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 Приемка изделия

Перед установкой Изделия (ПО JMS) необходимо убедиться, что:

1. комплектность Изделия соответствует комплектности поставки, указанной в документе «Формуляр» RU.АЛДЕ.03.16.001-04 30 01-1;
2. на носителях информации, входящих в состав поставки, отсутствуют сколы, царапины, целостность этикеток и пломб не нарушены;
3. контрольные суммы дистрибутива соответствуют заявленным в документе «Формуляр» RU.АЛДЕ.03.16.001-04 30 01-1.

## 2.2 Обеспечение безопасности информации при работе с ПО JMS

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

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

| Раздел обеспечения безопасности информации | Обеспечительные меры в ПО JMS |
|---|---|
| Действия по приемке поставленного средства | Действия по приемке Изделия (ПО JMS) приведены в разделе «Приемка изделия», с. 15 |
| Действия по безопасной установке и настройке средства | Действия по безопасной установке и настройке Изделия (ПО JMS) приведены в разделе «Обеспечение целостности и защиты от несанкционированного доступа файлов ПО JMS», с. 148 |
| Действия по реализации функций безопасности среды функционирования средства | Действия по реализации функций безопасности среды функционирования Изделия (ПО JMS) приведены в разделе «Настройка функций безопасности среды функционирования объекта оценки (JMS)», с. 148 |

## 2.3 Общие сведения

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

## 2.4 Состав JMS

В состав JMS входят следующие компоненты:

- JMS Server – серверный компонент JMS;
- JMS Admin – консоль управления JMS;
- JMS Client – пользовательский клиент JMS (кроме версии поставки JMS CA Edition);
- JaCarta Authentication Server – сервер аутентификации JAS (при условии покупки соответствующей лицензии).

## 2.5 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 настоящего руководства, в частности см. раздел «Подготовка к использованию протоколов SSL/TLS», с. 122.

## 2.6 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 в разделе «Настройка SSL/TLS для работы с Microsoft SQL Server», с. 125.

## 2.7 Дополнительная документация

Рекомендуется дополнительно ознакомиться со следующими документами:

- «JaCarta Management System. Руководство пользователя» [1];
- «JaCarta Management System. Руководство администратора. Часть 2. Функции администрирования» [3];
- «JaCarta Management System. Руководство администратора. Часть 3. Установка и настройка сервера аутентификации (JAS)» [4].

# 3. Описание пакетов установки

Дистрибутив JMS включает следующие пакеты установки и обновления (см. табл. 4).

*Табл. 4 - Дистрибутив JMS*

| Файл | Описание |
|---|---|
| **Aladdin.JMS.Server-x.x.x.xxxx-x86.msi**<br>**Aladdin.JMS.Server-x.x.x.xxxx-x64.msi** | Компонент JMS Server (для 32-битных и 64-битных систем соответственно), серверная часть JMS. Этот компонент следует устанавливать на серверной операционной системе. |
| **Aladdin.JMS.Admin-x.x.x.xxxx-x86.msi**<br>**Aladdin.JMS.Admin-x.x.x.xxxx-x64.msi** | Компонент JMS Admin (для 32-битных и 64-битных систем соответственно) - консоль управления JMS. Этот компонент следует устанавливать на компьютере или компьютерах, с которых будет осуществляться администрирование JMS. |
| **Aladdin.JMS.Client.STS-x.x.x.xxxx-x86.msi**<br>**Aladdin.JMS.Client.STS-x.x.x.xxxx-x64.msi** | Компонент JMS Client (для 32-битных и 64-битных систем соответственно), пользовательский клиент JMS. Этот компонент следует устанавливать на компьютерах пользователей JMS. |

# 4. Системные требования

## 4.1 Программные требования компонента JMS Server

| | |
|---|---|
| **Операционные системы** | • Microsoft Windows Server 2008 R2 SP1;<br>• Microsoft Windows Server 2012;<br>• Microsoft Windows Server 2012 R2;<br>• Microsoft Windows Server 2016;<br>• Microsoft Windows Server 2019 |
| **Базы данных** | • Microsoft SQL Server 2008;<br>• Microsoft SQL Server 2008 R2;<br>• Microsoft SQL Server 2012;<br>• Microsoft SQL Server 2014;<br>• Microsoft SQL Server 2016;<br>• Microsoft SQL Server 2017;<br>• Microsoft SQL Server 2019;<br>(При использовании СУБД Microsoft SQL Server необходимым компонентом является *SQL Server Database Engine*)<br>• PostgreSQL версии 12 или более поздних версий |
| **Дополнительное ПО** | .NET Framework 4.6 или 4.7 |

## 4.2 Программные требования компонентов JMS Admin, JMS Client

| | |
|---|---|
| **Операционные системы** | ○ Microsoft Windows XP SP3 (32-битные платформы), SP2 (64-битные платформы);<br>○ Microsoft Windows Vista SP2 (32/64-битные платформы);<br>○ Microsoft Windows 7 SP1 (32/64-битные платформы);<br>○ Microsoft Windows 8.1 (32/64-битные платформы);<br>○ Microsoft Windows 10 (32/64-битные платформы);<br>○ Microsoft Windows Server 2003 SP2 (32/64-битные платформы);<br>○ Microsoft Windows Server 2003 R2 SP2 (32/64-битные платформы);<br>○ Microsoft Windows Server 2008 SP2 (32/64-битные платформы);<br>○ Microsoft Windows Server 2008 R2 SP1;<br>○ Microsoft Windows Server 2012;<br>○ Microsoft Windows Server 2012 R2;<br>○ Microsoft Windows Server 2016;<br>○ Microsoft Windows Server 2019 |
| **Дополнительное ПО** | .NET Framework 4.6.2 или 4.7 |

## 4.3 Аппаратные требования компонентов ПО JMS

Требования к аппаратному обеспечению компонентов JMS (JMS Server, JMS Client и JMS Admin) приведены в документе RU.АЛДЕ.03.16.001-04 30 01-1 «Программное обеспечение JaCarta Management System v3.7. Формуляр».

Требования к аппаратному обеспечению различных конфигураций кластера JMS приведены в документе «Требования для развертывания продукта» [5].

## 4.4 Поддержка работы с электронными ключами и ПО для работы с ними

### 4.4.1 Требования к ПО для электронных ключей

Требования к программному обеспечению, необходимому для обеспечения работы поддерживаемых в JMS электронных ключей, приведены в документе

RU.АЛДЕ.03.16.001-04 30 01-1 «Программное обеспечение JaCarta Management System v3.7. Формуляр».

**Примечание.** В интерфейсе JMS:

- электронные ключи Рутокен отображаются как **RuToken**;
- электронные ключи JaCarta CryptoPro отображаются как **ФКН** (функциональный ключевой носитель);
- электронные ключи ESMART Token и ESMART Token ГОСТ отображаются как **ESMART** и **ESMART ГОСТ** соответственно.

### 4.4.2 Требования к ПО для считывателей смарт-карт Аладдин

| Модель | Программное обеспечение |
|---|---|
| JCR721-OAWRN | Единый Клиент JaCarta 2.12 и более поздние версии |

## 4.5 Использование КриптоПро CSP в качестве поставщика криптографии

JMS поддерживает работу со следующим поставщиками криптографии КриптоПро CSP для зашифрования криптохранилища, а также для выпуска электронных ключей в КриптоПро УЦ:

- КриптоПро CSP 3.6;
- КриптоПро CSP 3.9;
- КриптоПро CSP 4.0;
- КриптоПро CSP 5.0.

## 4.6 Поддерживаемые удостоверяющие центры

JMS поддерживает работу со следующими центрами сертификации:

- КриптоПро УЦ 1.5;
- КриптоПро УЦ 2.0;
- центр сертификации Microsoft CA;
- центр сертификации Microsoft CA с КриптоПро CSP;
- ViPNet УЦ.

# 5. Работа с центром сертификации Microsoft

## 5.1 Действия, необходимые для работы с внедоменными компьютерами

Действия, представленные в настоящем подразделе, необходимо выполнять только в том случае, если планируется использование совместно с JMS компьютеров, не входящих в домен Windows, в котором развернута система JMS.

Для обеспечения возможности работы JMS с внедоменными компьютерами, на сервере, на котором установлен центр сертификации Microsoft, должен быть установлен компонент **Служба регистрации в центре сертификации через Интернет**.

### 5.1.1 Редактирование свойств центра сертификации

1. В окне оснастки центра сертификации щелкните правой кнопкой на центре сертификации и выберите **Свойства**, как показано на рис. 1.

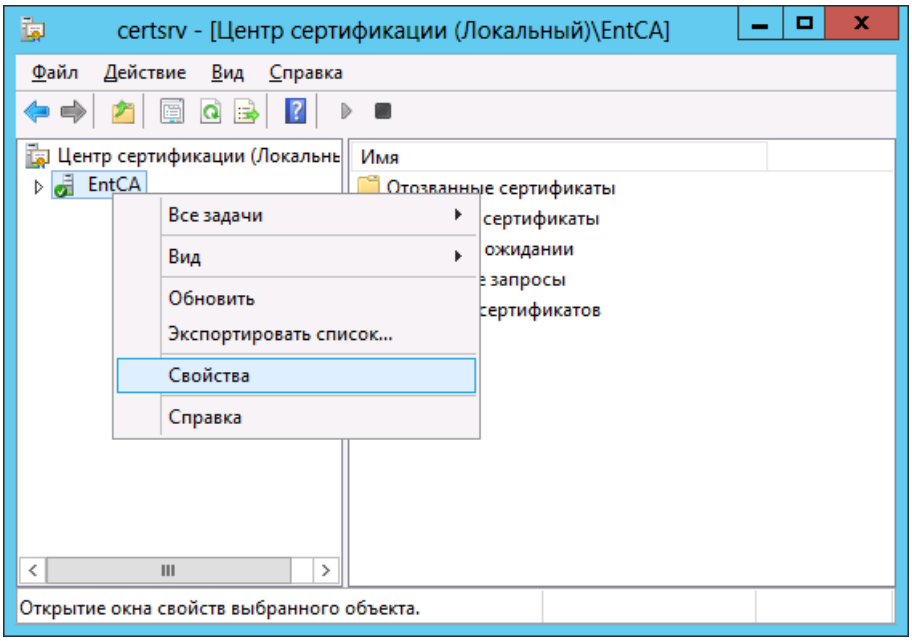



*Рис. 1 – Открытие окна свойств центра сертификации*

2. В отобразившемся окне перейдите на вкладку **Расширения**.
Окно примет следующий вид.

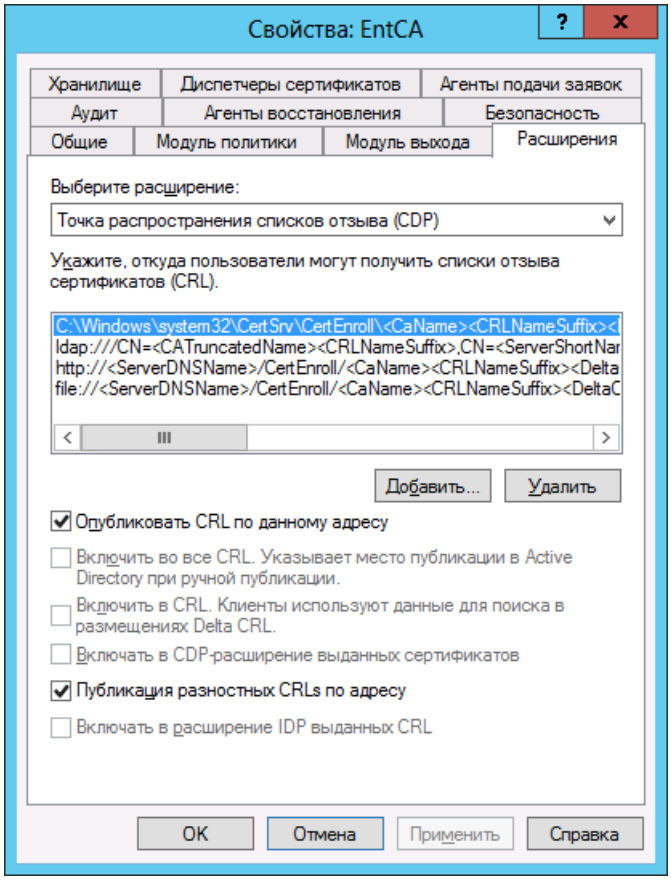



*Рис. 2 – Вкладка Расширения*

3. В списке **Укажите, откуда пользователи могут получить списки отзыва сертификатов (CRL)** выберите строку, начинающуюся с **http://**.
   Окно примет следующий вид.

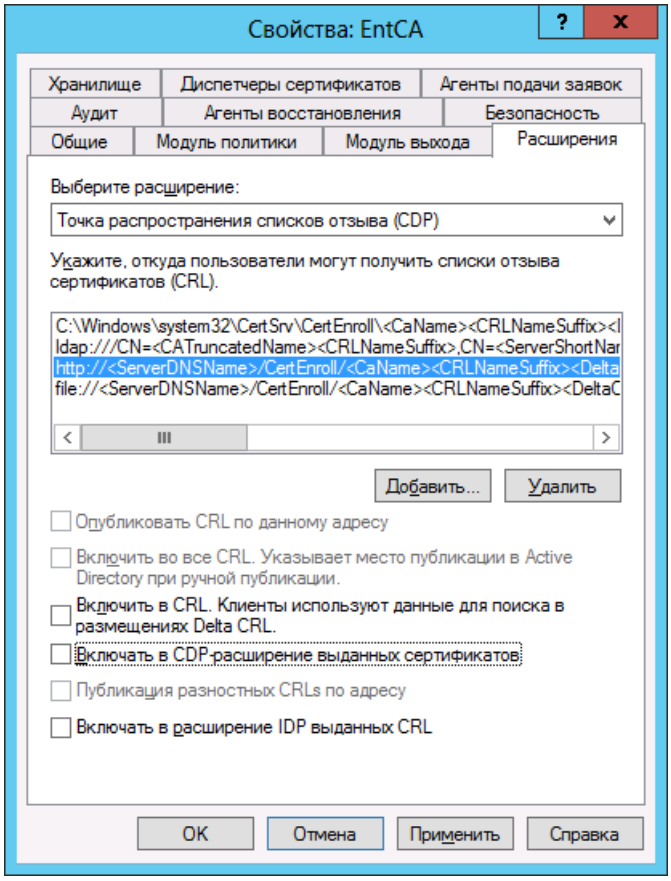



*Рис. 3 – Выбор источника списков отзыва сертификатов*

4. Установите следующие флаги:

   - **Включить в CRL. Клиенты используют данные для поиска в размещениях Delta CRL.**
   - **Включать в CDP-расширение выданных сертификатов**

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

### 5.1.2 Настройка точки размещения списков отзыва в Диспетчере служб IIS

1. На сервере, на котором установлен центр сертификации Microsoft, откройте оснастку **Диспетчер служб IIS**.

Отобразится следующее окно.

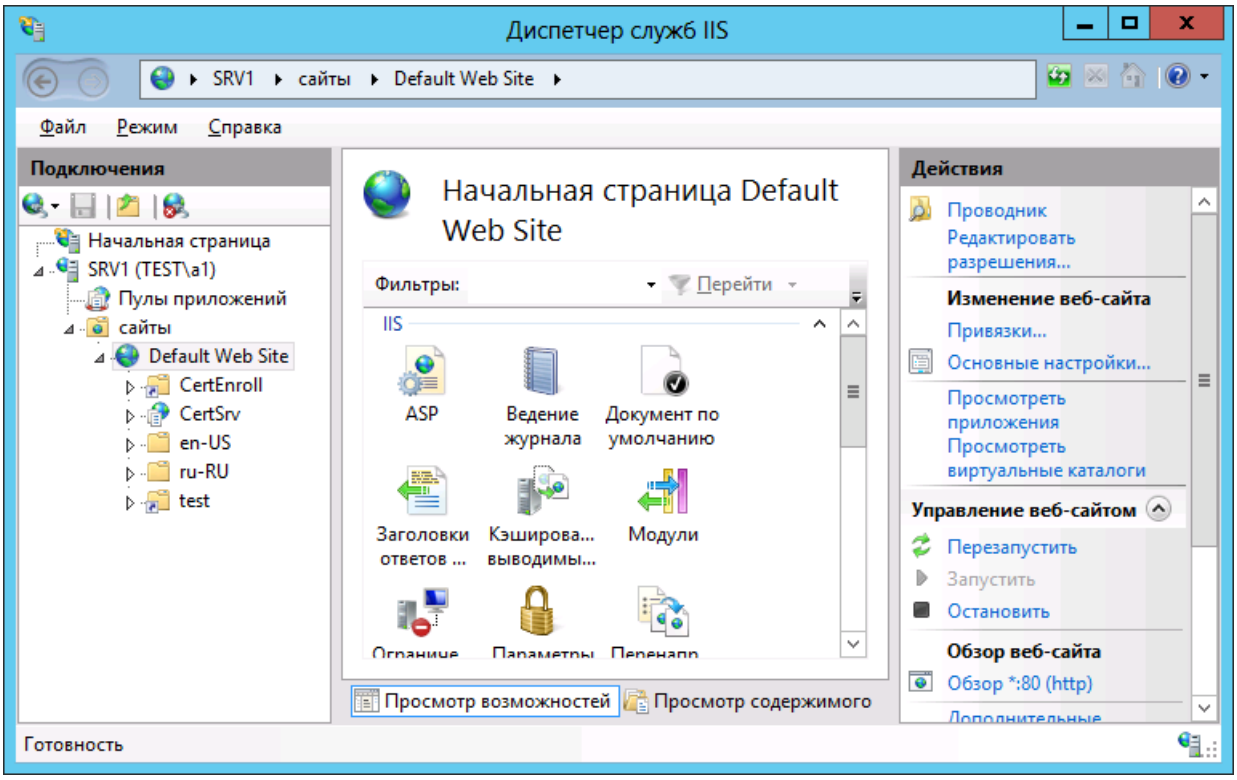



*Рис. 4 – Диспетчер служб IIS*

2. В панели **Подключения** слева выберите пункт **Default Web Site** (веб-сайт по умолчанию).
3. В колонке **Действия** в секции **Изменение веб-сайта** справа щелкните на ссылке **Основные настройки**.
   Отобразится следующее окно.

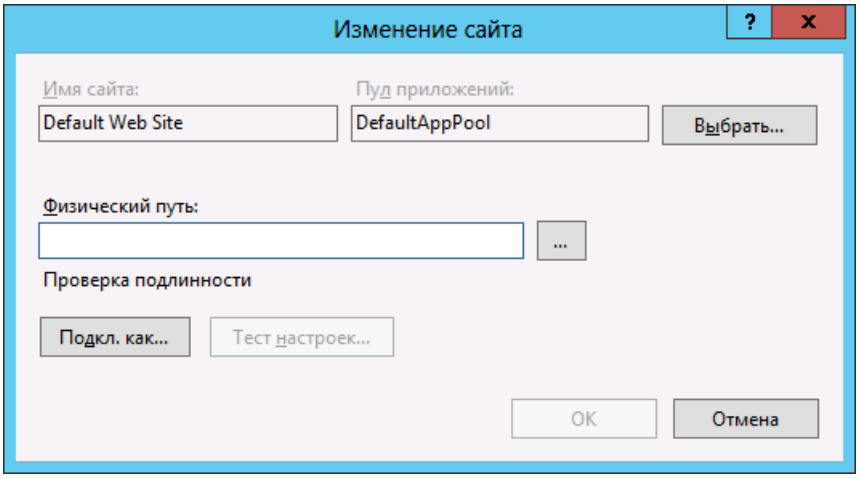



*Рис. 5 – Окно **Изменение сайта***

4. В поле **Физический путь** введите **C:\Windows\System32\certsrv**.

Окно примет следующий вид.

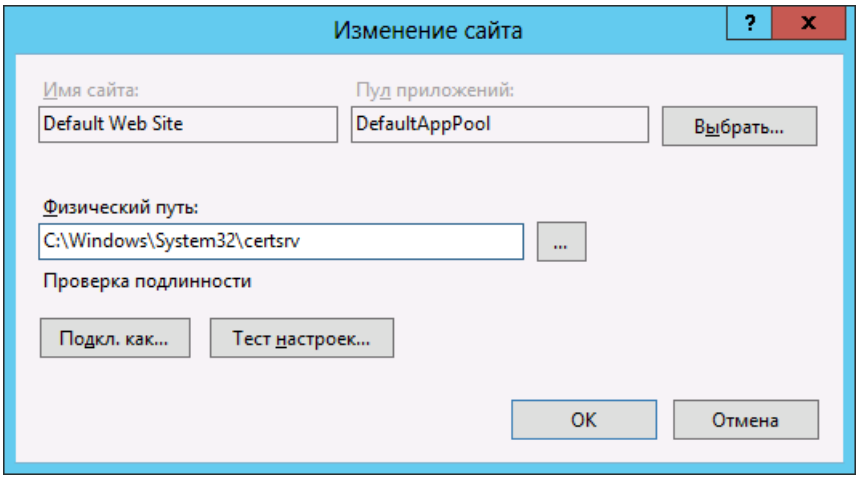



*Рис. 6 – Изменение поля **Физический путь***

5. Нажмите **OK**, чтобы сохранить изменения.
6. В центральной части окна двойным щелчком на значке перейдите в раздел **Фильтрация запросов**.
   Окно оснастки Диспетчера служб IIS примет следующий вид.

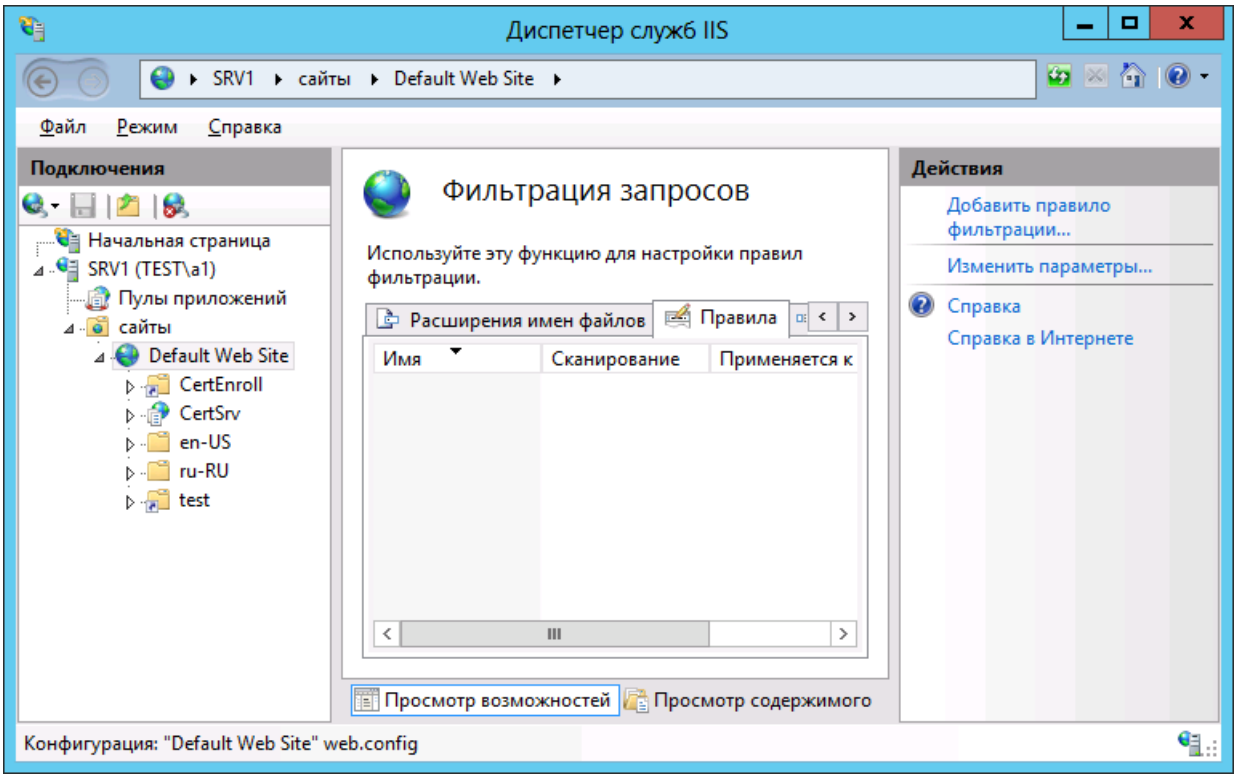



*Рис. 7 – Раздел **Фильтрация запросов***

7. В панели **Действия** справа щелкните на ссылке **Изменить параметры**.

Отобразится следующее окно.

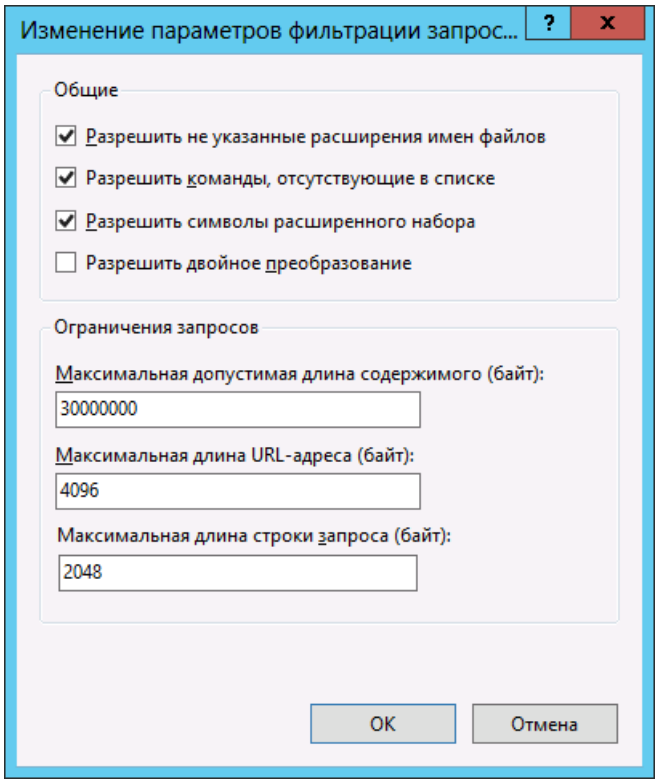



*Рис. 8 – Изменение параметров фильтрации запросов*

8. Установите флаг **Разрешить двойное преобразование**.
9. Нажмите **OK**, чтобы сохранить изменения.

### 5.1.3 Проверка доступности списков отзыва сертификатов

После того как выполнена настройка центра сертификации и настройка в Диспетчере служб IIS, необходимо убедиться в доступности полного и разностного списков отзыва сертификатов.

Для этого с внедоменного компьютера в браузере перейдите по следующим ссылкам (в каждом случае должно отображаться окно загрузки файла):

- полный список отзыва: **http://<Сервер_ЦС>/certenroll/<Имя_ЦС>.crl**;
- разностный список отзыва: **http://<Сервер_ЦС>/certenroll/<Имя_ЦС>+.crl**.

где:

**<Сервер_ЦС>** - полное имя сервера, на котором установлен центр сертификации Microsoft, включая имя компьютера и домен, например: **srv1.test.com**.

**<Имя_ЦС>** - имя центра сертификации Microsoft, например, **EntCA**.

Таким образом, если брать приведенные выше примеры, ссылки будут выглядеть следующим образом:

- полный список отзыва: **http://srv1.test.com/certenroll/entca.crl**;
- разностный список отзыва: **http://srv1.test.com/certenroll/entca+.crl**.

⚠ Впоследствии убедитесь в том, что HTTP-адрес точки размещения списков отзыва сертификатов содержится в сертификате, выпущенном для службы аутентификации JMS (см. «Выпуск сертификата в хранилище сертификатов компьютера», с. 42).

## 5.2 Сертификаты для работы с JMS

Для работы JMS вам могут понадобиться следующие сертификаты (см. табл. 5).

*Табл. 5 – Сертификаты центра сертификации Microsoft, используемые с JMS*

| Сертификат | Описание |
|---|---|
| Сертификат оператора JMS | Этот сертификат необходим для работы JMS.<br>Сертификат оператора JMS должен быть при выпуске записан в память электронного ключа, который будет использоваться в качестве ключа оператора JMS (напр., для монтирования криптохранилища JMS).<br>В настоящем руководстве настройка шаблона сертификата оператора JMS представлена на основе шаблона **Пользователь со смарт-картой**. |
| Сертификат службы аутентификации JMS | Этот сертификат необходим для работы JMS.<br>Сертификат, выпущенный по этому шаблону, должен быть помещен в хранилище сертификатов компьютера на сервере JMS, и используется для службы аутентификации JMS.<br>В настоящем руководстве настройка шаблона сертификата службы аутентификации JMS представлена на основе шаблона **Компьютер**. |
| Сертификат для обеспечения SSL-соединения между сервером JMS и административным агентом из состава JMS Admin<br>Сертификат для обеспечения SSL-соединения между сервером JMS и клиентским агентом из состава JMS Client<br>Сертификат для обеспечения SSL-соединения между сервером JMS и сервером SQL | Этот сертификат (сертификаты) необходим, только в том случае, если вы хотите защитить взаимодействие компонентов JMS посредством SSL.<br>Сертификат для обеспечения защиты соединения с помощью SSL нужен для защиты следующих типов взаимодействий:<br>• взаимодействие сервера JMS с административным агентом из состава JMS Admin;<br>• взаимодействие сервера JMS с клиентским агентом из состава JMS Client;<br>• взаимодействие сервера JMS с сервером SQL.<br>В первых двух случаях сертификат, выпущенный по этому шаблону, должен быть помещен в хранилище сертификатов компьютера на сервере JMS. Для обеспечения защиты взаимодействия указанных компонентов можно использовать как один сертификат, так и два разных сертификата.<br>В последнем случае сертификат должен быть помещен в хранилище сертификатов компьютера на сервере SQL.<br>В настоящем руководстве настройка шаблона сертификата для обеспечения защиты взаимодействия компонентов JMS по SSL представлена на основе шаблона **Компьютер**. |
| Сертификат агента регистрации | Этот сертификат необходим, если вы планируете выпускать электронные ключи с сертификатами центра сертификации Microsoft для пользователей JMS.<br>Сертификат, выпущенный по этому шаблону, должен быть помещен в хранилище сертификатов компьютера на сервере JMS и используется, когда выпуск электронных ключей с сертификатами центра сертификации Microsoft осуществляется администратором JMS от имени пользователей JMS или когда выпуск осуществляется пользователями JMS самостоятельно.<br>В настоящем руководстве настройка шаблона сертификата агента регистрации представлена на основе шаблона **Агент регистрации (Компьютер)**. В этом случае агентом регистрации является сервер JMS.<br>Агентом регистрации также может быть администратор JMS, выпускающий электронные ключи от имени пользователей в консоли управления JMS. Доступны следующие варианты. |

| Сертификат | Описание |
|---|---|
| | • Сертификат агента регистрации устанавливается в хранилище пользователя на компьютере, на котором установлена консоль управления JMS.<br>• Сертификат агента регистрации записывается в память электронного ключа, принадлежащего администратору JMS. В этом случае при выпуске сертификатов для пользователей администратор должен будет подсоединить свой электронный ключ к компьютеру.<br><br>В настоящем документе для примера сертификата агента регистрации в хранилище пользователя или в памяти электронного ключа будет использоваться шаблон **Агент регистрации**.<br><br>⚠ Если агентом регистрации является администратор JMS, установка сертификата агента регистрации для сервера JMS все равно необходима. |
| Сертификат для пользователей JMS | Это шаблон, который будет использоваться при выпуске для пользователей JMS электронных ключей с сертификатами центра сертификации Microsoft.<br><br>В настоящем руководстве рассматривается вариант, в котором выпуск электронных ключей с сертификатами центра сертификации Microsoft осуществляется администратором JMS от имени пользователей JMS.<br><br>В настоящем руководстве настройка шаблона сертификата для пользователей JMS представлена на основе шаблона **Пользователь со смарт-картой**. |

## 5.3 Создание шаблонов сертификатов

1. Запустите консоль центра сертификации Microsoft.
   Окно консоли будет выглядеть следующим образом.

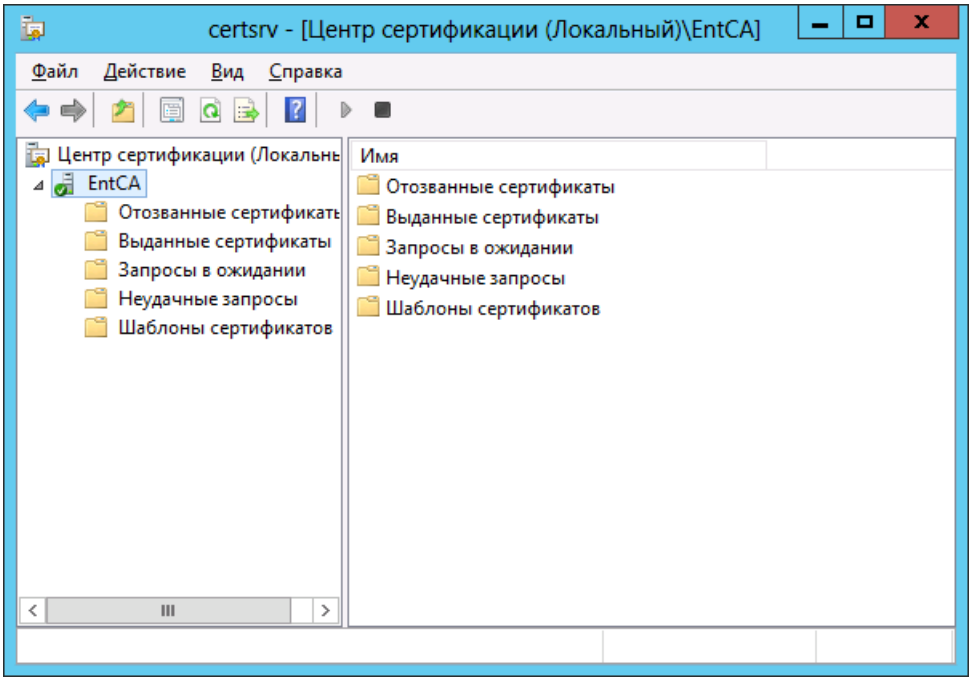



*Рис. 9 – Окно консоли центра сертификации*

2. В левой части окна разверните узел центра сертификации, щелкните правой кнопкой на пункте **Шаблоны сертификатов** и выберите **Управление** (см. рис. 10).

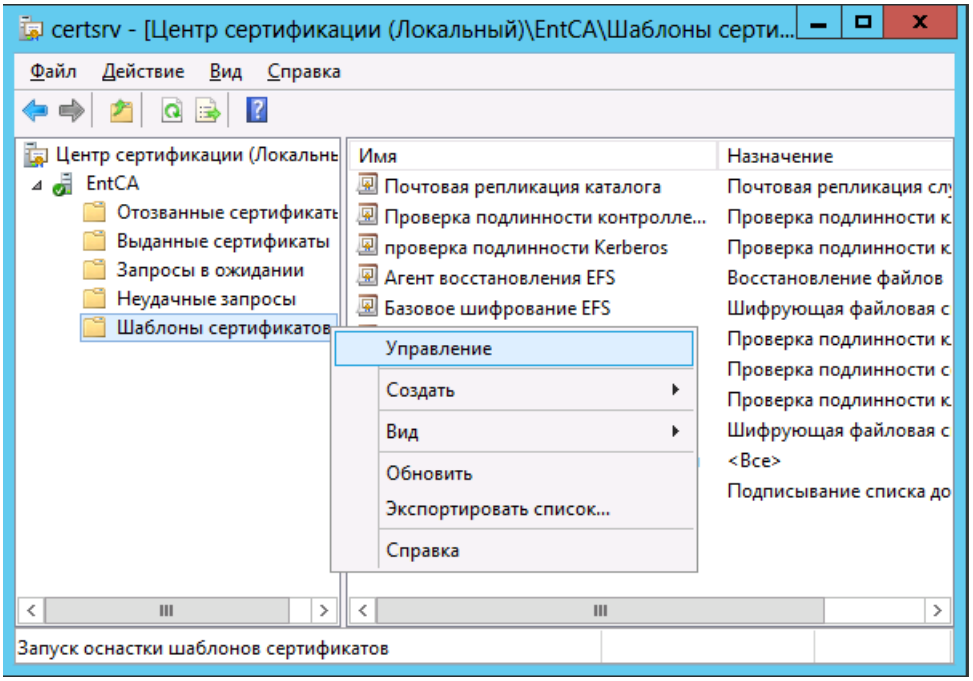



*Рис. 10 – Открытие окна управления шаблонами сертификатов*

3. В отобразившемся окне щелкните правой кнопкой на нужном шаблоне и нажмите **Скопировать шаблон** (см. рис. 11).

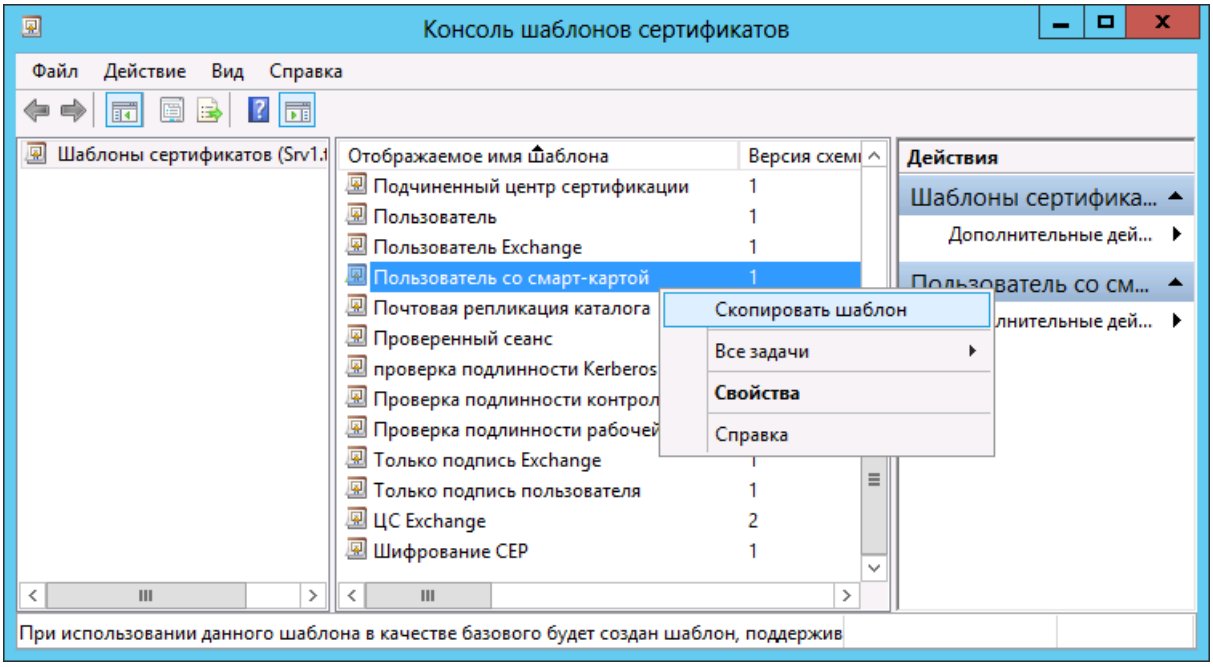



*Рис. 11 – Копирование шаблона сертификата*

4. Настройте шаблон:

Для корректной работы JMS необходимо использовать шаблон версии **Microsoft Windows Server 2003**.

- «Шаблон сертификата оператора JMS», с. 27;

- «Шаблон сертификата службы аутентификации JMS и серверов JMS/SQL», с. 28 (для сертификата службы аутентификации JMS, для сертификата/сертификатов поддержки SSL-соединения с сервером JMS, а также для сертификата поддержки SSL-соединения сервера JMS с сервером SQL);
- «Шаблон сертификата службы аутентификации JMS (для работы JMS в кластере)», с. 28;
- «Шаблон сертификата агента регистрации», с. 28;
- «Шаблон сертификата для пользователей JMS», с. 33.

### 5.3.1 Шаблон сертификата оператора JMS

Процедура представлена на примере копии шаблона **Пользователь со смарт-картой**.

1. На вкладке **Общие** в поле **Отображаемое имя шаблона** введите имя для скопированного шаблона, например, **Оператор JMS**.
2. Перейдите на вкладку **Шифрование**.
   Окно будет иметь следующий вид.

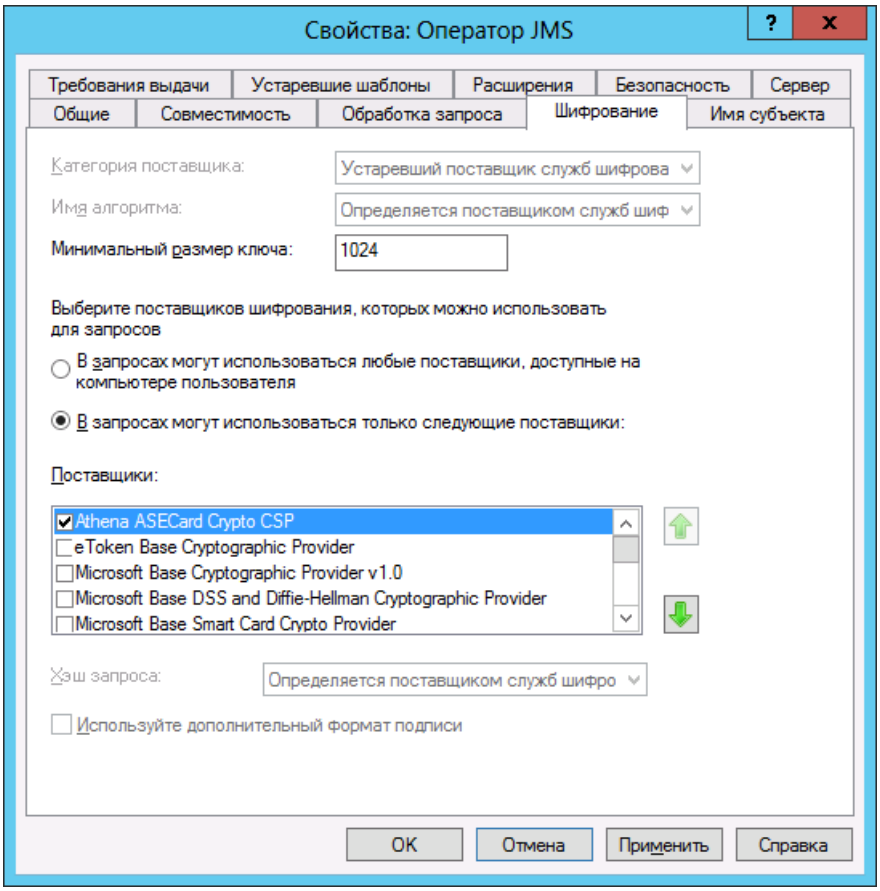



*Рис. 12 – Вкладка **Шифрование** шаблона сертификата для оператора JMS*

3. В поле **Минимальный размер ключа** установите минимальный размер ключа, начиная с 1024 бит.
4. Выберите пункт **В запросах могут использоваться только следующие поставщики** и в зависимости от используемого электронного ключа в списке **Поставщики** выберите поставщика криптографии:

   – электронные ключи eToken, а также JaCarta PKI с функцией обратной совместимости с продуктами компании Aladdin – **eToken base Cryptographic Provider**;
   – электронные ключи JaCarta (за исключением JaCarta PKI с функцией обратной совместимости с продуктами компании Aladdin) – **Microsoft Base Smart Card Crypto Provider**.

5. Перейдите на вкладку **Безопасность** и внесите необходимые изменения.

В настоящем документе процедура заявки на сертификат для оператора JMS производится самим будущим оператором JMS, таким образом, этому пользователю необходимы разрешения: **Чтение** и **Заявка**.

6. Нажмите **ОК** для сохранения шаблона.
7. Опубликуйте шаблон сертификата (см. «Публикация шаблона сертификата», с. 35).

### 5.3.2 Шаблон сертификата службы аутентификации JMS и серверов JMS/SQL

Шаблон сертификата для сервера JMS/SQL может быть использован для выпуска следующих сертификатов:

- сертификат для обеспечения работы службы аутентификации JMS;
- сертификат обеспечения SSL-соединения сервера JMS с административным агентом из состава JMS Admin;
- сертификат обеспечения SSL-соединения сервера JMS с клиентским агентом из состава JMS Client;

Для двух последних вариантов можно использовать как один и тот же сертификат, так и два разных.

- сертификат обеспечения SSL-соединения сервера JMS сервером SQL.

Процедура представлена на примере копии шаблона **Компьютер**.

1. На вкладке **Общие** в поле **Отображаемое имя шаблона** введите имя для скопированного шаблона, например, **SSL**.
2. Перейдите на вкладку **Безопасность** и добавьте компьютеру, который является сервером JMS, разрешения: **Чтение**, **Заявка** и **Запись**.
3. Нажмите **ОК** для сохранения шаблона.
4. Опубликуйте шаблон сертификата (см. «Публикация шаблона сертификата», с. 35).

### 5.3.3 Шаблон сертификата службы аутентификации JMS (для работы JMS в кластере)

Если вы планируете разворачивать JMS в кластере следует использовать копию шаблона **Компьютер**, применив следующие настройки.

1. На вкладке **Общие** в поле **Отображаемое имя шаблона** введите имя для скопированного шаблона.
2. Перейдите на вкладку **Обработка запроса** и установите флаг **Разрешить экспортировать закрытый ключ**.
3. Перейдите на вкладку **Имя субъекта** и выберите пункт **Предоставляется в запросе**.
4. В отобразившемся окне предупреждения нажмите **ОК**.
5. Перейдите на вкладку **Безопасность** и добавьте компьютеру, который является сервером JMS, разрешения: **Чтение**, **Заявка** и **Запись**.
6. Нажмите **ОК** для сохранения шаблона.
7. Опубликуйте шаблон сертификата (см. «Публикация шаблона сертификата», с. 35).

Более детально процедура создания шаблона и выпуска сертификата для кластера описана в руководстве по развертыванию кластерной конфигурации JMS [6].

### 5.3.4 Шаблон сертификата агента регистрации

В табл. 6 представлены варианты установки сертификата агента регистрации.

*Табл. 6 – Варианты установки сертификата агента регистрации*

| Тип агента регистрации | Вариант установки сертификата |
|---|---|
| Сервер JMS | В этом случае сертификат агента регистрации должен быть установлен в хранилище компьютера на сервере JMS. См. «Хранилище компьютера» ниже. |

| Тип агента регистрации | Вариант установки сертификата |
|---|---|
| | ⚠ Установка этого сертификата обязательна, даже если вы не планируете использовать сервер JMS в качестве агента регистрации. В случае же если служба JMS запускается от имени пользователя, то в качестве такого сертификата должен использоваться сертификат агента регистрации, выпущенного для пользователя, от чьего имени запускается служба JMS (см. «Хранилище пользователя», с. 31). |
| Администратор JMS | В этом случае существуют следующие варианты установки сертификата агента регистрации.<br><br>Сертификат агента регистрации устанавливается в хранилище пользователя администратора JMS на компьютере, на котором администратор JMS осуществляет выпуск сертификатов для пользователей. См. «Хранилище пользователя», с. 31.<br><br>Сертификат агента регистрации записывается в память электронного ключа, принадлежащего администратору JMS, в этом случае при выпуске сертификатов для пользователей в консоли управления JMS администратор JMS должен подсоединить свой электронный ключ к компьютеру. См. «Для хранения на электронном ключе», с. 32. |

#### 5.3.4.1 Хранилище компьютера

Процедура представлена на примере копии шаблона **Агент регистрации (компьютер)**.

1. На вкладке **Общие** в поле **Отображаемое имя шаблона** введите имя для скопированного шаблона, например, **Агент регистрации JMS**.

2. Перейдите на вкладку **Шифрование** и убедитесь в том, что в списке поставщиков отмечены следующие два поставщика криптографии (см. рис. 13):

   – Microsoft Enhanced Cryptographic Provider v 1.0;
   – Microsoft Base Cryptographic Provider v 1.0.

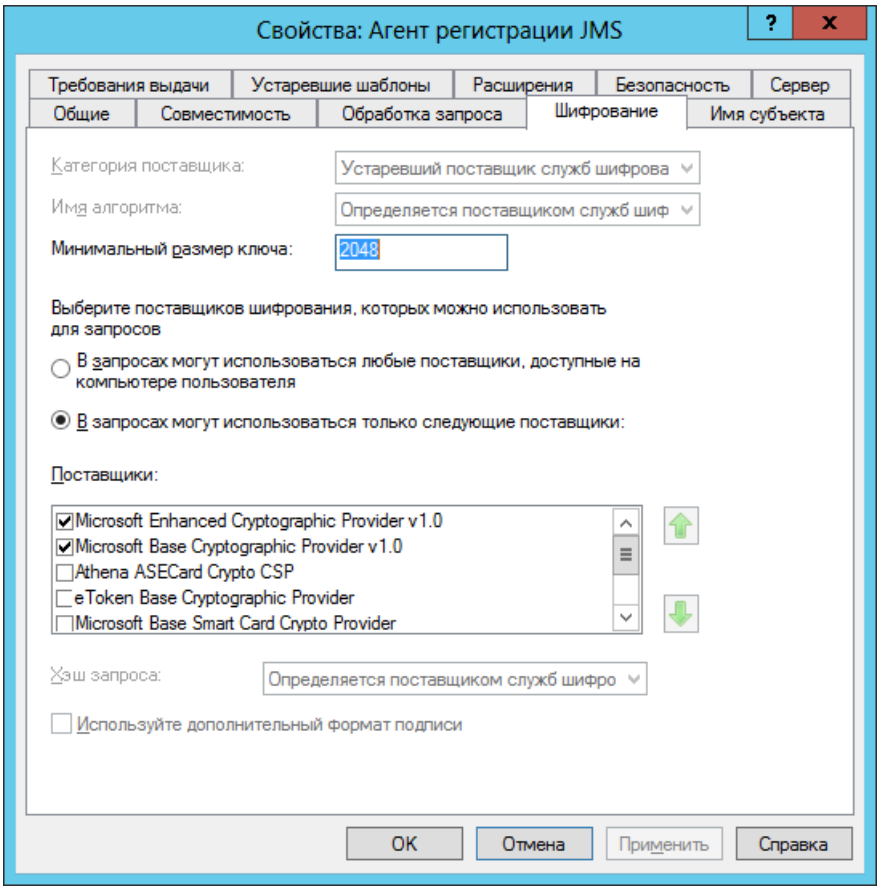



*Рис. 13 – Необходимые поставщики криптографии*

3. Перейдите на вкладку **Безопасность** и добавьте компьютеру, который является сервером JMS, разрешения: **Чтение**, **Заявка** и **Запись** (см. рис. 14).

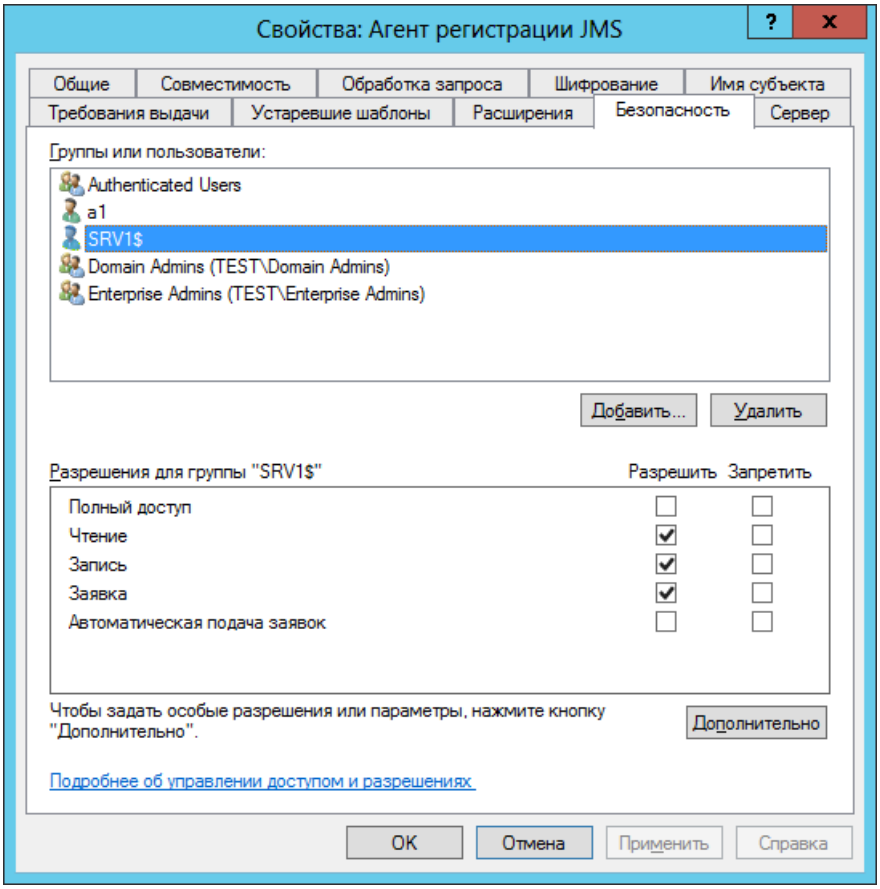



*Рис. 14 – Вкладка Безопасность шаблона сертификата агента регистрации*

4. Нажмите **OK** для сохранения шаблона.
5. Опубликуйте шаблон сертификата (см. «Публикация шаблона сертификата», с. 35).

#### 5.3.4.2 Хранилище пользователя

Процедура представлена на примере копии шаблона **Агент регистрации**.

1. На вкладке **Общие** в поле **Отображаемое имя шаблона** введите имя для скопированного шаблона, например, **Агент регистрации JMS**.

2. Перейдите на вкладку **Шифрование** и убедитесь в том, что в списке поставщиков отмечены следующие два поставщика криптографии (см. рис. 15):

   – Microsoft Enhanced Cryptographic Provider v 1.0;
   – Microsoft Base Cryptographic Provider v 1.0.

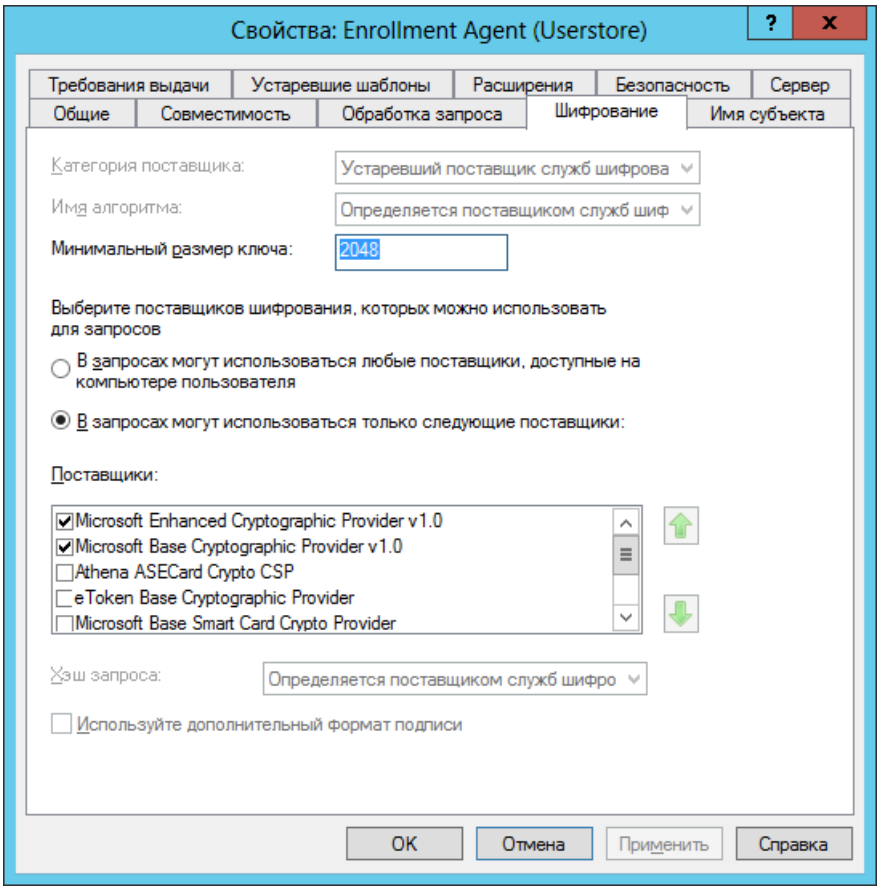



*Рис. 15 – Необходимые поставщики криптографии*

3. Перейдите на вкладку **Безопасность** и добавьте пользователю, который будет выполнять роль администратора JMS, разрешения: **Чтение**, **Заявка** и **Запись**.

⚠ В целях безопасности рекомендуется удалить эти разрешения после того, как сертификат агента регистрации будет выпущен.

4. Нажмите **OK** для сохранения шаблона.
5. Опубликуйте шаблон сертификата (см. «Публикация шаблона сертификата», с. 35).

#### 5.3.4.3 Для хранения на электронном ключе

Процедура представлена на примере копии шаблона **Агент регистрации**.

1. На вкладке **Общие** в поле **Отображаемое имя шаблона** введите имя для скопированного шаблона, например, **Агент регистрации JMS**.

2. Перейдите на вкладку **Шифрование** и отметьте один из следующих поставщиков криптографии (см. табл. 7).

*Табл. 7 - Поставщики криптографии для записи сертификата агента регистрации в память электронного ключа*

| Электронный ключ, на который будет выпускаться сертификат агента регистрации | Необходимый поствщик криптографии |
|---|---|
| JaCarta с приложением PKI<br>JaCarta с приложением PKI/BIO | **Microsoft Base Smart Card Crypto Provider** |
| Электронные ключи eToken (кроме eToken ГОСТ)<br>JaCarta с приложением PKI (обратная совместимость) | **eToken Base Cryptographic Provider** |

Чтобы в настройках шаблона появился поставщик криптографии **A eToken Base Cryptographic Provider**, на компьютере должно быть установлено соответствующе программное обеспечение для работы с электронными ключами (см. «Поддержка работы с электронными ключами и ПО для работы с ними», с. 17).

3. Перейдите на вкладку **Безопасность** и добавьте пользователю, который будет выполнять роль администратора JMS, разрешения: **Чтение**, **Заявка** и **Запись**.

В целях безопасности рекомендуется удалить эти разрешения после того, как сертификат агента регистрации будет выпущен.

4. Нажмите **ОК** для сохранения шаблона.
5. Опубликуйте шаблон сертификата (см. «Публикация шаблона сертификата», с. 35).

### 5.3.5 Шаблон сертификата для пользователей JMS

Процедура представлена на примере шаблона **Пользователь со смарт-картой**.

1. На вкладке **Общие** в поле **Отображаемое имя шаблона** введите имя для скопированного шаблона, например, **Пользователь JMS**.
2. Перейдите на вкладку **Требования выдачи** и выполните следующие действия.
3. Установите флаг **Указанного числа авторизованных подписей**.
4. В списке **В подписи требуется указать тип политики** выберите пункт **Политика применения**.

5. В списке **Политика применения** выберите пункт **Агент запроса сертификата** (см. рис. 16).

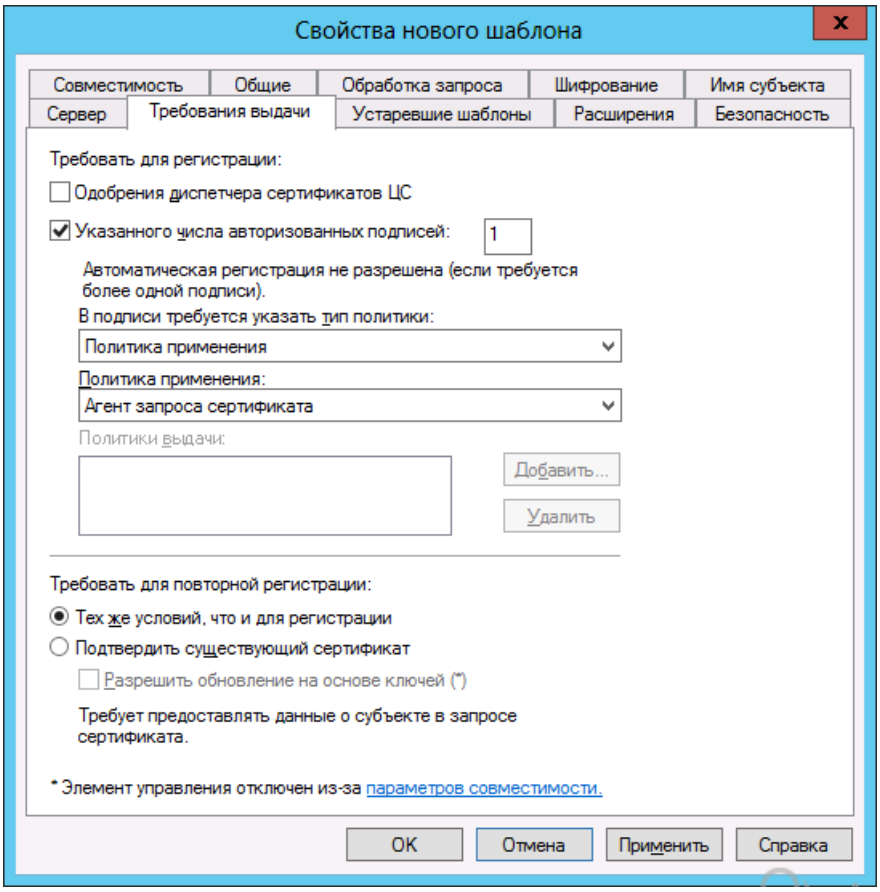



*Рис. 16 – Вкладка **Требования выдачи***

6. Перейдите на вкладку **Безопасность** и установите необходимые разрешения.

Компьютер, который является сервером JMS, должен иметь разрешения **Чтение** и **Заявка**.

7. Нажмите **OK** для сохранения шаблона и опубликуйте шаблон сертификата (см. «Публикация шаблона сертификата», с. 35).

## 5.4 Публикация шаблона сертификата

1. В окне консоли центра сертификации щелкните правой кнопкой на пункте **Шаблоны сертификатов** и выберите **Создать -> Выдаваемый шаблон сертификата** (см. рис. 17).

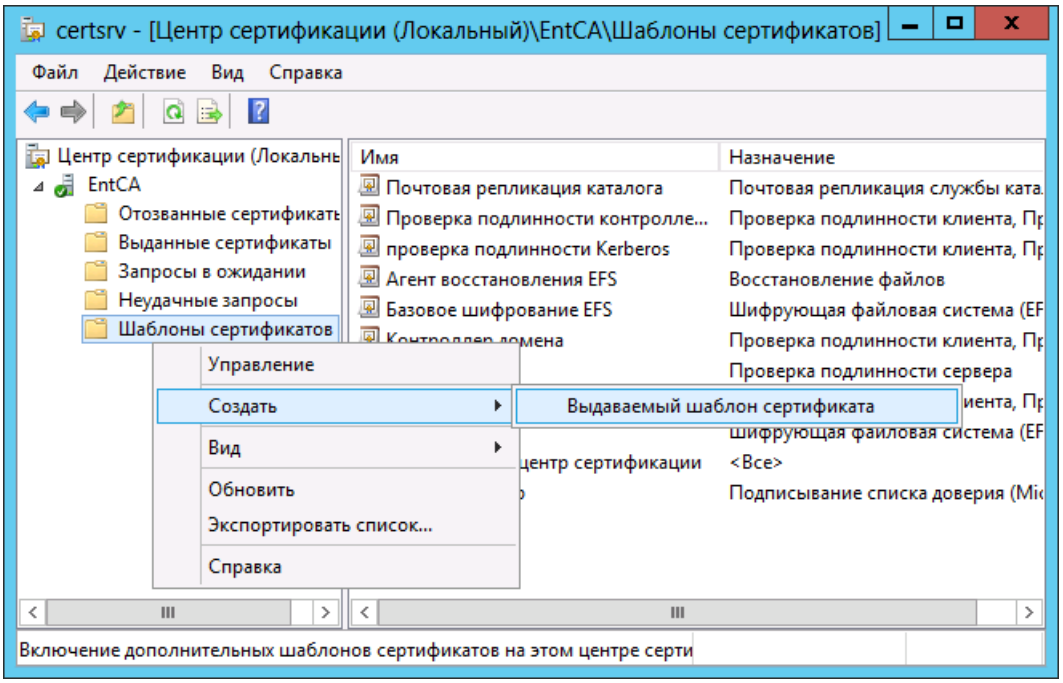
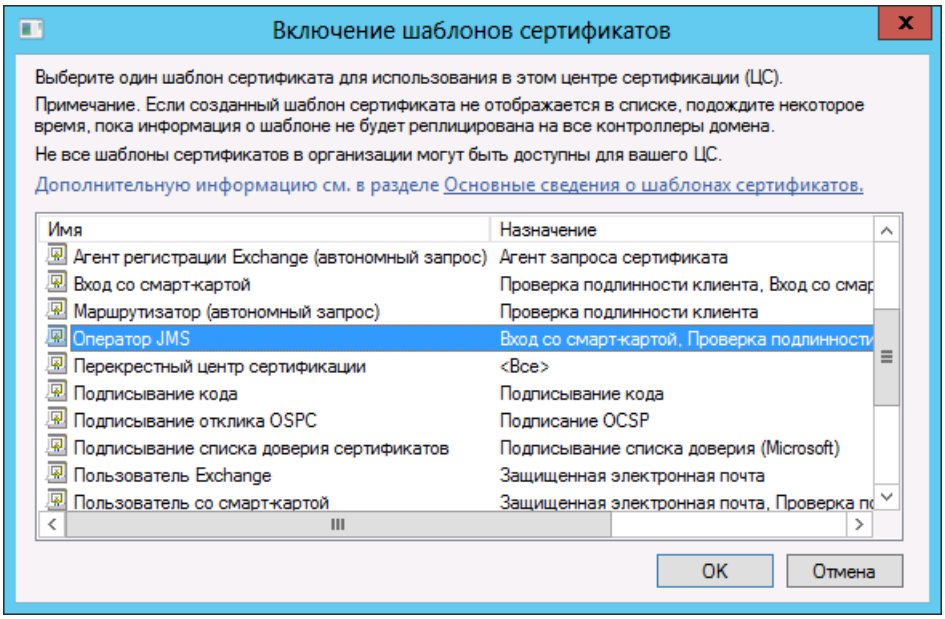



*Рис. 17 – Создание выдаваемого шаблона сертификата*

Отобразится следующее окно.




2. Выберите нужный шаблон или шаблоны и нажмите **OK**.

## 5.5 Выпуск сертификатов по подготовленным шаблонам

### 5.5.1 Запись сертификата в память электронного ключа

Процедура записи сертификата в память электронного ключа может быть использована для следующих сертификатов:

- сертификат оператора JMS;
- сертификат агента регистрации.

Чтобы выпустить электронный ключ оператора JMS с сертификатом, созданным по опубликованному шаблону (см. «Шаблон сертификата оператора JMS», с. 27), выполните следующие действия.

1. Подсоедините электронный ключ к компьютеру.
2. Из командной строки выполните команду **certmgr.msc**.
3. В отобразившимся окне щелкните правой кнопкой на пункте **Личное** и в контекстном меню выберите **Все задачи -> Запросить новый сертификат** (см. рис. 18).

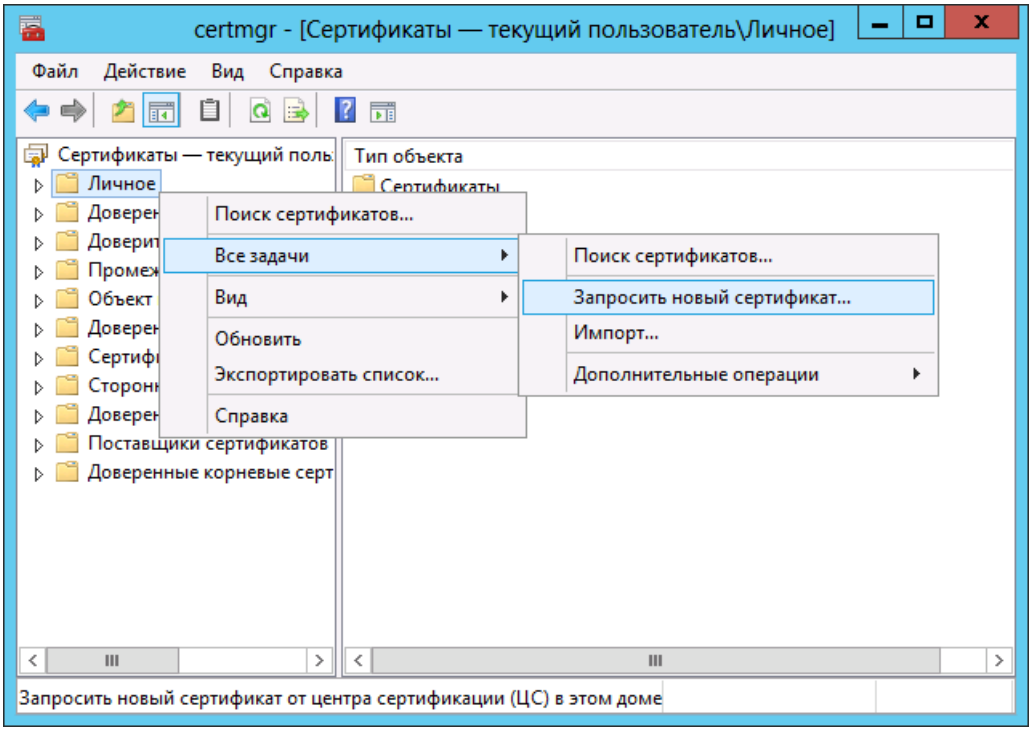



*Рис. 18 – Запрос нового сертификата*

Отобразится следующее окно.

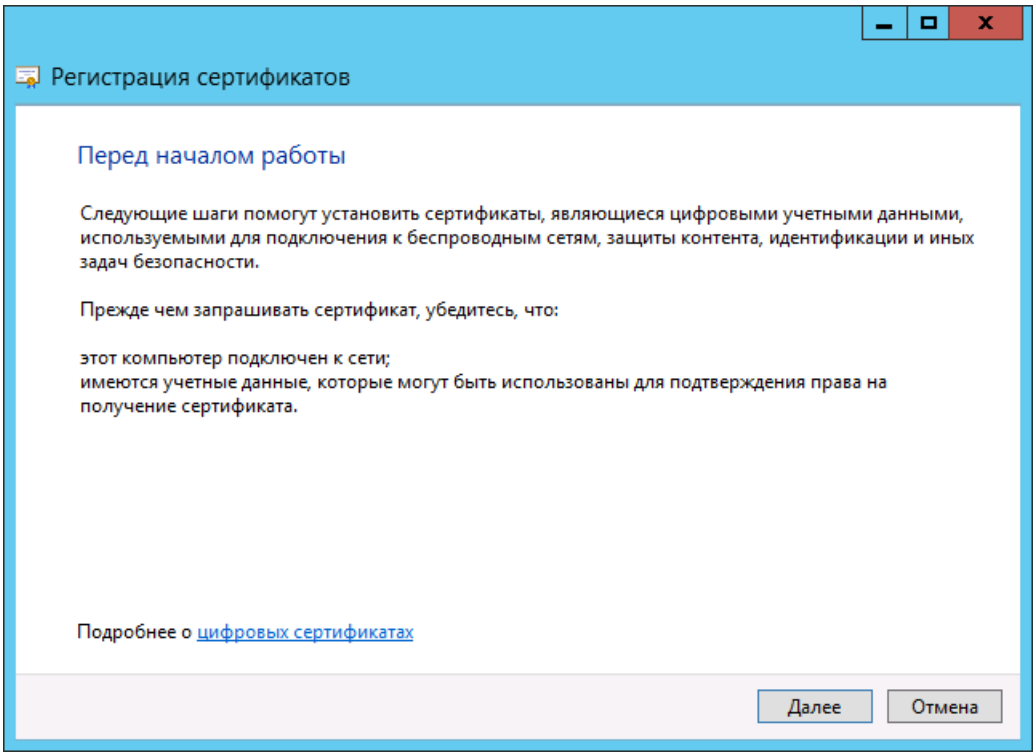



*Рис. 19 – Окно приветствия мастера запроса сертификата*

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

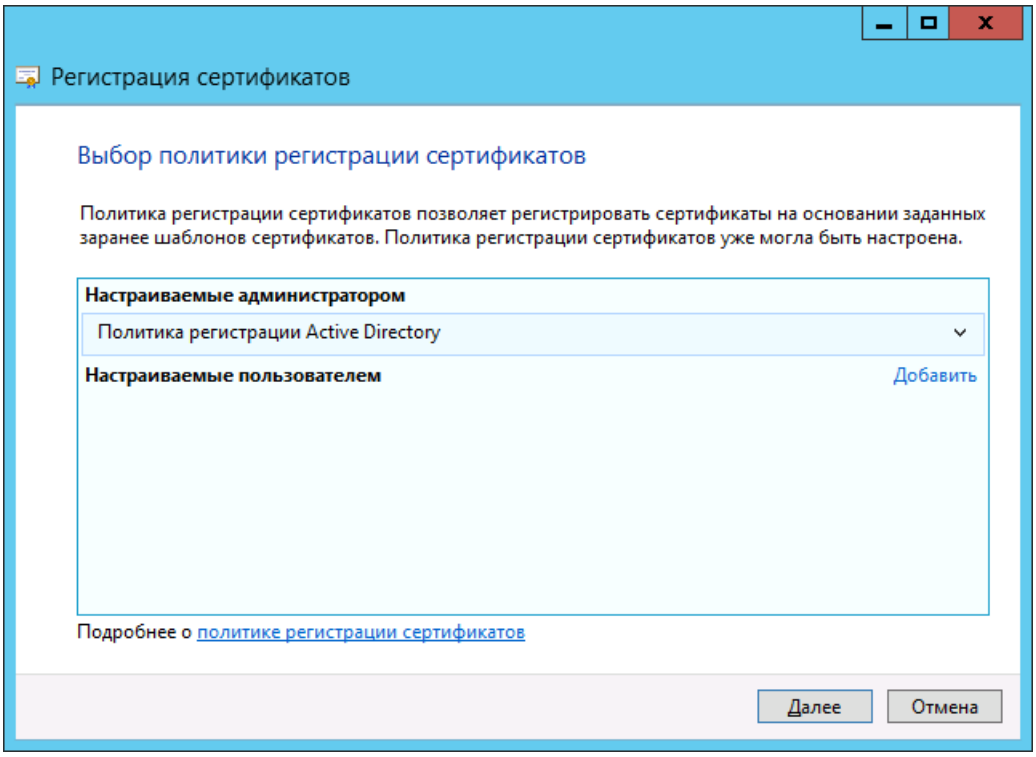



*Рис. 20 – Окно выбора политики регистрации сертификатов*

5. Нажмите **Далее**.

Отобразится следующее окно.

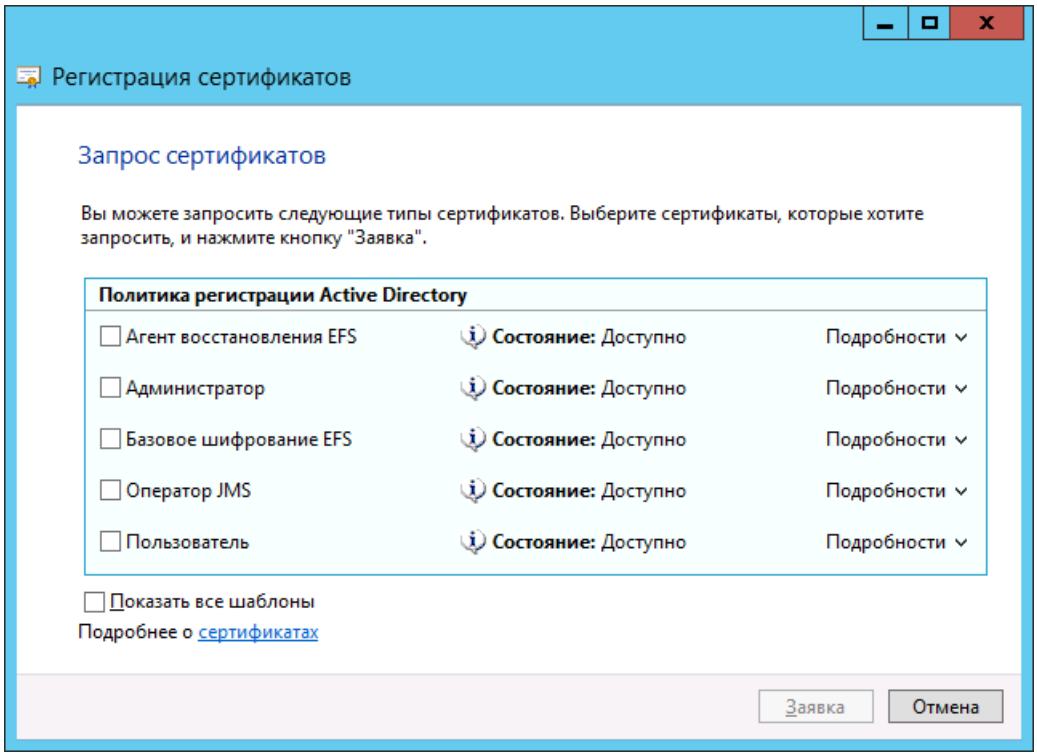



*Рис. 21 – Окно выбора шаблона сертификата*

6. Отметьте подготовленный шаблон сертификата оператора JMS и нажмите **Заявка**.
7. Введите PIN-код пользователя электронного ключа, когда появится соответствующее окно, и подтвердите выбор.
   При успешном завершении запроса отобразится следующее окно.

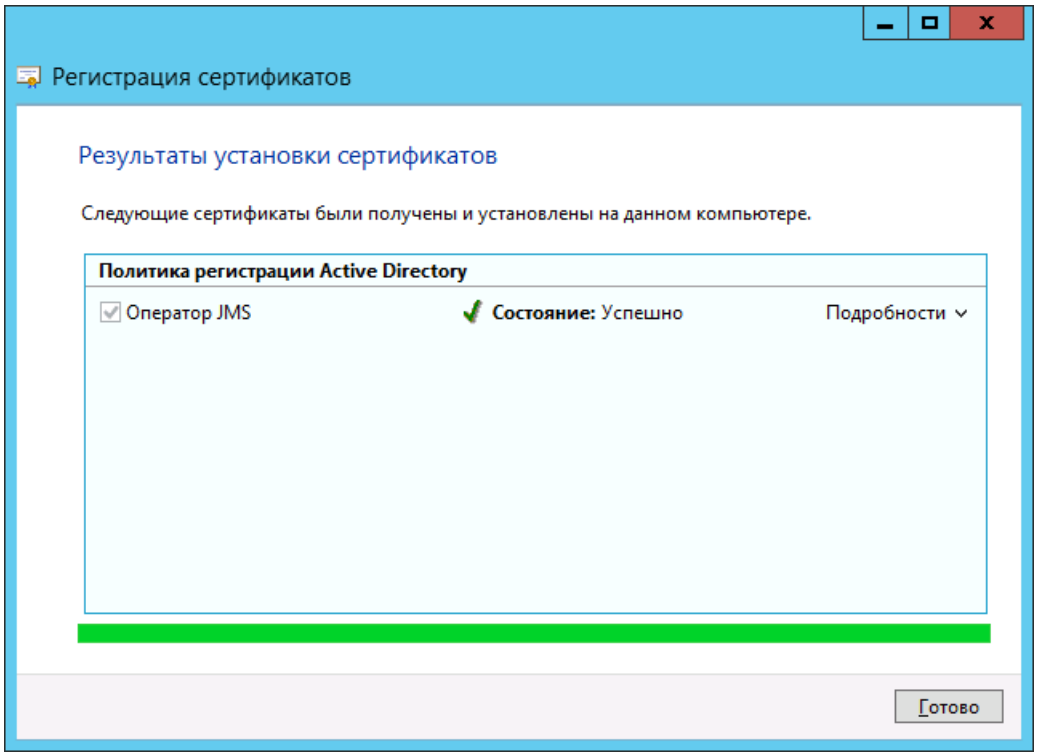



*Рис. 22 – Успешное завершение запроса сертификата*

8. Нажмите **Готово** для завершения процедуры.

### 5.5.2 Выпуск сертификата в хранилище пользователя

Процедура выпуска сертификата в хранилище текущего пользователя может быть использована для выпуска сертификата агента регистрации. Чтобы выпустить сертификат в хранилище текущего пользователя, выполните следующие действия.

1. Из командной строки выполните команду **certmgr.msc**.
   Отобразится следующее окно.

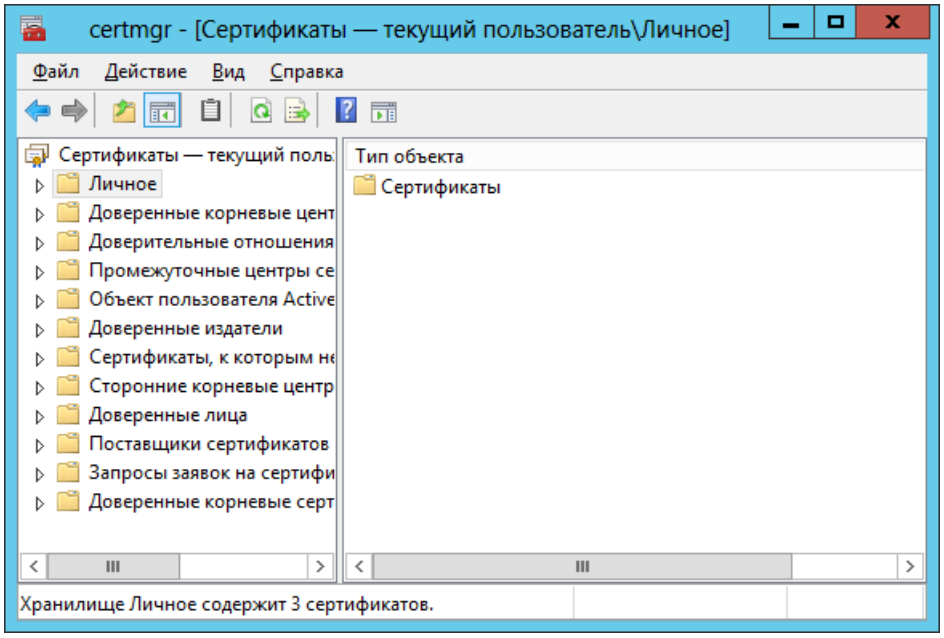



*Рис. 23 – Окно оснастки хранилища сертификатов пользователя*

2. Щелкните правой кнопкой на пункте **Личное** и выберите **Все задачи -> Запросить новый сертификат**.

Отобразится следующее окно.

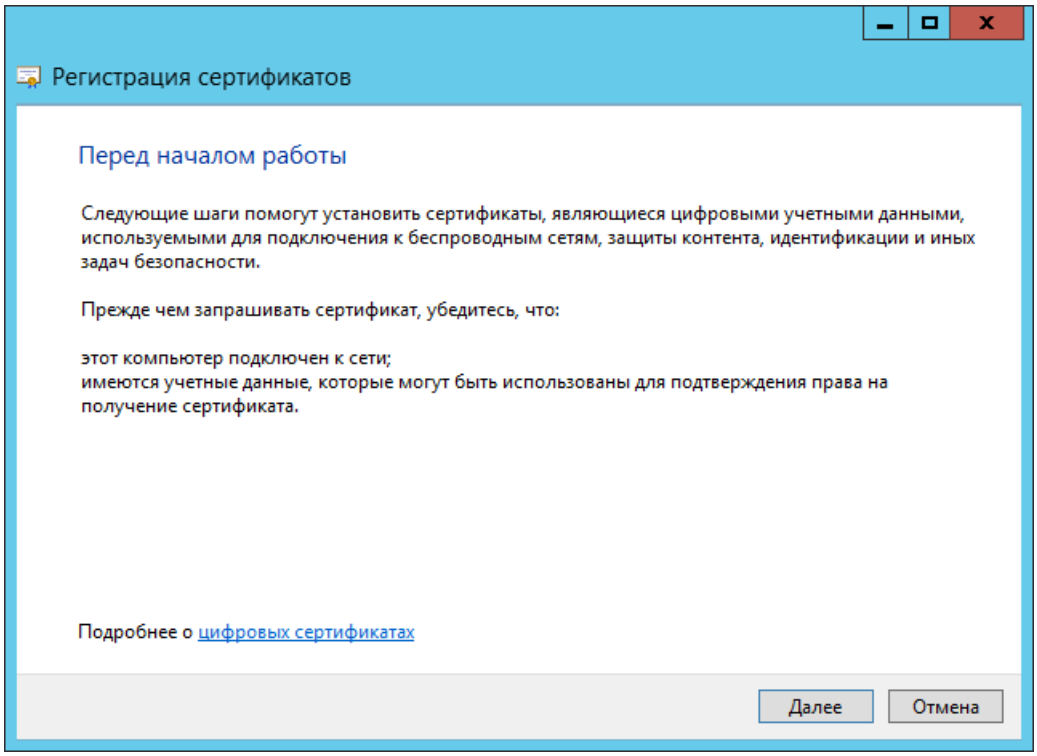



*Рис. 24 – Подготовка к запросу сертификата*

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

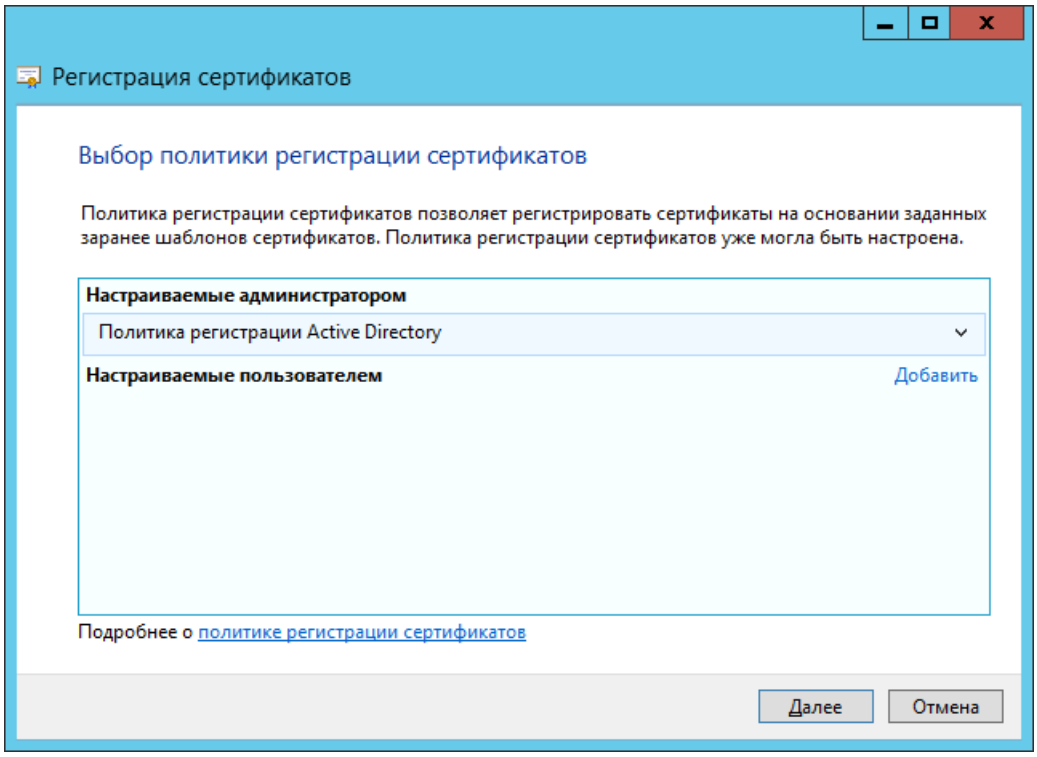



*Рис. 25 – Выбор политики регистрации сертификатов*

4. Нажмите **Далее**.

Отобразится следующее окно.

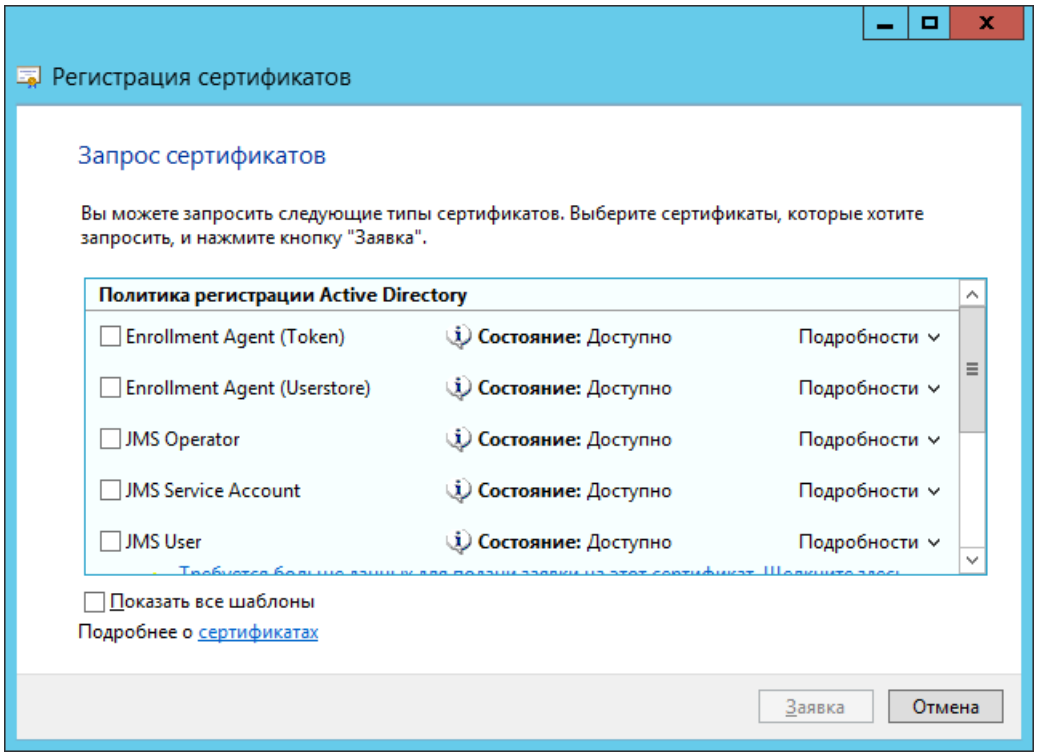



*Рис. 26 – Выбор шаблона выпускаемого сертификата*

5. Отметьте нужный шаблон сертификата, после чего нажмите **Заявка**.
При успешном выпуске отобразится следующее окно.

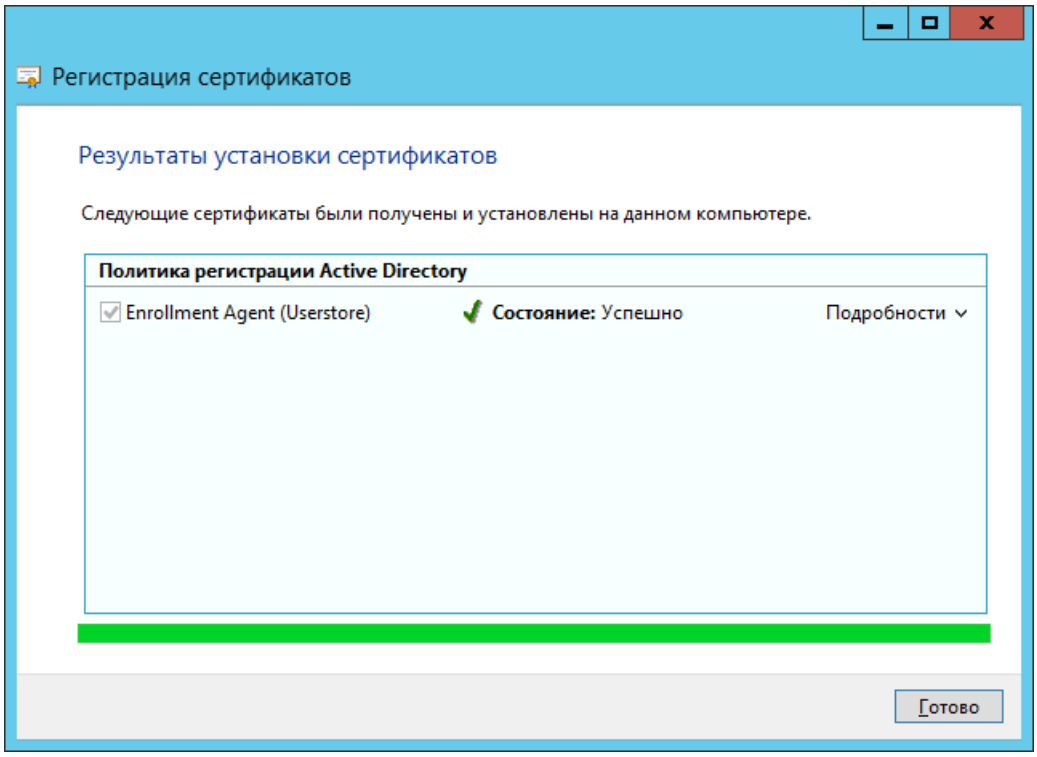



*Рис. 27 – Сертификат успешно выпущен*

6. Нажмите **Готово** для завершения процедуры.

### 5.5.3 Выпуск сертификата в хранилище сертификатов компьютера

Процедура выпуска сертификатов с помещением их в хранилище сертификатов компьютера актуальна для следующих сертификатов:

- сертификат для службы аутентификации JMS;
- сертификат для обеспечения SSL-соединения сервера JMS с административным агентом из состава JMS Admin;
- сертификат для обеспечения SSL-соединения сервера JMS с клиентским агентом из состава JMS Client;
- сертификат для обеспечения SSL-соединения сервера JMS с сервером SQL;
- сертификат агента регистрации для сервера JMS.

Чтобы выпустить сертификат в хранилище локального компьютера на сервере JMS, выполните следующие действия.

1. На сервере JMS из командной строки выполните команду **mmc**.
   Отобразится следующее окно.

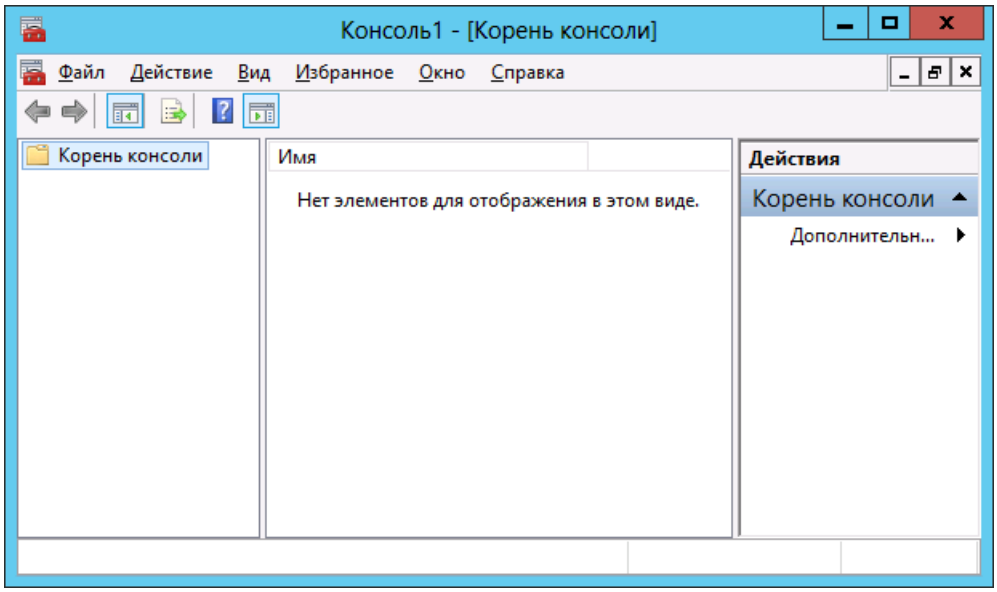



*Рис. 28 – Корень консоли оснасток mmc*

2. В верхней панели выберите **Файл -> Добавить или удалить оснастку** (или нажмите сочетание клавиш CTRL+M).

Отобразится следующее окно.

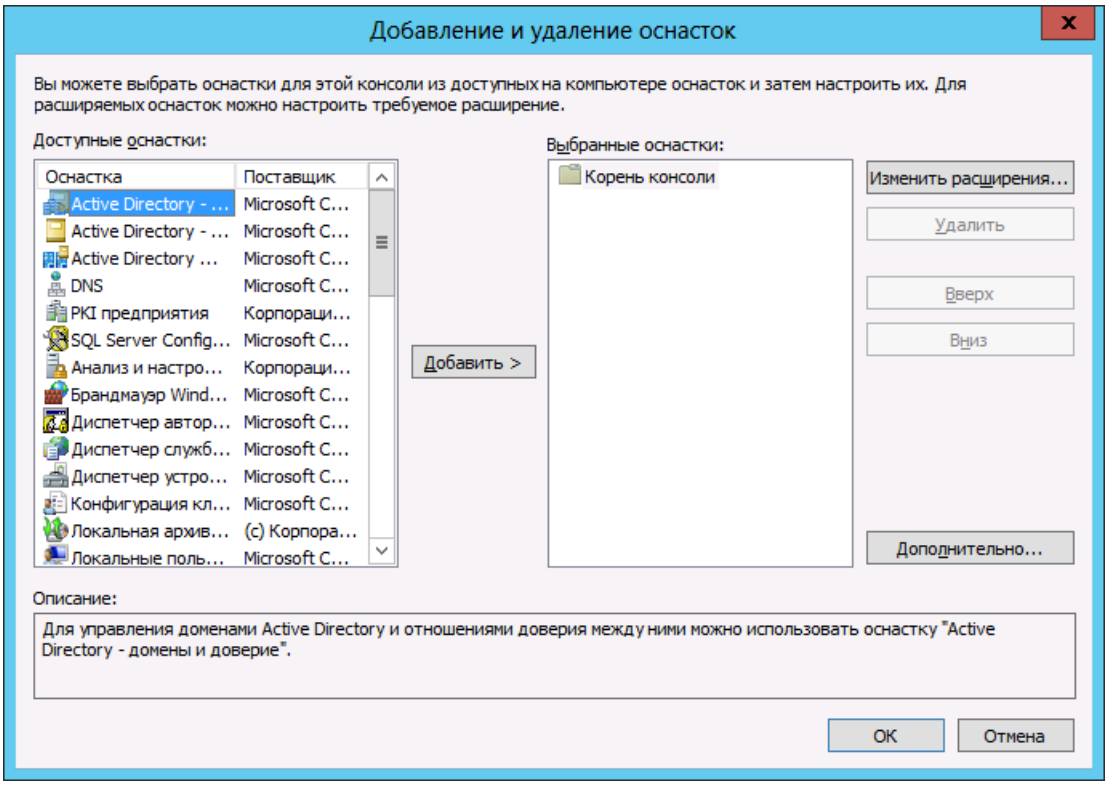



*Рис. 29 – Добавление или удаление оснасток*

3. В списке **Доступные оснастки** выберите оснастку **Сертификаты** и нажмите **Добавить**. Отобразится следующее окно.

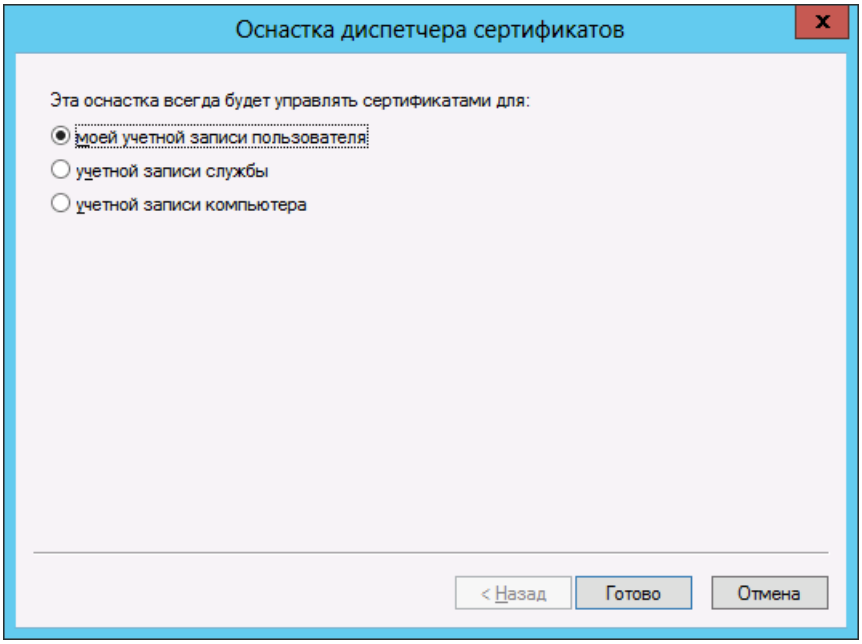



*Рис. 30 – Выбор типа оснастки*

4. Выберите **учетной записи компьютера** и нажмите **Готово**.

Отобразится следующее окно.

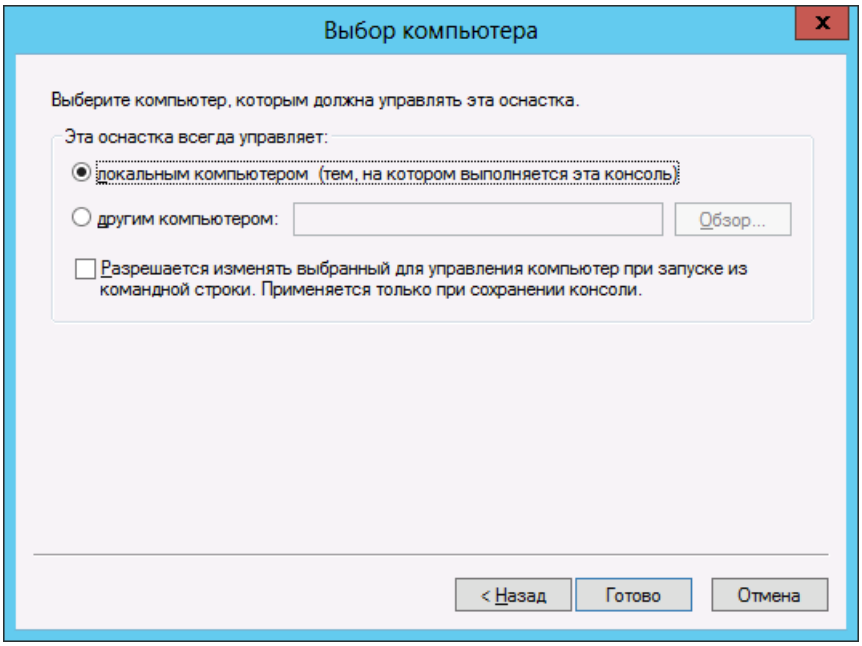



*Рис. 31 – Выбор компьютера*

5. Выберите **локальным компьютером** и нажмите **Готово**.
   Окно добавления и удаления оснасток будет выглядеть следующим образом.

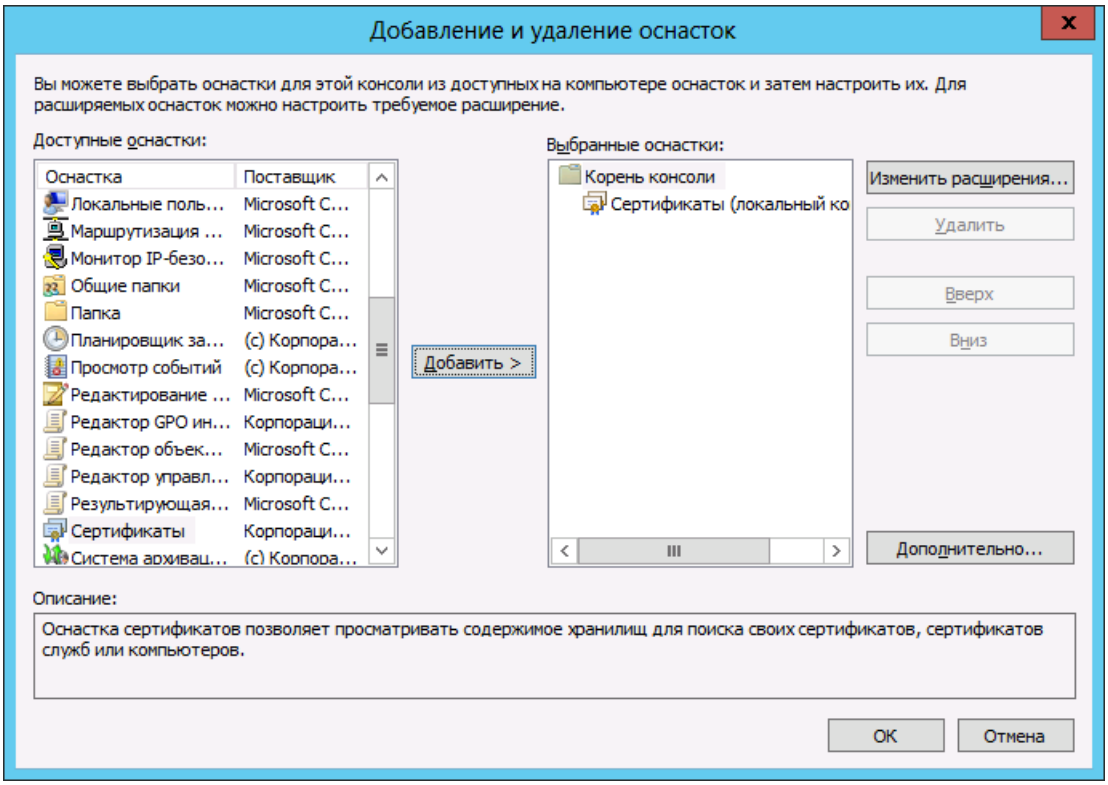



*Рис. 32 – Оснастка Сертификаты (локальный компьютер) добавлена*

6. Нажмите **OK**.

7. В отобразившемся окне оснастки выберите **Личное -> Все задачи -> Запросить новый сертификат** (см. рис. 33).

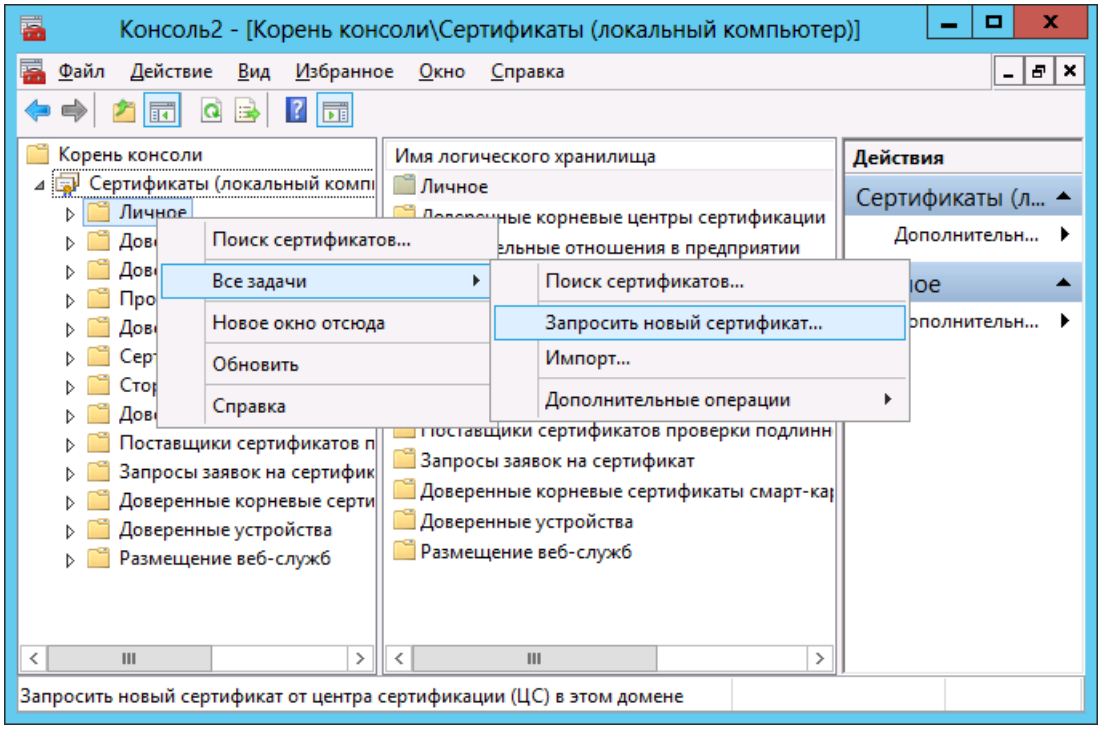



*Рис. 33 – Запрос сертификата*

Отобразится следующее окно.

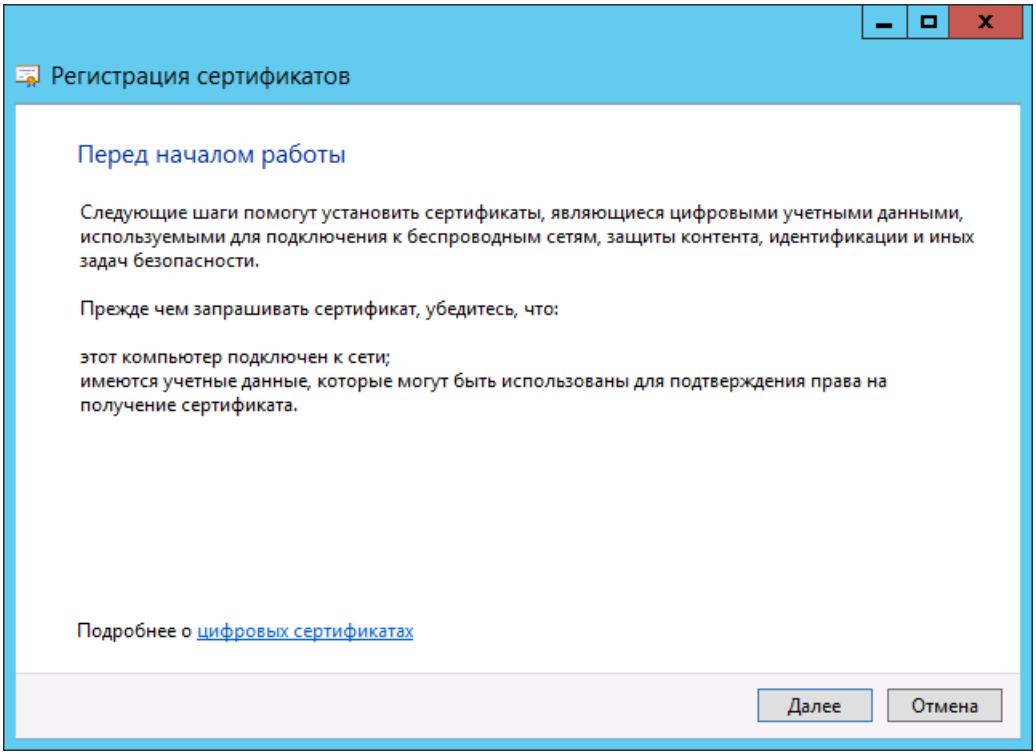



*Рис. 34 – Окно приветствия мастера регистрации сертификатов*

8. Нажмите **Далее**.

Отобразится следующее окно.

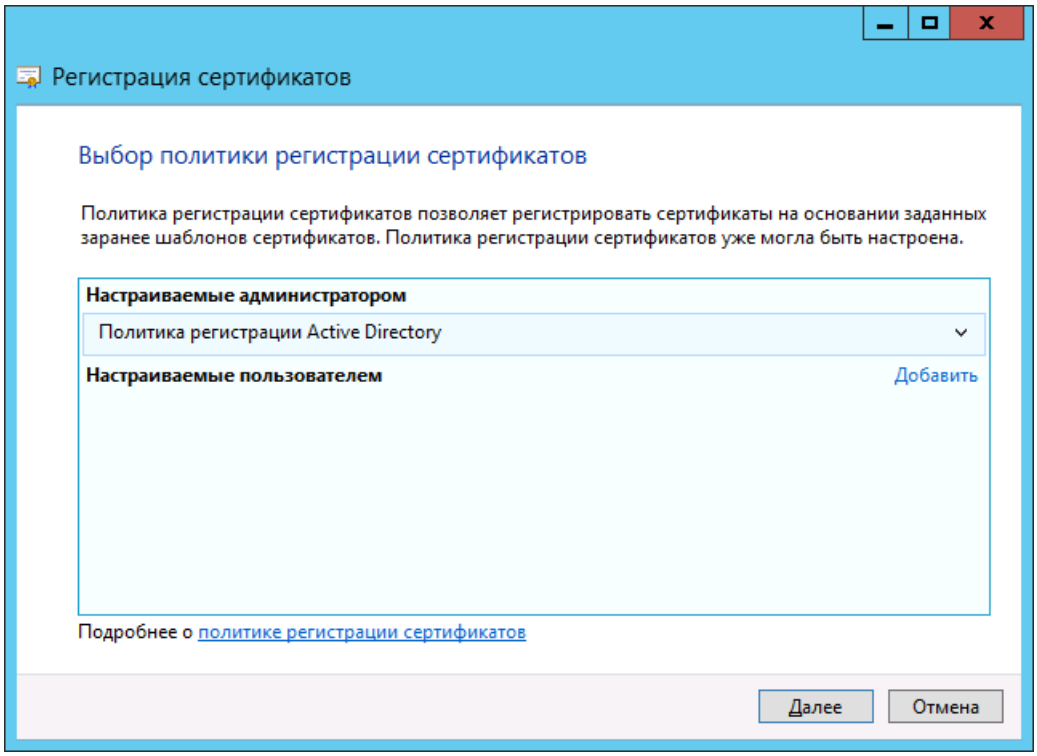



*Рис. 35 – Окно выбора политики регистрации сертификатов*

9. Нажмите **Далее** и продолжите процедуру в зависимости от типа запрашиваемого сертификата (см. табл. 8).

*Табл. 8 – Зависимость процедуры выпуска от типа запрашиваемого сертификата*

| Тип запрашиваемого сертификата | Процедура выпуска |
|---|---|
| • Сертификат для службы аутентификации JMS (если планируется единичная установка JMS без кластера);<br>• сертификат для обеспечения SSL-соединения сервера JMS с административным агентом из состава JMS Admin;<br>• сертификат для обеспечения SSL-соединения сервера JMS с административным агентом из состава JMS Client;<br>• сертификат для обеспечения SSL-соединения сервера JMS с сервером SQL;<br>• сертификат агента регистрации для сервера JMS (если планируется единичная установка JMS без кластера). | См. «Имя субъекта сертификата подставляется автоматически» ниже. |
| • Сертификат для службы аутентификации JMS (если планируется развертывание JMS в кластере);<br>• сертификат агента регистрации для сервера JMS (если планируется развертывание JMS в кластере). | См. «Имя субъекта сертификата вводится вручную», с. 48. |

#### 5.5.3.1 Имя субъекта сертификата подставляется автоматически

Отобразится следующее окно.

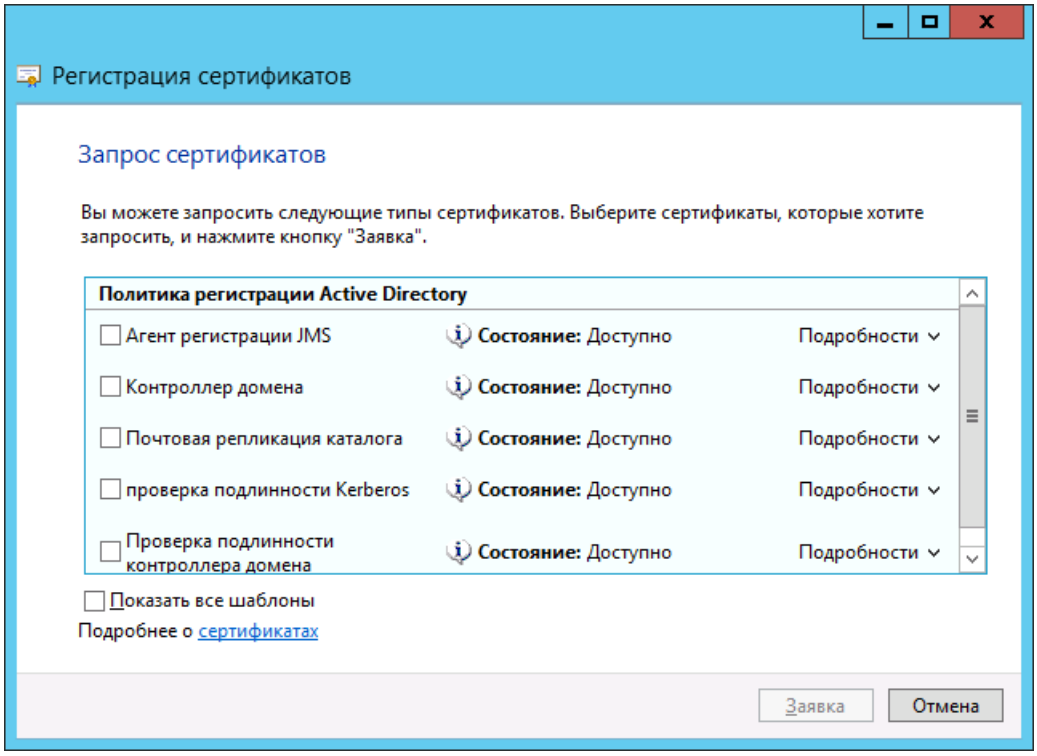



*Рис. 36 – Окно выбора шаблона сертификата*

1. Отметьте подготовленный сертификат (созданный на основе копии шаблона **Агент регистрации (компьютер)** или **Компьютер**) и нажмите **Заявка**.
   В случае успешного завершения операции отобразится следующее окно.

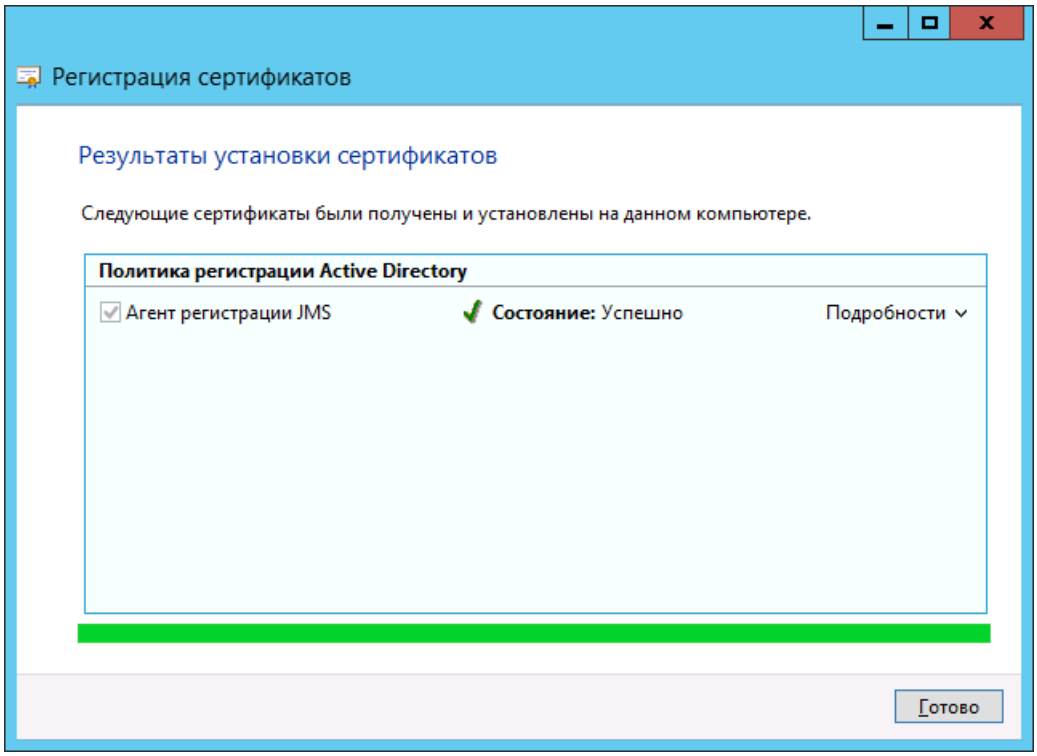



*Рис. 37 – Успешный выпуск сертификата*

2. Нажмите **Готово**, чтобы закрыть окно мастера регистрации сертификатов.
3. Убедитесь, что сертификат установлен в личное хранилище сервера JMS (см. рис. 38).

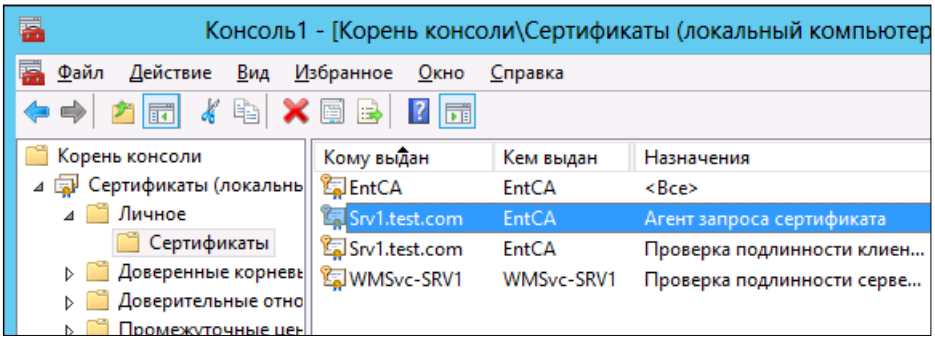



*Рис. 38 – Сертификат установлен в хранилище сертификатов компьютера*

4. Сохраните оснастку хранилища сертификатов компьютера на рабочем столе для удобства дальнейшего использования.

Если вы выпустили сертификат для службы аутентификации JMS и планируете использовать JMS с внедоменными компьютерами, убедитесь в том, что этот сертификат содержит настроенный HTTP-адрес точки распространения списков отзыва – см. рис. 39.

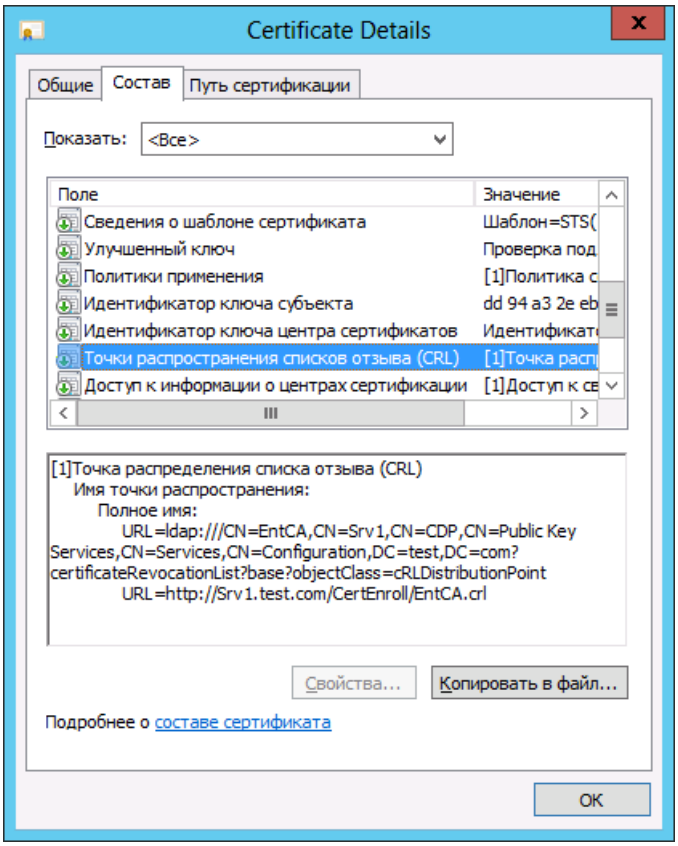



*Рис. 39 – HTTP-адрес точки распространения списков отзыва сертификатов*

### 5.5.3.2 Имя субъекта сертификата вводится вручную

**Примечание.** Материал в настящем подразделе приводится на примере подготовки сертификата службы аутентификации JMS для кластера. Более детально процедура создания шаблонов и выпуска сертификатов для кластера описана в руководстве по развёртыванию кластерной конфигурации JMS [6].

Отобразится следующее окно.

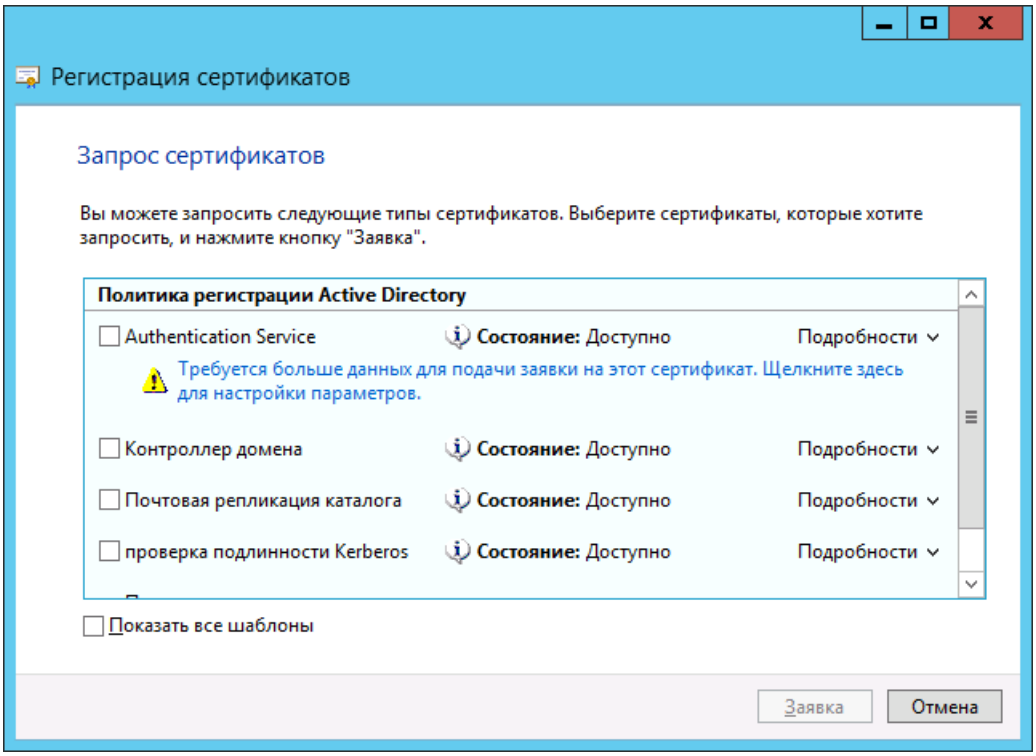



*Рис. 40 – Выбор шаблона сертификата*

1. Под шаблоном сертификата, для которого имя субъекта нужно вводить вручную, располагается ссылка **Требуется больше данных для подачи заявки на этот сертификат**. Щелкните на этой ссылке.

Отобразится следующее окно.

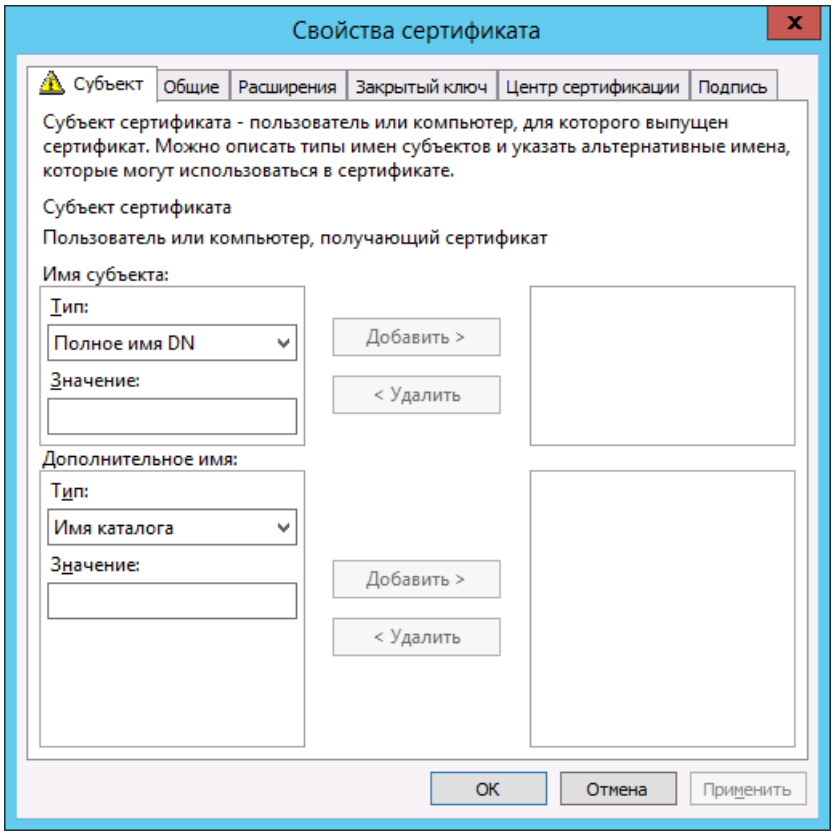



*Рис. 41 – Вкладка **Субъект** окна свойств сертификата*

2. В секции **Имя субъекта** из списка **Тип** выберите пункт **Общее имя**.
3. В поле **Значение** введите полное доменное имя кластера (FQDN), например, **JMS-Cluster.test.com**.
4. Нажмите **Добавить**.

Окно будет иметь следующий вид.

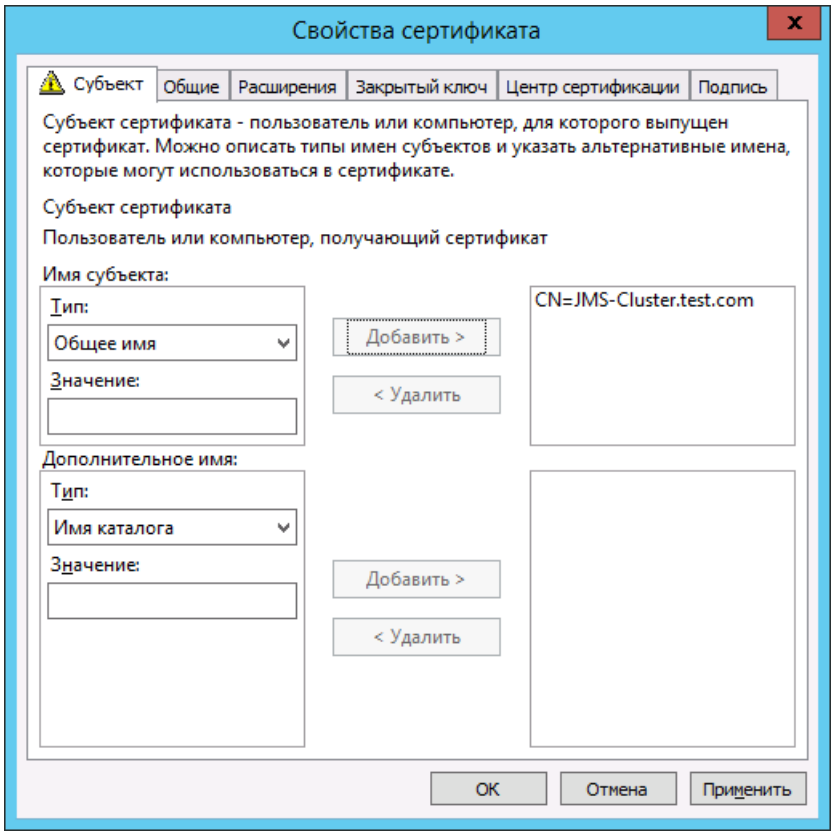



*Рис. 42 – Имя субъекта сертификата добавлено в запрос*

5. Перейдите на вкладку **Общие**.

Окно примет следующий вид.

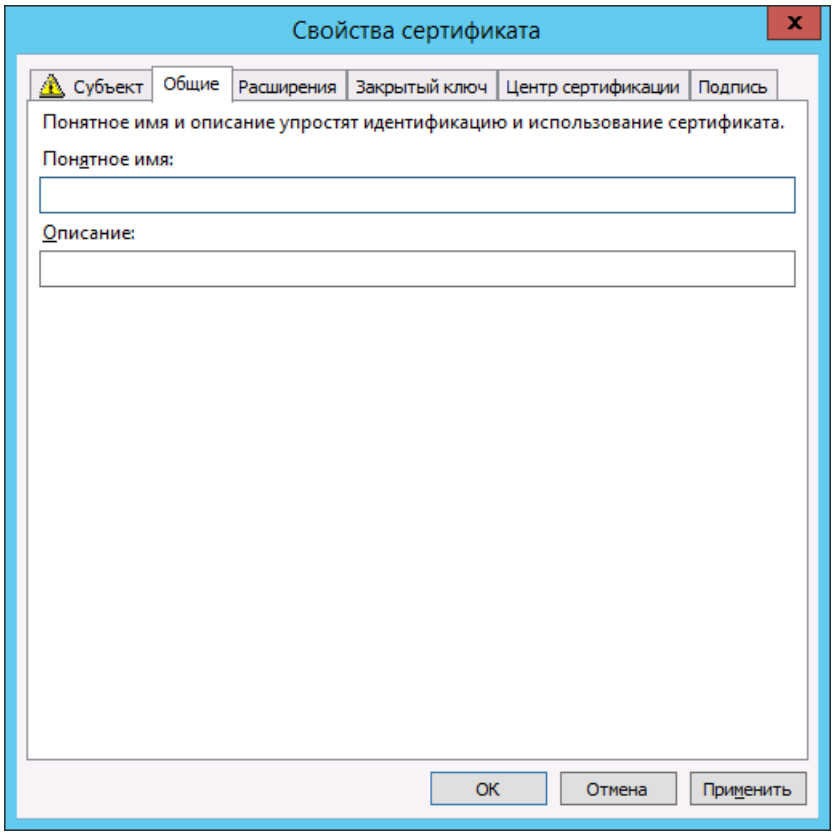



*Рис. 43 – Вкладка **Общие***

6. Заполните необходимые поля и перейдите на вкладку **Закрытый ключ**.

Окно примет следующий вид.

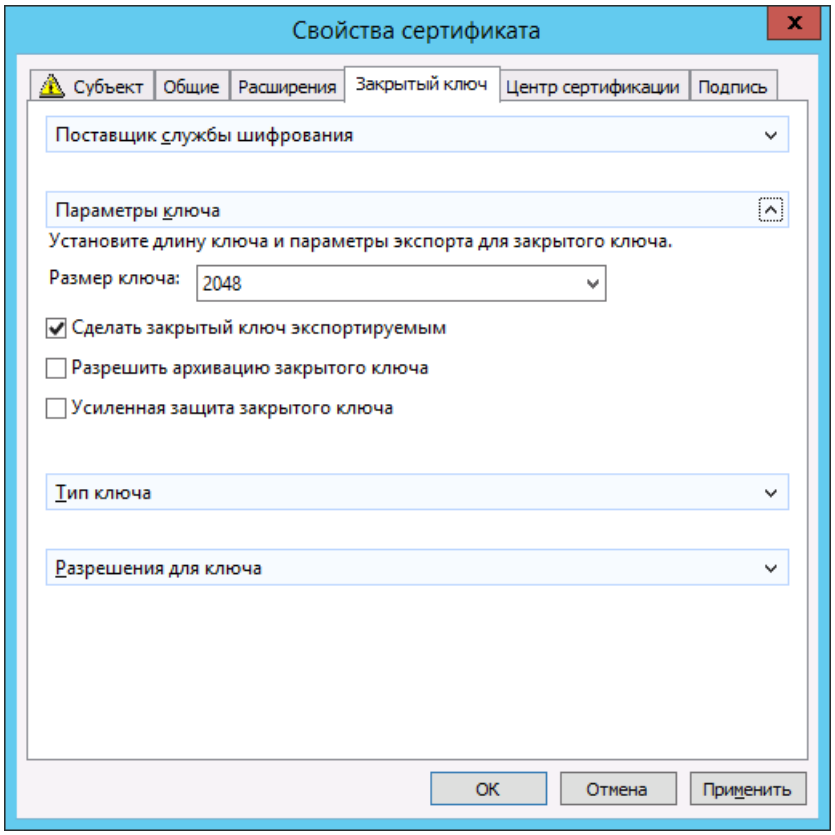



*Рис. 44 – Вкладка Закрытый ключ*

7. Убедитесь в том, что установлен флаг **Сделать закрытый ключ экспортируемым**.
8. Нажмите **OK**, чтобы сохранить изменения.
9. В окне регистрации сертификатов нажмите **Далее**.

При успешном выпуске отобразится следующее окно.

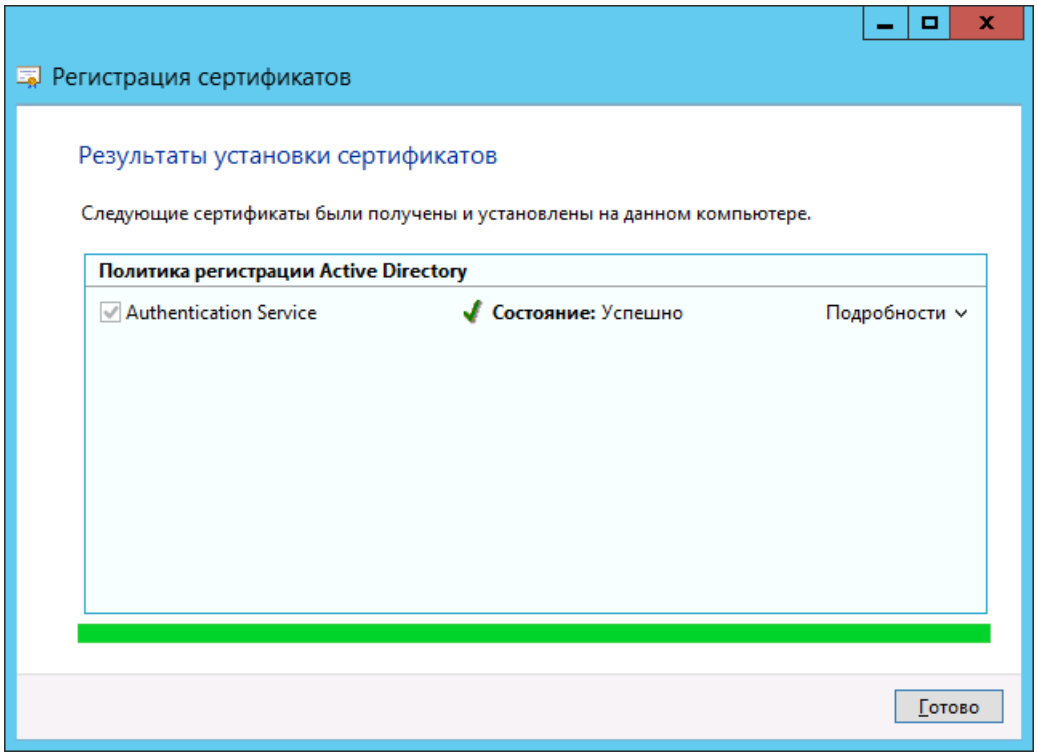



*Рис. 45 – Успешный выпуск сертификата*

10. Убедитесь в том, что в качестве субъекта сертификата указано полное доменное имя кластера JMS (например, **JMS-Cluster.test.com**), как показано рис. 46.

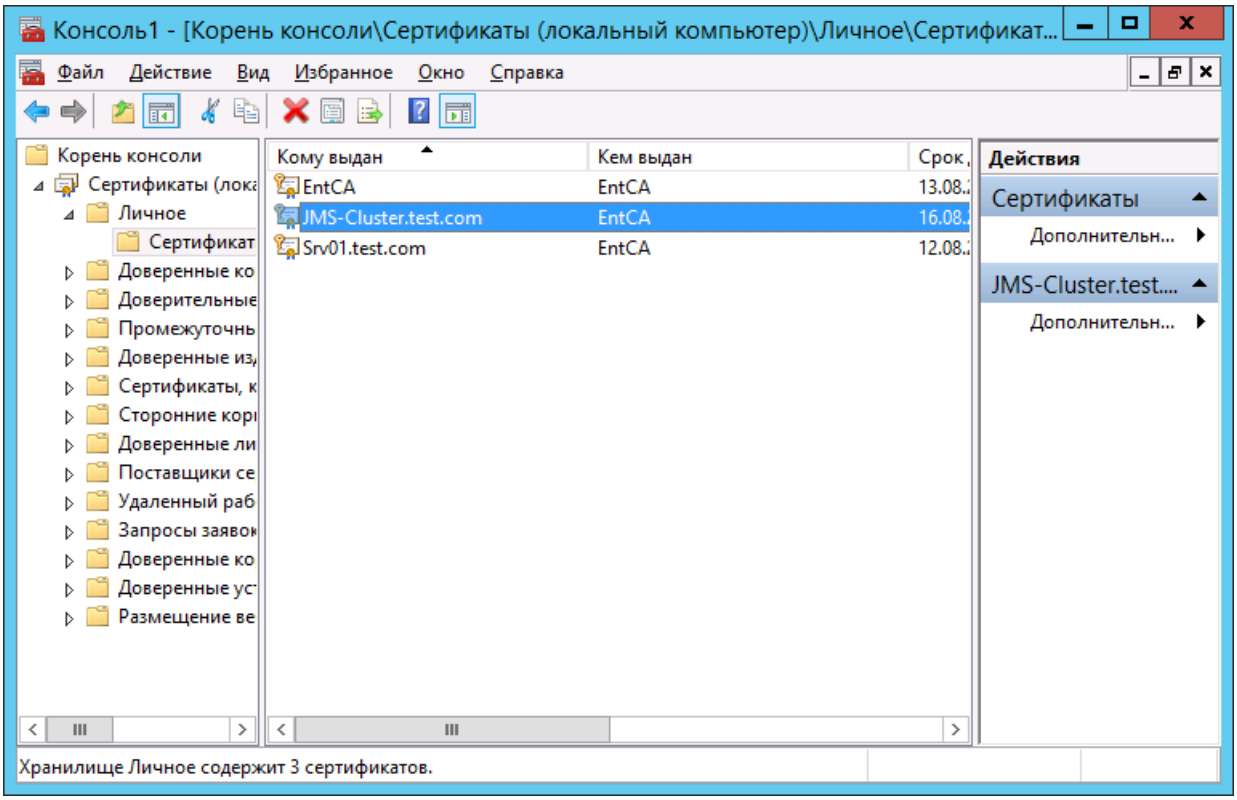



*Рис. 46 – Полное доменное имя кластера JMS указано в качестве субъекта сертификата*

# 6. Подготовка сервера MS SQL для работы по SSL/TLS

Выполните действия, представленные в настоящем разделе, если вы хотите настроить соединение сервера JMS и базы данных Microsoft SQL по протоколу SSL. В противном случае пропустите настоящий раздел.

⚠ Для выполнения настройки необходимо, чтобы на сервере Microsoft SQL был установлен компонент Диспетчер конфигурации SQL Server.

1. На сервере Microsoft SQL установите сертификат в хранилище компьютера (подробнее см. «Сертификаты для работы с JMS», с. 24).
2. Запустите **Диспетчер конфигурации SQL Server**.
   Отобразится следующее окно.

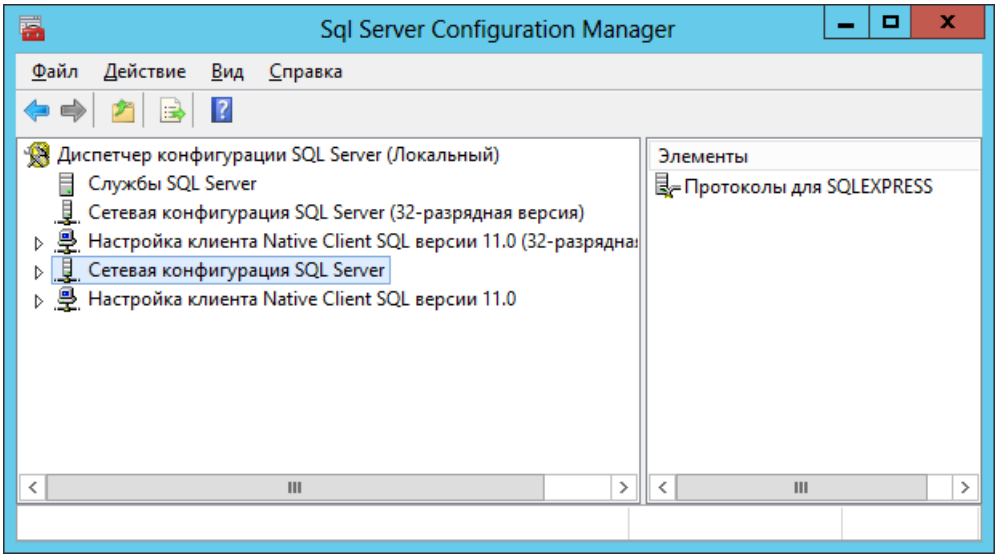



*Рис. 47 – Окно Диспетчера конфигурации сервера SQL*

3. В левой части окна выберите пункт **Службы SQL Server**.
   Окно примет следующий вид.

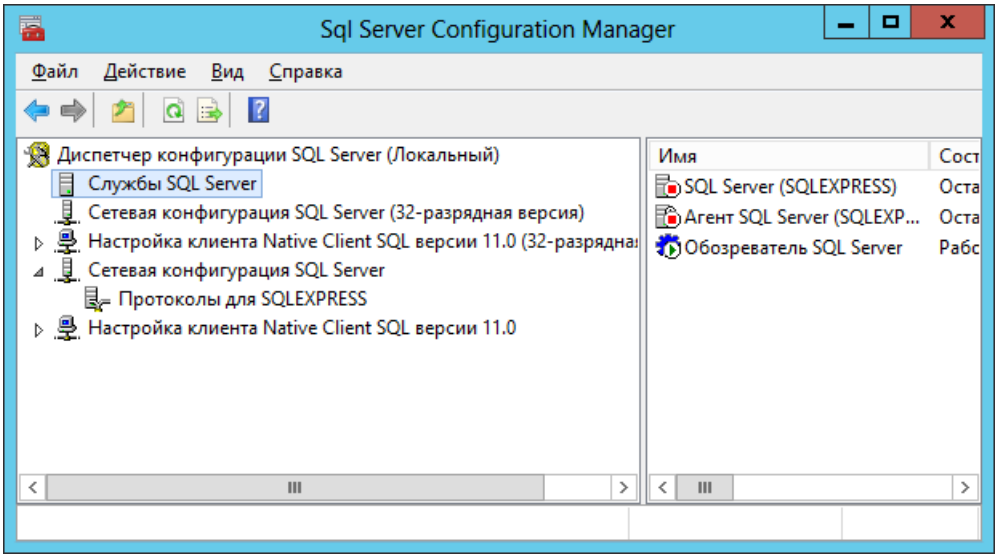



*Рис. 48 – Список служб сервера SQL*

4. В правой части окна выберите **SQL Server** и в верхней панели выберите **Действие -> Свойства**.

Отобразится следующее окно.

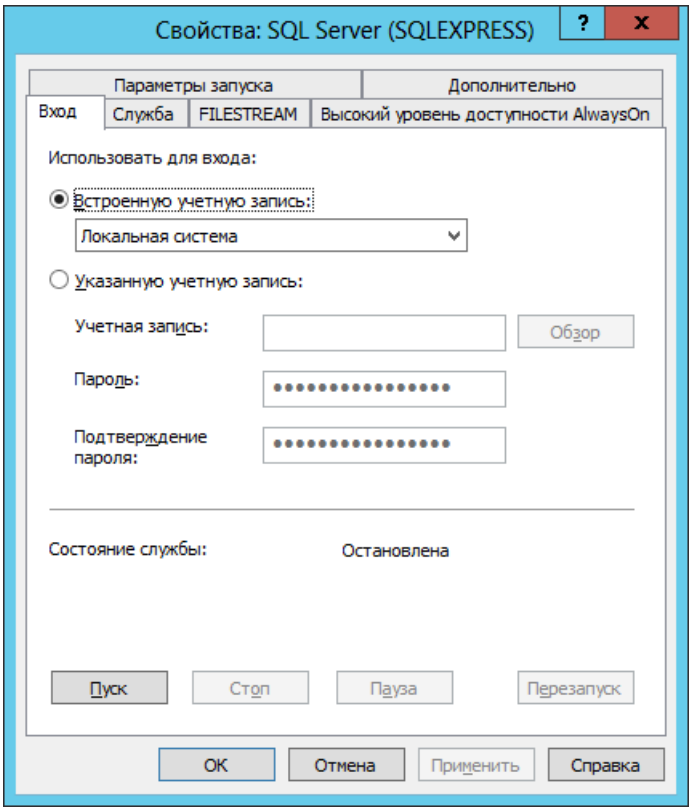



*Рис. 49 – Вкладка **Вход** окна свойств службы SQL Server*

5. Выберите учетную запись, от имени которой будет запускаться служба сервера SQL.

В настоящем документе для примера используется служба Локальная система.

6. Нажмите **OK**, чтобы сохранить изменения.
7. В окне Диспетчера конфигурации сервера SQL разверните узел **Сетевая конфигурация SQL Server** и выберите пункт, который начинается со слов **Протоколы для**.
8. В верхней панели выберите **Действие -> Свойства**.

Отобразится следующее окно.

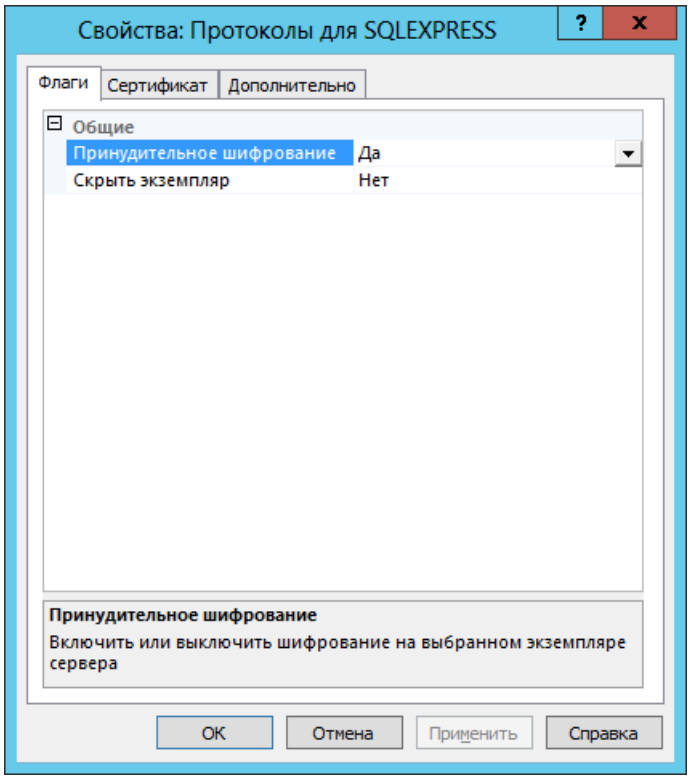



*Рис. 50 – Вкладка **Флаги** свойств протоколов для сервера SQL*

9. В списке **Принудительное шифрование** выберите **Да**, после чего перейдите на вкладку **Сертификат**.
   Окно примет следующий вид.

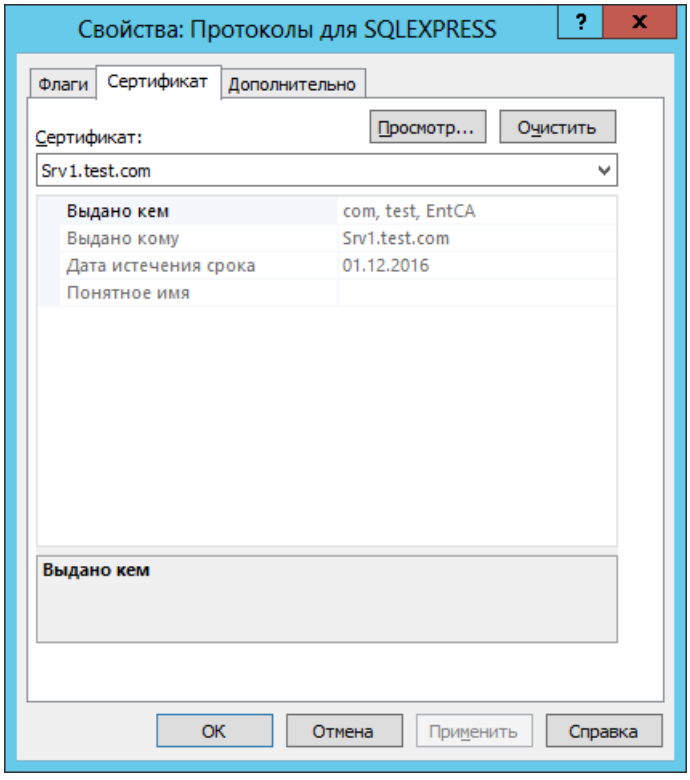



*Рис. 51 – Вкладка **Сертификат** свойств протоколов для сервера SQL*

10. В списке **Сертификат** выберите сертификат для сервера SQL, установленный в хранилище локального компьютера на сервере SQL.
11. Нажмите **OK**, чтобы сохранить изменения.
12. Подтвердите выбор в окне предупреждающего сообщения (см. рис. 52).

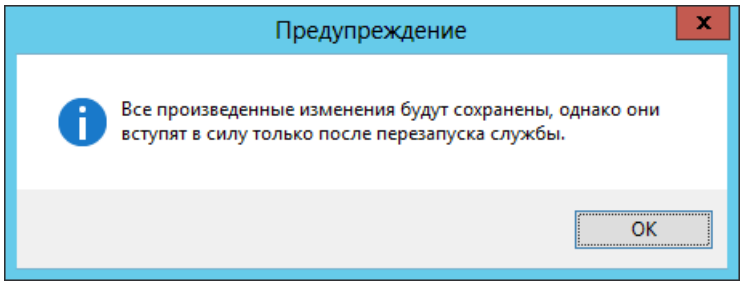



*Рис. 52 – Предупреждение о необходимости перезапуска службы SQL-сервера*

13. В левой части окна Диспетчера конфигурации сервера SQL выберите пункт **Службы SQL Server**.
14. В правой части окна Диспетчера конфигурации сервера SQL перезапустите службу SQL Server; также убедитесь в том, что служба **Обозреватель SQL Server запущена**.

# 7. Регистрация SPN-записи для службы сервера JMS

Для работы JMS необходимо, чтобы SPN-запись службы сервера JMS была зарегистрирована в Active Directory. Если учетная запись, от имени которой будет производиться первоначальная настройка конфигурации JMS, обладает достаточными правами (например, входит в группу **Администраторы домена**), SPN-запись будет зарегистрирована автоматически. В противном случае существует два способа регистрации SPN-записи:

- предоставление соответствующих прав учетной записи, от имени которой будет производиться первоначальная конфигурация JMS – если предоставить учетной записи соответствующие разрешения, регистрация SPN-записи произойдет автоматически при первоначальной настройке конфигурации JMS (подробнее см. «Настройка учетной записи, от имени которой будет производиться первоначальная настройка» ниже);
- ручная регистрация SPN-записи – перед первоначальной настройкой конфигурации JMS следует выполнить регистрацию SPN-записи службы сервера JMS вручную (подробнее см. «Ручная регистрация SPN-записи», с. 64).

## 7.1 Настройка учетной записи, от имени которой будет производиться первоначальная настройка

### 7.1.1 Случай запуска службы сервера JMS от имени Local System

В данном разделе рассматривается подготовка учетной записи пользователя, от имени которого будет производиться первоначальная настройка, для случая, когда службу JMS планируется запускать от имени локальной системной учетной записи (Local System).

Если учетная запись, от имени которой будет производиться первоначальная настройка JMS, не обладает полномочиями, достаточными для регистрации SPN-записи, вы можете предоставить ей соответствующие полномочия.

1. Откройте окно оснастки **Active Directory – пользователи и компьютеры**.

Окно будет иметь следующий вид.

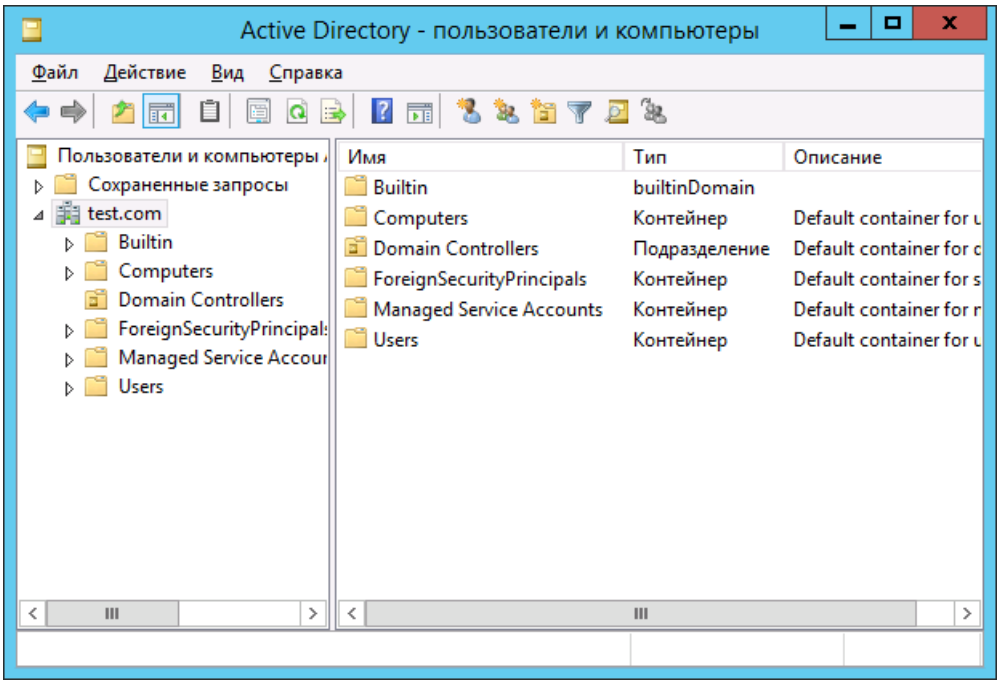



*Рис. 53 – Окно оснастки **Active Directory – пользователи и компьютеры***

2. В верхней панели выберите **Вид -> Дополнительные компоненты** (пункт **Дополнительные компоненты** должен быть отмечен), как показано на рис. 54.

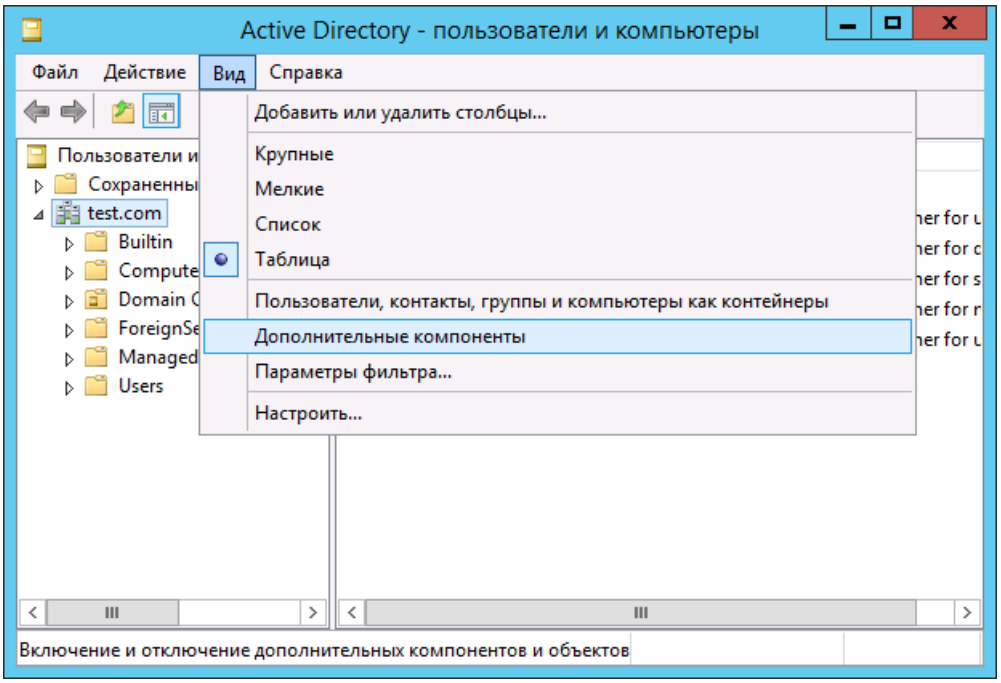



*Рис. 54 – Отображение дополнительных компонентов*

3. Щелкните правой кнопкой на имени домена и выберите **Свойства**.

Отобразится следующее окно.

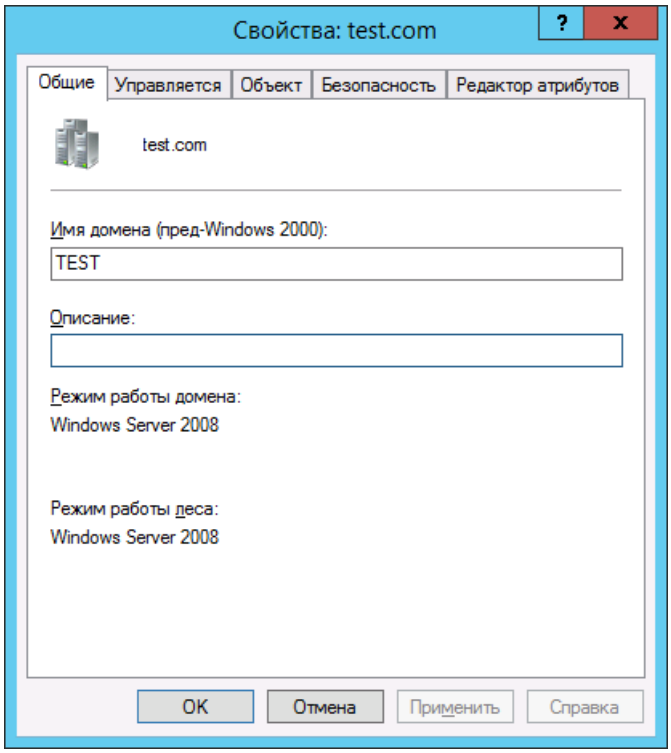



*Рис. 55 – Окно свойств домена*

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

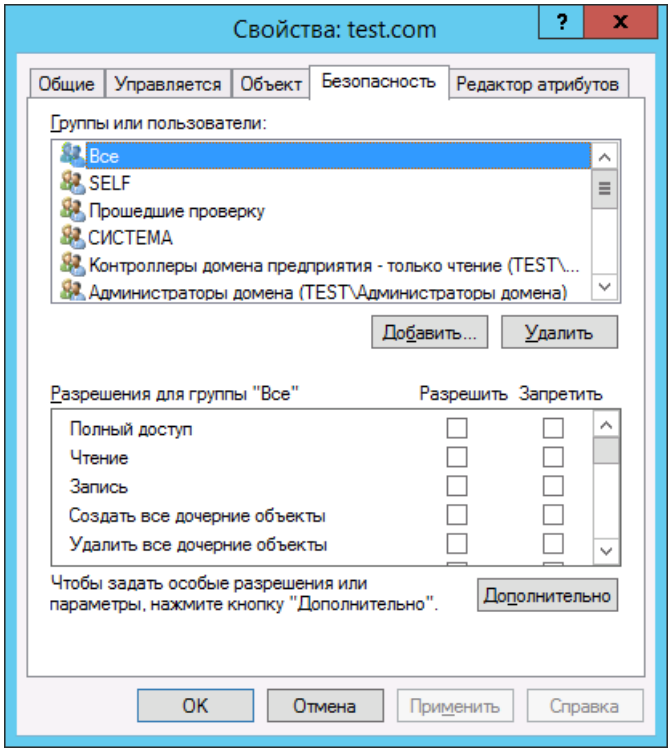



*Рис. 56 – Вкладка Безопасность свойств домена*

5. Нажмите **Дополнительно**.

Отобразится следующее окно.

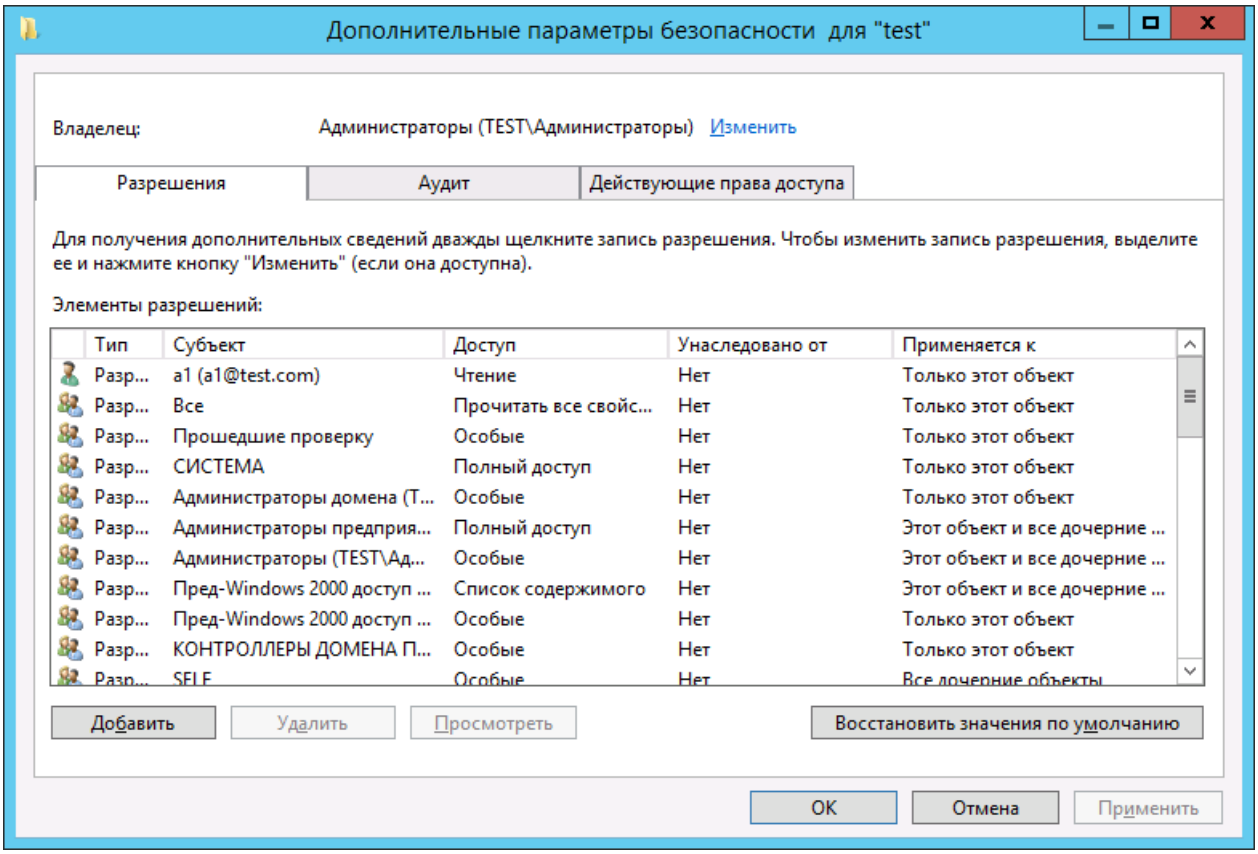



*Рис. 57 – Окно дополнительных параметров безопасности*

6. Нажмите **Добавить**.
Отобразится следующее окно.

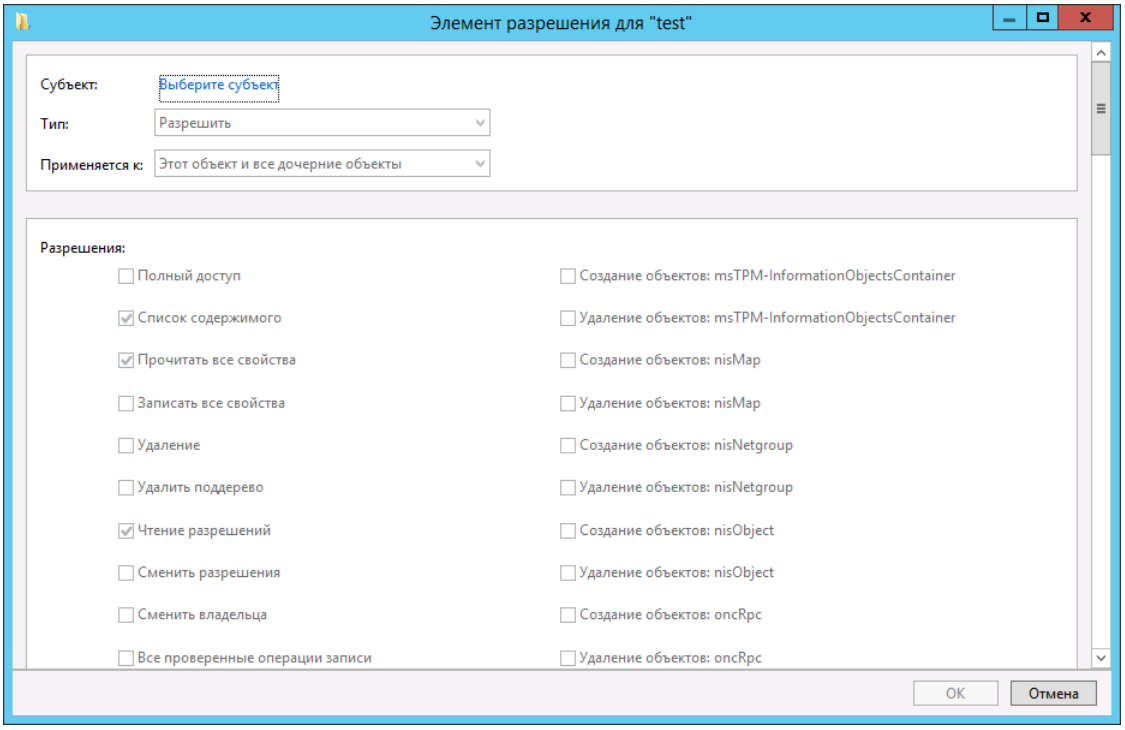



*Рис. 58 – Создание нового разрешения*

7. Щелкните на ссылке **Выберите субъект** и в отобразившемся окне введите пользователя, от имени которого будет производиться первоначальная настройка конфигурации JMS, после чего нажмите **OK**.
Окно создания нового разрешения будет выглядеть следующим образом.

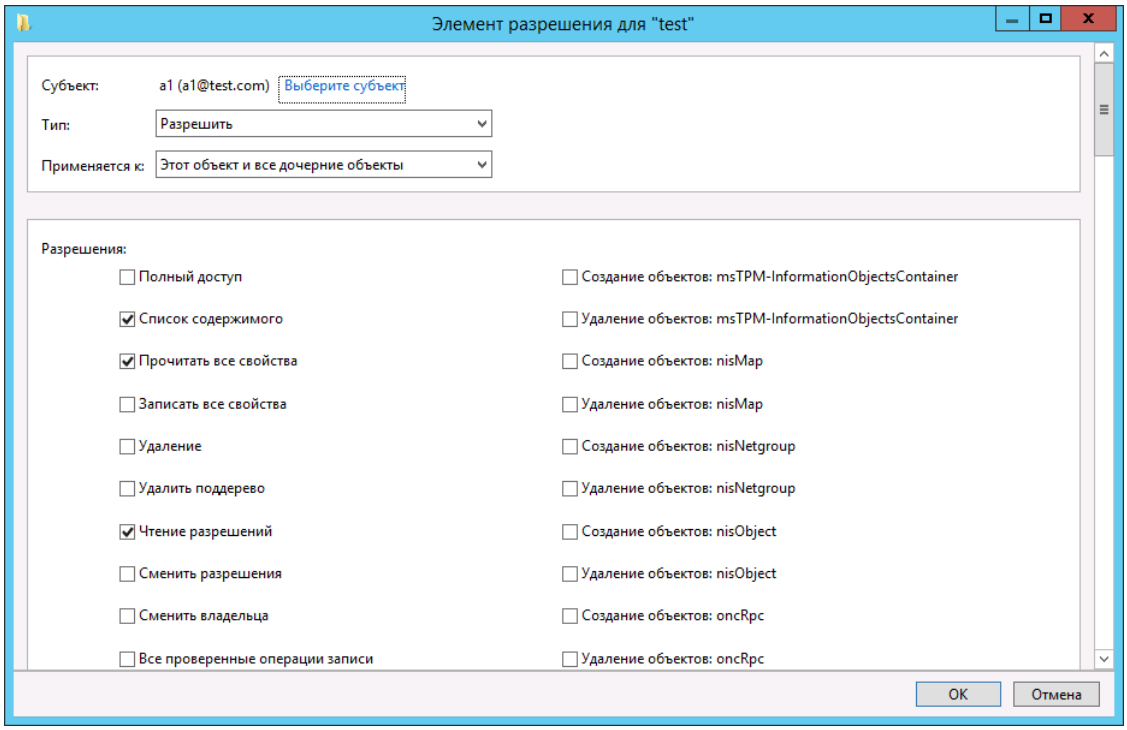



*Рис. 59 – Выбор пользователя для создания разрешения*

8. Выполните следующие действия:

8.1. убедитесь в том, что в списке **Тип** выбран пункт **Разрешить**;
8.2. в списке **Применяется к** выберите **Дочерние объекты: Компьютер**.

9. В секции **Разрешения** ниже установите флаг **Удостоверенная запись на узел с именем субъекта-службы**, как показано на рис. 60.

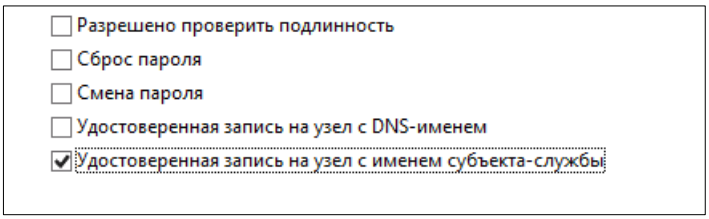



*Рис. 60 – Удостоверенная запись на узел с именем субъекта службы*

10. Последовательно нажмите **OK**, чтобы закрыть окно и сохранить сделанные изменения.

### 7.1.2 Случай запуска службы сервера JMS от имени служебной учетной записи

В данном разделе рассматривается подготовка учетной записи пользователя, от имени которого будет производиться первоначальная настройка, для случая, когда службу JMS планируется запускать от имени служебной учетной записи (т.е. не локальной системной учетной записи **Local System**).

Если учетная запись, от имени которой будет производиться первоначальная настройка JMS, не обладает полномочиями, достаточными для регистрации SPN-записи, вы можете предоставить ей соответствующие полномочия.

1. На контроллере домена в оснастке **Active Directory - пользователи и компьютеры** откройте учетную запись пользователя, от чьего имени будет запускаться служба JMS (в настоящем примере – ServiceAccount).
2. На вкладке **Безопасность** добавьте (если еще нет) пользователя, от чьего имени выполняется мастер первоначальной настройки (в настоящем примере Simple_User, Рис. 61) и установите у него разрешение **Запись: открытые сведения** (*Write public information*).

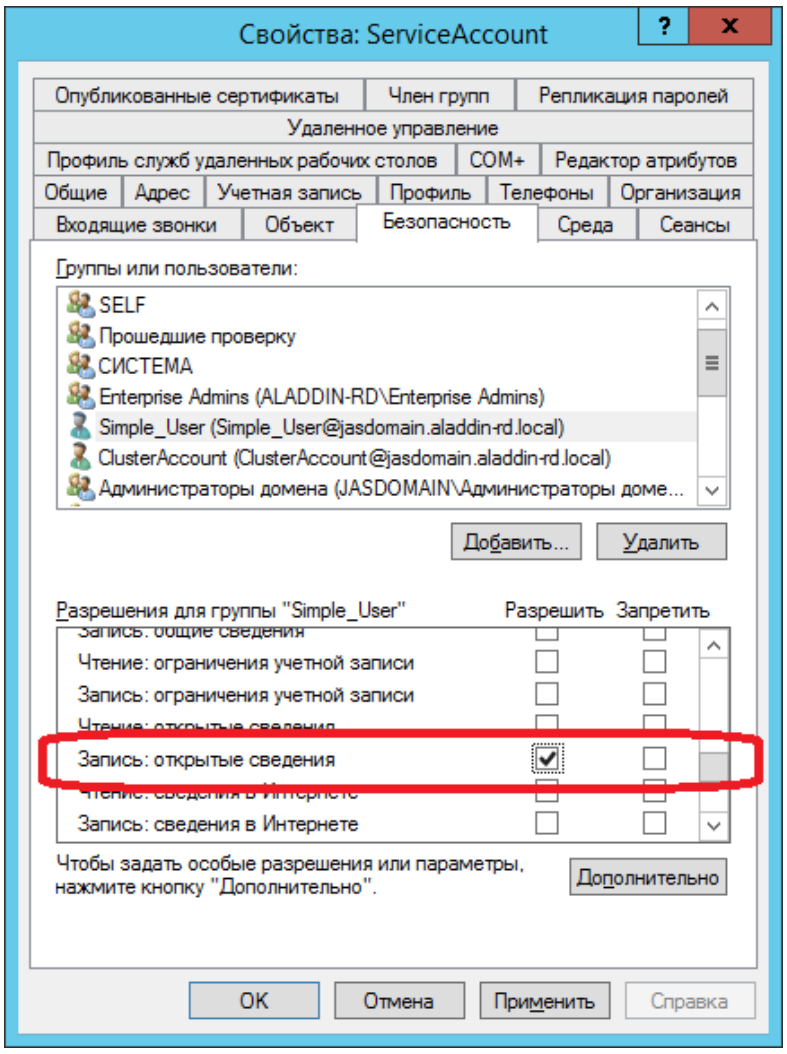



*Рис. 61 – Установка разрешения **Запись: открытые сведения***

3. Нажмите **OK**, чтобы закрыть окно и сохранить сделанные изменения.

Настоящая настройка позволит мастеру первоначальной настройки, выполняемому от имени пользователя Simple_User, автоматически выполнить SPN-запись для служебной учетной записи (ServiceAccount), от чьего имени будет выполняться запуск службы JMS.

## 7.2 Ручная регистрация SPN-записи

### 7.2.1 Случай запуска службы сервера JMS от имени Local System

В данном разделе рассматривается ручная регистрация SPN-записи для компьютера (учетная запись Local System), от имени которого планируется запускать службу JMS.

Чтобы выполнить ручную регистрацию SPN-записи службы сервера JMS, на контроллере домена запустите командную строку от имени администратора и выполните следующую команду.

**setspn -A ARDSJMS/<FQDN-имя сервера> <NetBIOS-имя сервера>**

где

- **<FQDN-имя сервера>** – полное доменное имя (FQDN) сервера JMS, например, **srv01.test.com**;
- **<NetBIOS-имя сервера>** – NetBIOS-имя сервера JMS, например, **srv01**.

⚠ Регистр имени сервера, используемый в исполняемой команде, должен совпадать с регистром, отображаемым в Active Directory. Например, если имя сервера в Active Directory – **Srv01**, то в исполняемой команде также следует указывать **Srv01** (а не **SRV01** или **srv01**).

### 7.2.2 Случай запуска службы сервера JMS от имени служебной учетной записи

В данном разделе рассматривается ручная регистрация SPN-записи для пользователя (служебной учетной записи), от имени которого планируется запускать службу JMS.

Чтобы выполнить ручную регистрацию SPN-записи службы сервера JMS, на контроллере домена запустите командную строку от имени администратора и выполните следующую команду.

**setspn -A ARDSJMS/<FQDN-имя сервера> <доменное имя пользователя>**

где

- **<FQDN-имя сервера>** – полное доменное имя (FQDN) сервера JMS, например, **srv01.test.com**;
- **<доменное имя пользователя >** – доменное имя пользователя в формате <имя домена>\<имя пользователя>, например **domain\ServiceAccount**.

⚠ Регистр имени сервера, используемый в исполняемой команде, должен совпадать с регистром, отображаемым в Active Directory. Например, если имя сервера в Active Directory – **Srv01**, то в исполняемой команде также следует указывать **Srv01** (а не **SRV01** или **srv01**).

☑ Если вы разворачиваете JMS в кластере, выполните эту команду для каждого узла кластера JMS.

# 8. Установка и первоначальная настройка

## 8.1 Установка компонента JMS Server

Чтобы установить компонент JMS Server, выполните следующие действия.

1. Запустите на выполнение файл: `Aladdin.JMS.Server-x.x.x.xxxx-x64.msi`.

Отобразится следующее окно.

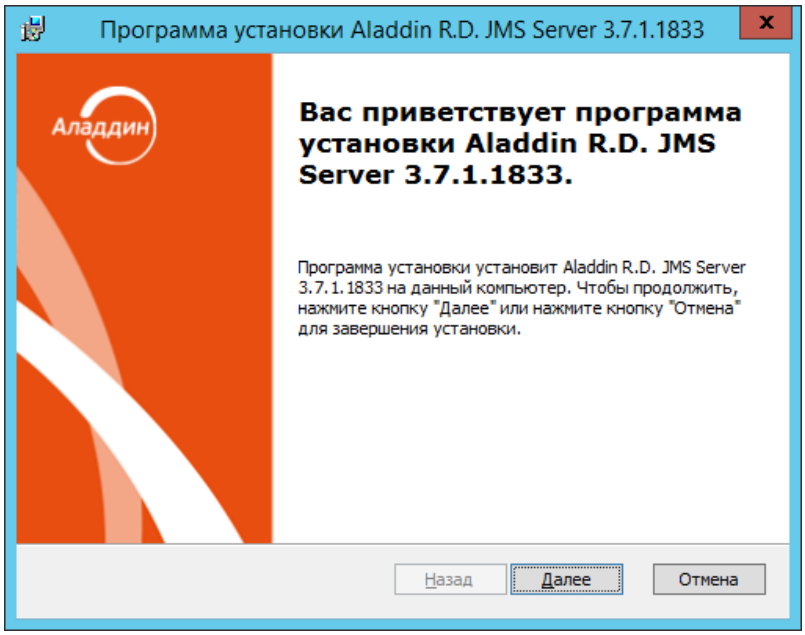



*Рис. 62 – Окно приветствия мастера установки компонента JMS Server*

2. Нажмите **Далее**.
   Отобразится следующее окно.

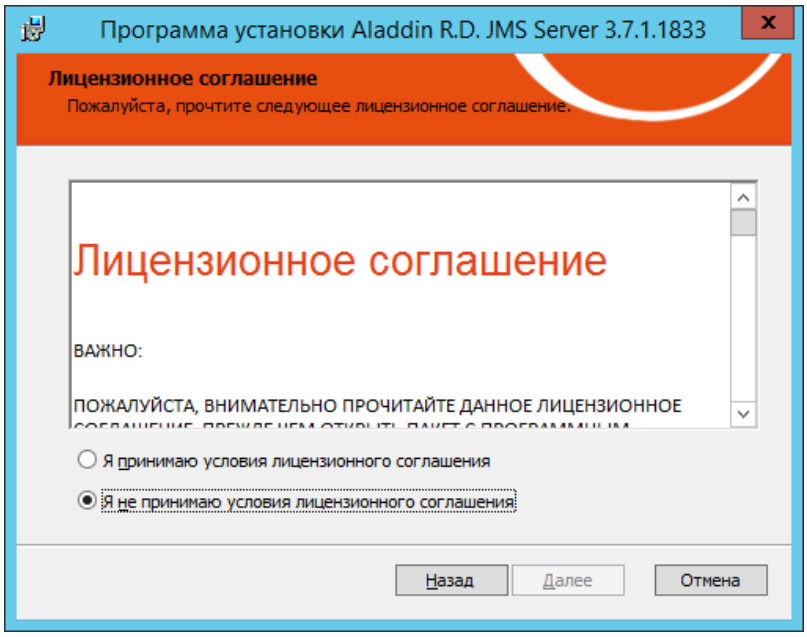



*Рис. 63 – Окно лицензионного соглашения*

3. Выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.

Отобразится следующее окно.

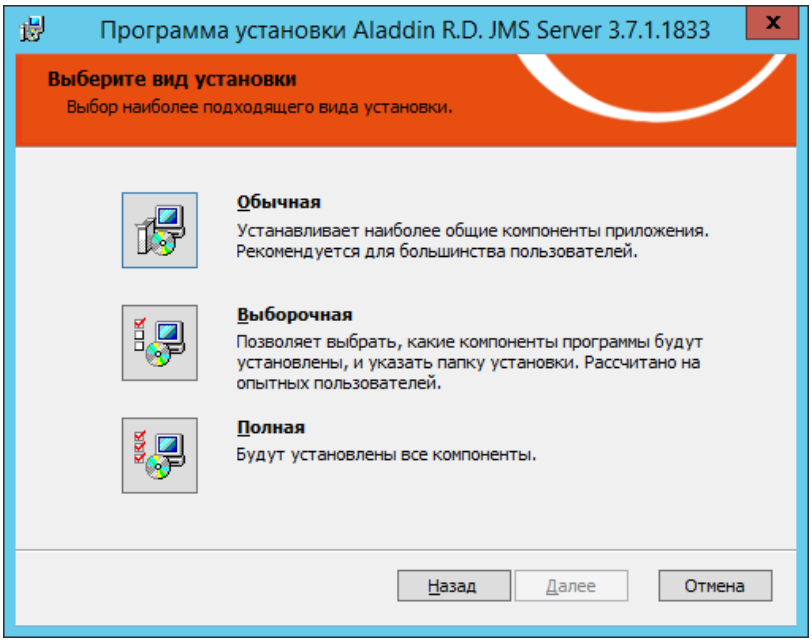



*Рис. 64 – Окно выбора варианта установки*

4. Щелкните на пункте **Полная**.

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

Отобразится следующее окно.

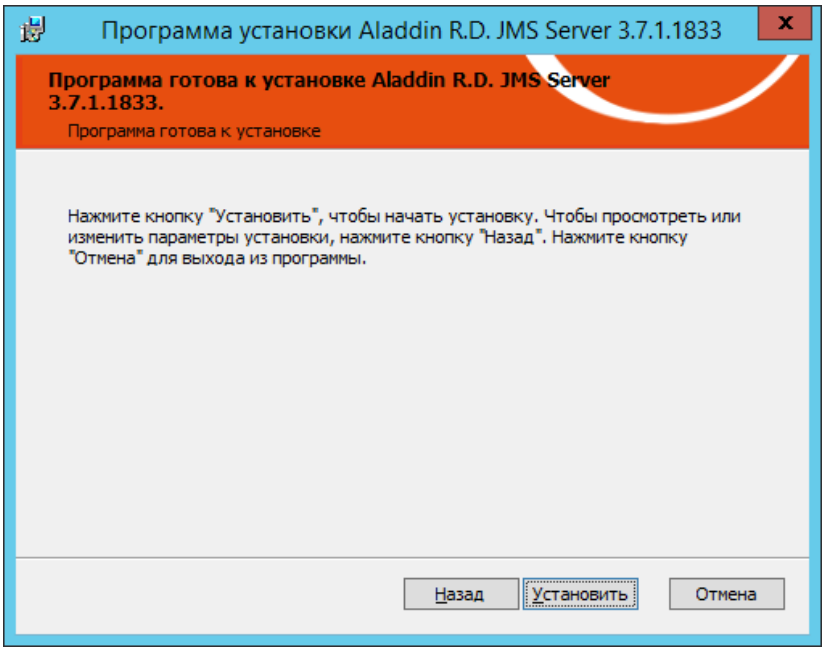



*Рис. 65 – Окно готовности к установке*

5. Нажмите **Установить**.

По завершении установки отобразится следующее окно.

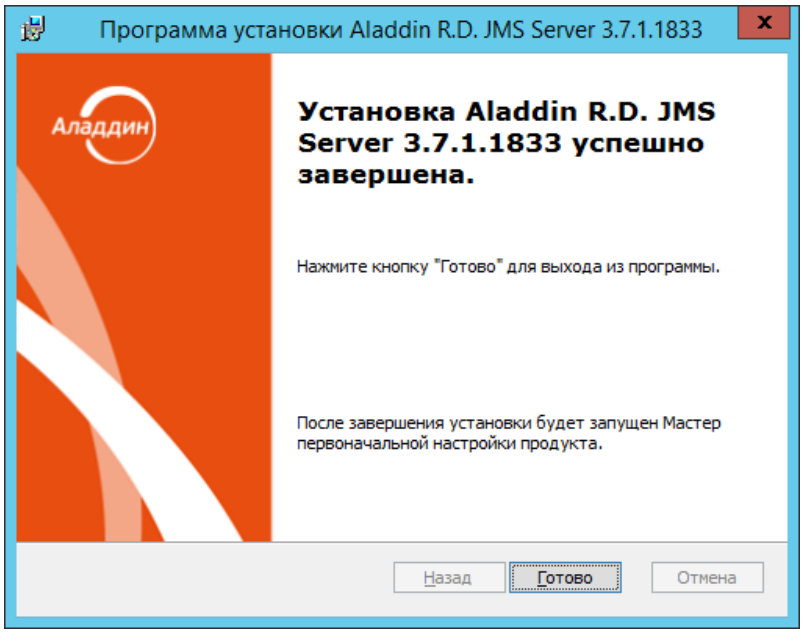



*Рис. 66 – Окно завершения установки*

6. Нажмите **Готово** для завершения процедуры.

## 8.2 Подготовка служебной учетной записи для запуска сервера JMS

Сервер JMS может запускаться от имени системной учетной записи или от имени специально созданной служебной учетной записи. Если вы планируете запускать сервер JMS от имени системной учетной записи, пропустите настоящий подраздел и переходите к подразделу «Первоначальная настройка конфигурации», с. 73. В противном случае выполните действия, представленные ниже.

### 8.2.1 Создание пользователя

На контроллере домена выполните следующие действия.

1. В оснастке **Active Directory – пользователи и компьютеры** щелкните правой кнопкой на нужном пункте (например, на пункте **Users** (Пользователи)) и выберите **Создать -> Пользователь**.

Отобразится следующее окно.

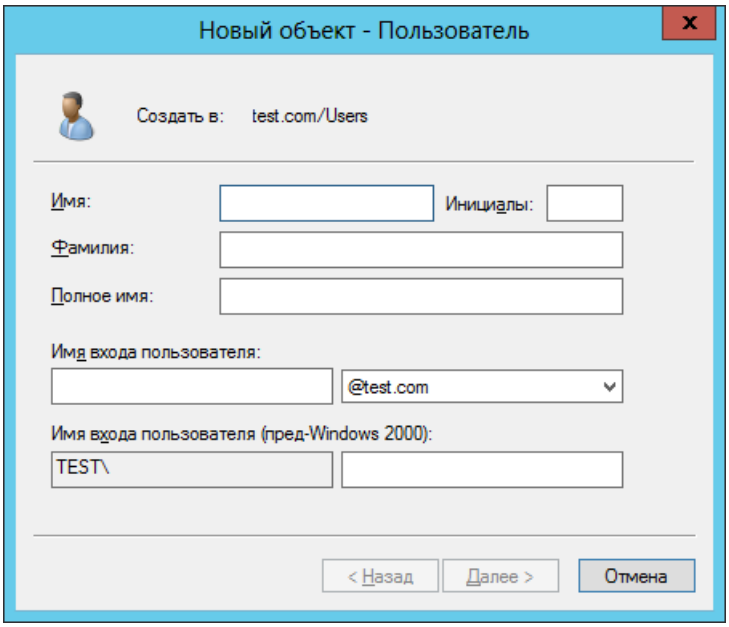



*Рис. 67 – Создание нового пользователя*

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

⚠ В настоящем документе для примера будет использоваться имя учетной запись **JMS_Server**.

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

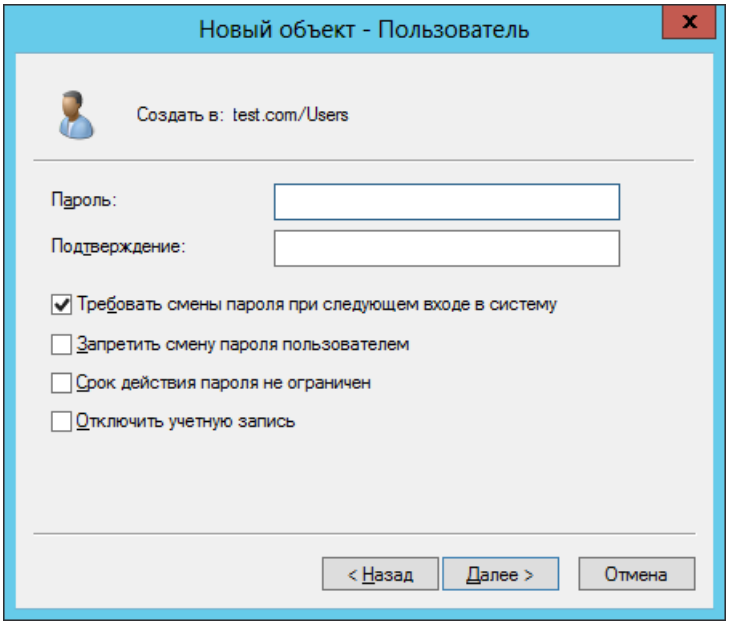



*Рис. 68 – Задание пароля пользователя*

4. Выполните следующие действия:

4.1. в полях **Пароль** и **Подтверждение** введите соответственно пароль служебной учетной записи и подтверждение;
4.2. снимите флаг **Требовать смены пароля при следующем входу в систему**;
4.3. установите флаг **Срок действия пароля не ограничен**;
4.4. нажмите **Далее**.

Отобразится следующее окно.

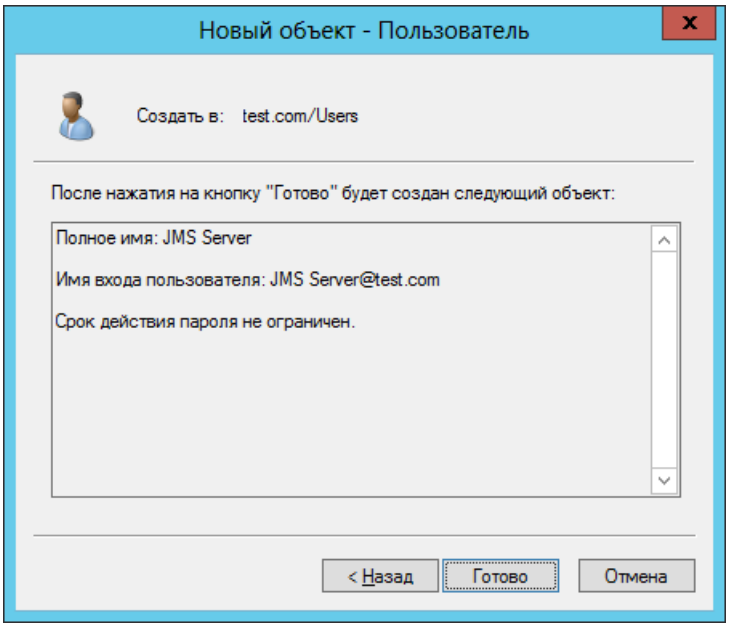



*Рис. 69 – Завершение процедуры создания учетной записи*

5. Нажмите **Готово**.

### 8.2.2 Настройка учетной записи для входа в качестве службы

**Примечания:**

1. Если мастер первоначальной настройки JMS запускается от имени пользователя, являющегося локальным администратором компьютера, данная настройка учетной записи для входа в качестве службы (если эта настройка требуется) будет выполнена автоматически в ходе выполнения мастера. В этом случае действия, описанные в настоящем подразделе, можно не выполнять.
2. Приведенным в настоящем разделе описанием следует руководствоваться в процессе эксплуатации JMS при смене служебной учетной записи, от имени которой запускается служба JMS.

На компьютере, в котором устанавливается компонент JMS Server, выполните следующие действия.

1. В *Панели управления* выберите пункт **Администрирование**.

Отобразится следующее окно.

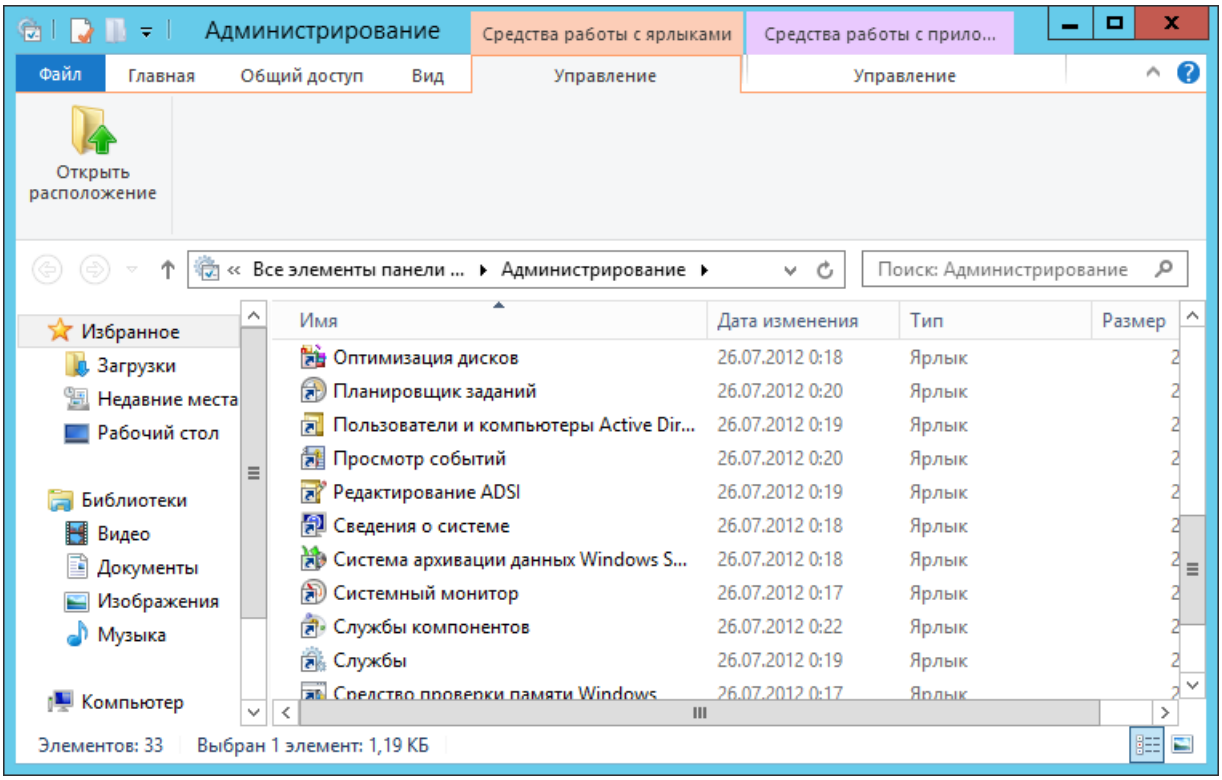



*Рис. 70 – Возможности администрирования*

2. Сделайте двойной щелчок на пункте **Локальная политика безопасности**.
Отобразится следующее окно.

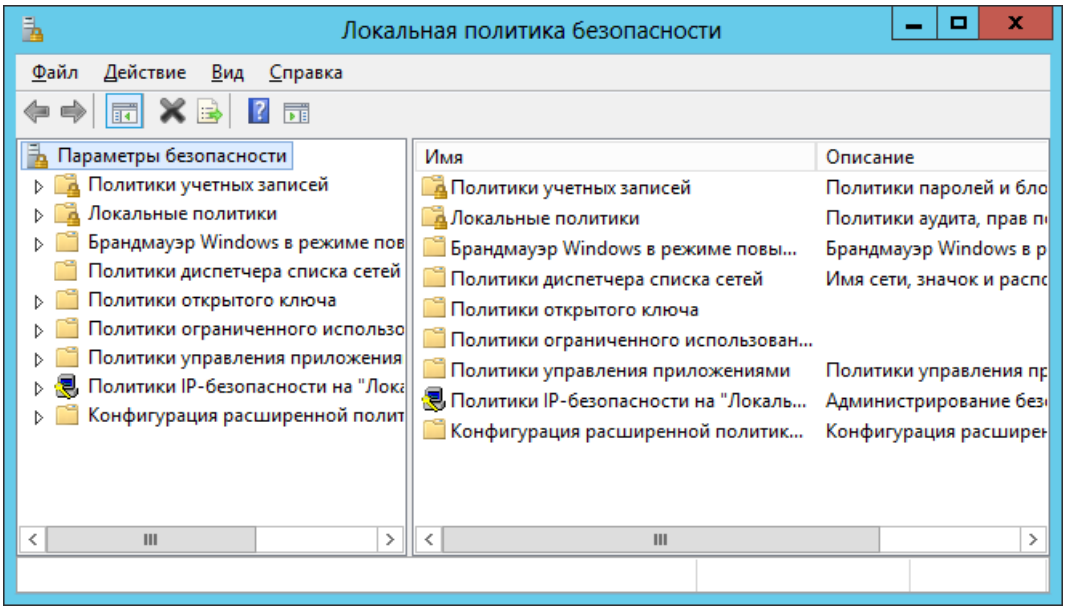



*Рис. 71 – Локальная политика безопасности*

3. В левой части окна выберите **Локальные политики -> Назначение прав пользователя**.

Окно примет следующий вид.

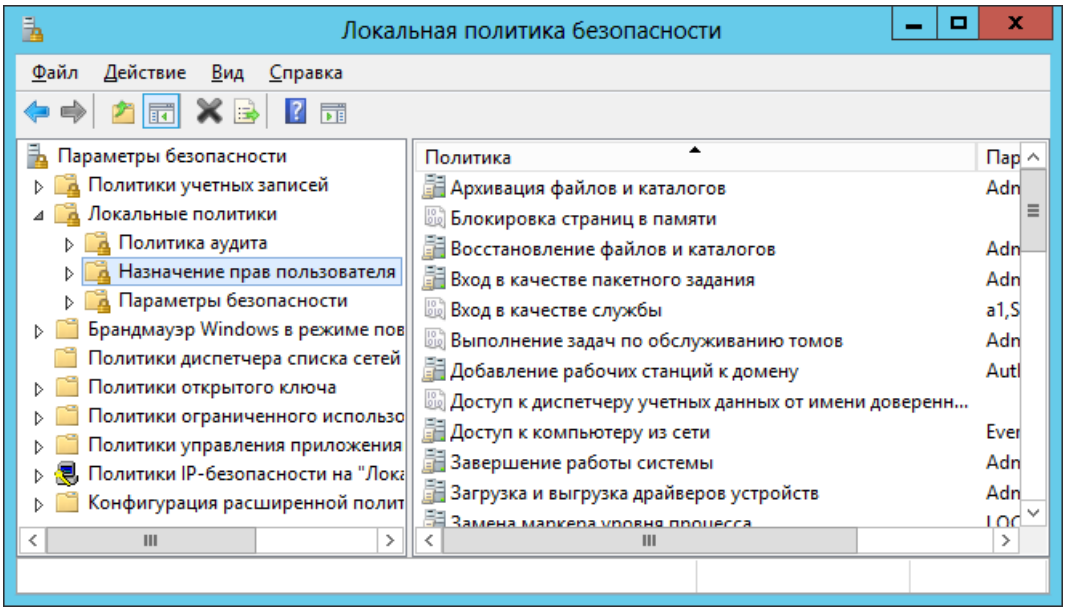



*Рис. 72 – Назначение прав пользователя*

4. В правой части окна сделайте двойной щелчок на пункте **Вход в качестве службы**. Отобразится следующее окно.

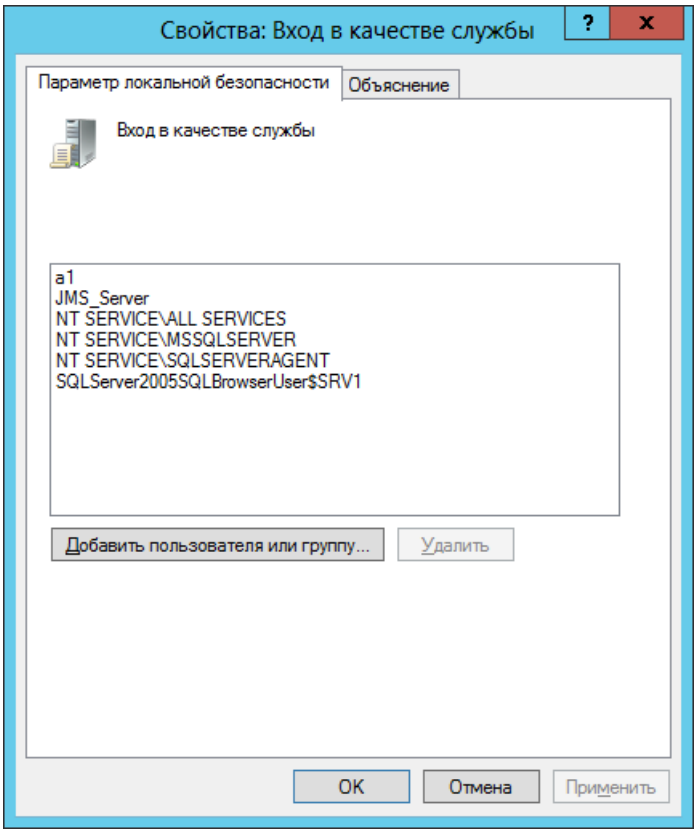



*Рис. 73 – Вход в качестве службы*

5. Нажмите **Добавить пользователя или группу** и в отобразившемся окне добавьте учетную запись, от имени которой будет запускаться сервер JMS (в настоящем примере это учетная запись **JMS_Server**).

6. Последовательно нажмите **OK**, чтобы закрыть окно добавления учетной записи и окно настройки входа в качестве службы.

### 8.2.3 Настройка запуска службы сервера JMS от имени служебной учётной записи

1. В Панели управления выберите **Администрирование -> Службы**.
Отобразится следующее окно.

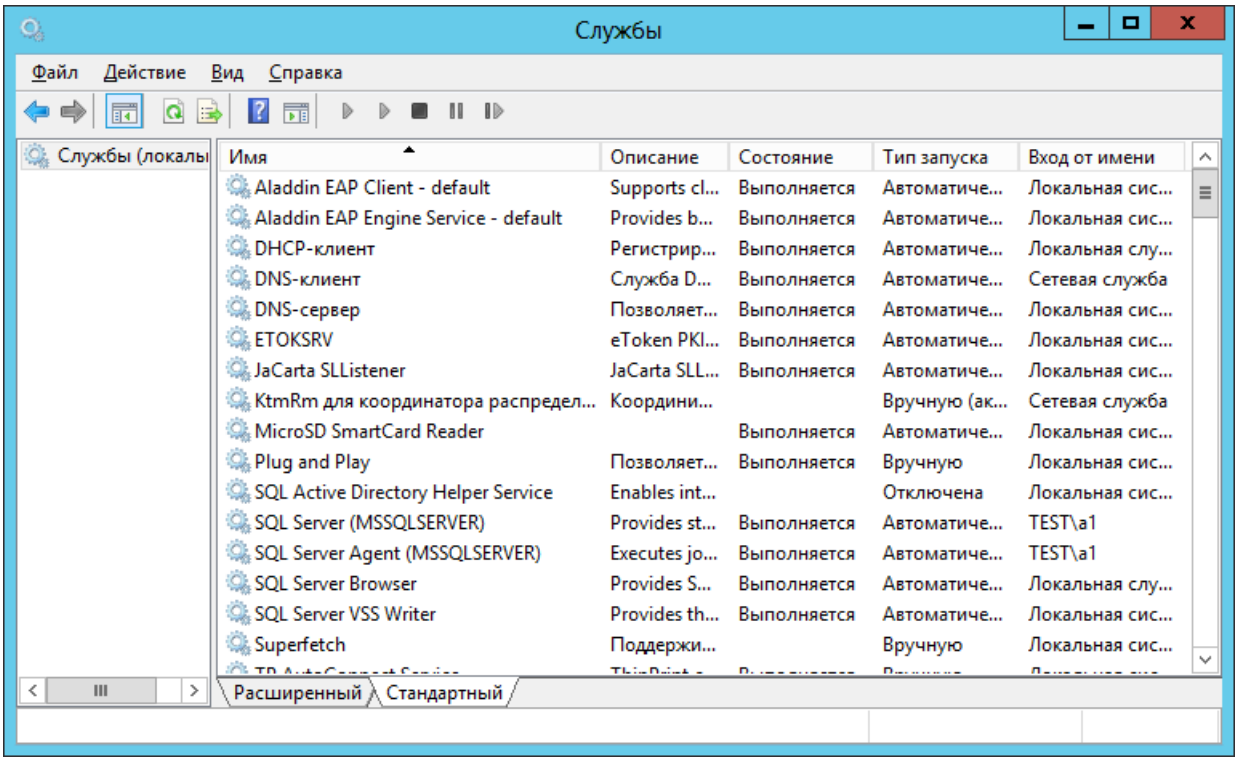



*Рис. 74 – Список служб*

2. Щелкните правой кнопкой на службе **Aladdin EAP Engine Service – default** и выберите **Свойства**.
3. В отобразившемся окне перейдите на вкладку **Вход в систему**.

Окно примет следующий вид.

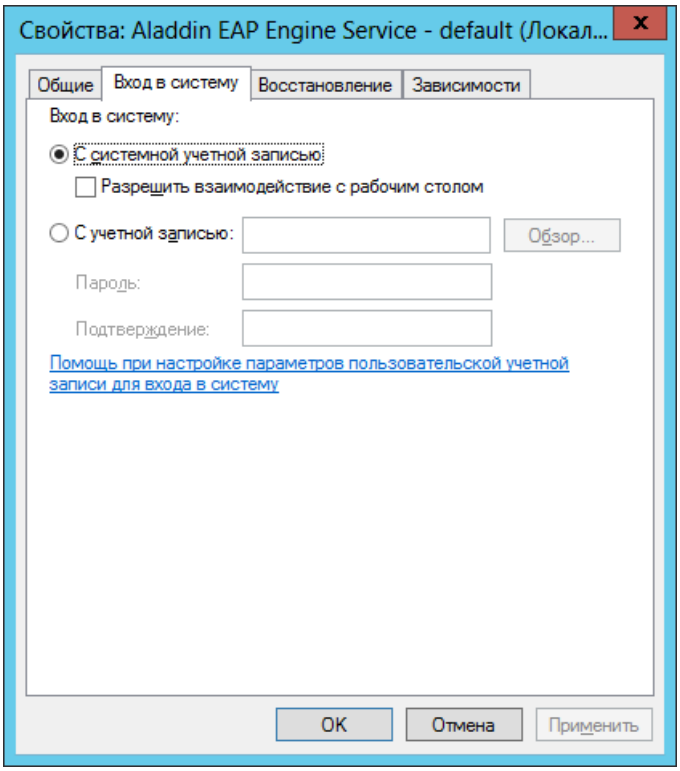



*Рис. 75 – Настройка входа в систему*

4. Выберите пункт **С учетной записью** и выполните следующие действия:

4.1. Воспользуйтесь кнопкой **Обзор**, чтобы указать имя служебной учетной записи (в настоящем примере это **JMS_Server**).

4.2. В полях **Пароль** и **Подтверждение** соответственно введите пароль и подтверждение пароля служебной учетной записи.

Если в будущем вы поменяете пароль для выбранной учетной записи, то новое значение пароля также необходимо изменить в настоящей настройке.

5. Нажмите **OK**, чтобы закрыть окно и сохранить изменения.
Отобразится следующее окно.

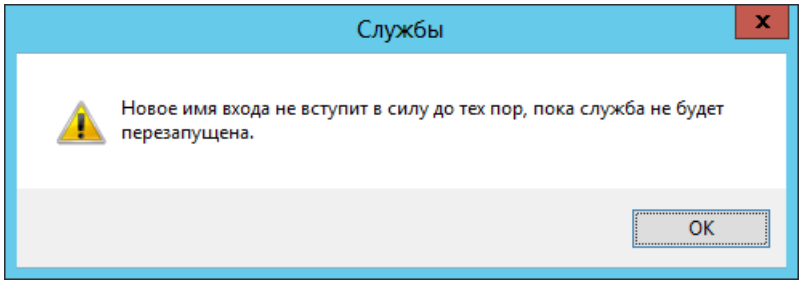



*Рис. 76 – Предупреждение о необходимости перезагрузки*

Перезапускать службу необязательно.

## 8.3 Первоначальная настройка конфигурации

После установки компонента JMS Server автоматически откроется окно мастера настройки первоначальной конфигурации JMS. Чтобы выполнить настройку базовой конфигурации, см. «Начало процедуры», с. 75.

Если вы закрыли окно мастера первоначальной настройки конфигурации, см. «Запуск мастера первоначальной настройки конфигурации» ниже.

### 8.3.1 Запуск мастера первоначальной настройки конфигурации

Если вы закрыли окно мастера первоначальной настройки конфигурации, вы можете вновь открыть его, выполнив следующую процедуру.

1. Щелкните правой кнопкой на значке (Сервер JMS) в области уведомлений и в контекстном меню выберите **Открыть**.
2. В отобразившемся окне перейдите на вкладку **Настройка**.
   Окно примет следующий вид.

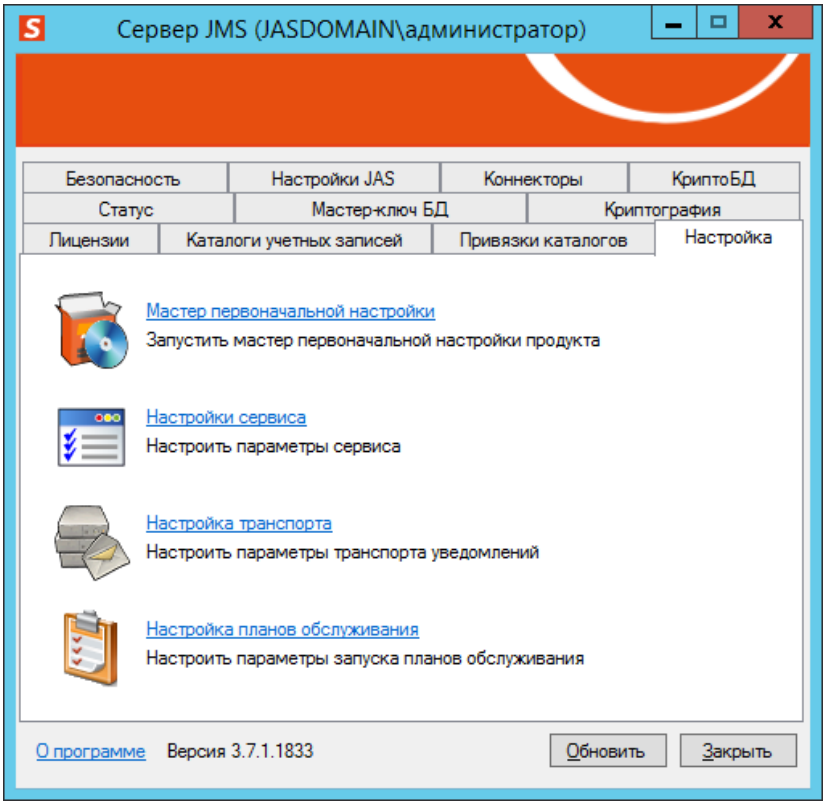



*Рис. 77 – Вкладка **Настройка***

3. Щелкните на ссылке **Мастер первоначальной настройки** – если отобразится окно **Перезапуск сервера управления**, нажмите **Да**.
   Отобразится окно мастера первоначальной настройки (см. «Начало процедуры»).

### 8.3.2 Начало процедуры и выбор конфигурации

Окно приветствия мастера первоначальной настройки конфигурации выглядит следующим образом.

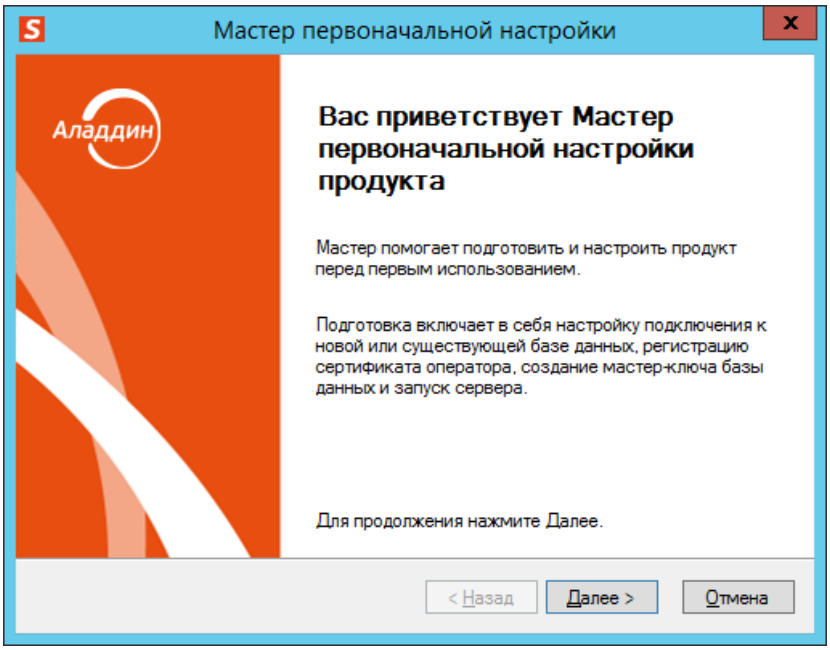



*Рис. 78 – Окно приветствия мастера первоначальной настройки JMS*

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

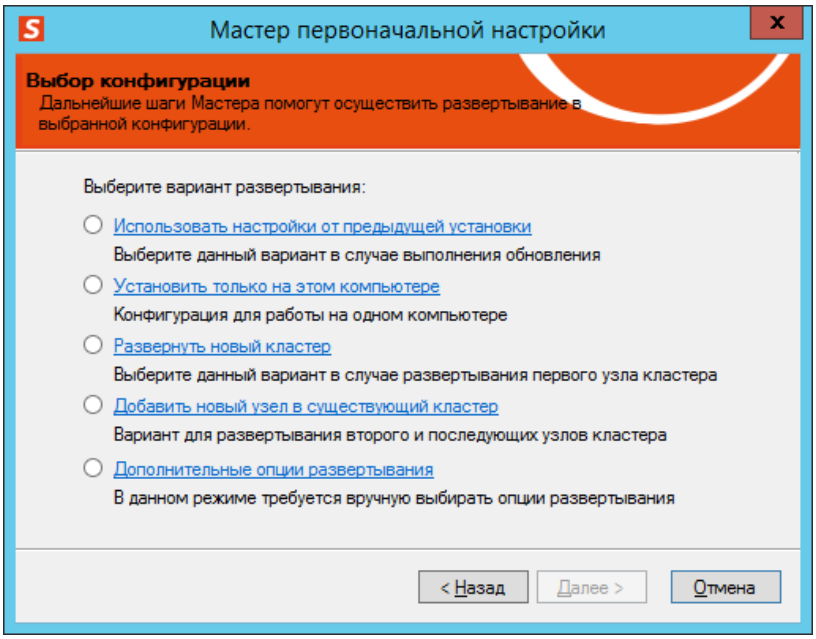



*Рис. 79 – Окно выбора конфигурации*

5. Выберите пункт нужную конфигурацию и нажмите **Далее**.

В настоящем документе рассматривается вариант конфигурации **Установить только на этом компьютере**.

Описание сценариев по пунктам **Развернуть новый кластер** и **Добавить новый узел в существующий кластер** приведены в руководстве по развертыванию кластерной конфигурации [6], с. 257.

В зависимости от выбранной конфигурации процесс первоначальной настройки будет состоять из следующих этапов (см. табл. 9).

*Табл. 9 – Этапы настройки первоначальной конфигурации*

| Ссылка на этап настройки | Установка единственного сервера JMS | Создание кластера JMS* | Добавление нового узла в существующий кластер* |
|---|---|---|---|
| «Настройка каталога учетных записей», с. 77. | Да | Да | Нет |
| «Выбор лицензии», с. 82. | Да | Да | Нет |
| «Создание мастер-ключа БД», с. 83. | Да | Да | Нет |
| «Настройка сервиса (службы) аутентификации JMS», с. 86. | Да | Да | Нет |
| «Настройка подключения к базе данных», с. 90. | Да | Да | Да |
| «Создание базы данных», с. 96. | Да | Да | Нет |
| «Обновление базы данных», с. 101. | Нет | Нет | Опционально |
| «Запуск серверной службы», с. 103. | Да | Да | Да |
| «Настройка расширений JMS», с. 104. | Да | Да | Да |
| «Запуск сервера JMS», с. 106. | Да | Да | Да |
| «Монтирование криптохранилища», с. 107. | Опционально | Опционально | Опционально |
| «Завершение первоначальной настройки», с. 107. | Да | Да | Да |

* Подробно порядок развертывания кластерной конфигурации JMS приведен в соответствующем руководстве [6].

### 8.3.3 Настройка каталога учетных записей

Отобразится следующее окно.

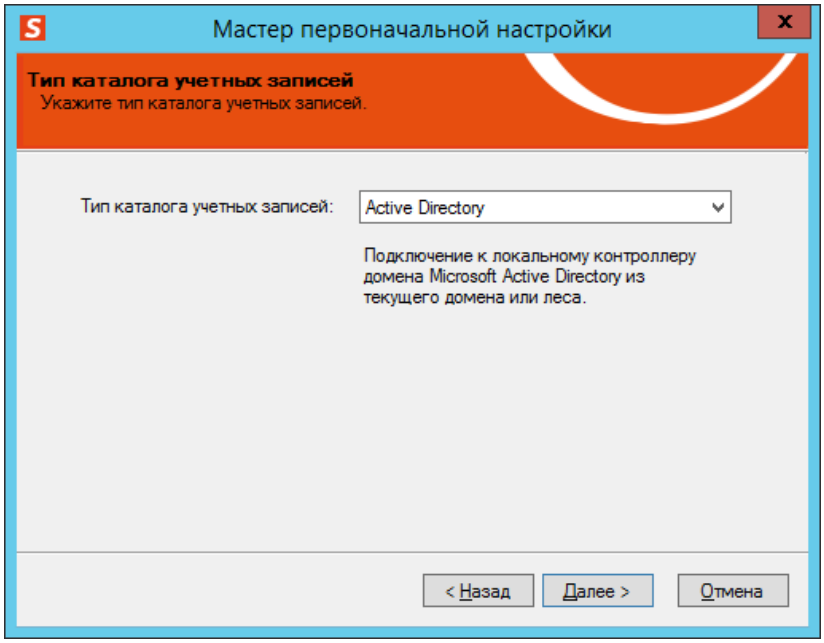



*Рис. 80 – Окно выбора каталога учетных записей*

6. Выберите из списка тип каталога учетных записей. Список состоит из четырех пунктов:

   - **Active Directory**;
   - **Remote Active Directory** (Удаленные службы Active Directory);
   - **КриптоПро УЦ 1.5;**
   - **КриптоПро УЦ 2.0**.

⚠ При первоначальной настройке конфигурации **КриптоПро УЦ 2.0** не может использоваться в качестве каталога учетных записей – сначала в качестве каталога учетных записей необходимо настроить **Active Directory** или **Remote Active Directory** (Удаленные службы Active Directory). В настоящем документе описывается пример настройки с использованием каталога **Active Directory**.

7. Оставьте в списке выбранным пункт **Active Directory** и нажмите **Далее**.

Отобразится следующее окно.

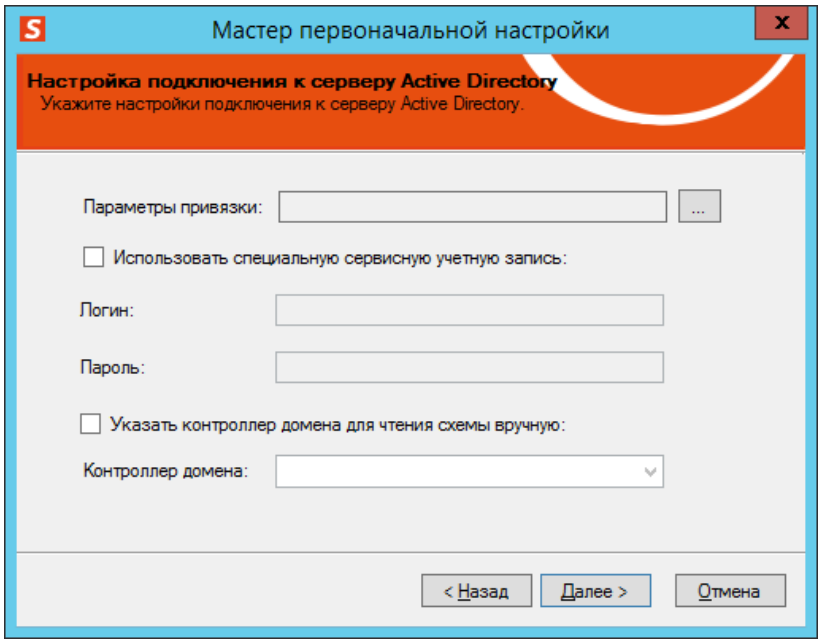



*Рис. 81 – Окно настройки подключения к серверу Active Directory.*

8. Щелкните на кнопке ... (Обзор).
Отобразится следующее окно.

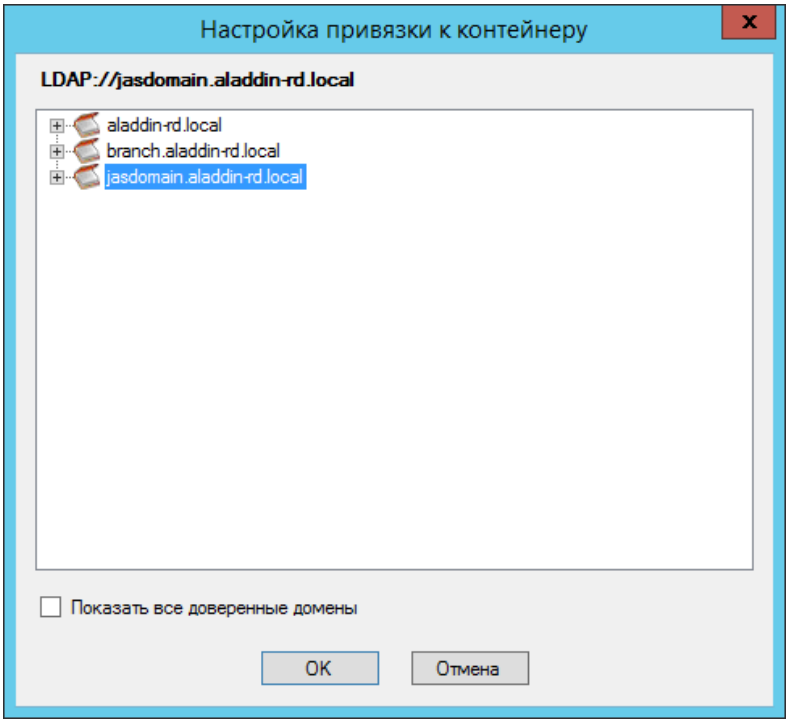



*Рис. 82 – Окно выбора домена*

9. Выберите домен или организационную единицу и нажмите **OK**.

Окно настройки подключения к серверу Active Directory будет выглядеть следующим образом.

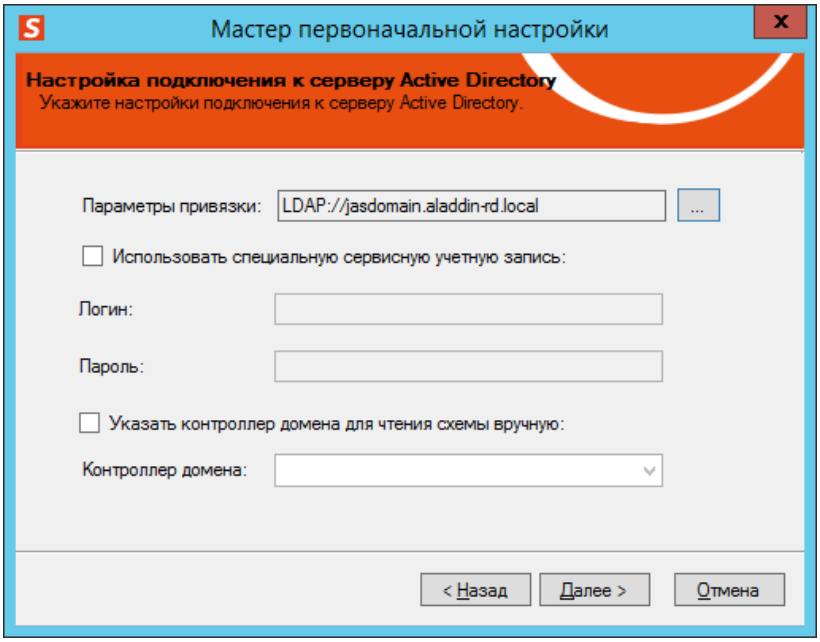



*Рис. 83 – Окно настройки подключения к серверу Active Directory*

10. Выполните необходимые настройки, руководствуясь табл. 10.

*Табл. 10 – Настройка подключения к Active Directory*

| Настройка | Описание |
|---|---|
| **Использовать специальную сервисную учетную запись** | Выберите учетную запись, от имени которой JMS будет обращаться к Active Directory - доступны следующие варианты:<br>• чтобы использовать локальную системную учетную запись (**Local System**), оставьте флаг **Использовать специальную сервисную учетную запись** неотмеченным и переходите к следующему шагу процедуры;<br>• чтобы использовать произвольную учетную запись, установите флаг **Использовать специальную сервисную учетную запись** и в полях **Логин** и **Пароль** задайте соответственно имя (в формате **DOMAIN\username** или **username@domain.com**) и пароль выбранной вами учетной записи.<br>⚠ Служебная учетная запись JMS должна обладать правами на чтение Active Directory. |
| **Указать контроллер домена для чтения схемы вручную** | Установка этого флага позволяет в списке **Контроллер домена** вручную указать контроллер домена каталога Active Directory, из которого будут считываться учетные записи пользователей. Этой возможностью следует пользоваться, только если по завершении первоначальной настройки по каким-то причинам JMS не может считать учетные записи пользователей в указанном каталоге Active Directory. |

11. Нажмите **Далее**.

Отобразится следующее окно.

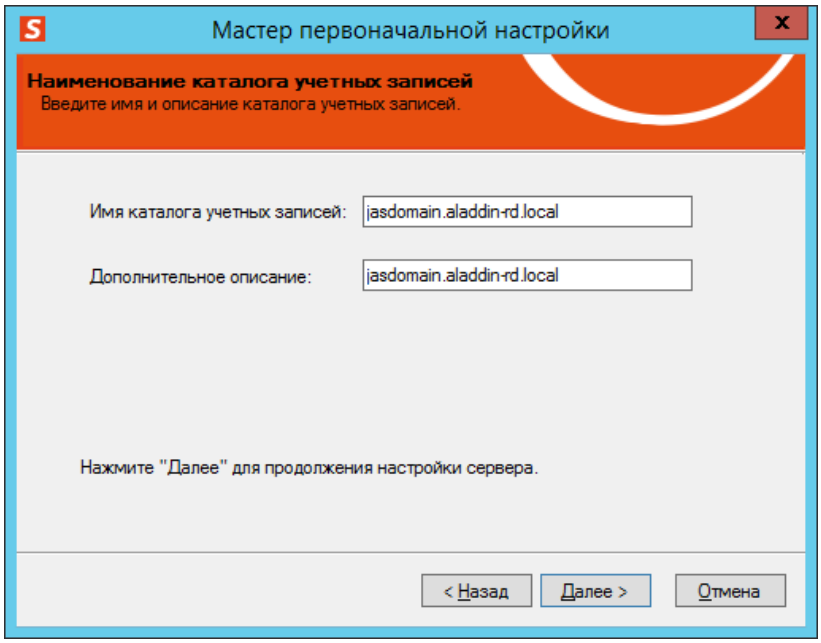



*Рис. 84 – Окно ввода имени каталога учетных записей*

12. При необходимости введите дополнительное описание в соответствующее поле и нажмите **Далее**.
Отобразится следующее окно.

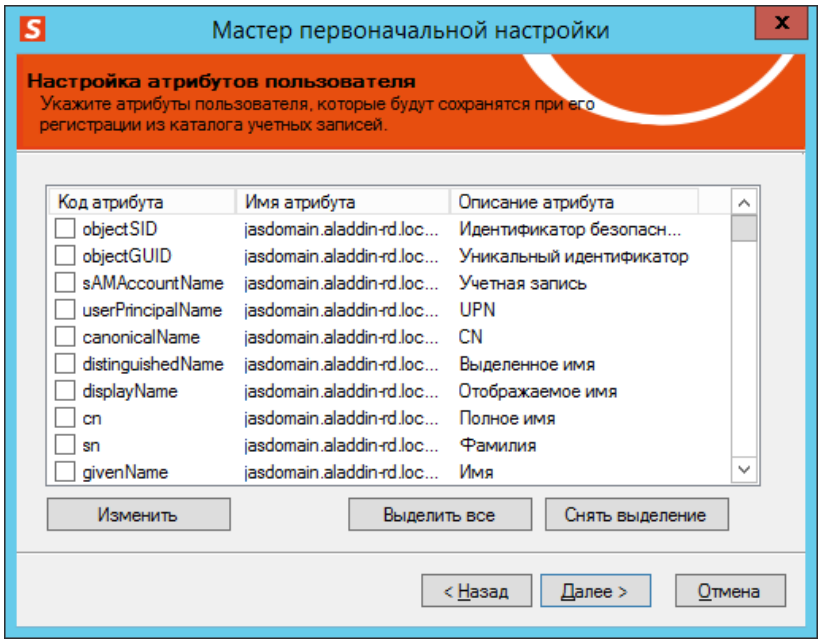



*Рис. 85 – Атрибуты пользователей*

13. Отметьте атрибуты пользователей, которые будут сохраняться в базе данных JMS при регистрации, после чего нажмите **Далее**.

**Примечание.** Отмеченные атрибуты впоследствии могут быть использованы:

- для осуществления поиска в JMS учетных записей пользователей по данным атрибутам;

- для формирования шаблона параметров запроса на сертификат (см. «Руководство администратора. Часть 2» [3], раздел «Настройка шаблонов полей сертификата»);
- для отслеживания изменений значений атрибутов пользователя в ресурсной системе (см. «Руководство администратора. Часть 2» [3], раздел «Настройки на вкладке Ключевые атрибуты»).

### 8.3.4 Настройка поддерживаемых приложений

Отобразится следующее окно.

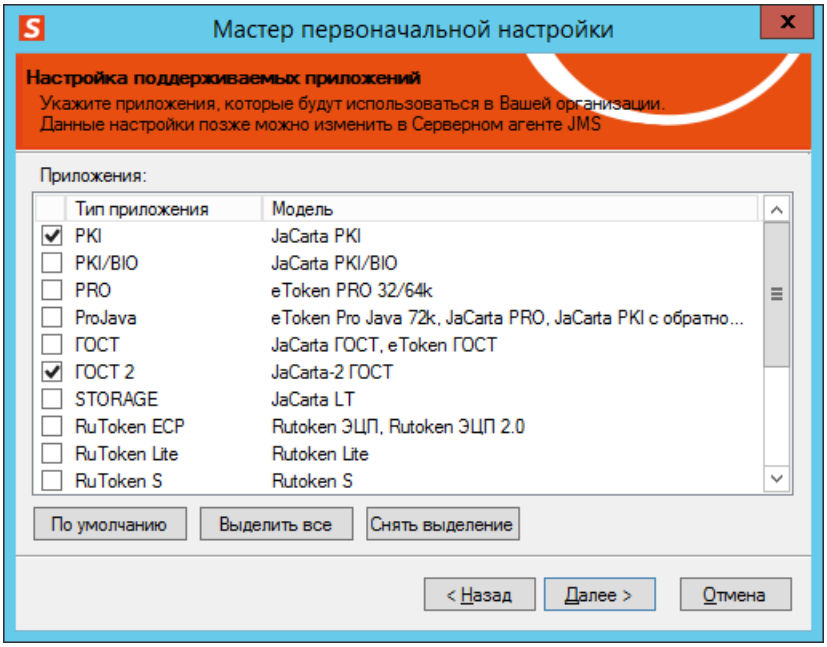



*Рис. 86 – Окно настройки поддерживаемых приложений*

14. В левом столбце отметьте приложения, которые необходимо поддерживать на электронных ключах, эксплуатирующихся в вашей организации. Для удобства в столбце справа отображаются те модели ключей, в которых устанавливается выбранное приложение. Наиболее часто используемые приложения уже установлены по умолчанию.

**Примечание.** Настройка поддерживаемых приложений используется, чтобы облегчить чтение конфигураций продукта, а именно – чтобы избежать загромождения пользовательского интерфейса при эксплуатации JMS. Данную настройку можно выполнить также в любой момент после первоначальной настройки продукта, см. раздел «Настройка поддерживаемых приложений», с. 193.

15. Нажмите **Далее**.

### 8.3.5 Выбор лицензии

Отобразится следующее окно.

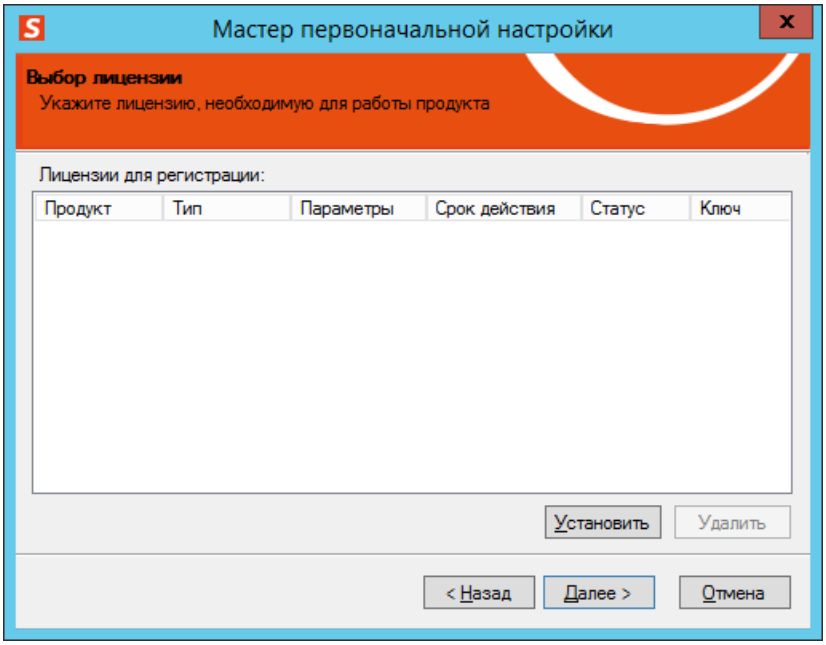



*Рис. 87 – Окно добавления лицензии*

16. Воспользовавшись кнопкой **Установить**, укажите путь к лицензии, предоставленной компанией «АО Аладдин Р. Д.». (Подробнее о типах лицензий см. в разделе «Версии поставки продукта и лицензионные опции» с. 174).
Отобразится следующее окно.

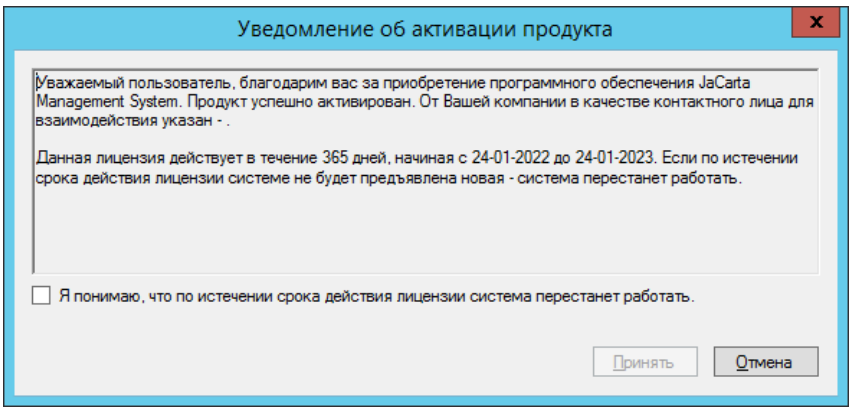



*Рис. 88 – Уведомление об активации продукта*

17. Прочтите уведомление об активации продукта, отметьте поле согласия и нажмите **Принять**.

После добавления лицензии окно будет выглядеть следующим образом.

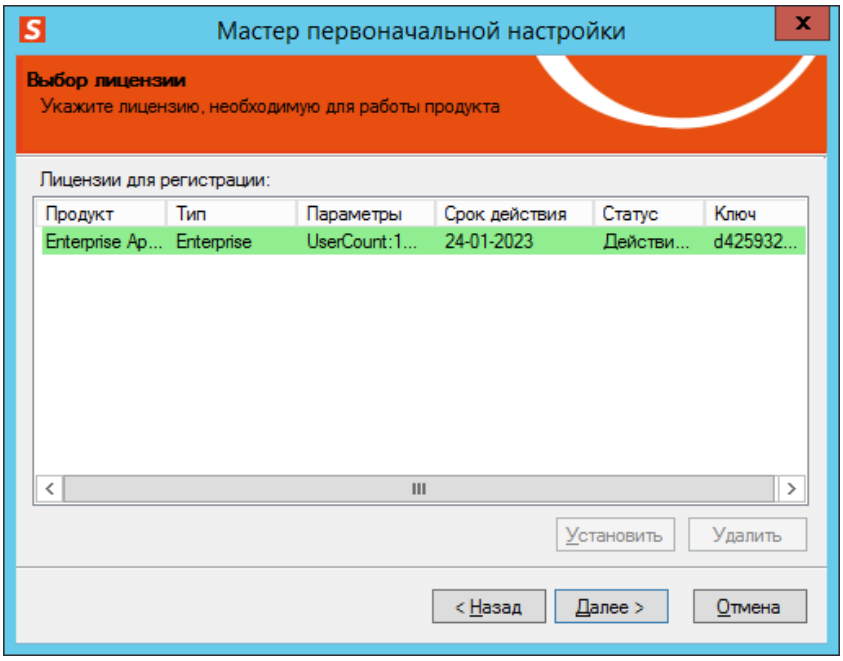



*Рис. 89 – Отображение добавленной лицензии*

18. Нажмите **Далее**.

### 8.3.6 Создание мастер-ключа БД

Отобразится следующее окно.

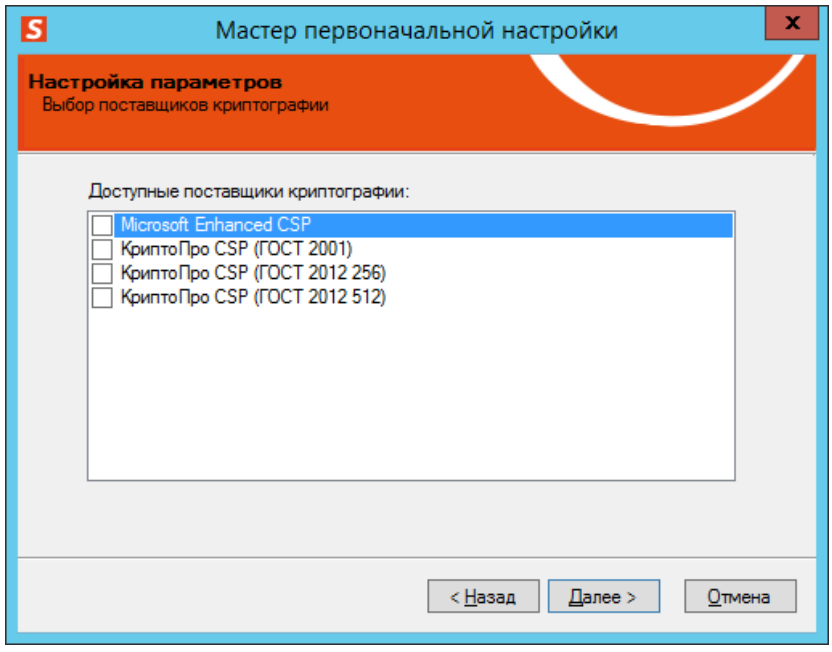



*Рис. 90 – Выбор поставщика криптографии*

В настоящей процедуре приведен пример настройки поставщика криптографии **Microsoft Enhanced CSP**. Если вы настраиваете другой поставщик криптографии, см. «Подключение поставщика криптографии», с. 169.

19. Установите флаг напротив поставщика криптографии, который будет использоваться в работе JMS, и нажмите **Далее**.

Отобразится следующее окно.

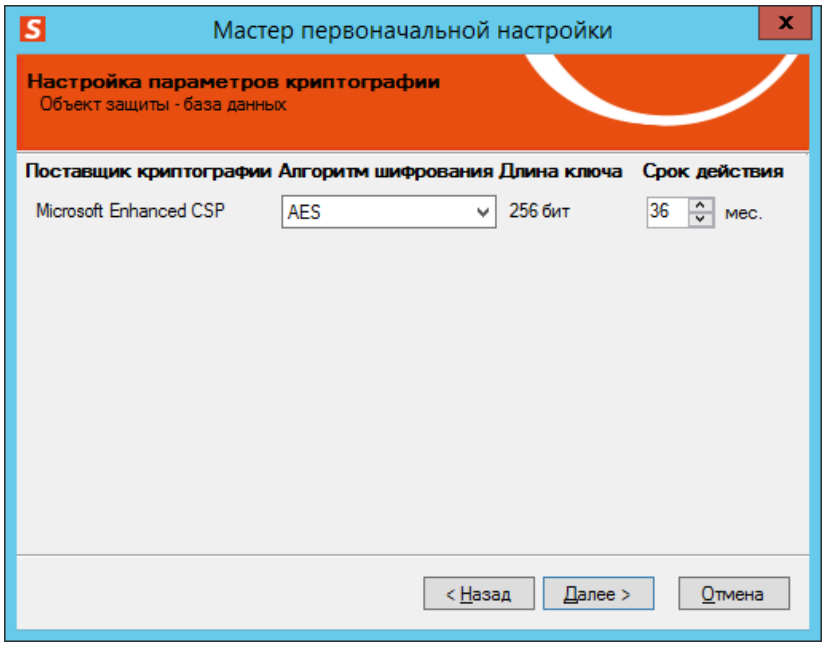



*Рис. 91 – Окно настройки параметров криптографии*

20. Если требуется, внесите необходимые изменения и нажмите **Далее**.
Отобразится следующее окно.

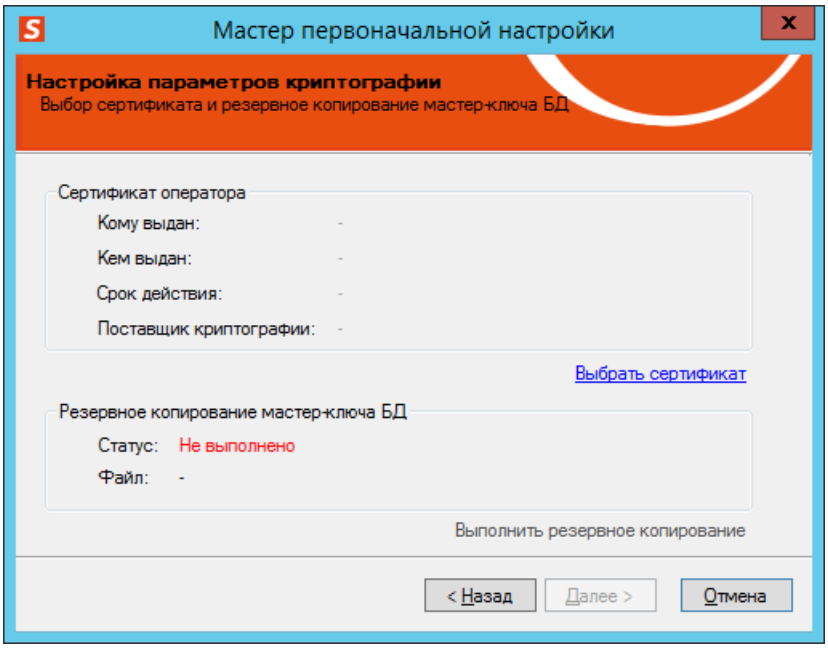



*Рис. 92 – Окно выбора сертификата оператора JMS*

21. Подсоедините подготовленный электронный ключ оператора JMS (см. «Запись сертификата в память электронного ключа», с. 36) к компьютеру, после чего щелкните на ссылке **Выбрать сертификат**.

Отобразится следующее окно.

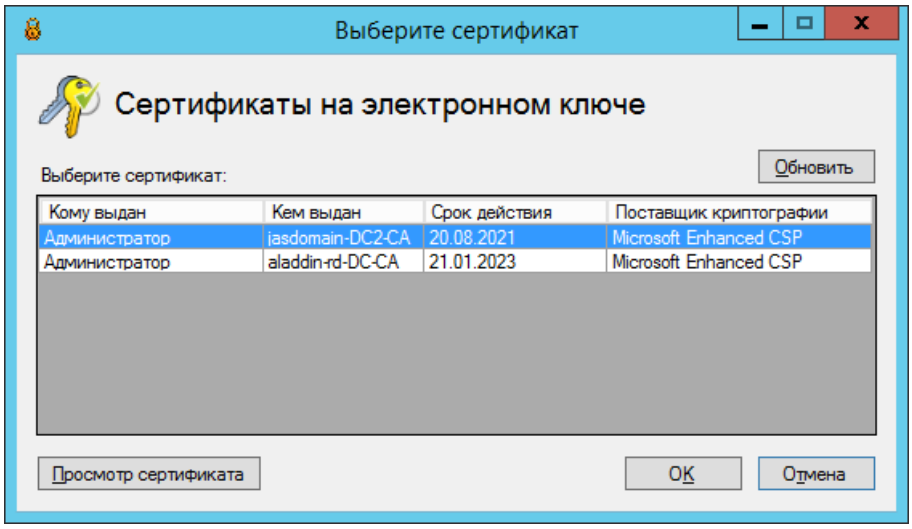



*Рис. 93 – Окно выбора сертификата*

22. Выберите нужный сертификат и нажмите **OK**.
Окно выбора сертификата оператора будет выглядеть следующим образом.

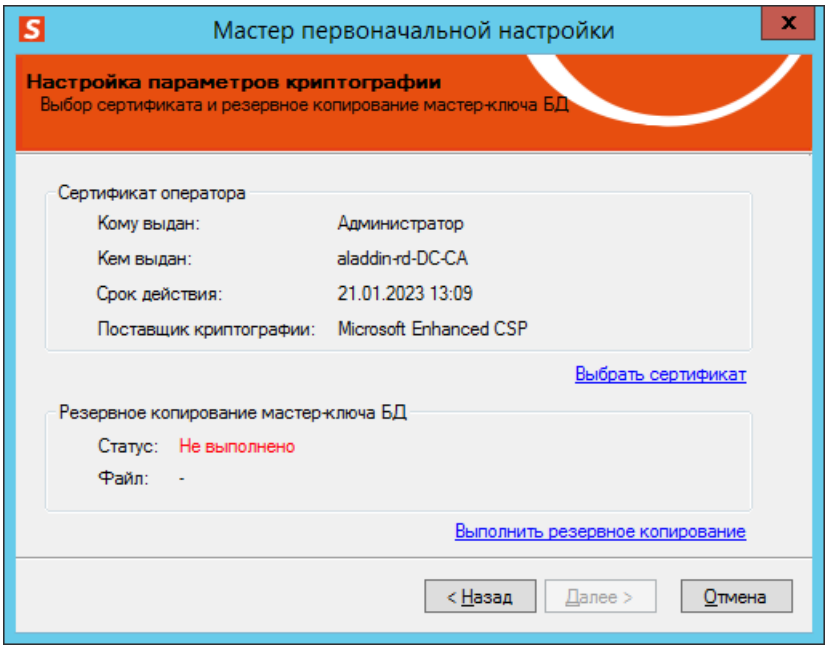



*Рис. 94 – Сертификат оператора успешно выбран*

23. Щелкните на ссылке **Выполнить резервное копирование** и выполните процедуру, приведенную в пункте «Резервное копирование мастер-ключа БД», с. 153.

24. В поле **Статус** секции **Резервное копирование мастер-ключа БД** будет значиться **Выполнено** (см. рис. 95).

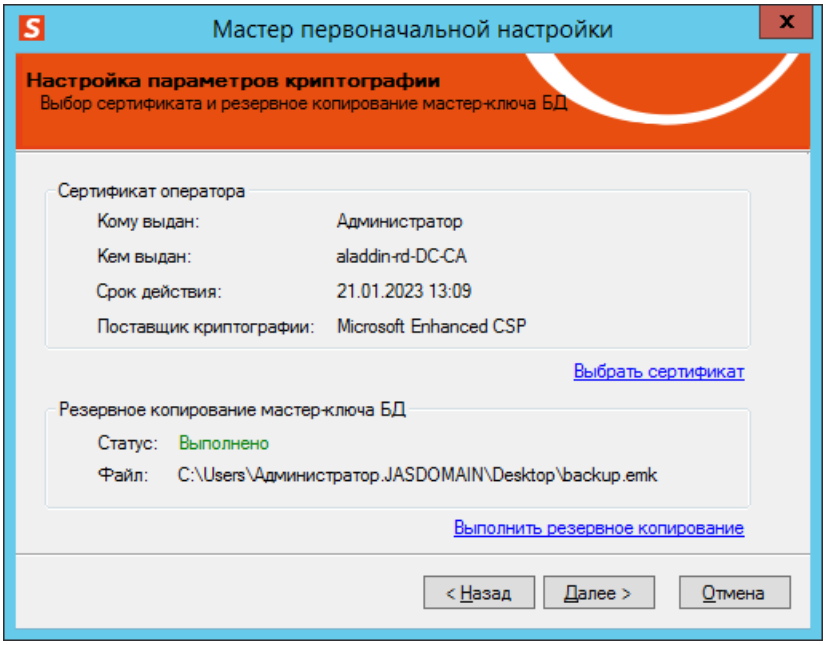



*Рис. 95 – В поле Статус отображается значение Выполнено*

25. Нажмите **Далее**.

### 8.3.7 Настройка сервиса (службы) аутентификации JMS

Отобразится следующее окно.

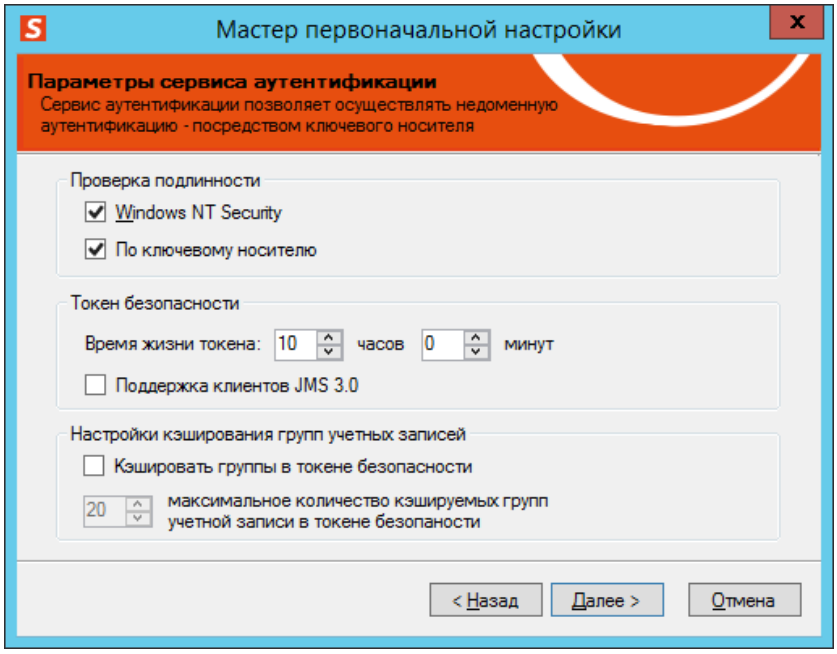



*Рис. 96 – Настройка службы аутентификации JMS*

26. Выполните настройку, руководствуясь табл. 11.


Служба аутентификации JMS позволяет пользователю аутентифицироваться на сервере JMS посредством клиента JMS. Таким образом, прошедший аутентификацию пользователь может выполнять операции с электронными ключами.

*Табл. 11 – Настройка службы аутентификации JMS*

| Секция | Настройка | Описание |
|---|---|---|
| **Проверка подлинности** | **Windows NT Security** | Аутентификация производится на основе встроенной проверки подлинности Windows, т.е. для успешной аутентификации электронный ключ не требуется. |
| | **По ключевому носителю** | Аутентификации производится с использованием электронного ключа. Для этого электронный ключ должен быть предварительно выпущен через JMS. В процессе выпуска, на электронный ключ запишется аутентификатор, с помощью которого будет осуществляться открытие сеанса. |
| **Токен безопасности** | *Токен безопасности* – программный билет, который служба аутентификации JMS предоставляет клиенту JMS в результате успешного прохождения пользователем аутентификации. Токен безопасности позволяет открыть сеанс связи между клиентом JMS и сервером, после чего можно будет осуществлять операции с электронными ключами.<br><br>Если аутентификация была произведена на основе внутренней проверки подлинности Windows, по истечении времени жизни токена безопасности новый будет выдан автоматически. Если аутентификация была произведена с использованием электронного ключа, по истечении времени жизни токена безопасности пользователь должен будет ввести PIN-код своего электронного ключа. | |
| | **Время жизни токена** | Воспользовавшись соответствующими полями, укажите (в часах и минутах) время жизни токена безопасности. |
| | **Поддержка клиентов JMS 3.0** | Установите флаг в том случае, если в JMS требуется поддержка унаследованных JMS-клиентов версии 3.0. В противном случае будет обеспечена поддержка только унаследованных JMS-клиентов версии 3.1.1. (Подробнее о настройке поддержки унаследованных клиентов см. «Руководство администратора. Часть 2» [3], раздел «Поддержка унаследованных клиентов JMS»). |
| **Настройки кэширования групп учетных записей** | Секция содержит параметры для ускорения работы сервера JMS за счет сохранения в токене безопасности (см. выше) заранее вычисленных перечней групп AD и глобальных групп JMS, которым принадлежит пользователь, выполнивший аутентификацию в JMS. | |

| Секция | Настройка | Описание |
|---|---|---|
| | **Кэшировать группы в токене безопасности** | При установке данного признака сервер JMS осуществляет кэширование перечней групп AD и глобальных групп JMS пользователя в токене безопасности (установка данного параметра обеспечивает значительное ускорение работы сервера JMS). |
| | **Максимальное количество кэшируемых групп учетной записи в токене безопасности** | Параметр определяет предельное число групп AD и глобальных групп JMS, к которым приписан пользователь, для выполнения их кэширования в токене безопасности. В случае если число групп, которым принадлежит пользователь, превышает это значение, то кэширование групп для такого пользователя выполняться не будет.<br><br>Значение по умолчанию: 20 (рекомендуемое); максимальное допустимое значение – 100. |

27. Нажмите **Далее**.
Отобразится следующее окно.

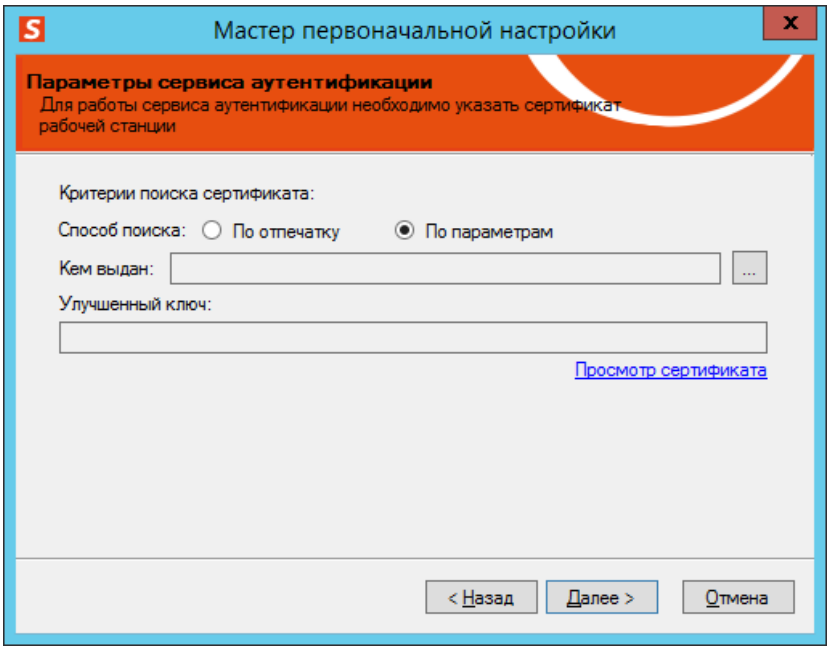



*Рис. 97 – Критерии поиска сертификата*

28. Выберите сертификат службы аутентификации JMS, после чего нажмите **Далее**.

Если вы создаете кластер, в настройке **Способ поиска** необходимо выбрать пункт **По отпечатку**.

При необходимости вы впоследствии сможете изменить эти настройки в окне управления сервером JMS (см. «Настройки сервиса аутентификации JMS», с. 194).

### 8.3.8 Настройка служебной учетной записи

Отобразится следующее окно.

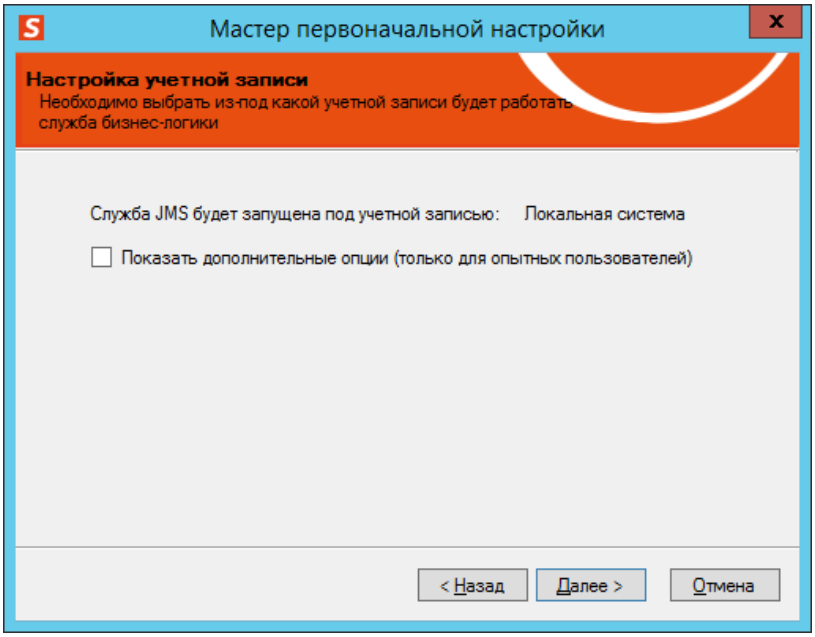



*Рис. 98 – Настройка служебной учетной записи (настройка по умолчанию)*

29. Если службы JMS должна выполняться под учетной записью локальной системы (типовая настройка для развертывания единичного экземляра сервра JMS, т.е. без использования кластера), то нажмите **Далее** (и переходите к шагу 32).
30. Если вы планируете развертывание кластера JMS, или вам требуется особая конфигурация запуска службы сервера JMS, нажмите флаг **Показать дополнительные опции (только для опытных пользователей)**.
    Окно примет следующий вид.

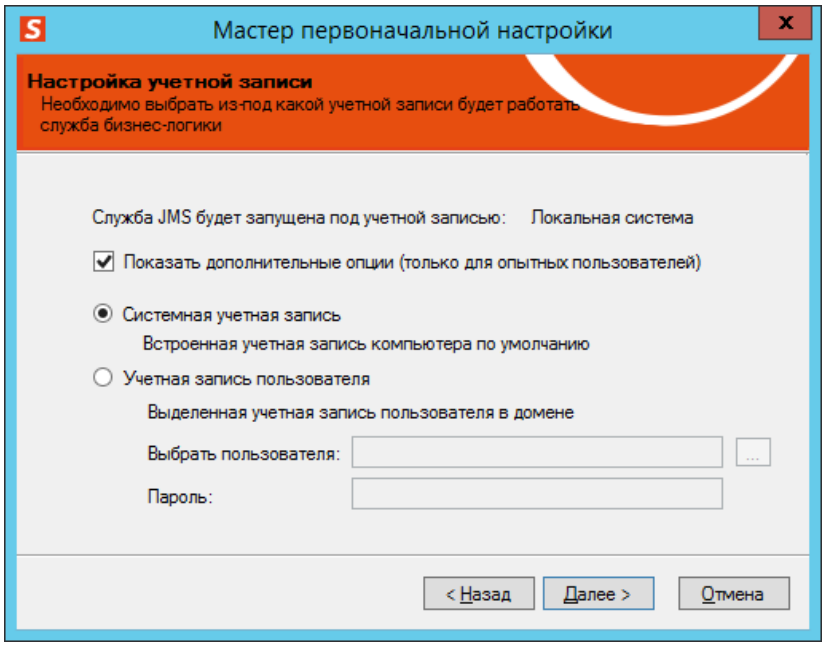



*Рис. 99 – Настройка служебной учетной записи*

31. Выберите тип учетной записи, от имени которой будет запускаться сервер JMS и выполните необходимые действия, руководствуясь табл. 12.

*Табл. 12 – Выбор учетной записи для запуска сервера JMS*

| Тип учетной записи | Описание |
|---|---|
| Системная учетная запись | В этом случае будет использоваться системная учетная запись. Дополнительных действий не требуется - нажмите **Далее**. |
| Учетная запись пользователя | В этом случае будет использоваться подготовленная служебная учетная запись. Если вы выполнили действия, представленные в подразделе «Подготовка служебной учетной записи для запуска сервера JMS», с. 67, необходимые данные должны подставиться автоматически. Если по какой-либо причине этого не произошло, выполните следующие действия.<br>1. Воспользуйтесь кнопкой ... напротив поля **Выбрать пользователя**, чтобы выбрать подготовленную служебную учетную запись (в настоящем документе для примера используется учетная запись **JMS_Server**).<br>2. В поле **Пароль** введите пароль выбранной служебной учетной записи.<br>3. Нажмите **Далее**.<br>**Примечание.** При выборе опции **Учетная запись пользователя** после шага создания БД (см. «Создание базы данных», с. 96) следует предоставить данной учетной записи права на владение БД JMS (см. «Создание имени входа на сервере базы данных для служебной учетной записи сервера JMS», с. 96). Данные шаги описаны ниже в порядке последовательности их выполнения.<br>**Важно!** В случае установки узла кластера JMS допускается выбор только пункта **Учетная запись пользователя**. Подробнее смотри описание в руководстве по развертыванию кластерной конфигурации JMS [6]. |

### 8.3.9 Настройка подключения к базе данных

32. Отобразится следующее окно.

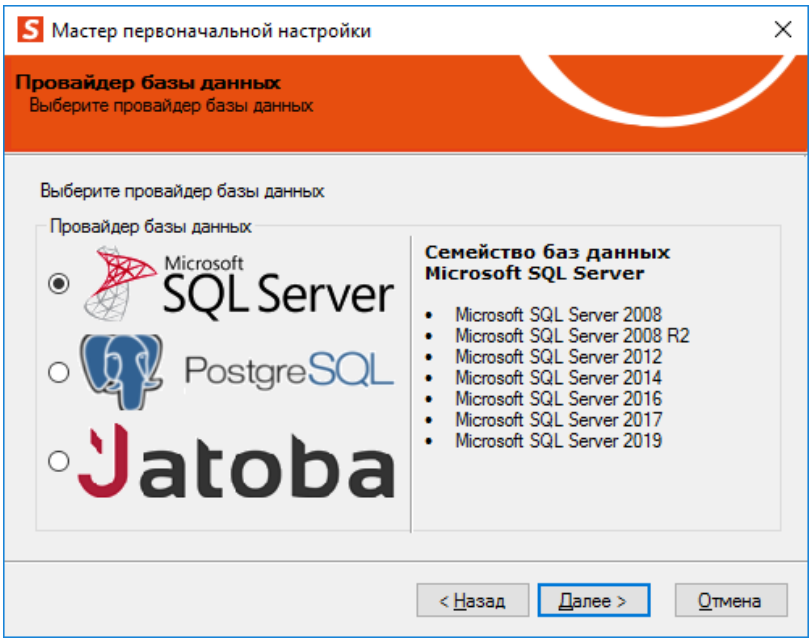



*Рис. 100 – Окно выбора провайдера базы данных*

33. Выберите тип СУБД (MS SQL Server, PostgreSQL или Jatoba), в которой планируется размещать БД JMS и нажмите **Далее**.
34. В зависимости от выбранного на предыдущем шаге типа СУБД отобразится одно из окон подключения к БД JMS (см. Рис. 101 – случай расположения БД в СУБД MS SQL Server, Рис. 102 – случай расположения БД в СУБД PostgreSQL или Jatoba).

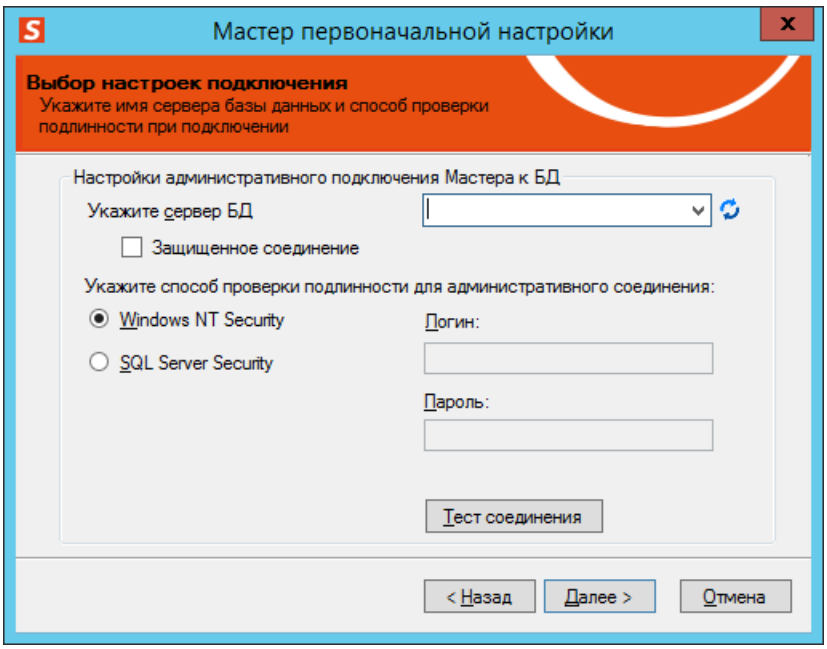



*Рис. 101 – Окно настройки подключения к серверу СУБД MS SQL Server*

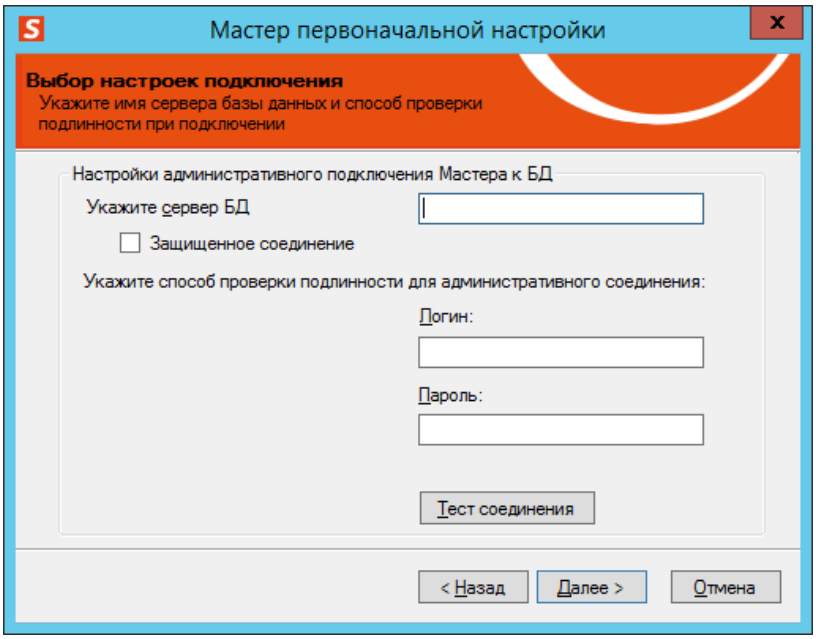



*Рис. 102 – Окно настройки подключения к серверам СУБД PostgreSQL или Jatoba*

35. Выполните необходимые настройки, руководствуясь табл. 13.

*Табл. 13 – Настройки подключения к серверу БД*

| Настройка | Описание |
|---|---|
| **Укажите сервер БД** | В случае использования СУБД MS SQL Server 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.<br><br>**Примечание.** В случае если для подключения к SQL-серверу используется протокол SSL/TLS (см. параметр **Защищенное соединение**, ниже), адрес SQL-сервера следует указать вручную в формате FQDN, например: `sql.test.ru`, а именно следует указать то имя, на которое был выпущен SSL-сертификат для данного сервера.<br><br>В случае использования СУБД PostgreSQL или Jatoba введите IP-адрес хоста, на котором функционирует SQL-сервер. |
| **Защищенное соединение** | Установите этот флаг, если хотите использовать для подключения к базе данных SSL-соединение. |
| **Windows NT Security**<br><br>(опция доступна только при использовании СУБД MS SQL Server) | Выберите этот пункт для подключения к базе данных с использованием аутентификации типа «*проверка подлинности Windows*». Для подключения к СУБД учетная запись пользователя, от имени которой запущен *мастер первоначальной настройки*, должна быть наделена административными правами (SA) на SQL-сервере, к которому происходит подключение. |

| Настройка | Описание |
|---|---|
| **SQL Server Security**<br><br>(опция включена по умолчанию и не отображается при использовании СУБД PostgreSQL или Jatoba) | Выберите этот пункт для подключения к базе данных с использованием стандартной аутентификации на сервере СУБД (при подключении к СУБД PostgreSQL или Jatoba установлена по умолчанию и не отображается). Поля **Логин** и **Пароль** необходимо заполнять в зависимости от следующих условий:<br>• если вам известны аутентификационные данные пользователя СУБД с административными полномочиями (SA), то следует ввести эти аутентификационные данные, достаточные для создания БД JMS в данной СУБД;<br>• если вам недоступны административные полномочия на СУБД, следует выполнить шаги, описанные в разделе «Подготовка СУБД к автоматическому созданию БД JMS без административных прав», с. 108, получить от администратора СУБД аутентификационные данные владельца БД JMS и ввести их в соответствующих полях (**Логин** и **Пароль**). |

36. Чтобы проверить корректность настроек, нажмите **Тест соединения**.
Если соединение настроено верно, отобразится следующее сообщение.

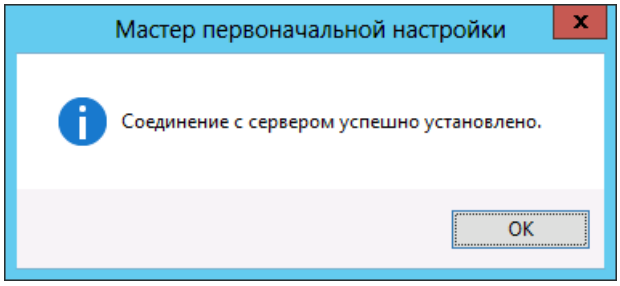



*Рис. 103 – Сообщение об успешной установке соединения с сервером*

37. Нажмите **OK** и в окне мастера первоначальной настройки конфигурации нажмите **Далее**.
38. В случае если отобразится предупреждение следующего вида (Рис. 104), необходимо выполнить (если ещё не выполнены) действия, согласно Табл. 13 (выше, настройки при выборе опции **SQL Server Security**), и перейти к шагам, описанным в разделе «Порядок подключения к БД JMS без административных прав СУБД», с. 110.

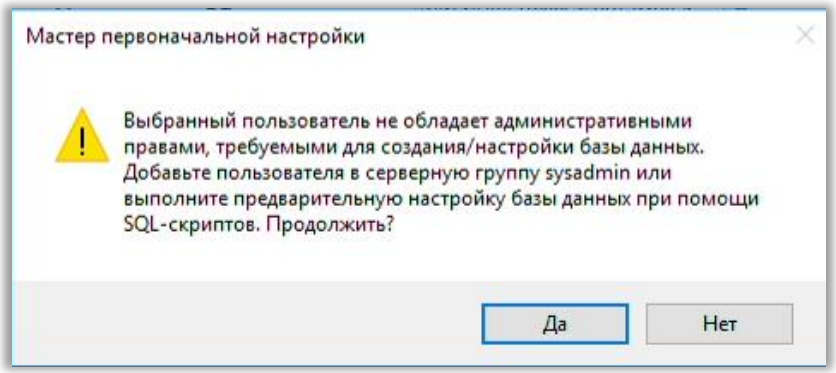



*Рис. 104 – Предупреждение об отсутствии административных прав на СУБД у учетной записи, указанной на предыдущем шаге*

В противном случае переходите к следующему шагу.

39. Отобразится следующее окно.

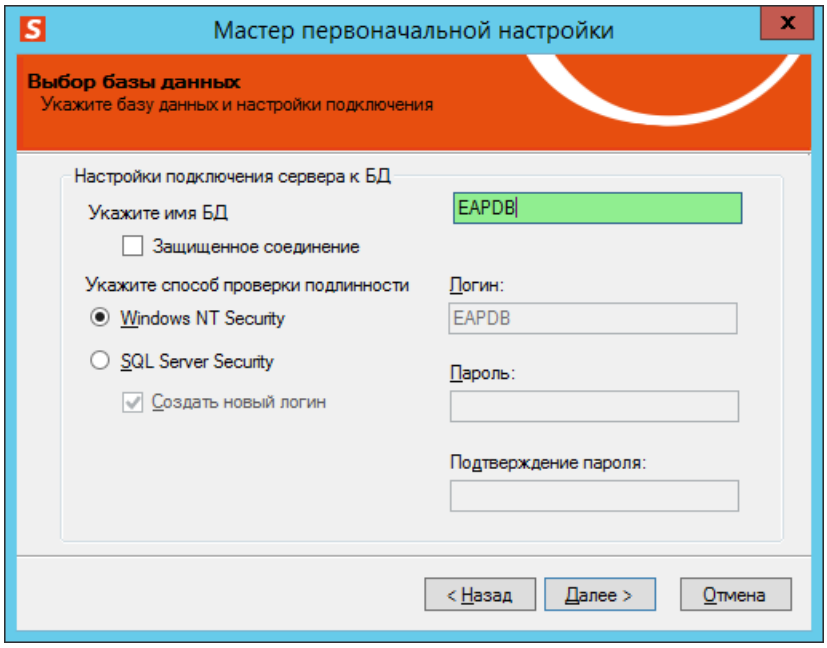



*Рис. 105 – Окно создания или выбора БД JMS при использовании СУБД MS SQL Server*

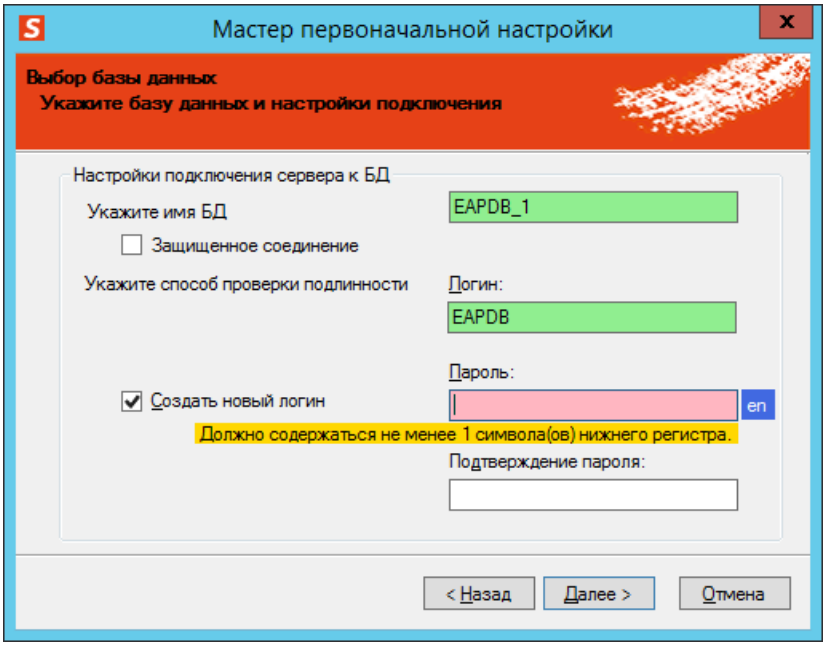



*Рис. 106 – Окно создания или выбора БД JMS при использовании СУБД PostgreSQL или Jatoba*

40. Выполните настройки в соответствии с Табл. 14.

*Табл. 14 – Настройки подключения к базе данных*

| Настройка | Описание |
|---|---|
| **Укажите имя БД** | В зависимости от настраиваемой конфигурации выполните следующие действия:<br>• единственный сервер JMS или создание кластера – в поле **Укажите имя БД** укажите имя новой базы данных, которая будет создана в процессе первоначальной настройки конфигурации;<br>• добавление нового узла к существующему кластеру – в поле **Укажите имя БД** выберите имя существующей базы данных, которая является общей для всего кластера. |

| Настройка | Описание |
|---|---|
| **Защищенное соединение** | Установите флаг, если необходимо настроить шифрование соединения между сервером и базой данных (т.е. включить использование SSL/TLS) |
| **Windows NT Security**<br><br>(опция доступна только при использовании СУБД MS SQL Server) | При выборе пункта **Windows NT Security** (проверка подлинности Windows) и настройке подключения серверной службы JMS к удаленной БД - в создаваемой базе данных будет создано специализированное имя входа, позволяющее обращаться к БД от имени **Системной учетной записи** – учетной записи доменного компьютера, сервера JMS (Local System). Если предполагается запуск серверной службы под доменной **Учетной записью пользователя** (см. «Настройка служебной учетной записи», с. 89), то после шага создания БД (см. «Создание базы данных», с. 96) следует предоставить данной учетной записи права на владение БД JMS (см. «Создание имени входа на сервере базы данных для служебной учетной записи сервера JMS», с. 96). Данные шаги описаны ниже в порядке последовательности их выполнения. |
| **SQL Server Security**<br><br>(опция включена по умолчанию и не отображается при использовании СУБД PostgreSQL или Jatoba) | При выборе пункта **SQL Server Security** создание базы данных и последующее обращение к ней будет производиться либо от вновь созданного имени входа (флаг **Создать новый логин** установлен ), либо от имени ранее созданного на SQL-сервере имени входа (флаг **Создать новый логин** сброшен) |

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

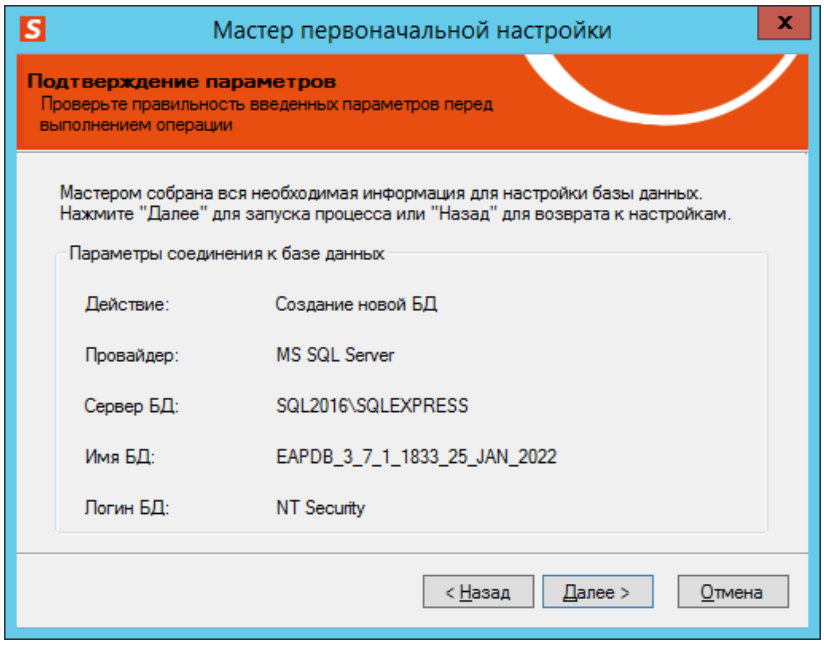



*Рис. 107 – Окно подтверждения параметров подключения к базе данных*

Нажмите **Далее**.

### 8.3.10 Создание базы данных

Отобразится окно следующего вида.

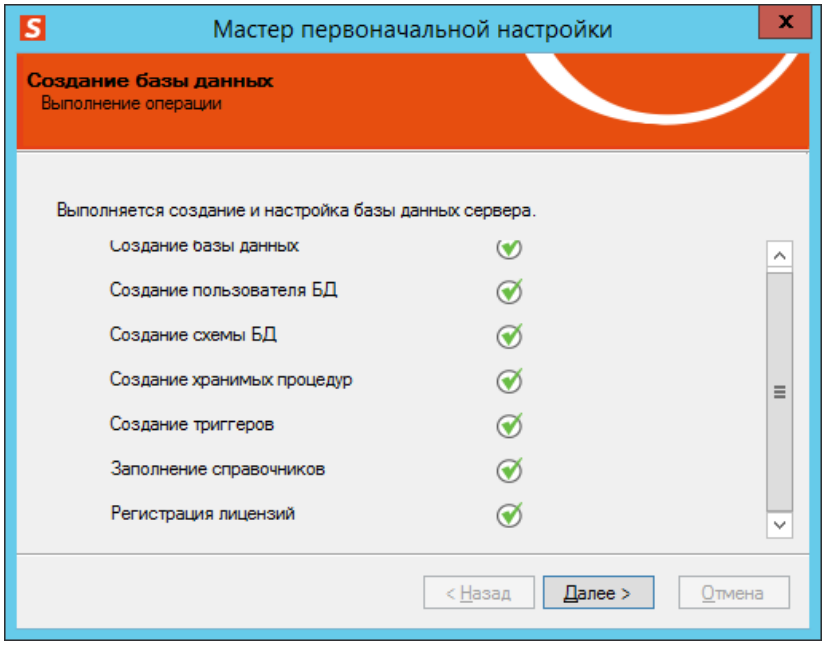



*Рис. 108 – Окно результатов создания и настройки базы данных (на примере использования СУБД MS SQL)*

Нажмите **Далее**.

### 8.3.11 Создание имени входа на сервере базы данных для служебной учетной записи сервера JMS

Содержимое настоящего раздела относится только к установке JMS с использованием СУБД MS SQL Server (не относится к установке с использованием СУБД PostgreSQL или Jatoba).

В зависимости от типа выбранной служебной учетной записи в пункте «Настройка служебной учетной записи», с. 89 выполните следующие действия:

- **Системная учетная запись**, переходите к пункту «Обновление базы данных», с. 101;
- **Учетная запись пользователя** - выполните действия, представленные в настоящем пункте.

В последнем случае не закрывайте окно мастера первоначальной настройки конфигурации JMS.

Если сервер JMS будет запускаться от имени подготовленной служебной учетной записи пользователя, то этой учетной записи необходимо назначить разрешения для доступа к базе данных JMS. Процедура назначения таких разрешений различается в зависимости от того, установлена ли на сервере **Среда SQL Server Management Studio** из состава MS SQL Server:

- см. «Среда SQL Server Management Studio установлена», с. 96;
- см. «Среда SQL Server Management Studio не установлена», с. 100.

В настоящем документе в качестве сервера базы данных для примера используется версия MS SQL Server 2012.

#### 8.3.11.1 Среда SQL Server Management Studio установлена

1. В меню Пуск выберите **Microsoft SQL Server 2012 -> Среда SQL Server Management Studio**.

Отобразится следующее окно.

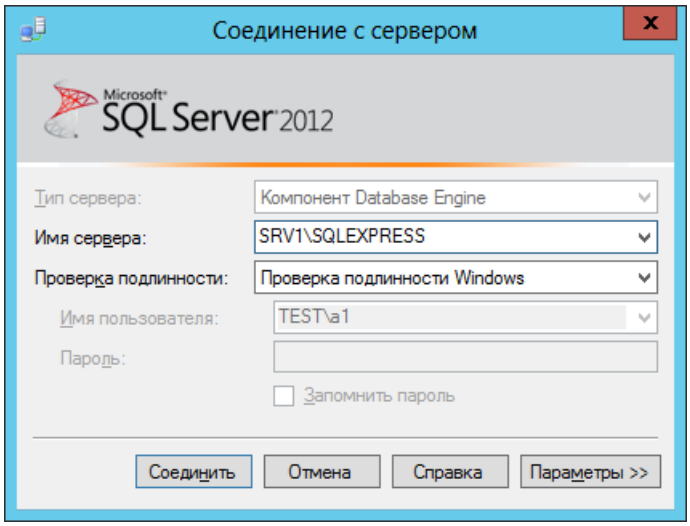



*Рис. 109 – Окно настроек соединения с сервером базы данных*

2. Введите необходимые данные для соединения с севером базы данных и нажмите **Соединить**. Отобразится следующее окно.

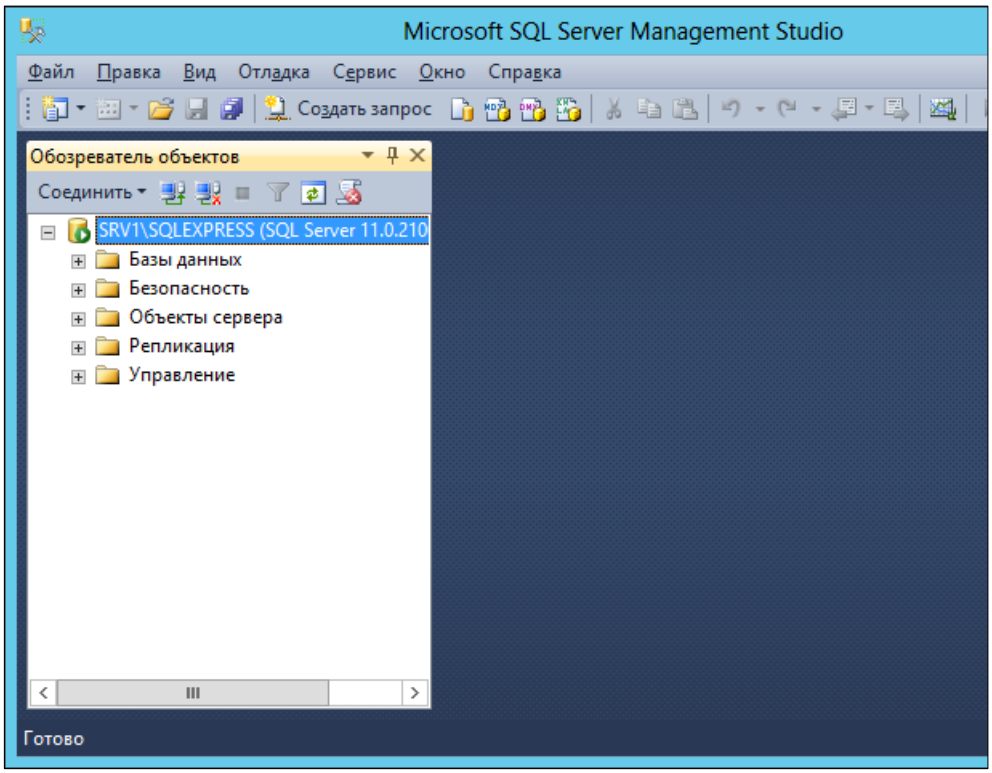



*Рис. 110 – Microsoft SQL Server Management Studio*

3. В панели **Обозреватель объектов** разверните пункт **Безопасность**, щелкните правой кнопкой на пункте **Имена входа** и выберите **Создать имя входа**, как показано на изображении ниже.

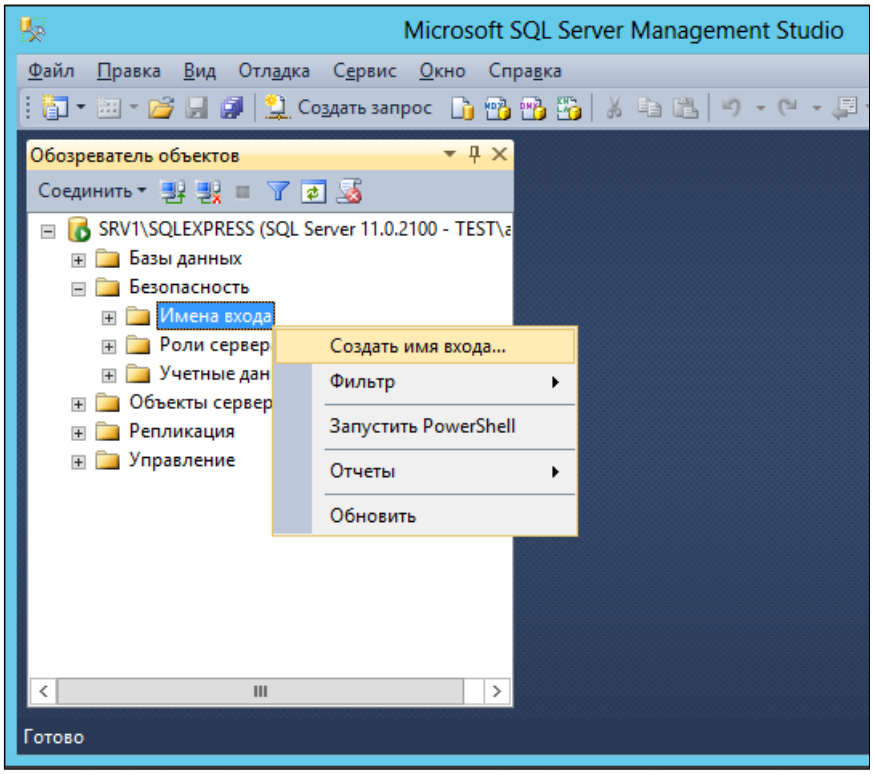



*Рис. 111 – Создание нового имени входа*

4. В отобразившемся окне в левой панели выберите пункт **Общие**.
Окно примет следующий вид.

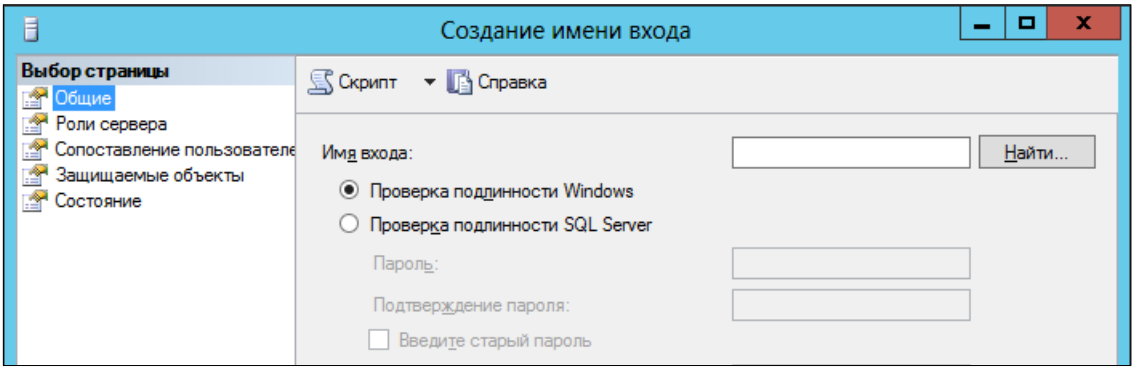



*Рис. 112 – Общие параметры создаваемого имени входа.*

5. Воспользуйтесь кнопкой **Найти** напротив поля **Имя входа**, чтобы выбрать служебную учетную запись, от имени которой будет запускаться сервер JMS (в настоящем документе для примера используется учетная запись **JMS_Server**).

6. В левой панели выберите пункт **Роли сервера** и убедитесь в том, что в списке **Роли сервера** отмечен пункт **public**, как показано на изображении ниже.

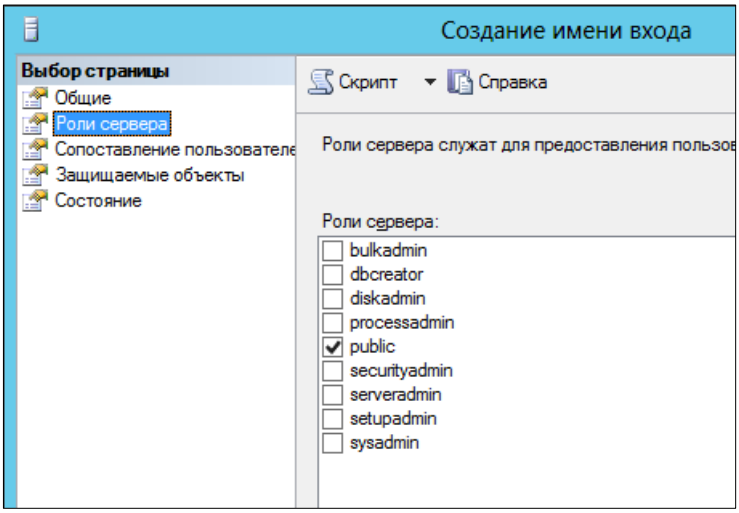



*Рис. 113 – Роли сервера*

7. В левой панели выберите пункт **Сопоставление пользователей**. Отобразится следующее окно.

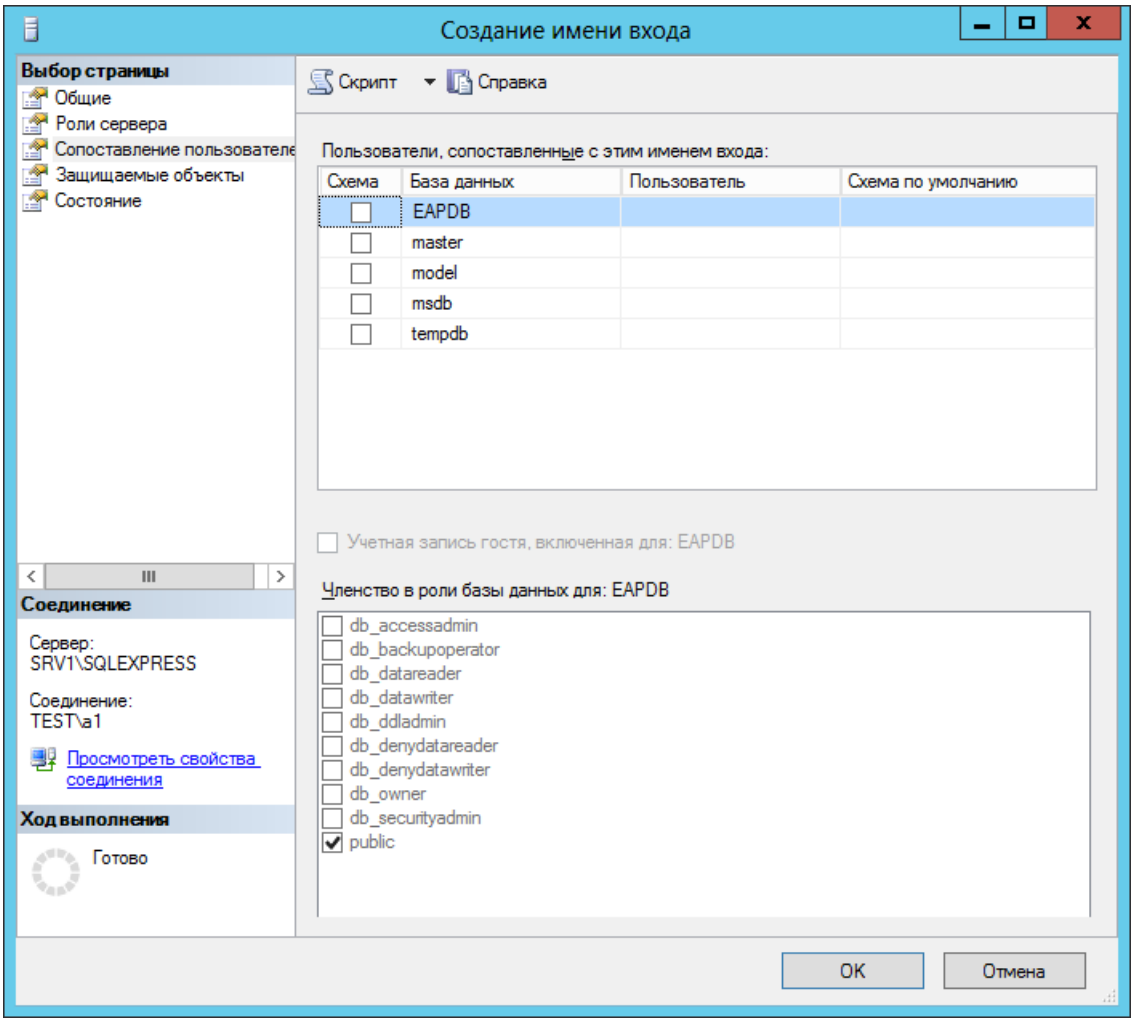



*Рис. 114 – Сопоставление пользователей*

8. Выполните следующие действия:

8.1. В секции **Пользователи**, сопоставленные с этим именем входа отметьте имя базы банных JMS (по умолчанию – это имя **EAPDB**, подробнее см. рис. 105, с. 94).
8.2. В секции **Членство в роли базы данных для** отметьте пункт **db_owner** и оставьте отмеченным пункт **public**.

9. Нажмите **OK**, чтобы сохранить изменения.
10. Переходите к пункту к пункту «Обновление базы данных», с. 101.

### 8.3.11.2 Среда SQL Server Management Studio не установлена

Если среда **Среда SQL Server Management Studio** не установлена на сервере, необходимо создать сценарий и выполнить его с помощью утилиты командной строки **sqlcmd**, входящей в состав MS SQL Server.

Подробные сведения о работе с этой утилитой представлены на сайте Microsoft: https://msdn.microsoft.com/ru-ru/library/ms162773%28v=sql.120%29.aspx.

Чтобы назначить служебной учетной записи сервера JMS необходимые разрешения, выполните следующие действия.

1. С помощью текстового редактора (например, с помощью программы Блокнот) создайте файл и заполните его следующим содержимым.

```
USE [master]

GO

CREATE LOGIN [TEST\JMS_Server] FROM WINDOWS WITH DEFAULT_DATABASE=[master]

GO

USE [EAPDB]

GO

CREATE USER [TEST\JMS_Server] FOR LOGIN [TEST\JMS_Server]

GO

USE [EAPDB]

GO

ALTER ROLE [db_owner] ADD MEMBER [TEST\JMS_Server]

GO
```

Здесь:

- **TEST\JMS_Server** – имя служебной учетной записи, от имени которой будет запускаться сервер JMS в формате **ДОМЕН\Пользователь** (подробнее см. «Подготовка служебной учетной записи для запуска сервера JMS», с. 67).
- **EAPDB** – имя базы данных JMS (см. рис. 105, с. 94).

2. Сохраните файл с расширением **sql**, например, **script.sql**.
3. Из командной строки выполните команду следующего вида:

```
sqlcmd -S <Имя сервера>\<Имя экземпляра> -i <путь к файлу сценария>
```

например:

```
sqlcmd -S SRV1\SQLEXPRESS -i C:\script.sql
```

### 8.3.12 Обновление базы данных

Если на этапе подключения к существующей БД будет обнаружено, что ее версия ниже минимально поддерживаемой сервером, отобразится окно обновления базы данных. В противном случае переходите к пункту «Запуск серверной службы», с. 103.

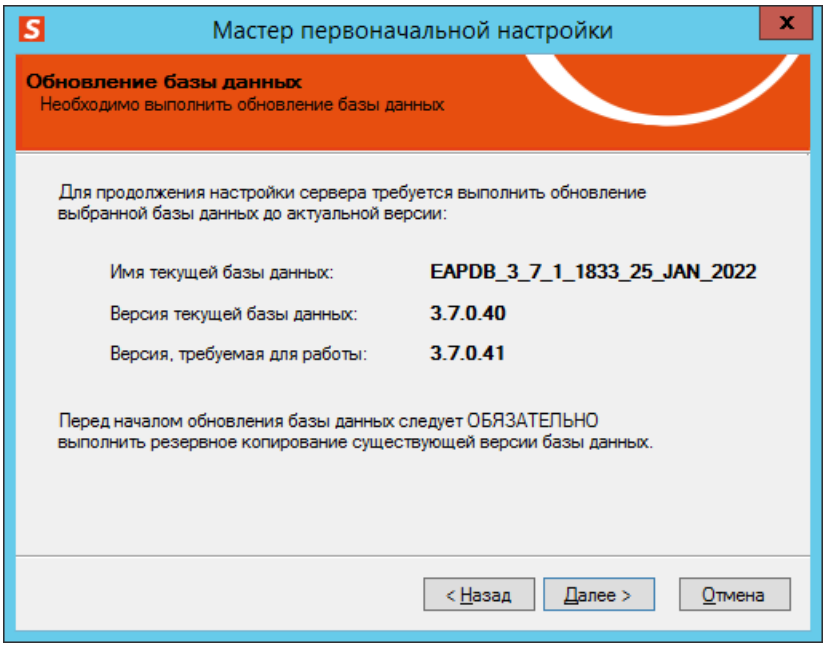



*Рис. 115 – Начало процедуры обновления базы данных*

4. Нажмите **Далее**.

⚠ Перед началом обновления базы данных настоятельно рекомендуется выполнить резервное копирование существующей версии базы данных. Также, по возможности, следует завершить все ранее начатые операции, связанные с обращением к мастер-ключу БД.

Отобразится следующее окно.

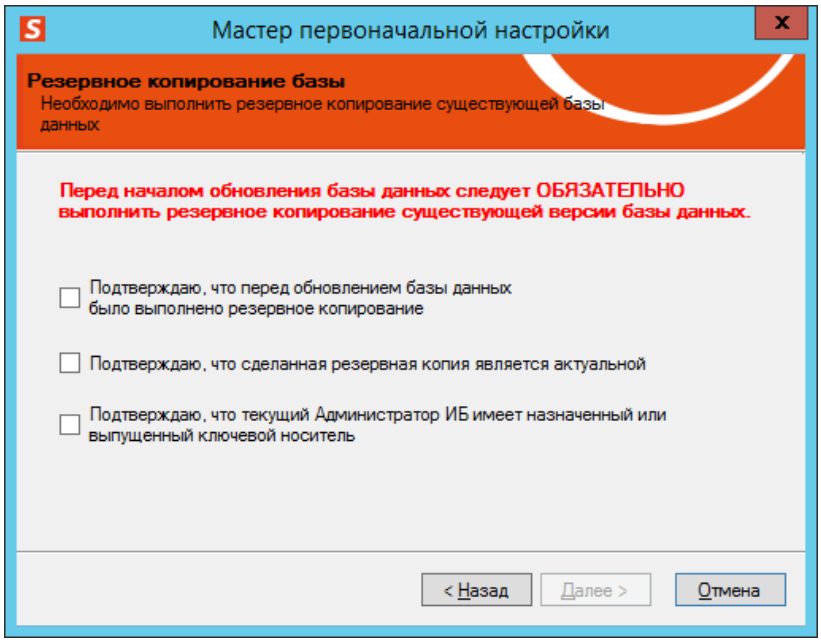



*Рис. 116 – Начало процедуры обновления базы данных*

5. Установите флаги подтверждения, после чего нажмите **Далее**.
6. Дождитесь завершения операции обновления базы данных. В зависимости от объема данных этот процесс может занять несколько минут.
   По завершении обновления отобразится окно с детализацией обновления.

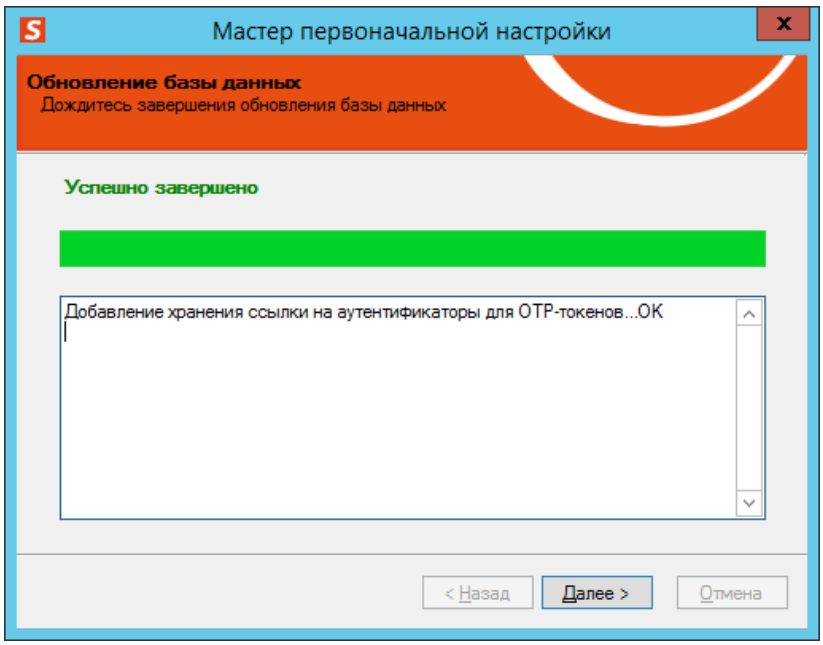



*Рис. 117 – Детализация обновления БД*

7. Нажмите **Далее**.

По завершении обновления отобразится следующее окно.

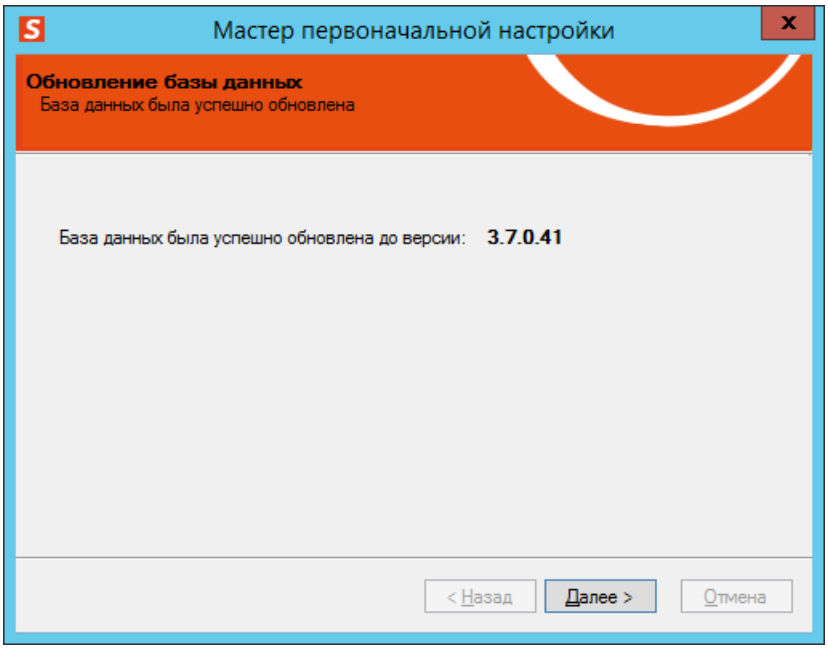



*Рис. 118 – Завершение процедуры обновления базы данных*

8. Нажмите **Далее**.

### 8.3.13 Запуск серверной службы

Отобразится следующее окно.

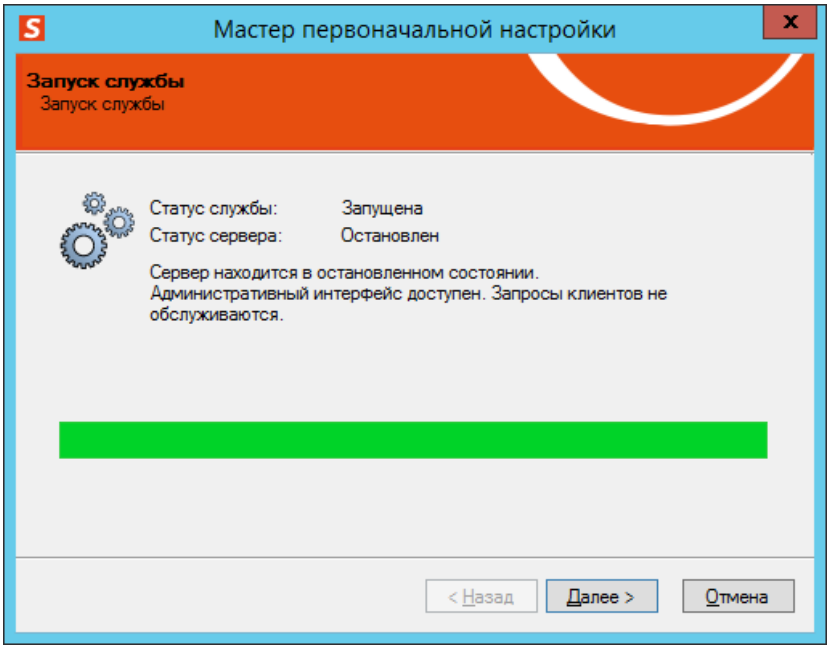



*Рис. 119 – Окно запуска службы JMS*

Нажмите **Далее**.

### 8.3.14 Настройка расширений JMS

Отобразится следующее окно.

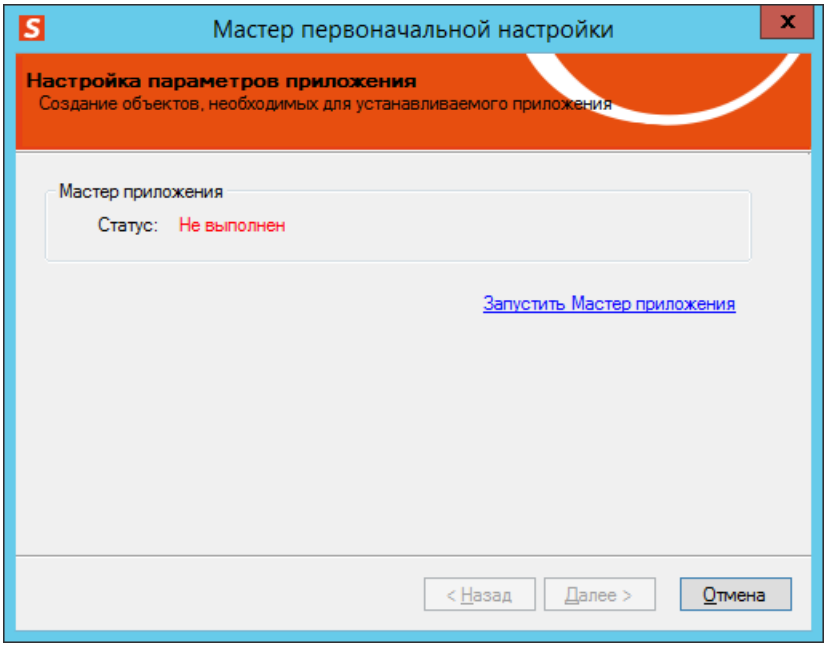



*Рис. 120 – Окно статуса мастера приложения*

9. Щелкните на ссылке **Запустить Мастер приложения**.
Отобразится следующее окно.

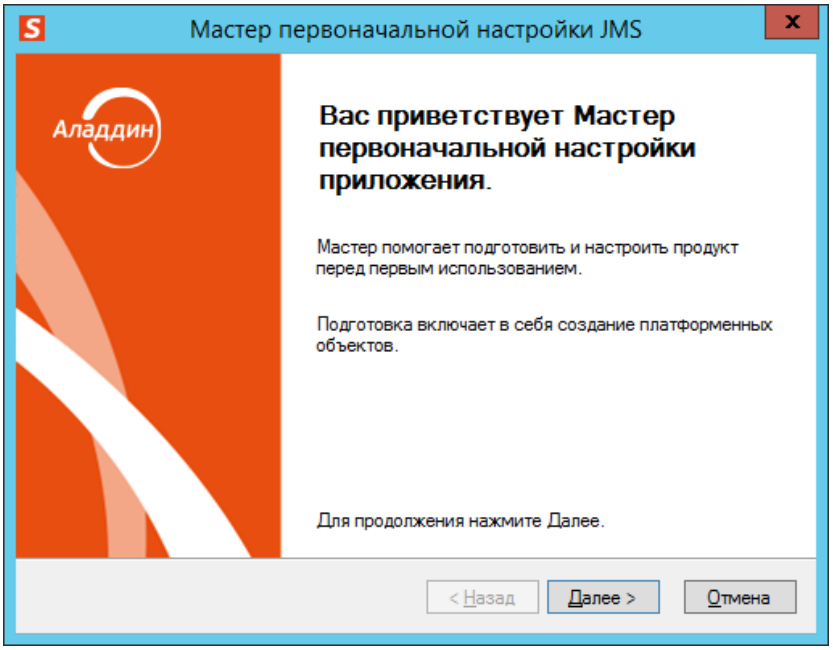



*Рис. 121 – Окно приветствия мастера первоначальной настройки приложения*

10. Нажмите **Далее**.

Отобразится следующее окно.

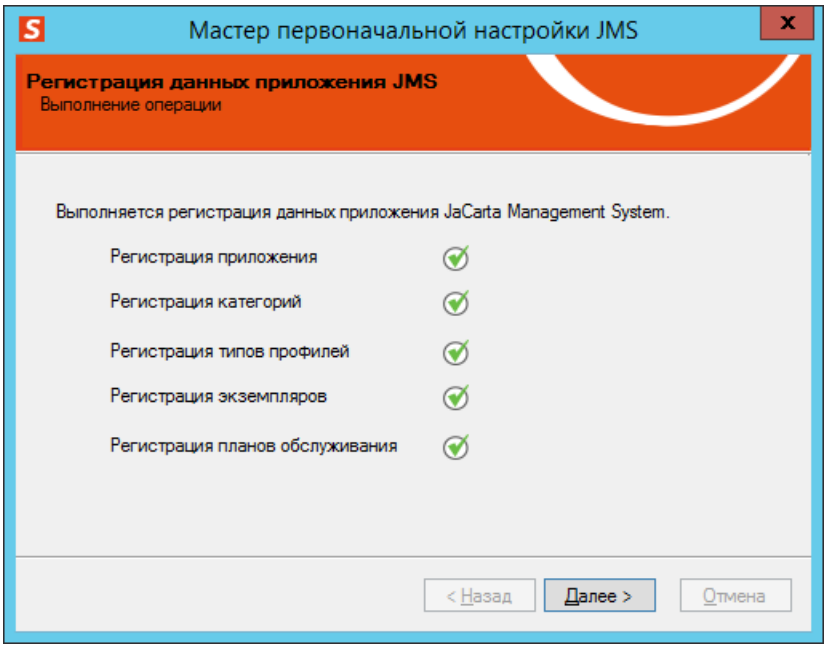



*Рис. 122 – Окно регистрации данных серверного приложения JMS*

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

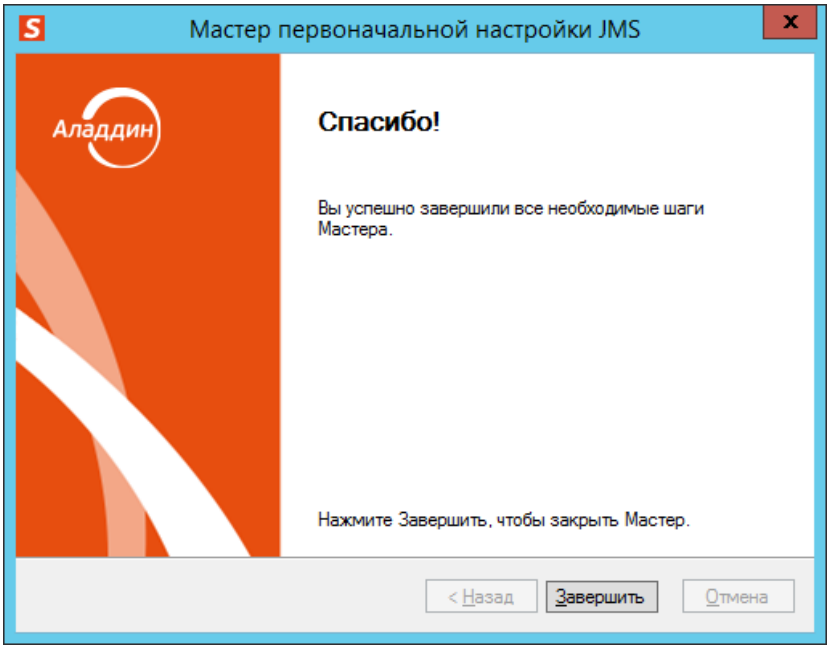



*Рис. 123 – Окно завершения работы мастера первоначальной настройки серверного приложения JMS*

12. Нажмите **Завершить**, чтобы вернуться в окно мастера первоначальной настройки конфигурации.

Окно мастера первоначальной настройки конфигурации будет выглядеть следующим образом.

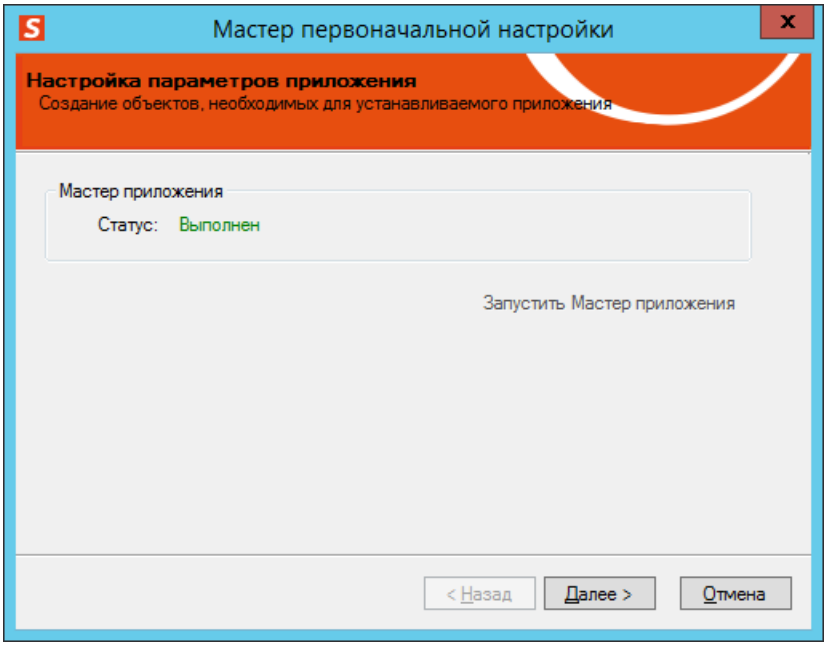



*Рис. 124 – Поле **Статус** имеет значение **Выполнен***

13. Нажмите **Далее**.

### 8.3.15 Запуск сервера JMS

Отобразится следующее окно.

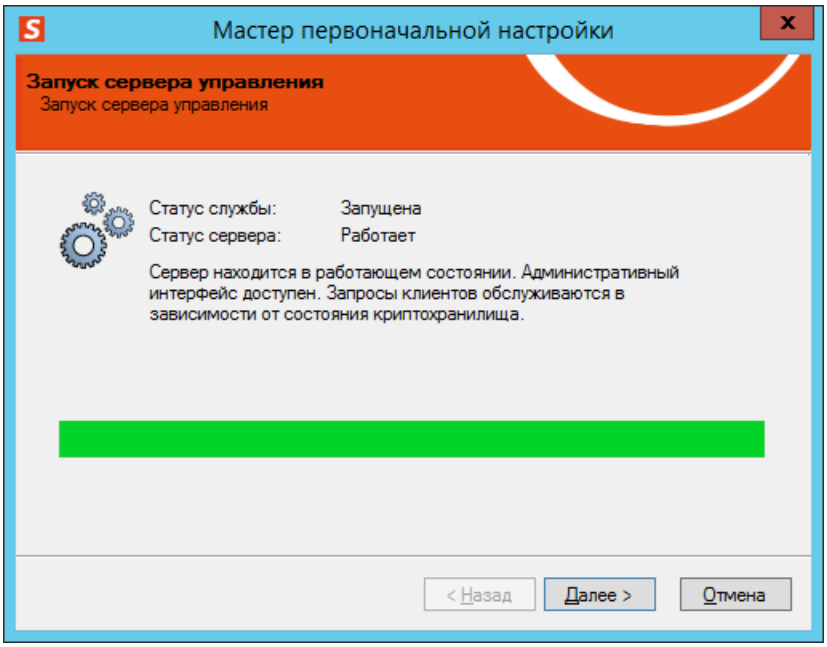



*Рис. 125 – Окно запуска сервера управления*

14. Нажмите **Далее**.

### 8.3.16 Монтирование криптохранилища

Отобразится следующее окно.

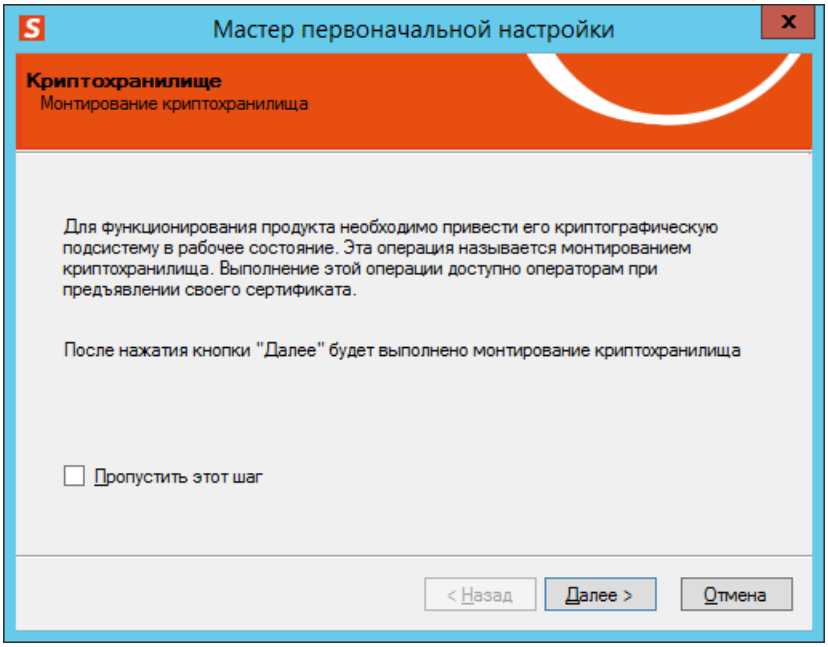



*Рис. 126 – Окно монтирования криптохранилища*

15. Если вы хотите смонтировать криптохранилище позже, установите флаг **Пропустить этот шаг**, после чего нажмите **Далее**, в противном случае – просто нажмите **Далее**.

### 8.3.17 Завершение первоначальной настройки

Отобразится следующее окно.

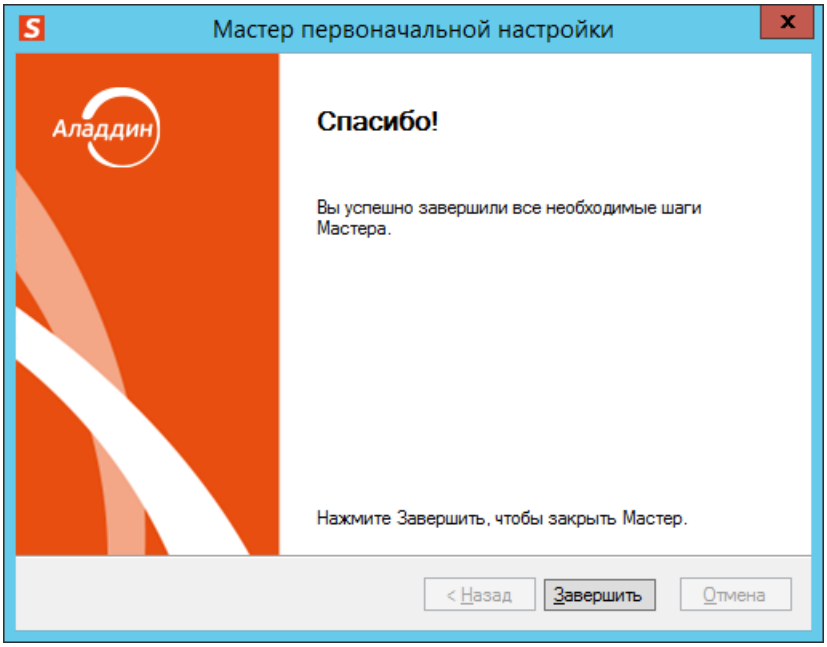



*Рис. 127 – Окно завершения работы мастера первоначальной настройки конфигурации JMS*

16. Нажмите **Завершить** для окончания процедуры.

После первоначальной настройки конфигурации значок сервера JMS в области уведомлений будет выглядеть следующим образом: (Сервер JMS).

### 8.3.18 Подготовка СУБД к автоматическому созданию БД JMS без административных прав

Если корпоративными правилам ИБ запрещено назначение административных прав в СУБД неуполномоченным пользователям (например, администратору JMS), то при установке JMS предусмотрен сценарий, не требующий наличия таких прав у администратора JMS.

Данный сценарий подразумевает подготовительный шаг вне процедуры *мастера первоначальной настройки*, выполняемый администратором СУБД без передачи административных прав администратору JMS. Суть данного шага в создании пустой БД JMS и ее владельца с последующей передачей аутентификационных данных (владельца БД) администратору JMS. Наполнение же такой пустой базы данных таблицами производится в автоматическом режиме в ходе выполнения *мастера первоначальной настройки* (допускается запуск мастера по сценариям **Установить только на этом компьютере**, см. Рис. 79, с. 75, или **Дополнительные опции развертывания** -> **Создание новой базы данных**).

Ниже описан порядок подготовительных действий для случаев создания БД JMS:

- в СУБД MS SQL Server (см. «Ручное создание пустой БД JMS в СУБД MS SQL Server», ниже);
- в СУБД PostgreSQL (см. «Ручное создание пустой БД JMS в СУБД PostgreSQL», с. 109).

#### 8.3.18.1 Ручное создание пустой БД JMS в СУБД MS SQL Server

Для создания пустой базы данных JMS в MS SQL Server в качестве подготовительного шага к развертыванию JMS при отсутствии административных прав на СУБД следует выполнить следующий самодокументированный скрипт. (Данный скрипт должен быть передан для выполнения администратору СУБД).

```
--1) Открыть данный скрипт в SQL Server Management Studio
--2) Подключиться к СУБД с правами администратора
--3) Переключиться в режим SQLCMD (если он не включен по умолчанию) - Query -> SQLCMD Mode
--4) Выполнить подстановку параметров - имя БД, имя пользователя (логин) и пароль в блоке setvar
--5) Выполнить скрипт командой Execute
--6) Будет создана новая пустая БД и недаминистративный логин пользователя
--7) Запустить Мастер создания новой БД JMS и в качестве параметров подключения использовать
созданную БД и логин

:setvar DatabaseName "EAPDB_NOSA"
:setvar UserName "EAPDB_NOSA"
:setvar UserPassword "ZXasqw12!@"

CREATE DATABASE [$(DatabaseName)]
GO

ALTER DATABASE [$(DatabaseName)]
SET READ_COMMITTED_SNAPSHOT ON;
GO

ALTER DATABASE [$(DatabaseName)]
SET ALLOW_SNAPSHOT_ISOLATION ON;
GO

USE [$(DatabaseName)]

IF NOT EXISTS (SELECT * FROM master.dbo.syslogins WHERE loginname = '$(UserName)')
BEGIN
EXEC sp_addlogin [$(UserName)], [$(UserPassword)], [$(DatabaseName)], N'us_english'
END

IF NOT EXISTS (SELECT * FROM dbo.sysusers WHERE name = '$(UserName)' AND uid < 16382)
BEGIN
EXEC sp_grantdbaccess [$(UserName)], [$(UserName)]
END
```

```
EXEC sp_addrolemember N'db_datareader', [$(UserName)]
EXEC sp_addrolemember N'db_datawriter', [$(UserName)]
EXEC sp_addrolemember N'db_owner',        [$(UserName)]
```

По окончании выполнения сценария администратор СУБД передает имя БД, логин владельца БД и его пароль администратору JMS для дальнейшего использования на шаге подключения к СУБД (см. «Настройка подключения к базе данных», Рис. 101, с. 91)

#### 8.3.18.2 Ручное создание пустой БД JMS в СУБД PostgreSQL

Для создания пустой базы данных JMS в PostgreSQLM в качестве подготовительного шага к развертыванию JMS при отсутствии административных прав на СУБД следует выполнить следующий самодокументированный скрипт. (Данный скрипт должен быть передан для выполнения администратору СУБД).

```
--1) Открыть данный скрипт в notepad или аналогичном текстовом редакторе
--2) Выполнить глобальную замену переменных
$DatabaseName - имя БД JMS (например, EAPDB_NOSA)
$UserName - имя пользователя БД JMS (например, EAPDB_NOSA)
$UserPassword - пароль пользователя БД JMS
--3) Подключиться к СУБД с правами администратора через pgAdmin или psql
--4) Выполнить блоки 1 и 2 - будет создана новая БД JMS и выданы все необходимые разрешения
--5) Открыть новое подключение к только что созданной БД
--6) Выполнить блок 3 - скрипт создаст необходимые для работы JMS расширения
--7) Запустить Мастер создания новой БД JMS и в качестве параметров подключения использовать
созданную БД и логин

--БЛОК 1
CREATE DATABASE "$DatabaseName"
ENCODING UTF8
TEMPLATE template0

--БЛОК 2
do $$
begin
if not exists (select * from pg_roles where rolname = '$UserName') then
create user "$UserName" with password '$UserPassword';
end if;

grant all privileges on database "$DatabaseName" to "$UserName";

grant all privileges on all tables in schema public to "$UserName";
grant all privileges on all sequences in schema public to "$UserName";

alter default privileges in schema public grant all privileges on tables to "$UserName";

alter default privileges in schema public grant all privileges on sequences to "$UserName";
end $$


--БЛОК 3 - ВЫПОЛНИТЬ В НОВОМ ПОДКЛЮЧЕНИИ К ТОЛЬКО ЧТО СОЗДАННОЙ БД
CREATE EXTENSION "uuid-ossp";
```

По окончании выполнения сценария администратор СУБД передает имя БД, логин владельца БД и его пароль администратору JMS для дальнейшего использования на шаге подключения к СУБД (см. «Настройка подключения к базе данных», Рис. 102, с. 92)

### 8.3.19 Порядок подключения к БД JMS без административных прав СУБД

В случае запуска *мастера первоначальной настройки* при отсутствии административных прав на СУБД, шаги подключения к БД JMS (см. раздел «Настройка подключения к базе данных», рис. Рис. 105, Рис. 106 с. 94) несколько отличаются от типовых.

При отображении окна выбора базы данных (Рис. 128 и Рис. 129, ниже) в полях аутентификационных данных (**Логин** и **Пароль**) автоматически подставляются значения, введенные на предыдущем шаге (соответственно Рис. 101 и Рис. 102, с. 92).

Пользователю необходимо только выбрать имя в поле **Укажите имя БД** (имя пустой БД, созданной на подготовительном этапе, см. раздел «Подготовка СУБД к автоматическому созданию БД JMS без административных прав», с. 108)

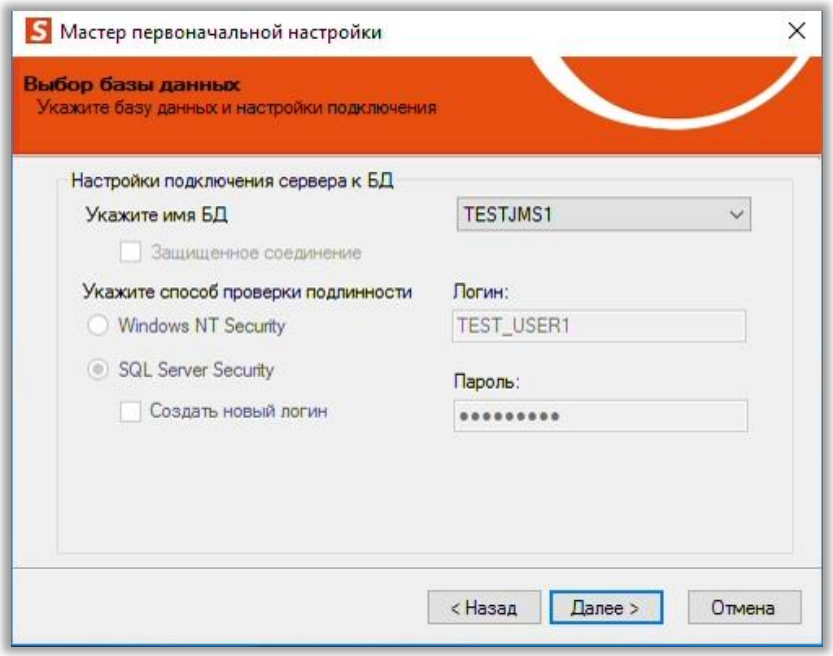



*Рис. 128 – Окно подключения к пустой БД JMS при использовании СУБД MS SQL Server*

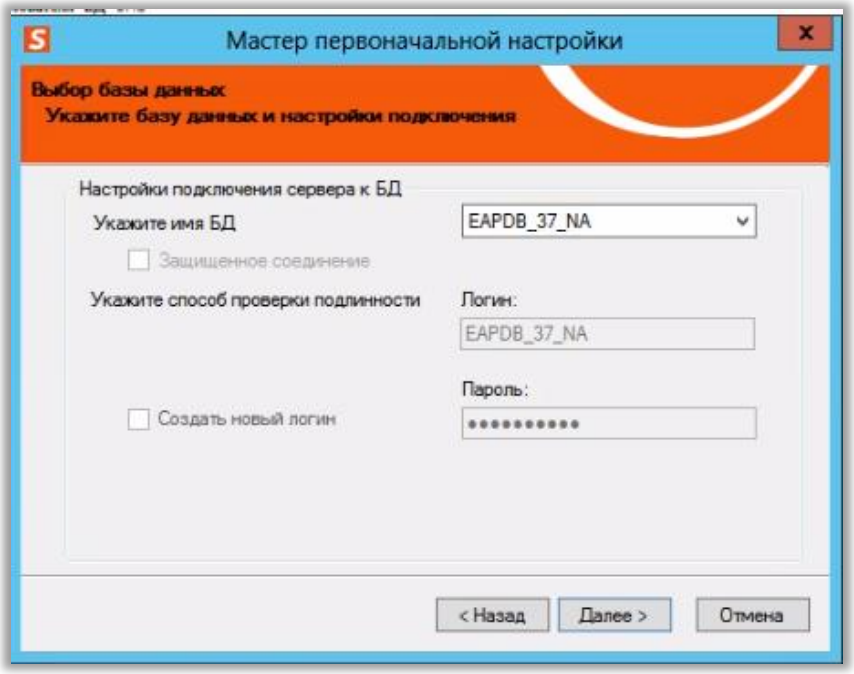



*Рис. 129 – Окно подключения к пустой БД JMS при использовании СУБД PostgreSQL*

По выполнении данных действий, переходите к шагу 41 мастера первоначальной настройки (см. Рис. 107, с. 95).

## 8.4 Централизованная настройка подключения к серверу JMS

Существует возможность выполнить централизованную настройку подключения к серверу JMS посредством создания соответствующих записей на DNS-сервере. Эту настройку можно пропустить, однако в этом случае адрес сервера JMS придется указывать вручную в файлах конфигурации JMS Admin и в реестре компьютера, на котором установлен JMS Client, после установки.

Чтобы настроить подключение к серверу JMS, выполните следующие действия.

Процедуру необходимо выполнить для консоли управления JMS, клиента JMS и службы аутентификации JMS отдельно.

1. На сервере DNS откройте окно оснастки **Диспетчер DNS**. Для этого из окна командной строки выполните команду **dnsmgmt.msc**.

Отобразится следующее окно.

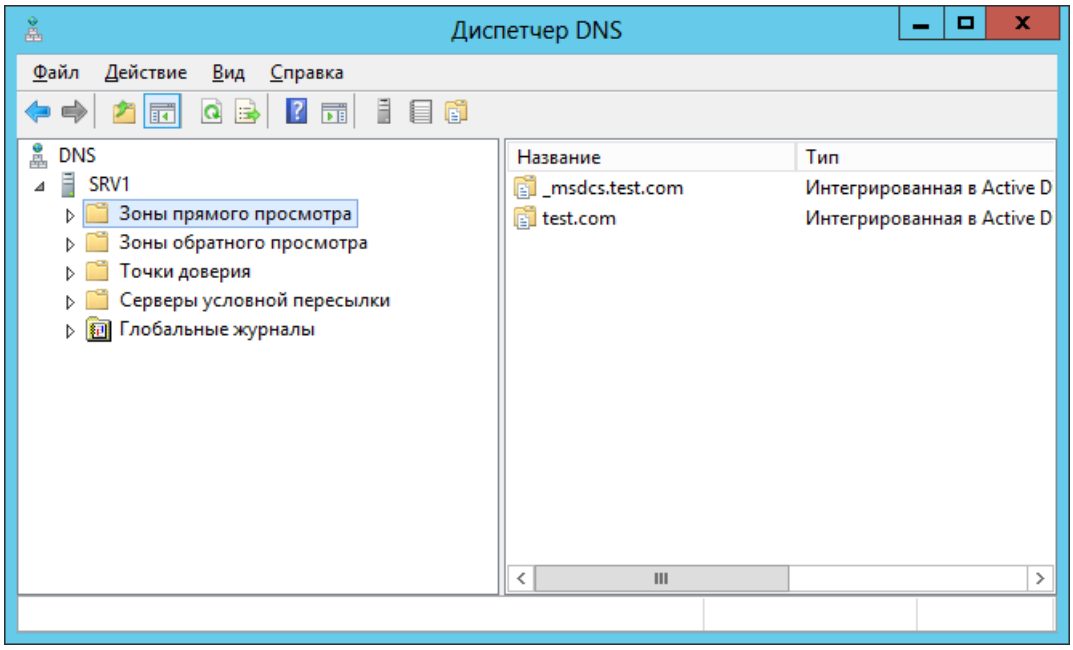



*Рис. 130 – Окно Диспетчер DNS*

Настройка подключения к серверу JMS представлена на примере Microsoft Windows Server 2012.

2. Разверните узел **Зоны прямого просмотра** и выберите **Имя домена -> _tcp** (см. рис. 131).

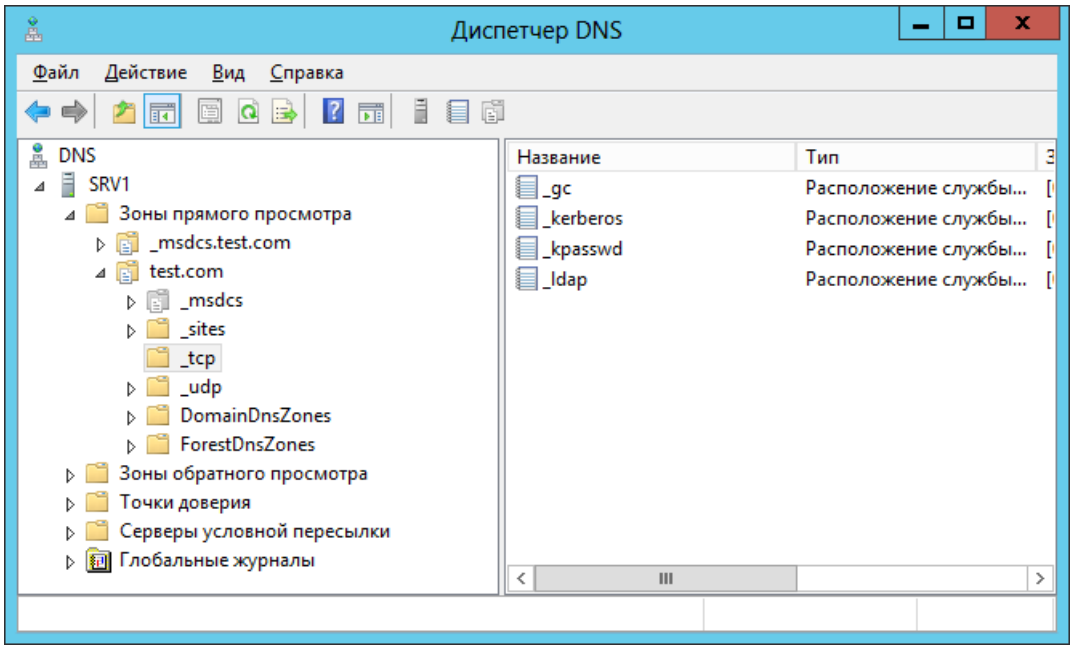



*Рис. 131 – Выбор протокола*

3. В верхней панели выберите **Действие -> Другие новые записи** (см. рис. 132).

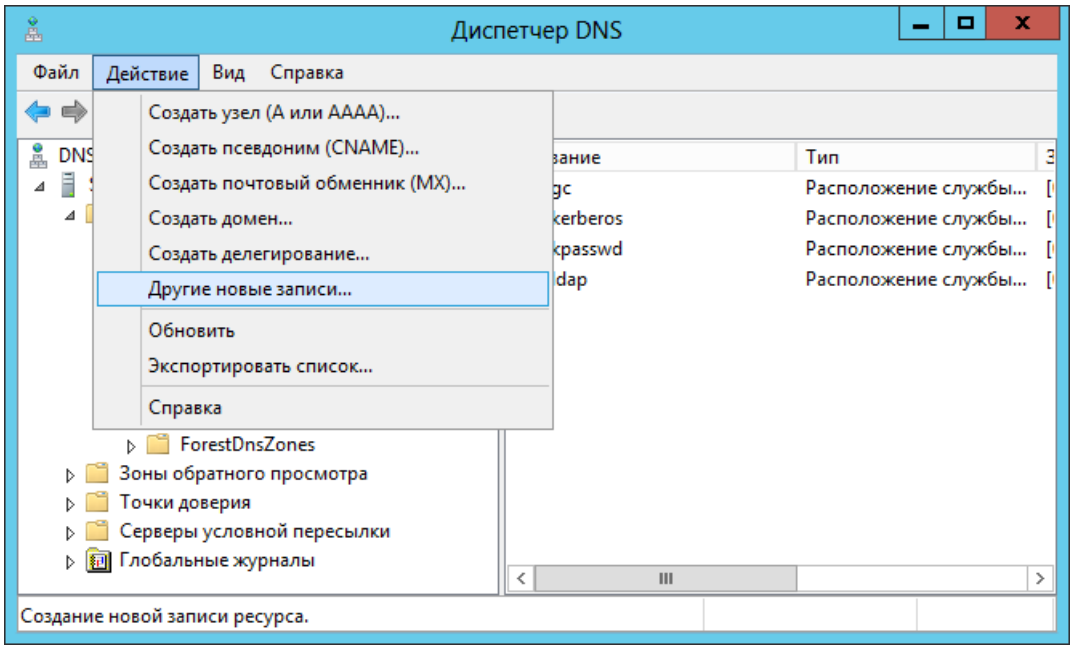



*Рис. 132 – Создание новой записи*

Отобразится следующее окно.

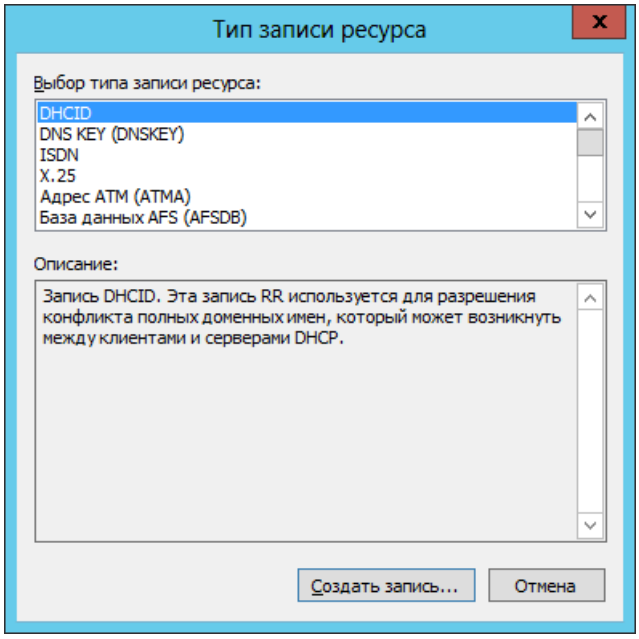



*Рис. 133 – Выбор типа записи ресурса*

4. В списке **Выбор типа записи ресурса** выберите **Расположение службы (SRV)** и нажмите **Создать запись**.

Отобразится следующее окно.

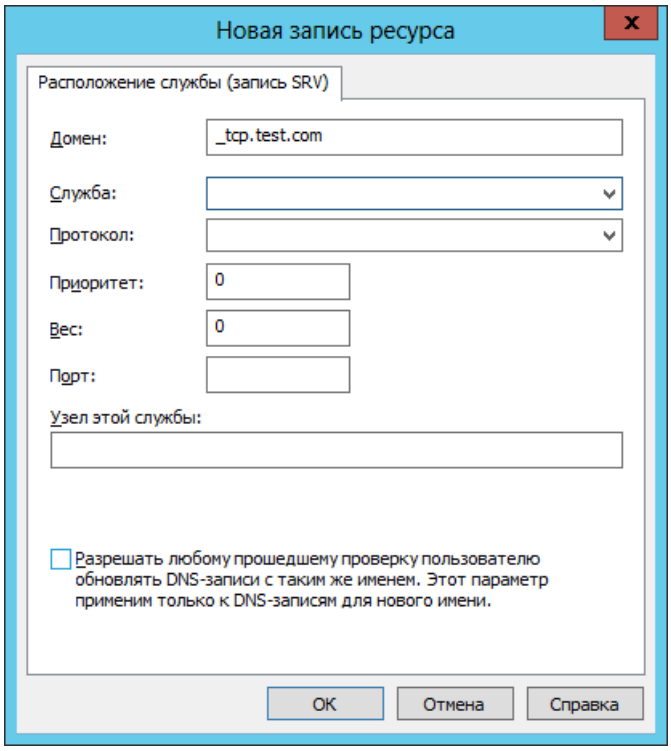



*Рис. 134 – Окно создания новой записи ресурса*

5. Выполните настройки в соответствии с табл. 15.

*Табл. 15 – Настройка записи ресурса*

| Параметр | Значение |
|---|---|
| **Служба** | • Для JMS Admin (консоль управления JMS):<br>– **_eap_server** – незащищенное соединение (по умолчанию)<br>ИЛИ<br>– **_eap_server_secure** – соединение, защищенное с помощью SSL.<br>• Для JMS Client (клиент JMS):<br>– **_eap_client** – незащищенное соединение (по умолчанию)<br>ИЛИ<br>– **_eap_client_secure** – соединение, защищенное с помощью SSL;<br>• **_eap_sts** – служба аутентификации JMS. |
| **Протокол** | В раскрывающемся списке выберите **_tcp** или введите это значение вручную, если в списке оно отсутствует. |
| **Приоритет** | Без изменений. |
| **Вес** | Без изменений. |
| **Порт** | Порт для соединения:<br>• **9010** - для JMS Admin (консоль управления JMS),<br>• **9009** - для JMS Client (клиент JMS);<br>• **9011** – для службы аутентификации JMS. |
| **Узел службы** | Укажите полное доменное имя (FQDN) сервера JMS, например: |

| Параметр | Значение |
|---|---|
| | **srv1.test.com.**<br>В случае развертывания кластера в данном поле следует указать полное доменное имя кластера JMS, например **JMS-Cluster.test.com.** Порядок создание DNS-записи кластера описан в руководстве по развертыванию кластерной конфигурации [6]. |
| **Разрешать любому прошедшему проверку пользователю обновлять DNS-записи с таким же именем.** | Без изменений. |

6. Нажмите **OK**.
7. В окне **Тип записи ресурса** нажмите **Готово**.
8. Двойным щелчком откройте окно свойств созданной записи ресурса – в отобразившемся окне перейдите на вкладку **Безопасность** и выставьте следующие разрешения (см. табл. 16).

*Табл. 16 – Разрешения для записей служб*

| Запись | Разрешения |
|---|---|
| **_eap_server/_eap_server_secure** | Для записи требуются права на чтение для всех пользователей, которые являются администраторами JMS (Для простоты администрирования можно добавить группу **Пользователи домена**). |
| **_eap_client/_eap_client_secure** | Для записи требуются права на чтение для всех рабочих станций, на которых будет использоваться клиент JMS (например, для предоставления права на чтения рабочим станциями домена следует добавить группу **Компьютеры домена**). |
| **_eap_sts** | Для записи требуются права на чтение для всех рабочих станций, на которых будет использоваться клиент JMS (например, для предоставления права на чтения рабочим станциями домена следует добавить группу **Компьютеры домена**). |

9. В окне свойств записи нажмите **OK**.
10. Повторите необходимые действия для оставшихся служб.

## 8.5 Разрешения, необходимые для работы клиентских приложений JMS

Поскольку служба DNS используется в качестве сетевого справочника при подключении клиентских приложений (т.е. клиентских агентов –приложение *Клиент JMS;* и административных консолей –приложение *Консоль управления JMS*), к серверу JMS, то доменным компьютерам, на которых эти клиентские приложения установлены, и доменным пользователям, от имени которых данные приложения запускаются, необходимо предоставить доступ к чтению справочников DNS.

Для удобства вы можете создать группу безопасности в Active Directory и добавить туда:
- все доменные компьютеры, на которых будут установлены клиентские приложения JMS;
- всех доменных пользователей, от имени которых будут запущены данные клиентские приложения.

После добавления доменного компьютера в группу безопасности рекомендуется его перезагрузить.

Для этого выполните следующие действия.

11. В оснастке **Диспетчер DNS** нажмите правой кнопкой мыши на сервере DNS и выберите **Свойства**.

12. Перейдите на вкладку **Безопасность** и установите:
    - для доменного компьютера, на котором установлено клиентское приложение (или группе, в которую он входит);
    - для доменного пользователя, от имени которого будет запускаться клиентское приложение (или группе, в которую он входит);

    разрешение на чтение.

**Примечание.** В случае использования внедоменных рабочих станций для доступа к JMS, таким компьютерам также необходимо предоставить доступ на чтение записей DNS.

## 8.6 Разрешения, необходимые для работы сервера/серверов JMS

Для корректной работы JMS необходимо установить для компьютеров, которые является серверами JMS, следующие разрешения (см. содержимое настоящего подраздела).

**Примечания:**

1. Для удобства вы можете создать группу безопасности в Active Directory и добавить туда все компьютеры, которые будут выполнять роль серверов JMS. После добавления сервера JMS в группу безопасности рекомендуется перезагрузить компьютер.
2. В случае если сервер JMS (служба сервера) запускается от имени учетной записи пользователя (а не системной учётной записи, см. Рис. 99, с. 89, раздел «Настройка служебной учетной записи»), разрешения, указанные в данном разделе, необходимо применить к данной учётной записи, а не к учётной записи доменного компьютера — сервера JMS.

### 8.6.1 Разрешения в центре сертификации Microsoft

13. В оснастке **Центр сертификации** выберите центр сертификации и выберите **Свойства**.
14. Перейдите на вкладку **Безопасность** и установите компьютеру, который является сервером JMS (или группе, в которую он входит), следующие разрешения:

- **Чтение**;
- **Выдача и управление сертификатами**;
- **Управлять ЦС**;
- **Запросить сертификаты**.

### 8.6.2 Разрешения в каталоге Active Directory

Воспользовавшись оснасткой **Active Directory – пользователи и компьютеры**, добавьте компьютер, который является сервером JMS (или группе, в которую он входит), в группу **Доступ DCOM службы сертификации**.

Это разрешение необходимо только при работе сервера в распределенной среде с несколькими доменами и экземплярами центра сертификации Microsoft.

### 8.6.3 Разрешения для принудительного входа по смарт-карте и открытия входа по паролю AD

Настоящий раздел описывает разрешения, необходимые для включения с помощью JMS опции принудительного входа по смарт-карте и для предоставления доступа в Active Directory по паролю. Соответствующие разрешения для сервера JMS (или для группы, в которую он входит) можно установить как в настройках безопасности учетной записи сервера или его группы, так и с помощью настроек делегирования:

- см. «Редактирование параметров безопасности в Active Directory» below;
- см. «Настройка параметров делегирования в Active Directory», с. 118.

### 8.6.3.1 Редактирование параметров безопасности в Active Directory

1. В оснастке Active Directory – пользователи и компьютеры откройте окно свойств сервера JMS (или группы, в которую он входит) и перейдите на вкладку **Безопасность**.

Если вкладка не отображается, в верхней панели оснастки **Active Directory – пользователи и компьютеры** выберите **Вид -> Дополнительные компоненты**.

2. На вкладке **Безопасность** щелкните на кнопке **Дополнительно**.
3. В отобразившемся окне щелкните на кнопке **Добавить**.
   Отобразится следующее окно.

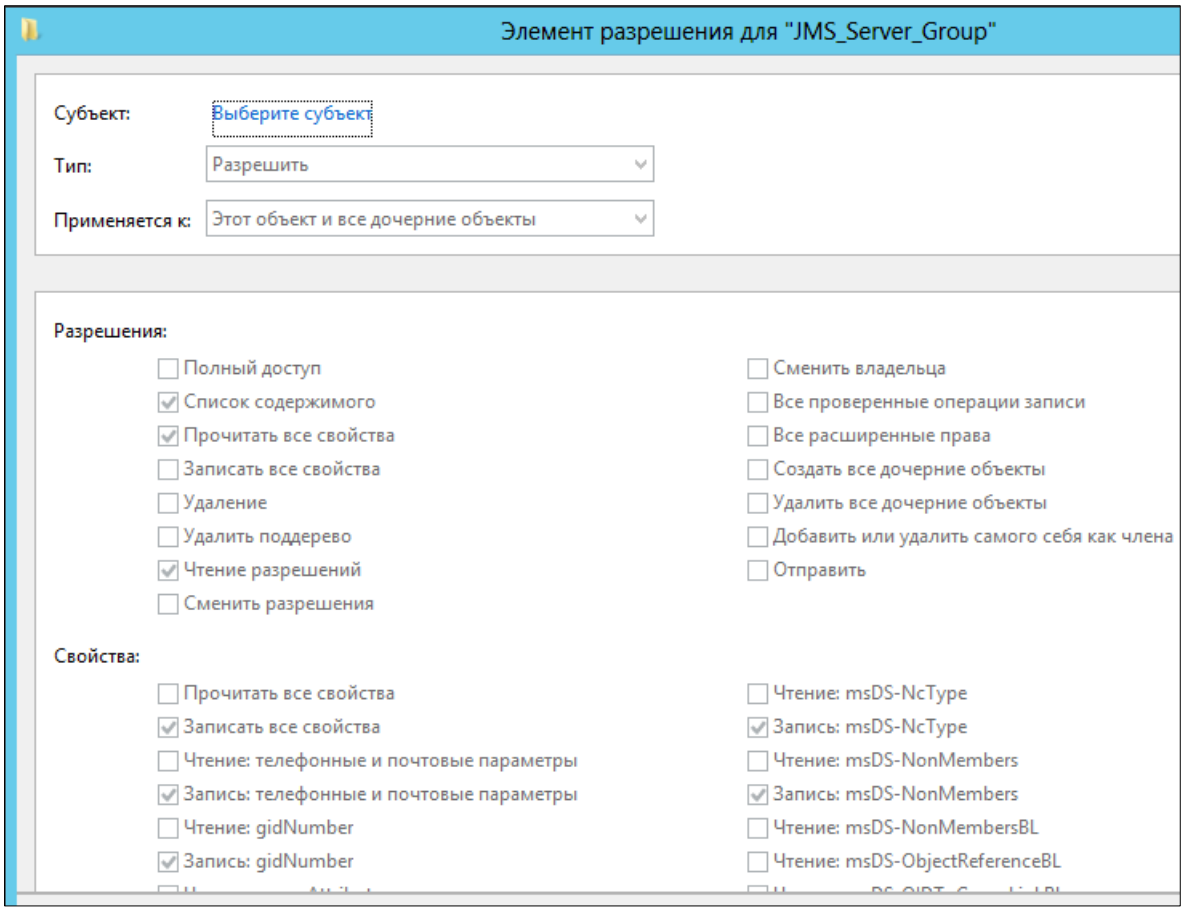



*Рис. 135 – Создание элемента разрешения*

4. Воспользуйтесь ссылкой **Выберите субъект** и выберите компьютер, который будет использоваться в качестве сервера JMS (или группу, в которую он входит).
5. В списке **Тип** оставьте выбранным пункт **Разрешить**.
6. В списке **Применяется к** выберите пункт **Дочерние объекты: Пользователь**.
7. В зависимости от необходимого типа разрешений, выполните действия, представленные в табл. 17.

*Табл. 17 – Необходимые разрешения*

| Тип разрешений | Разрешения |
|---|---|
| Установка принудительного входа по смарт-карте | В секции **Свойства** должен быть установлен флаг **Записать все свойства**. |

| Тип разрешений | Разрешения |
|---|---|
| Предоставление доступа в Active Directory по паролю | • В секции **Разрешения** должны быть установлены флаги:<br>– **Сброс пароля**;<br>– **Смена пароля**.<br>• В секции **Свойства** должен быть установлен флаг **Записать все свойства**. |

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

### 8.6.3.2 Настройка параметров делегирования в Active Directory

1. В оснастке **Active Directory – пользователи и компьютеры** щелкните правой кнопкой на домене или на контейнере с пользователями и выберите **Делегирование управления...**. Отобразится окно мастера делегирования управления.

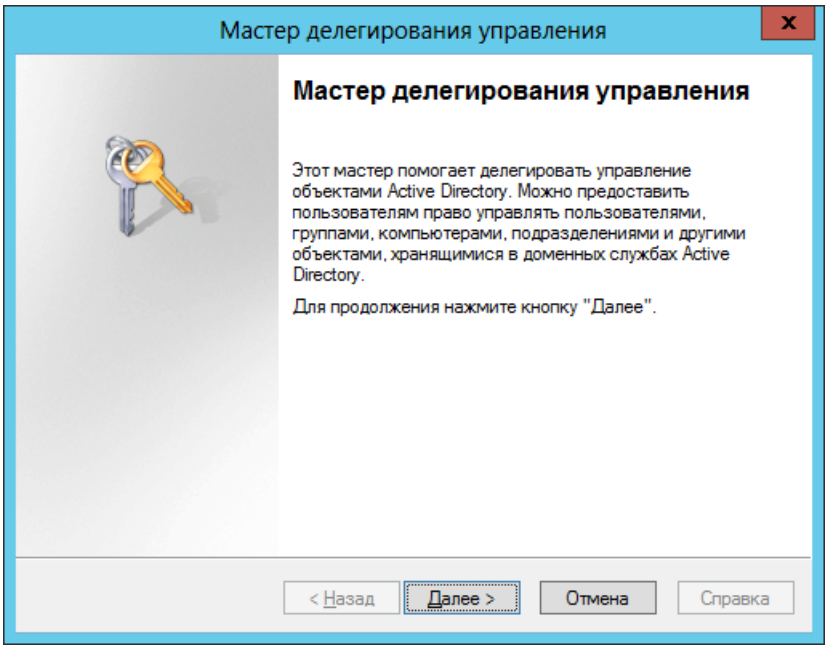



*Рис. 136 – Окно приветствия мастера делегирования управления*

2. Нажмите **Далее**.

Отобразится следующее окно.

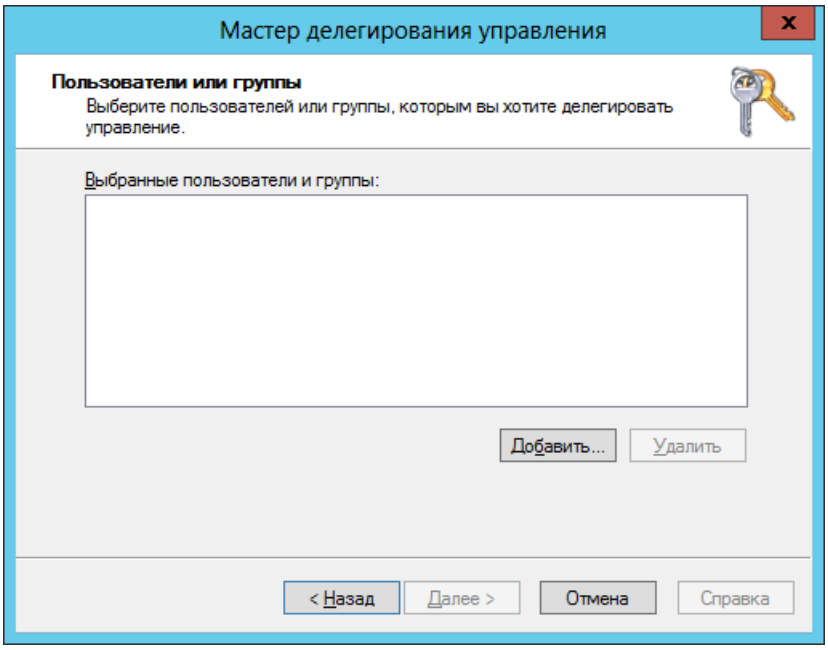



*Рис. 137 – Окно добавления учетной записи в настройку делегирования*

3. Воспользуйтесь кнопкой **Добавить**, чтобы добавить в настройку учетную запись компьютера, который будет использоваться в качестве сервера JMS (или группу, в которую он входит).
4. Нажмите **Далее**.
   Отобразится следующее окно.

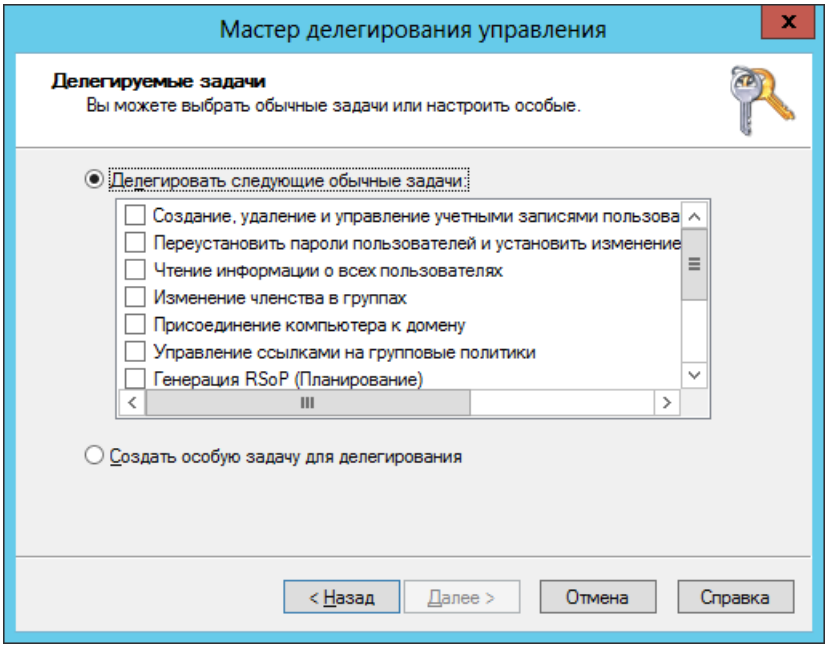



*Рис. 138 – Список делегируемых задач*

5. Выберите **Создать особую задачу для делегирования** и нажмите **Далее**.

Отобразится следующее окно.

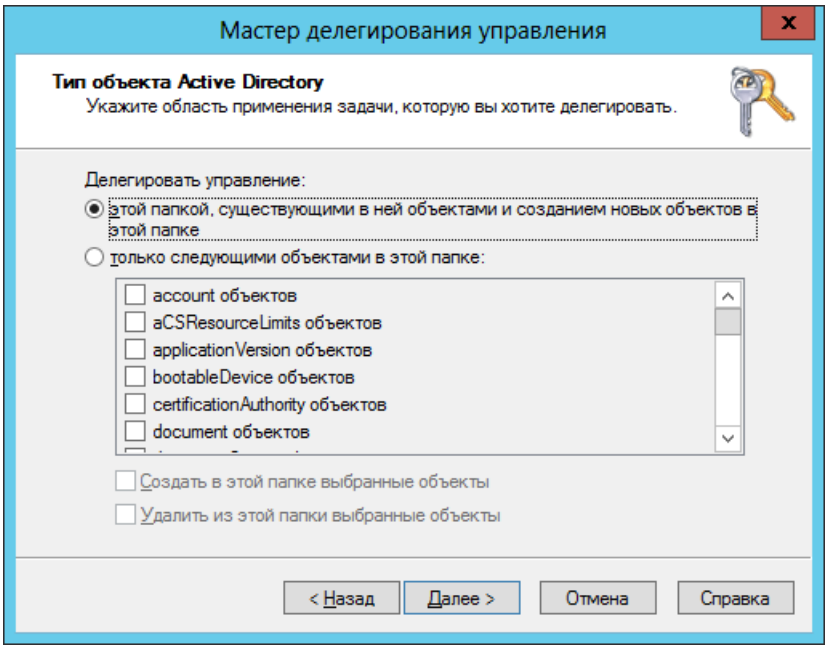



*Рис. 139 – Выбор типа объекта Active Directory*

6. Выполните следующие действия:

   – выберите пункт **только следующими объектами в этой папке**;
   – в списке ниже установите флаг напротив пункта **Пользователь объектов**;

7. нажмите **Далее**.
   Отобразится следующее окно.

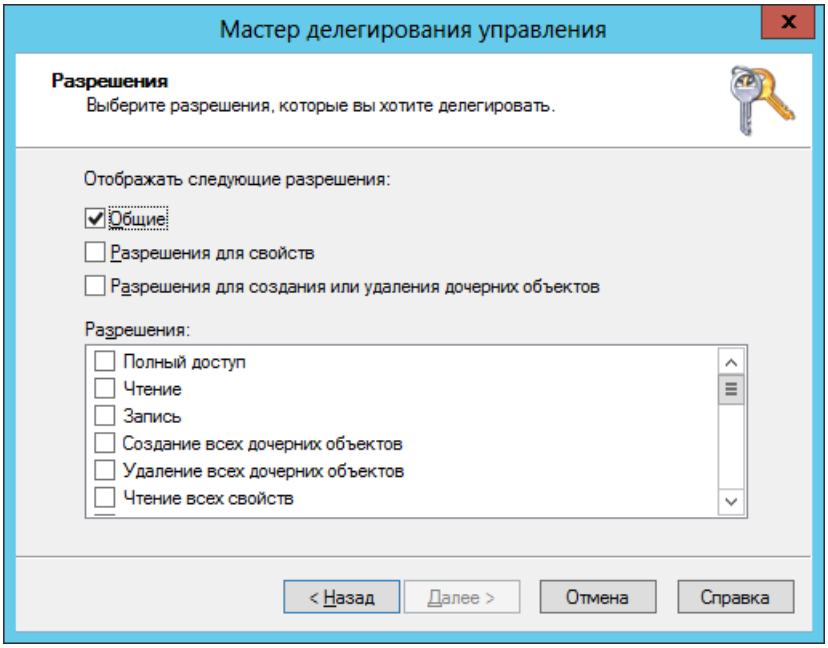



*Рис. 140 – Установка делегируемых разрешений*

8. В секции **Отображать следующие разрешения** установите флаг **Разрешения для свойств**.

9. В списке **Разрешения** установите флаги напротив пунктов (см. табл. 18).

*Табл. 18 – Необходимые разрешения*

| Требуемая возможность | Необходимые разрешения |
|---|---|
| Установка принудительного входа по смарт-карте | Должны быть установлены следующие флаги:<br>• **Чтение UserAccountControl**;<br>• **Запись UserAccountControl**. |
| Установка входа в Active Directory по паролю Windows | Должны быть установлены следующие флаги:<br>• **Смена пароля**;<br>• **Сброс пароля**. |

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

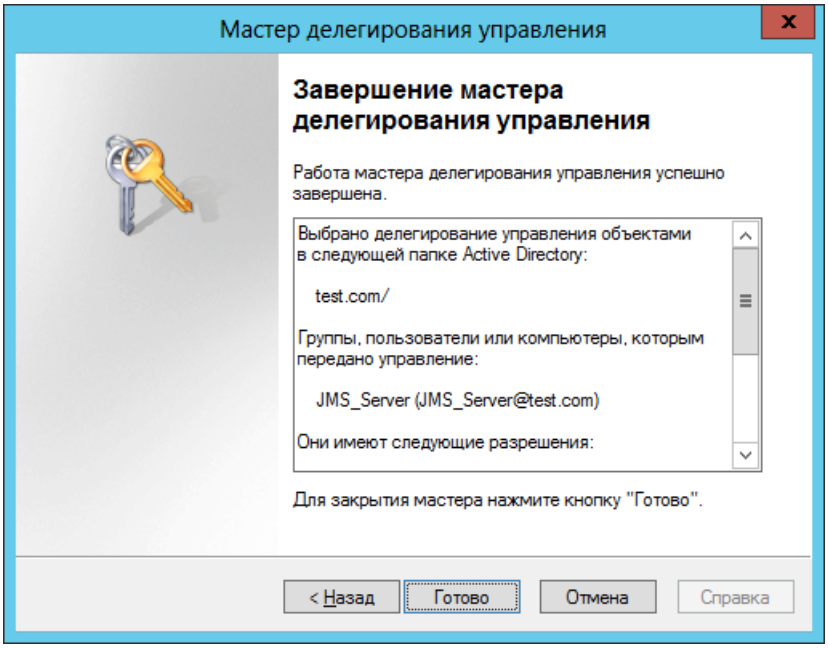



*Рис. 141 – Завершение мастера делегирования управления*

11. Нажмите **Готово**.

### 8.6.4 Разрешения в КриптоПро УЦ 2.0

Для использования в качестве КриптоПро УЦ 2.0 необходимы следующие минимальные права для оператора на стороне УЦ.

*Табл. 19 – Разрешения в КриптоПро УЦ 2.0*

| Тип действий | Разрешения |
|---|---|
| Чтение атрибутов | **Папки::Чтение свойств**.<br>Также убедитесь, что в свойствах папки на стороне УЦ установлен флаг **Настроить параметры по умолчанию учетных записей пользователей**. Это необходимо для чтения атрибутов пользователей. |
| Управление жизненным циклом сертификатов через КриптоПро УЦ 2.0. | • Для регистрации пользователей, **дополнительно - Пользователи::Чтение свойств**;<br>• для создания и редактирования профилей дополнительных прав не нужно;<br>• для выпуска электронных ключей с сертификатами УЦ, **дополнительно - Пользователи::Запрос Регистрации**, **::Одобрение регистрации**, **::Запрос** |

| Тип действий | Разрешения |
|---|---|
| | **переименования**, **::Одобрение переименования**, **::Запрос сертификата**, **::Одобрение сертификата**, **Шаблоны::Запрос сертификата**, **::Одобрение сертификата**;<br>• для синхронизации, замены и отзыва сертификатов, **дополнительно - Пользователи::Запрос аннулирования**, **::Одобрение аннулирования**;<br>• для отключения/включения сертификатов, **дополнительно - Пользователи::Запрос приостановления**, **::Одобрение приостановления**, **::Запрос возобновления**, **::Одобрение возобновления**. |

## 8.7 Подготовка к использованию протоколов SSL/TLS

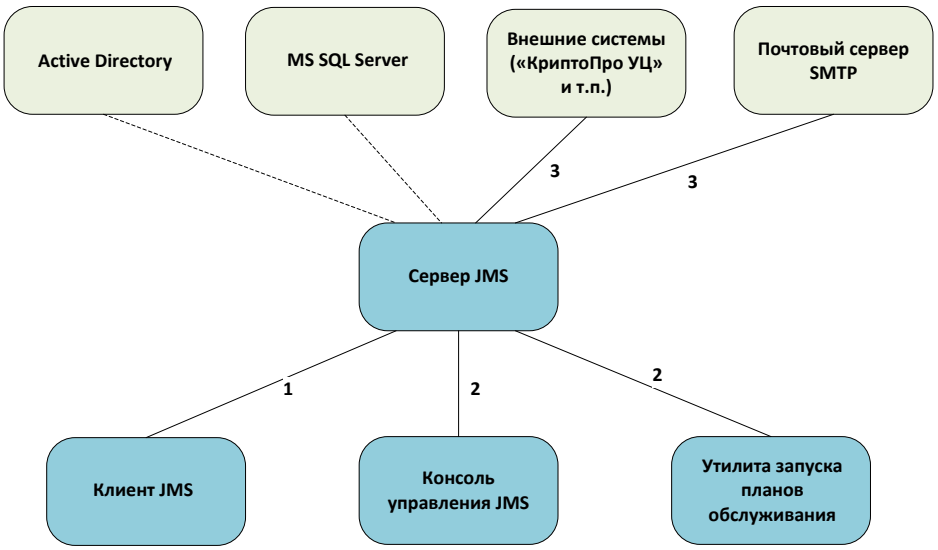
В JMS реализована поддержка следующих версий протоколов защиты транспортного уровня:

- SSL 3.0;
- TLS 1.0;
- TLS 1.1;
- TLS 1.2.

По умолчанию в JMS включена поддержка всех указанных версий протоколов (разделе «Настройки использования SSL/TLS» с. 191). Техническая возможность использования того или иного протокола и его автоматический выбор будет зависеть от следующих параметров:

- настройка операционной системы Windows;
- версия установленного пакета .NET Framework;
- настройки протоколов защиты транспортного уровня в компонентах JMS (сервер, клиент, административная консоль).

Таким образом, для обеспечения поддержки этих протоколов необходимо выполнить ряд настроек как на стороне сервера JMS, так и на другой стороне соединения (Рис. 142).




Настройками протоколов можно управлять на уровне операционной системы

Настройками протоколов можно управлять при помощи прикладных параметров JMS

Для поддержки TLS 1.1 и 1.2 необходимо установить .NET Framework 4.5 и выше (рекомендуется 4.7)

Для поддержки TLS 1.1 и 1.2 может потребоваться установка дополнительных обновлений – SP, КриптоПро CSP 4.0 и т.п.

**1** – Настройка через реестр клиента JMS, раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Client\Default\TransportManager`

**2** – Настройка через реестр консоли управления JMS, раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\EAP Administrative Client\Settings`

**3** – Настройка в серверном агенте JMS, на вкладке **Безопасность**

*Рис. 142 – Схема настроек SSL/TLS на сторонах – участниках защищенного соединения*

Настройка поддержки протоколов на сервере JMS описана в разделе «Настройки использования SSL/TLS» с. 191.

### 8.7.1 Настройка SSL/TLS в операционной системе

Операционная система Windows на целевой машине (сервере или клиенте JMS, внешней системе, почтовом сервере, сервере СУБД и т.д.) должна поддерживать требуемый протокол SSL/TLS. Настройки протоколов задаются в разделе реестра

**`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`**

Для настройки протоколов SSL/TLS в операционной системе обратитесь к ее документации.

После редактирования реестра с целью настройки SSL/TLS необходимо перезагрузить операционную систему.

### 8.7.2 Требование к версиям .NET Framework

Различные версии платформы .NET Framework поддерживают различные версии протоколов SSL и TLS. Для включения поддержки TLS 1.2 (наиболее защищенного протокола) рекомендуется установить обновление .NET Framework версии 4.6 или более поздней на сервере JMS и остальных взаимодействующих с ним по TLS компонентах.

*Табл. 20 – Поддержка SSL/TLS в .NET и дополнительные настройки для JMS*

| Версия .NET | Перечень поддерживаемых протоколов | Протоколы по умолчанию | Как включить поддержку TLS 1.2 |
|---|---|---|---|
| .NET 4.0 | SSL 3.0, TLS 1.0 | SSL 3.0 или TLS 1.0 | Не поддерживается |
| .NET 4.5 | SSL 3.0, TLS 1.0, TLS 1.1,<br>TLS 1.2 | SSL 3.0 или TLS 1.0 | Явно задать настройку в JMS или включить в реестре:<br>**[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]**<br>**"SchUseStrongCrypto"=dword:00000001**<br>**[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319]**<br>**"SchUseStrongCrypto"=dword:00000001** |
| .NET 4.6 и выше | SSL 3.0, TLS 1.0, TLS 1.1,<br>TLS 1.2 | TLS 1.2 | Включен по умолчанию в JMS |

### 8.7.3 Настройка SSL/TLS на стороне клиента JMS

Для настройки протоколов SSL/TLS на компьютере с клиентом JMS в разделе реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Client\Default\TransportManager** создайте или отредактируйте параметр

**SecurityProtocol=Ssl3, Tls, Tls11, Tls12**

Разрешается указывать один или несколько протоколов.

Значение по умолчанию – **All** (разрешены все протоколы).

**Важно!** После редактирования реестра, связанного с настройкой SSL/TLS, следует перезапустить службу клиента JMS и клиентский агент (приложение Клиент JMS).

Процедура настройки защищенного по SSL/TLS соединения на стороне сервера JMS описана в разделе «Настройка SSL-соединения на стороне сервера JMS», с. 126.

Ручная настройка компонента JMS Client для поддержки SSL/TLS описана в разделе «Настройка соединения JMS Client с сервером JMS», с. 134.

Централизованная настройка клиентов JMS для поддержки SSL/TLS описана в разделе «Централизованная настройка подключения к серверу JMS», с. 111.

### 8.7.4 Настройка SSL/TLS на стороне консоли управления JMS

Для настройки протоколов SSL/TLS на компьютере с консолью управления JMS в разделе реестра **HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\EAP Administrative Client\Settings**

создайте или отредактируйте параметр **SecurityProtocol=Ssl3, Tls, Tls11, Tls12**

Разрешается указать один или несколько протоколов.

Значение по умолчанию – **All** (разрешены все протоколы).

Данная настройка действует также на утилиту запуска планов обслуживания системе (см. «Руководство администратора. Часть 2» [3], раздел «Запуск планов обслуживания с помощью утилиты MaintenancePlanRunner»).

Процедура настройки защищенного по SSL/TLS соединения на стороне сервера JMS описана в разделе «Настройка SSL-соединения на стороне сервера JMS», с. 126.

Ручная настройка конфигурационного файла консоли управления JMS для поддержки SSL/TLS описана в разделе «Настройка соединения JMS Admin с сервером JMS», с. 129.

Для централизованной настройки защищенного по SSL/TLS подключения к серверу JMS из консоли управления JMS необходимо выполнить также действия, описанные в разделе «Централизованная настройка подключения к серверу JMS», с. 111.

### 8.7.5 Настройка SSL/TLS для работы с Microsoft SQL Server

При использовании шифрованного подключения к базе данных из JMS также может потребовать гибкая настройка протоколов защиты транспортного уровня. Версии MS SQL Server 2008 и выше по умолчанию поддерживают протоколы SSL 3.0, TLS 1.0 и TLS 1.1. Для включения поддержки TLS 1.2 может потребоваться установка соответствующего обновления для сервера БД:

https://support.microsoft.com/ru-ru/help/3135244/tls-1-2-support-for-microsoft-sql-server

Из-за особенностей реализации SQL Server Native Client невозможно программно установить версию используемого протокола, используемую сервером JMS при подключении к базе данных. Поэтому следует руководствоваться следующими рекомендациями по включению TLS 1.2:

*Табл. 21 – Рекомендации по настройке TLS 1.2 для Microsoft SQL Server*

| Версия .NET | Протоколы по умолчанию | Как включить поддержку TLS 1.2 |
|---|---|---|
| .NET 4.5 | SSL 3.0 или TLS 1.0 | Заблокировать на уровне Windows старые протоколы SSL 3.0 и TLS 1.0. Явно включить только TLS 1.2 |
| .NET 4.6 и выше | TLS 1.2 | Не требуется дополнительных действий – протокол TLS 1.2 используется по умолчанию |

Дополнительная информация по использованию TLS 1.2 совместно с Microsoft SQL Server: https://blogs.msdn.microsoft.com/sqlreleaseservices/tls-1-2-support-for-sql-server-2008-2008-r2-2012-and-2014/

Порядок подготовки самого сервера SQL к защищенному соединению по SSL описан в разделе «Подготовка сервера MS SQL для работы по SSL/TLS», с. 55.

Для получения дополнительной информации, необходимой при подготовке SQL-сервера к работе по протоколу SSL, см. соответствующие описания на сайте Microsoft:

- https://technet.microsoft.com/ru-ru/library/ms189067(v=sql.105).aspx;
- https://msdn.microsoft.com/ru-ru/library/bb879935(v=sql.110).aspx.

### 8.7.6 Настройка SSL/TLS для работы с КриптоПро УЦ 2.0

Версии КриптоПро CSP 3.6/3.9 работают исключительно с TLS 1.0.

Для включения TLS 1.1 или 1.2 необходимо как на УЦ (КриптоПро УЦ 2.0), так и на сервере JMS установить CSP 4.0 или более позднюю версию.

Также на сервере с КриптоПро УЦ 2.0 необходимо проверить поддержку TLS 1.2 на уровне операционной системы.

## 8.8 Настройка SSL-соединения на стороне сервера JMS

Настойки SSL-соединения на стороне сервера JMS выполняются на вкладке **Безопасность** приложения Сервер JMS (серверный агент) в секции **Настройки использования SSL/TLS** (подробнее см. раздел «Настройки использования SSL/TLS», с. 191)

**Примечание.** В случае настройки SSL-соединения на стороне сервера JMS в кластерной конфигурации, прежде чем приступить к стандартной, как указано выше, процедуре, следует вручную изменить в реестре адреса (параметр **Address**) интерфейсов **IntegrationManager** и **ClientManager**, указав в них FQDN-имя кластера. Подробнее см. руководство по кластеру JMS [6] , раздел «Настройка SSL/TLS на стороне узла кластера JMS».

## 8.9 Установка и первоначальная настройка компонента JMS Admin

### 8.9.1 Установка JMS Admin

Чтобы установить компонент JMS Admin, выполните следующие действия.

1. В зависимости от разрядности операционной системы запустите один из следующих файлов.

   – 32-бит: Aladdin.JMS.Admin-x.x.x.xxxx-x86.msi;
   – 64-бит: Aladdin.JMS.Admin-x.x.x.xxxx-x64.msi.

   Отобразится следующее окно.

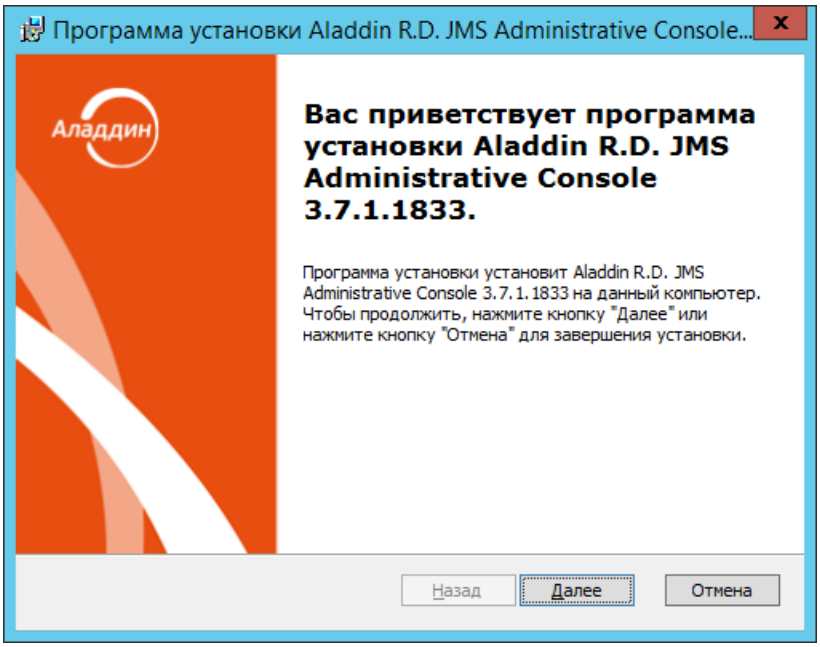



*Рис. 143 – Окно приветствия мастера установки компонента JMS Admin*

2. Нажмите **Далее**.

Отобразится следующее окно.

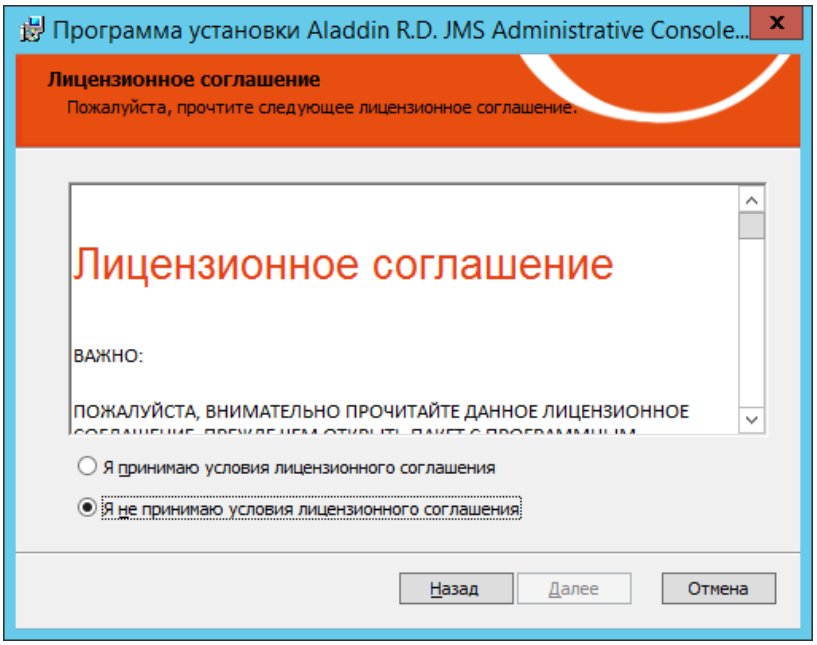



*Рис. 144 – Окно лицензионного соглашения*

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

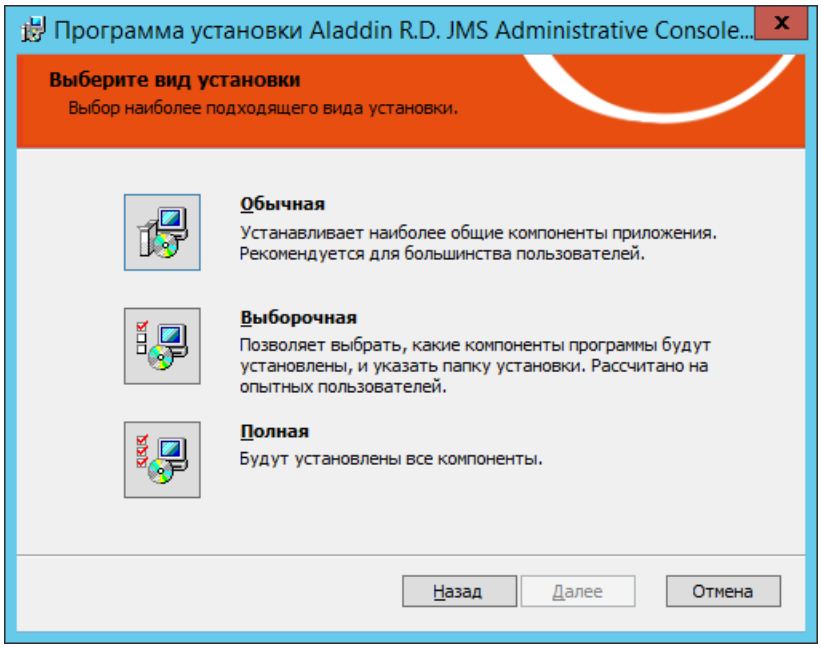



*Рис. 145 – Окно выбора варианта установки*

4. Щелкните на пункте **Полная**.

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

Отобразится следующее окно.

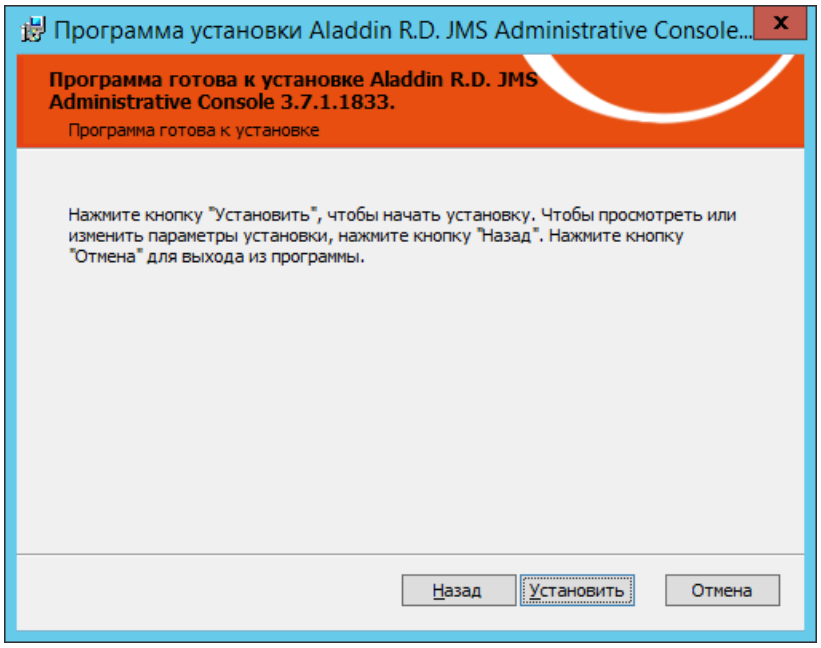



*Рис. 146 – Окно готовности к установке*

5. Нажмите **Установить**.
   По завершении установки отобразится следующее окно.

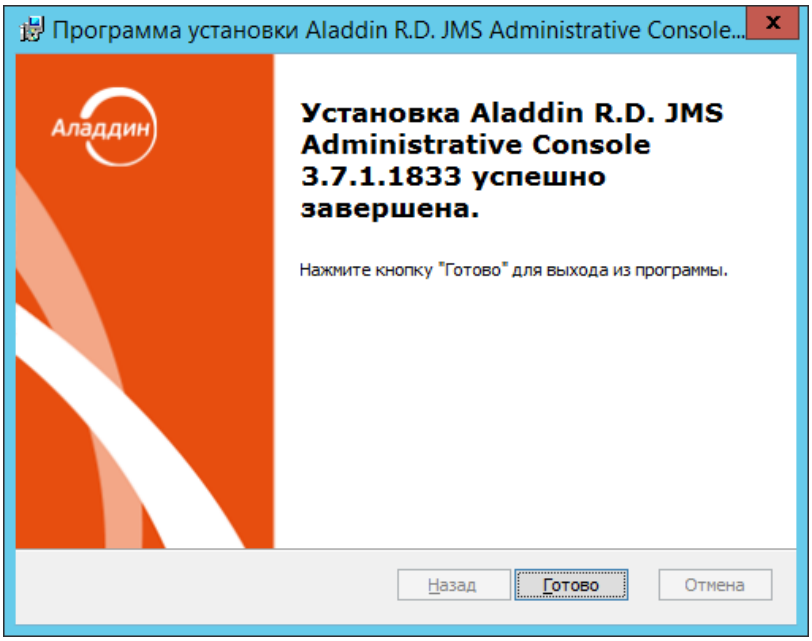



*Рис. 147 – Окно завершения установки*

6. Нажмите **Готово** для завершения процедуры.

### 8.9.2 Настройка соединения JMS Admin с сервером JMS

Существуют следующие варианты настройки соединения JMS Admin с сервером JMS (см. табл. 22).

*Табл. 22 – Варианты настройки подключения JMS Admin к серверу JMS*

| Способ настройки соединения с сервером JMS | Описание |
|---|---|
| Централизованная настройка подключения к серверу JMS | Если была выполнена процедура, представленная в подразделе «Централизованная настройка подключения к серверу JMS», с. 111, дальнейшая настройка не требуется (в том числе в случае поддержки защиты соединения с помощью SSL). |
| Ручная настройка подключения к серверу JMS | Ручную настройку обычного подключения следует выполнять в том случае, если не используется централизованная настройка подключения к серверу JMS или по каким-то причинам после выполнения централизованной настройки подключение не работает.<br><br>Чтобы вручную настроить подключение к серверу JMS, в файле конфигурации **Aladdin.EAP.Admin.UI.exe.config** (по умолчанию он устанавливается в следующий каталог: **C:\Program Files\EAP Administrative Client**) измените значение параметра **ServerUrl** на одно из следующих:<br>• **http://<Сервер_JMS>:9010/EAPEngine/Default/IntegrationManager** - обычное подключение к серверу JMS (без SSL);<br>• **https://<Сервер_JMS>:9010/EAPEngine/Default/IntegrationManager** - подключение к серверу JMS с поддержкой SSL.<br>Где **<Сервер_JMS>** - полное имя сервера JMS, включая имя домена и имя компьютера, например: **srv1.test.com**.<br><br>Кроме того, для отключения поиска сервера JMS по DNS (во избежание конфликтов) в том же конфигурационном файле отредактируйте значение параметра UseDNSSearch, присвоив ему значение false:<br>`<add key="UseDNSSearch" value="false"/>` |

### 8.9.3 Первый запуск Консоли управления JMS

При первом запуске компонента JMS Admin (консоли управления JMS) следует зарегистрировать электронный ключ (ЭК), при помощи которого пользователь с ролью *Администратор информационной безопасности* (Администратор ИБ) будет выполнять аутентификацию в JMS.

**Важно!** При утере такого ЭК запуск консоли управления в будущем будет невозможен.

Для регистрации *электронного ключа Администратора ИБ* при первом запуске консоли управления выполните следующие действия.

1. Подключите ЭК, предназначенный для Администратора ИБ, к компьютеру с консолью управления JMS.
2. Запустите на выполнение консоль управления JMS. Для этого в меню **Пуск** выберите **JaCarta Management System** -> **Консоль управления JMS**.

Отобразится окно следующего вида.

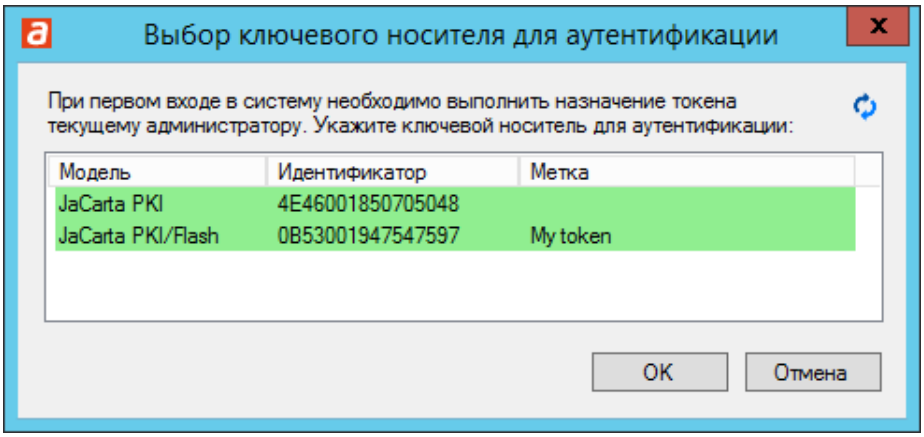



*Рис. 148 – Окно выбора ЭК Администратора ИБ*

3. Выберите в меню ЭК, который будет назначен Администратору ИБ, и нажмите **OK**. Отобразится окно следующего вида.

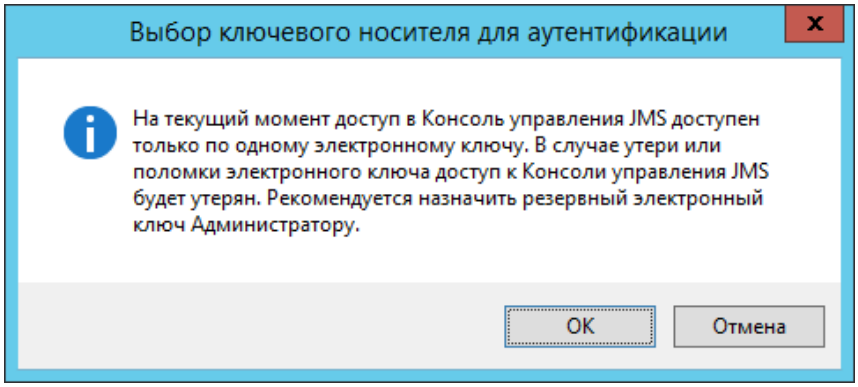



*Рис. 149 – Уведомление о необходимости создании резервного ЭК Администратора ИБ*

4. Нажмите **OK**. Отобразится окно запроса PIN-кода пользователя для выбранного ЭК.

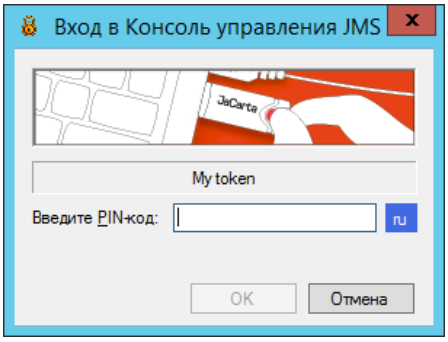



*Рис. 150 – Окно ввода PIN-кода пользователя*

5. Введите PIN-код и нажмите **OK**.

Отобразится окно консоли управления JMS.

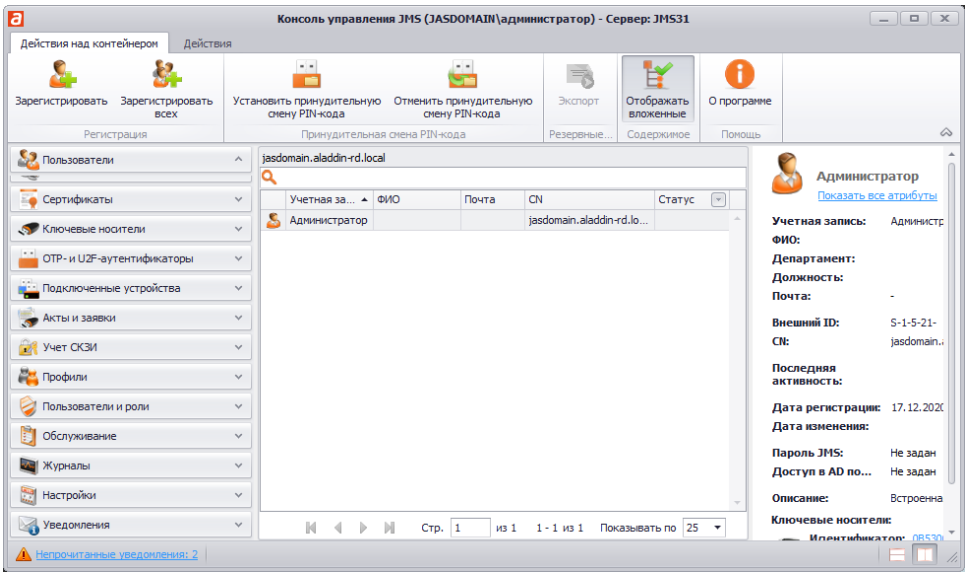



*Рис. 151 – Окно консоли управления JMS*

Установка ЭК *Администратора ИБ* закончена.

В дальнейшем для запуска консоли управления JMS используйте зарегистрированный ЭК.

Для создания электронных ключей для аутентификации других пользователей JMS, роли которых имеют полномочия доступа к консоли управления JMS, следует назначить данным пользователям соответствующие ЭК (подробнее см. Руководство администратора, Часть.2 [3]).

Аналогичным образом выполняется создание резервных ключей для аутентификации пользователей в JMS.

В дальнейшем при каждом новом открытии консоли управления JMS для аутентификации администратора ИБ (или пользователя с другой ролью) необходимо будет использовать соответствующий электронный ключ и предъявить его PIN-код пользователя (Рис. 150)

### 8.9.4 Конфигурационный файл приложения JMS Admin (Консоли управления JMS)

Конфигурационный файл `Aladdin.EAP.Admin.UI.exe.config` приложения JMS Admin по умолчанию располагается в папке `C:\Program Files\EAP Administrative Client\`

## 8.10 Установка и первоначальная настройка компонента JMS Client

### 8.10.1 Установка JMS Client

Чтобы установить компонент JMS Client, выполните следующие действия.

1. В зависимости от разрядности операционной системы запустите один из следующих файлов.

   – 32-бит: Aladdin.JMS.Client.STS-x.x.x.xxxx-x86.msi;
   – 64-бит: Aladdin.JMS.Client.STS-x.x.x.xxxx-x64.msi.

Отобразится следующее окно.

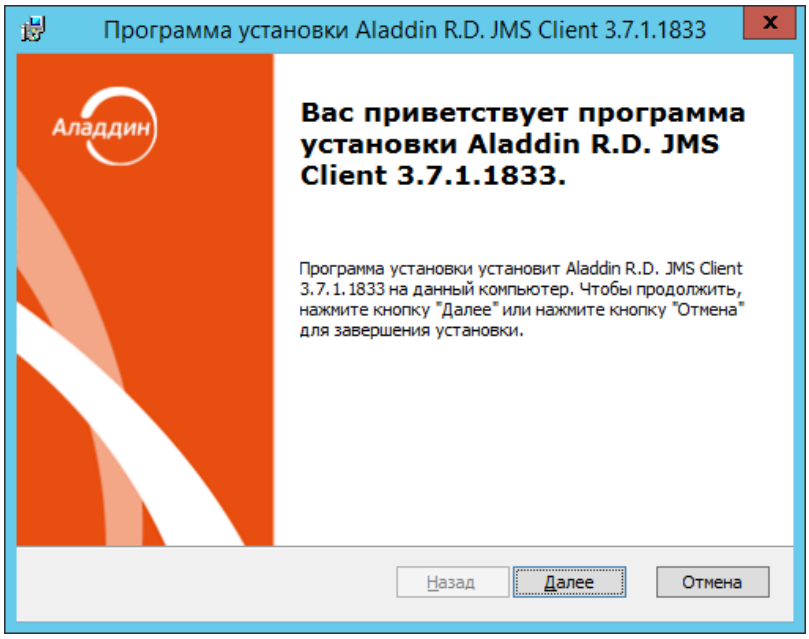



*Рис. 152 – Окно приветствия мастера установки JMS Client*

2. Нажмите **Далее**.
   Отобразится следующее окно.

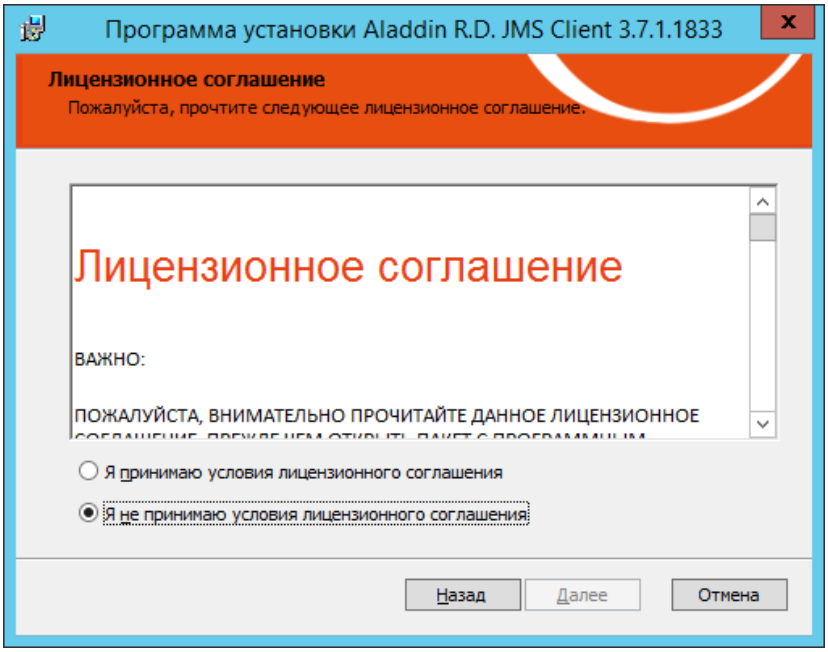



*Рис. 153 – Окно лицензионного соглашения*

3. Выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.

Отобразится следующее окно.

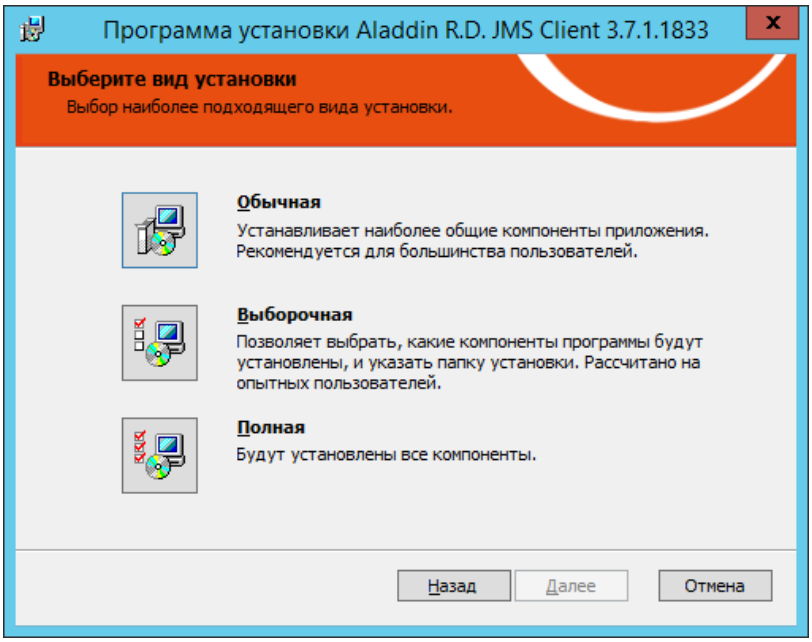



*Рис. 154 – Окно выбора варианта установки.*

4. Щелкните на пункте **Полная**.

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

Отобразится следующее окно.

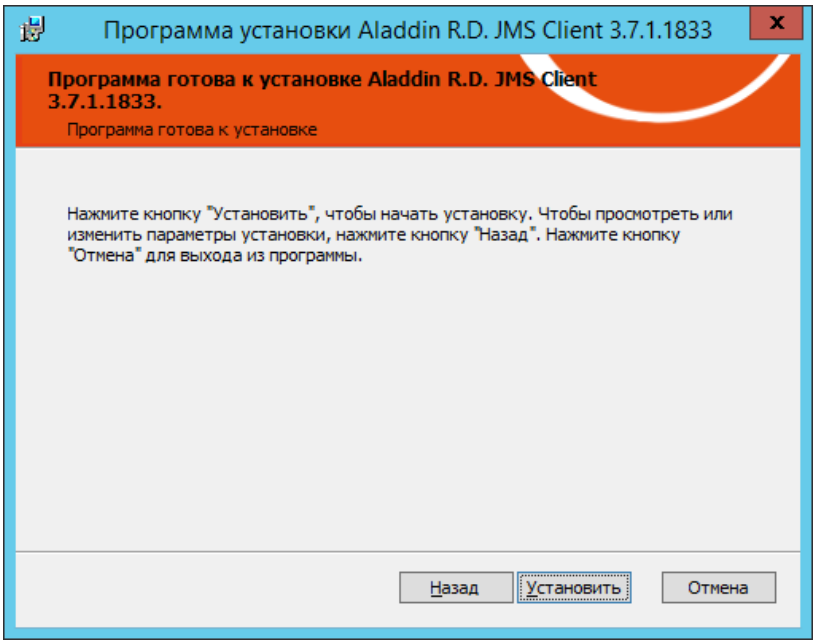



*Рис. 155 – Окно готовности к установке*

5. Нажмите **Установить**.

По завершении установки отобразится следующее окно.

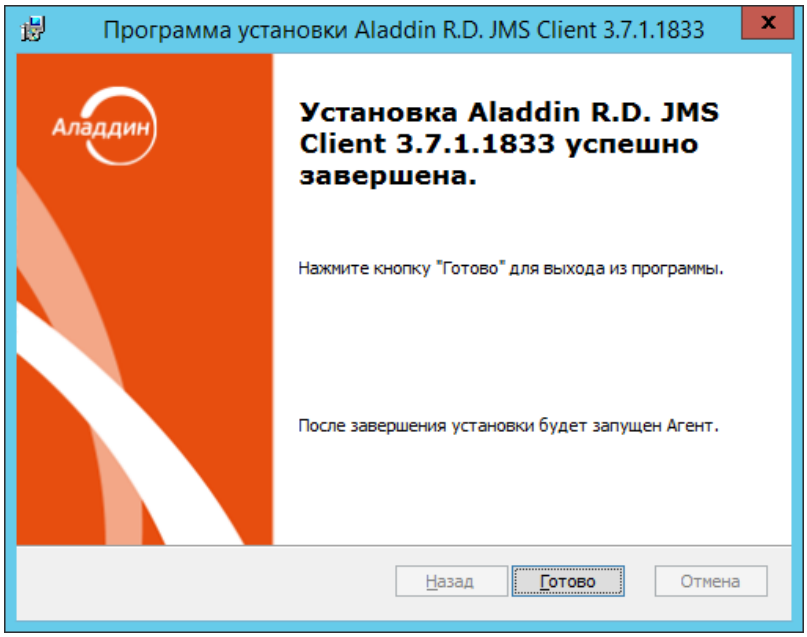



*Рис. 156 – Окно завершения установки*

6. Нажмите **Готово** для завершения процедуры.
   Меню быстрого запуска JMS Client будет отображаться в области уведомлений в виде значка (Клиент JMS).

### 8.10.2 Настройка соединения JMS Client с сервером JMS

Существуют следующие варианты настройки соединения JMS Client с сервером JMS (см. табл. 23).

*Табл. 23 – Варианты настройки подключения JMS Client к серверу JMS*

| Способ подключения | Описание |
|---|---|
| Централизованная настройка подключения к серверу JMS (т.е. использование DNS для адресации к серверу JMS) | В случае централизованной настройки подключния к серверу JMS следует выполнить процедуру, представленную в подразделе «Централизованная настройка подключения к серверу JMS», с. 111.<br><br>Кроме этого, в случае если клиент JMS установлен на внедоменной рабочей станции системе (см. «Руководство администратора. Часть 2» [3], раздел «Внедоменные рабочие станции»), в ее реестре следует выполнить следующие настройки:<br><br>1. В редакторе реестра перейдите в раздел **HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Client\Default\TransportManager**<br><br>(если такой раздел отсутствует, создайте его).<br><br>2. В случае если в данном разделе реестра уже определен строковый параметр **UseDNSSearch,** присвойте ему значение **true** (*true* является значением по умолчанию).<br><br>3. Создайте строковый параметр **DnsName** и присвойте ему имя домена, в котором были созданы записи ресурсов (в примере из раздела «Централизованная настройка подключения к серверу JMS», с. 111, – это домен **test.com**).<br><br>4. В области уведомлений щелкните правой кнопкой на значке и выберите **Выход**.<br><br>5. Перезапустите службу **Aladdin EAP Client - default**. |

| Способ подключения | Описание |
|---|---|
| Ручная настройка подключения к серверу JMS | Ручную настройку обычного подключения следует выполнять в том случае, если не используется централизованная настройка подключения к серверу JMS или по каким-то причинам после выполнения централизованной настройки подключение не работает.<br><br>Чтобы вручную настроить подключение к серверу JMS, выполните следующие действия.<br><br>1. В редакторе реестра перейдите в раздел **HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Client\Default\TransportManager**<br><br>(если такой раздел отсутствует, создайте его).<br><br>2. Для соединения со службой аутентификации JMS создайте строковый параметр **StsAddress** и присвойте ему следующее значение:<br><br>**http://<Сервер_JMS>:9011/EAPEngine/Default/STS**<br><br>Здесь и далее **<Сервер_JMS>** - полное доменное имя (FQDN) сервера JMS, например: **srv1.test.com**.<br><br>3. Для соединения с серверной службой создайте строковый параметр **ServerAddress** и в зависимости от типа соединения присвойте ему одно из следующих значений:<br>– **http://<Сервер_JMS>:9009/EAPEngine/Default/ClientManager** - для обычного соединения с сервером JMS (без поддержки SSL);<br>– **https://<Сервер_JMS>:9009/EAPEngine/Default/ClientManager** - для соединения с сервером JMS с поддержкой SSL.<br><br>4. Для отключение поиска по DNS (во избежание конфликтов) создайте строковый параметр **UseDNSSearch** и присвойте ему значение **false** (ложь).<br><br>5. В области уведомлений щелкните правой кнопкой на значке и выберите **Выход**.<br><br>6. Перезапустите службу **Aladdin EAP Client - default**. |

### 8.10.3 Настройка проверки сертификата службы аутентификации JMS для внедоменной рабочей станции

Настройка проверки сертификата службы аутентификации JMS состоит из нескольких этапов.

1. См. «Настройка преобразования имен серверов» ниже.
2. См. «Загрузка и установка сертификата центра сертификации Microsoft», с. 136.
3. См. «Непосредственная настройка проверки сертификата службы аутентификации JMS», с. 138.

#### 8.10.3.1 Настройка преобразования имен серверов

Чтобы настроить преобразования имен серверов, выполните действия, представленные в табл. 24.

*Табл. 24 – Варианты настройки преобразования имен серверов*

| Вариант настройки | Описание |
|---|---|
| Настройка DNS | См. «Централизованная настройка подключения к серверу JMS», с. 111 и «Настройка соединения JMS Client с сервером JMS», с. 134.<br><br>**Примечания:**<br>1. Настройка DNS выполняется единожды (для каждого DNS-сервера, в случае если их несколько) для всех внедоменных рабочих станций.<br>2. В случае централизованной настройки подключения к серверу JMS (т.е. использования службы DNS) для корректной работы службы аутентификации JMS на внедоменных рабочих станциях этим станциям следует предоставить право на чтение записей *_eap_client/_eap_client_secure* и *_eap_sts* и в службе DNS (см. раздел «Централизованная настройка подключения к серверу JMS», с. 111). |

| Вариант настройки | Описание |
|---|---|
| Редактирование файла **hosts** | На рабочей станции, где установлен компонент JMS Client, добавьте в файл **hosts** IP-адреса и полные доменные имена (FQDN):<br>• сервера JMS;<br>• центра сертификации Microsoft, который выдавал сертификат для службы аутентификации JMS.<br>Например.<br>**192.168.200.100 JMSServer.test.com**<br>**192.168.200.105 MSCA.test.com** |

### 8.10.3.2 Загрузка и установка сертификата центра сертификации Microsoft

Действия, приведенные в этом пункте, необходимо выполнять для компьютеров с установленным компонентом JMS Client, которые при этом не входят в домен, в котором развернута система JMS.

1. С компьютера, на котором установлен компонент JMS Client, с помощью браузера зайдите на сайт центра сертификации: **http://<Сервер_ЦС>/certsrv** (где **<Сервер_ЦС>** - полное имя компьютера, на котором установлен центр сертификации Microsoft, включая имя компьютера и домен, например, **srv1.test.com**).
2. При необходимости введите учетные данные для доступа к сайту и нажмите **OK**. Отобразится страница центра сертификации Microsoft (см. рис. 157)

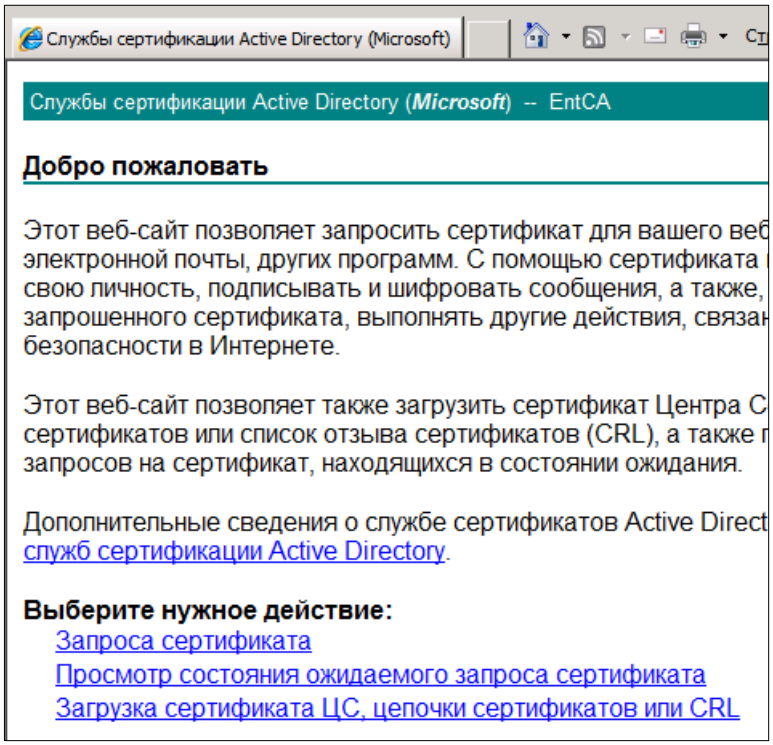



*Рис. 157 – Страница центра сертификации Microsoft*

3. Щелкните на ссылке **Загрузка сертификата ЦС, цепочки сертификатов или CRL**.

Отобразится следующая страница.

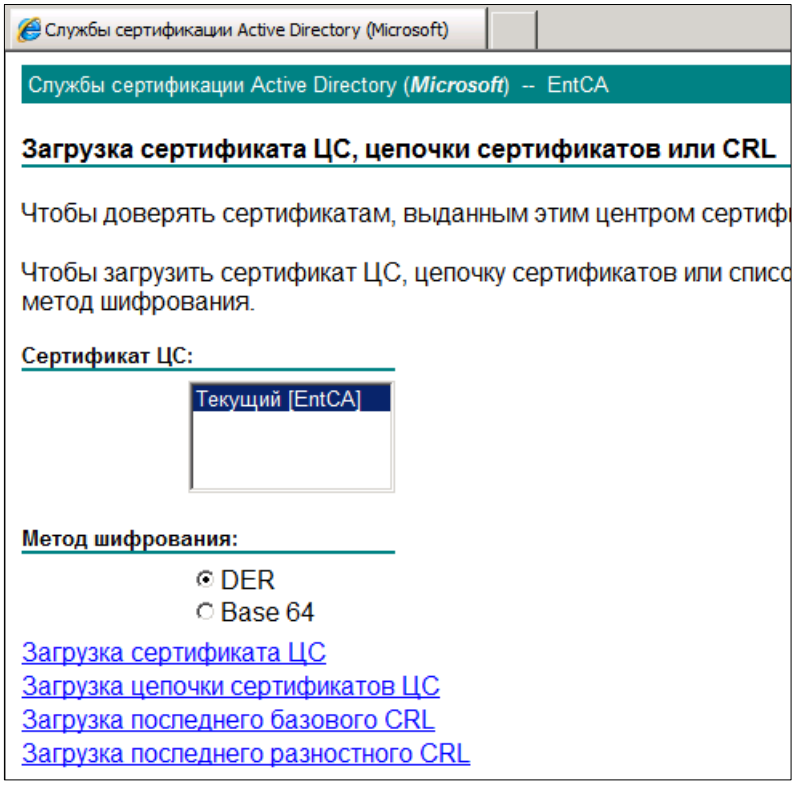



*Рис. 158 – Страница загрузки сертификата центра сертификации Microsoft*

4. Щелкните на ссылке **Загрузка сертификата ЦС**.
   Отобразится следующее окно.

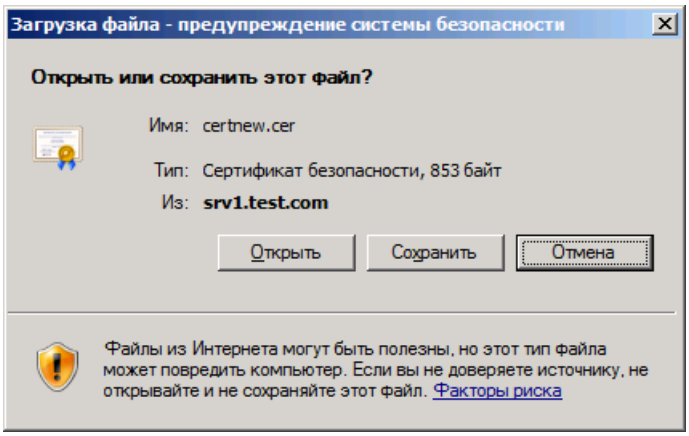



*Рис. 159 – Сохранение корневого сертификата центра сертификации Microsoft*

5. Нажмите **Сохранить** и укажите путь к сохранению корневого сертификата центра сертификации Microsoft.
6. Установите корневой сертификат центра сертификации Microsoft в хранилище **Доверенные корневые центры сертификации** (см. табл. 25).

⚠ Сертификат должен быть установлен как в хранилище пользователя, так и в хранилище компьютера.

*Табл. 25 – Установка корневого сертификата центра сертификации Microsoft*

| Тип хранилища | Действия |
|---|---|
| Хранилище пользователя | 1. Двойным щелчком откройте окно свойств сохраненного сертификата.<br>2. В отобразившемся окне нажмите **Открыть**.<br>3. В окне свойств сертификата на вкладке **Общие** нажмите **Установить сертификат**.<br>4. В отобразившемся окне мастера импорта сертификатов нажмите **Далее**.<br>5. В отобразившемся окне выберите пункт **Поместить все сертификаты в следующее хранилище**, после чего нажмите **Обзор**.<br>6. В окне выбора хранилища сертификата отметьте пункт **Доверенные корневые центры сертификации**, после чего нажмите **ОК**.<br>7. В окне мастера импорта сертификатов нажмите **Далее**.<br>8. В отобразившемся окне нажмите **Готово**. |
| Хранилище компьютера | 1. Из командной строки выполните команду **mmc**.<br>2. В панели управления отобразившегося окна выберите **Файл -> Добавить или удалить оснастку** (или нажмите сочетание клавиш CTRL+M).<br>3. В левой части окна добавления и удаления оснасток выберите **Сертификаты** и нажмите **Добавить**.<br>4. В отобразившемся окне выберите **учетной записи компьютера** и нажмите **Далее**.<br>5. В отобразившемся окне выберите **локальным компьютером** и нажмите **Готово**.<br>6. В окне добавления и удаления оснасток нажмите **ОК**.<br>7. В окне оснастки сертификатов локального компьютера щелкните правой кнопкой на пункте **Доверенные корневые центры сертификации** и выберите **Все задачи -> Импорт**.<br>8. В окне мастера импорта сертификатов нажмите **Далее**.<br>9. В отобразившемся окне укажите путь к сохраненному файлу центра сертификации Microsoft (при необходимости воспользуйтесь кнопкой **Обзор**), после чего нажмите **Далее**.<br>10. В отобразившемся окне убедитесь, что отмечен пункт **Поместить все сертификаты в следующее хранилище** и в поле **Хранилище сертификатов** указано **Доверенные корневые центры сертификации**.<br>11. Нажмите **Далее**.<br>12. В отобразившемся окне нажмите **Готово**. |

### 8.10.3.3 Непосредственная настройка проверки сертификата службы аутентификации JMS

Возможны два варианта настройки проверки сертификата службы аутентификации JMS см. Табл. 26 .

*Табл. 26 – Варианты настройки проверки службы аутентификации JMS*

| Вариант настройки | Описание |
|---|---|
| Отключение проверки сертификата службы аутентификации JMS | На компьютере, на котором установлен компонент JMS Client, в ветке реестра **[HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Client\Default\TransportManager]** добавьте строковый параметр **DisableCrlValidation** со значением и присвойте ему значение **true** (истина). |

| Вариант настройки | Описание |
|---|---|
| Настройка проверки сертификата службы аутентификации JMS на сервере центра сертификации Microsoft | Выполните процедуру, приведенную ниже в настоящем подпункте.<br>**Примечания:**<br>1. Данная процедура выполняется единожды для всех внедоменных рабочих станций.<br>2. В случае если до выполнения данной процедуры на сервере JMS уже был выпущен сертификат службы аутентификации JMS, данный сертификат будет замещен сертификатом, выпущенным в результате выполнения данной процедуры. |

Чтобы настроить проверку сертификата службы аутентификации JMS на сервере центра сертификации Microsoft, выполните следующие действия.

На сервере центра сертификации Microsoft должен быть установлен сервер IIS. Если сервер не установлен, выполните его установку до выполнения процедуры.

1. На сервере центра сертификации Microsoft откройте оснастку центра сертификации.
2. Щелкните правой кнопкой на центре сертификации и выберите **Свойства**.
3. В отобразившемся окне перейдите на вкладку **Расширения**.
   Окно примет следующий вид.

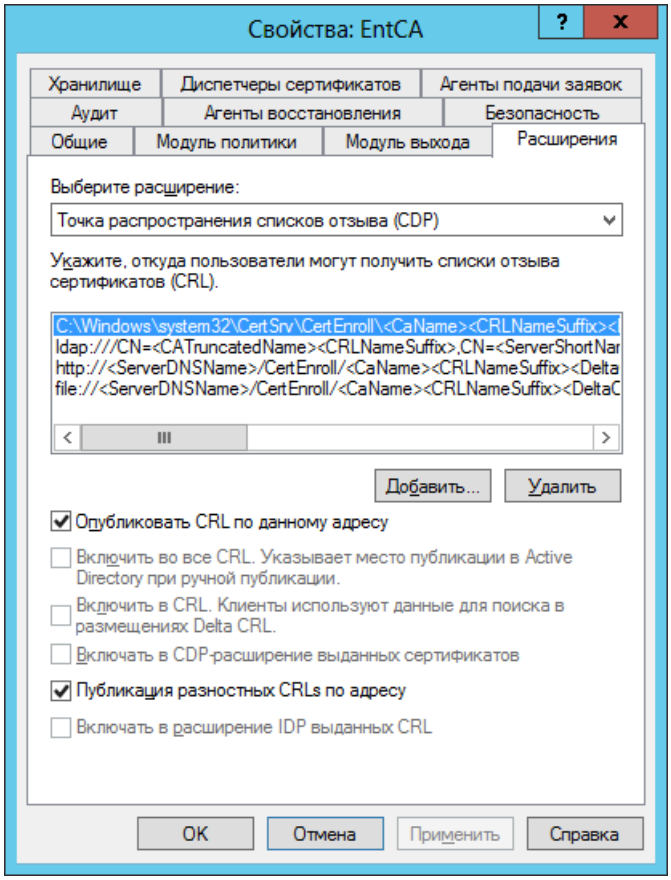



*Рис. 160 – Вкладка Расширения окна свойств центра сертийикации Microsoft*

4. В списке **Укажите, откуда пользователи могут получить списки отзыва сертификатов (CRL)** отметьте строку, которая начинается с **http://**.
5. Ниже установите флаги:

   – **Включить в CRL. Клиенты используют данные для поиска в размещениях Delta CRL**;
   – **Включать в CDP-расширение выданных сертификатов**.

6. Нажмите **Применить** для сохранения изменений, не закрывая окно свойств центра сертификации Microsoft (позже понадобится путь к спискам отзыва сертификатов, указанный

в первой строке списка **Укажите, откуда пользователи могут получить списки отзыва сертификатов (CRL)**).

7. В окне предупреждения о перезагрузке сервера нажмите **Да** для подтверждения действия.
8. Откройте оснастку сервера IIS.
9. В левой части окна разверните щелкните правой кнопкой на пункте **Сайты** и выберите **Добавить веб-сайт** (см. рис. 161).

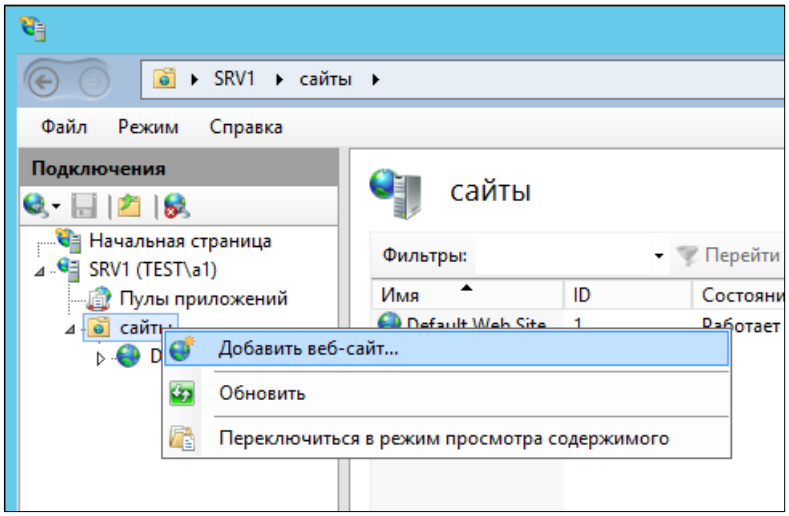



*Рис. 161 – Добавление нового веб-сайта*

Отобразится следующее окно.

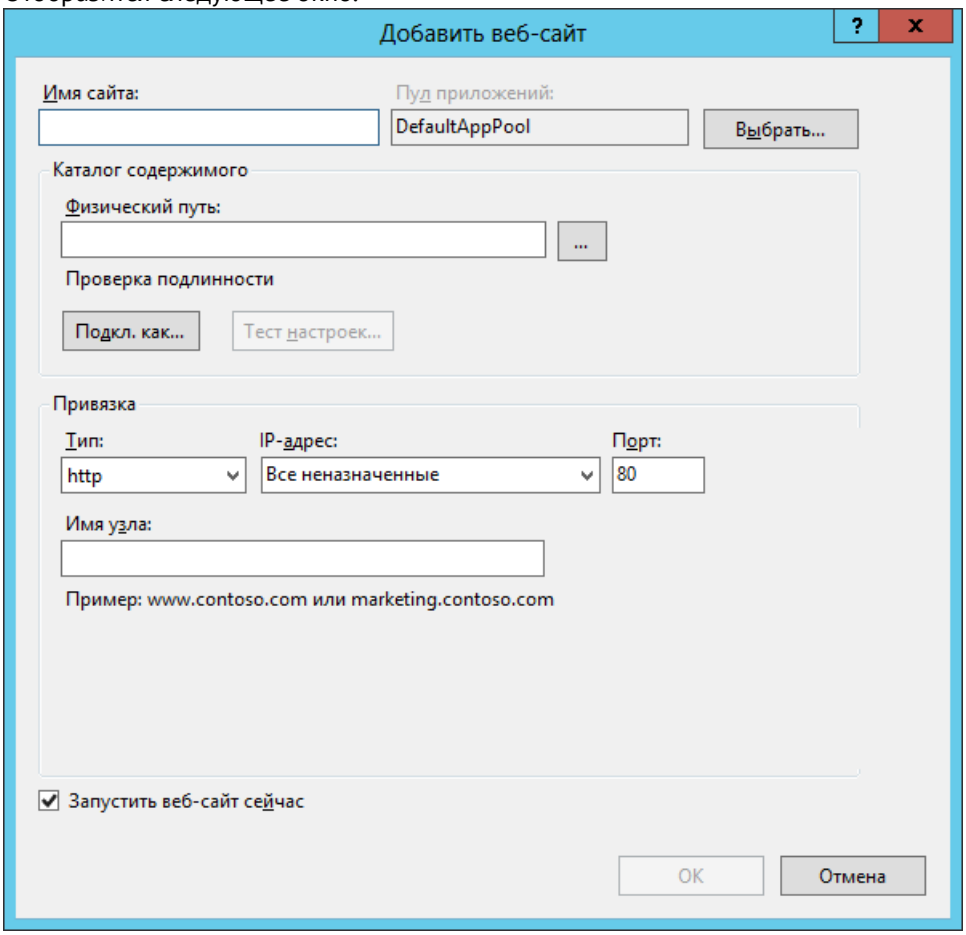



*Рис. 162 – Окно добавления нового веб-сайта*

10. Выполните следующие настройки:

10.1. В поле **Имя сайте** введите имя сайта.
10.2. В поле **Физический путь** укажите путь к каталогу со списками отзыва сертификата (см. рис. 160, с. 139).

Путь следует указывать до **CertSrv** включительно. По умолчанию это путь: **C:\Windows\system32\ CertSrv**.

11. Нажмите OK, чтобы сохранить изменения.
12. В левой части окна щелкните отметьте созданный сайт, после чего в центральной части экрана двойным щелчком откройте настройки **Фильтрация запросов**.
13. В настройках фильтрации запросов в колонке **Действия** справа щелкните на ссылке **Изменить параметры**.
Отобразится следующее окно.

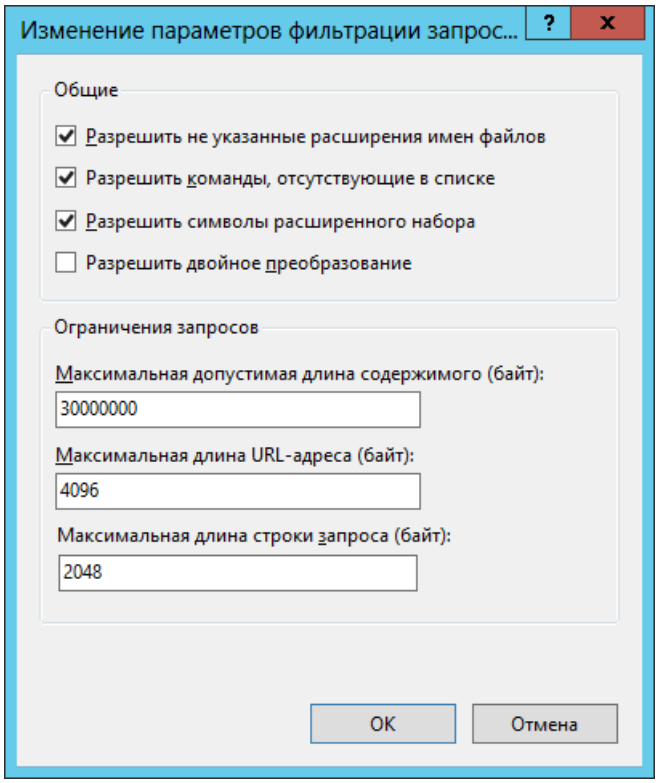



*Рис. 163 – Параметры фильтрации запросов*

14. Установите флаг **Разрешить двойное преобразование** и нажмите **OK**, чтобы сохранить изменения.
15. Убедитесь в том, что через браузер можно загрузить целостный список отзыва сертификатов и разностный список отзыва сертификатов по следующим ссылкам:

- **http://<домен>/CertEnroll/<Имя ЦС>.crl** (целостный список отзыва сертификатов);
- **http://<домен>/CertEnroll/<Имя ЦС>+.crl** (разностный список отзыва сертификатов).
- Например:
- **http://test.com/CertEnroll/EntCA.crl**;
- **http://test.com/CertEnroll/EntCA+.crl**.

16. Выпустите новый сертификат для службы аутентификации JMS по шаблону **Компьютер** и подставьте его в настройку службы аутентификации JMS (см. «Настройки сервиса аутентификации JMS», с. 194)и убедитесь в том, что в свойствах сертификата указан нужный путь к списку отзыва сертификатов (в нашем примере: **http://test.com/CertEnroll/EntCA.crl**).

### 8.10.4 Настройка параметров автоматического открытия/закрытия клиентского сеанса

JMS позволяет настроить автоматическое открытие или закрытие клиентского сеанса по наступлении следующих событий (см. табл. 27).

*Табл. 27 – Возможные события открытия/закрытия клиентского сеанса*

| Действие | Событие |
|---|---|
| Открытие сеанса | • Запуск утилиты Клиент JMS.<br>• Подсоединение электронного ключа к компьютеру. |
| Закрытие сеанса | • Отсоединение электронного ключа, с помощью которого был открыт текущий сеанс.<br>• Потеря соединения с сервером JMS. |

По умолчанию автоматическое открытие/закрытие клиентского сеанса по наступлении соответствующего события отключено. Чтобы включить автоматическое открытие/закрытие клиентского сеанса, выполните следующие действия.

1. На компьютере, на котором установлен компонент JMS Client, запустите редактор реестра (для этого выполните из командной строки команду **regedit**).
2. В отобразившемся окне перейдите в раздел **HKEY_CURRENT_USER\SOFTWARE\Aladdin\Enterprise Application Platform Client\SessionManager** (если раздел отсутствует, создайте его).
3. Отредактируйте (или создайте, если они отсутствуют) следующие строковые параметры (см. табл. 28).

*Табл. 28 – Настройка событий открытия/закрытия сеанса*

| Действие | Строковый параметр | Описание |
|---|---|---|
| Открытие сеанса | **OpenSessionOnAppStart** | Открывать сеанс при запуске утилиты Клиент JMS. Допустимые значения:<br>• **true** - настройка включена;<br>• **false** – настройка отключена.<br>Настройка по умолчанию: **false** (настройка отключена). |
| | **OpenSessionOnDeviceConnected** | Открывать сеанс при подсоединении электронного ключа к компьютеру. Допустимые значения:<br>• **true** - настройка включена;<br>• **false** – настройка отключена.<br>Настройка по умолчанию: **false** (настройка отключена). |
| | **OpenSessionOnResume** | Открывать сеанс при выходе из ждущего или спящего режима компьютера. Допустимые значения:<br>• **true** - настройка включена;<br>• **false** – настройка отключена.<br>Настройка по умолчанию: **false** (настройка отключена). |
| | **OpenSessionOnSwitchOnline** | Открывать сеанс при восстановлении соединения с сервером или с клиентской службой. Допустимые значения:<br>• **true** - настройка включена;<br>• **false** – настройка отключена.<br>Настройка по умолчанию: **false** (настройка отключена). |

| Действие | Строковый параметр | Описание |
|---|---|---|
| Закрытие сеанс | **CloseSessionOnSwitchOffline** | Закрывать сеанс при потере соединения с сервером JMS. Допустимые значения:<br>• **true** - настройка включена;<br>• **false** – настройка отключена.<br>Настройка по умолчанию: **false** (настройка отключена). |
| | **CloseSessionOnDeviceDisconnected** | Закрывать сеанс при отсоединении электронного ключа, с помощью которого был открыт текущий сеанс. Допустимые значения:<br>• **true** - настройка включена;<br>• **false** – настройка отключена.<br>Настройка по умолчанию: **false** (настройка отключена). |

4. Перезапустите утилиту **Клиент JMS**.

### 8.10.5 Логика открытия клиентского сеанса

В зависимости от типа события, запускающего клиентский сеанс используется разная логика входа:

- **OpenSessionOnDeviceConnected** (подсоединение электронного ключа) – см. табл. 29, с. 144;
- **OpenSessionOnAppStart** (запуск утилиты Клиент JMS) – см. табл. 30, с. 144;
- **OpenSessionOnResume** (открытие сеанса при выходе из ждущего или спящего режима компьютера) – см. табл. 30, с. 144;
- **OpenSessionOnSwitchOnline** (открытие сеанса при восстановления соединения с сервером или с клиентской службой) - см. табл. 30, с. 144.

*Табл. 29 – Условия открытия клиентского сеанса по событию OpenSessionOnDeviceConnected*

| Условие | Варианты выполнения условия | | |
|---|---|---|---|
| **Прошлый вход сохранен** | Да | Нет | Да |
| **Вход осуществляется в домене** | Не имеет значения | Не имеет значения | Не имеет значения |
| **Способ прошлого входа** | По электронному ключу | Не имеет значения | По паролю Windows |
| **Кол-во подсоединенных электронных ключей** | 1 и более | 1 | 1 |
| **На подсоединенном электронном ключе есть аутентификатор** | Да | Да | Да |
| **Аутентификатор подсоединенного электронного ключа соответствует ранее сохраненному** | Да | Не актуально | Не актуально |
| **Результат** | Сеанс открывается с помощью электронного ключа, чей аутентификатор был сохранен во время прошлого входа. | Сеанс открывается с помощью единственного подсоединенного электронного ключа. | Сеанс открывается с помощью единственного подсоединенного электронного ключа. |

*Табл. 30 – Условия открытия клиентского сеанса по событиям OpenSessionOnAppStart, OpenSessionOnResume, OpenSessionOnSwitchOnline*

| Условие и результат | Варианты соблюдения условий и результат | |
|---|---|---|
| **Прошлый вход сохранен** | Да | Нет |

| Условие и результат | Варианты соблюдения условий и результат | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Вход осуществляется в домене** | Не имеет значения | Да | Нет | Нет | | Да | | | | |
| **Способ прошлого входа** | По электронному ключу | По паролю Windows | По паролю Windows | Не актуально | | Не актуально | | | | |
| **Настройка приоритета** | Не актуально | Не актуально | Не актуально | Не актуально | Не актуально | Не актуально | Не задана | Вход по паролю Windows | Вход по электронному ключу | |
| **Кол-во подсоединенных электронных ключей** | 1 и более | 0 и более | 0 и более | 1 | 0 или более 1 | 0 | Не имеет значения | Не имеет значения | 1 | Более 1 |
| **На подсоединенном ключе есть аутентификатор** | Да | Не имеет значения | Не имеет значения | Да | Не имеет значения | Не актуально | Не имеет значения | Не имеет значения | Да | |
| **Аутентификатор подсоединенного электронного ключа соответствует ранее сохраненному** | Да | Не имеет значения | Не имеет значения | Не актуально | Не актуально | Не актуально | Не имеет значения | Не имеет значения | | |
| **Результат** | Вход осуществляется по электронному ключу, по | Вход осуществляется по доменной | На экране пользователя отображается окно | Клиентский сеанс открывается по подсоединен | Пользователю отображается окно | Вход осуществляется по доменной | Открытие клиентского сеанса осуществляется с | Вход осуществляется по доменной | Вход осуществляется по | На экране пользователя отображается окно |

| Условие и результат | Варианты соблюдения условий и результат | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | которому вход был осуществлен в прошлый раз. | учетной записи. | выбора типа входа. | ному электронному ключу | аутентификации | учетной записи. | использованием доменной учетной записи | учетной записи. | электронному ключу | аутентификации |

### 8.10.6 Настройка уведомлений клиентских агентов

JMS Client позволяет отображать на экране пользователя сообщения следующих типов:

- информационные сообщения;
- предупреждения;
- ошибки.

Пользователь JMS с помощью меню в области уведомлений может явно указать, отображать или нет тот или иной тип сообщения (см. рис. 164).

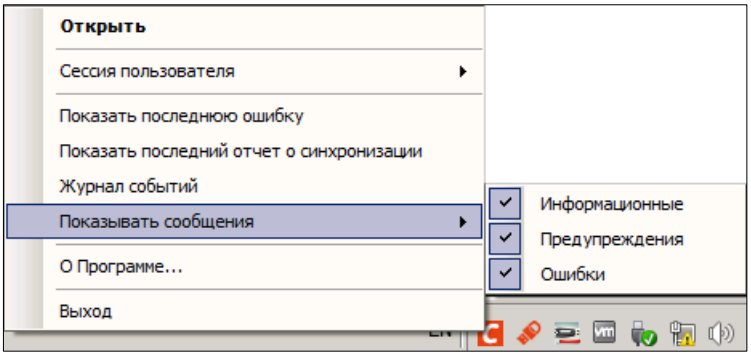



*Рис. 164 – Включение/отключение уведомлений*

Также существует возможность настроить параметры отображения сообщений для всех пользователей компьютера посредством редактирования реестра – при этом пользовательские настройки все равно имеют приоритет. Таким образом, общие настройки отображения уведомлений будут иметь силу до тех пор, пока пользователь не изменит эти настройки.

Чтобы настроить параметры отображения уведомлений, выполните следующие действия.

1. В разделе реестра **HKEY_LOCAL_MACHINE\Software\Aladdin\Enterprise Application Platform Client** создайте параметр DWORD **BaloonShowLevel**.
2. Присвойте созданному параметру нужное значение, руководствуясь табл. 31.

*Табл. 31 – Настройка отображения уведомлений на экране пользователей*

| Значение | Показывать информационные сообщения | Показывать предупреждения | Показывать ошибки |
|---|---|---|---|
| **0** | Нет | Нет | Нет |
| **1** | Да | Нет | Нет |
| **2** | Нет | Да | Нет |
| **3** | Да | Да | Нет |
| **4** | Нет | Нет | Да |
| **5** | Да | Нет | Да |
| **6** | Нет | Да | Да |
| **7** | Да | Да | Да |

# 9. Обеспечение целостности и защиты от несанкционированного доступа файлов ПО JMS

Для обеспечения целостности ПО JMS каталоги для установки его компонентов, а именно:

- C:\Program Files\Enterprise Management System Server\ — для компонента JMS Server;
- C:\Program Files\EAP Administrative Client\ — для компонента JMS Admin;
- C:\Program Files\EAP Client\ — для компонента JMS Client;
- C:\Program Files\Aladdin\JaCarta Authentication Server\ — для компонента JAS [4]

не должны быть доступны непривилегированным пользователям для добавления и модификации файлов.

**Примечание.** В перечне указаны каталоги для установки по умолчанию. В случае выбора в мастере установки опции «Выборочная» (см. например, Рис. 64, с. 66) требование относится к указанному в мастере каталогу установки для конкретного компонента JMS.

# 10. Настройка функций безопасности среды функционирования объекта оценки (JMS)

Для защиты информации, хранящейся в БД ПО JMS, следует установить и настроить наложенное криптографическое средство защиты информации (СКЗИ) «Крипто БД».

Установку и настройку СКЗИ «Крипто БД» для работы с JMS следует производить в соответствии разделом «Установка и настройка плагина СКЗИ «Крипто БД» для JMS и JAS», с. 237.

В остальном объект оценки (JMS) не накладывает дополнительных требований к настройке среды функционирования.

Для управления настройкой элементов среды функционирования (операционных систем) объекта оценки следует использовать документацию из комплекта поставки данных ОС.

# 11. Обновление JMS

**Важно!** Перед обновлением убедитесь в выполнении следующих условий:

- для обновляемой версии JMS создана актуальная резервная копия БД JMS;
- Администратор ИБ, выполняющий обновление JMS, имеет назначенный при установке JMS или выпущенный в текущей версии JMS электронный ключ.

Для обновления JMS на новую версию сначала удалите все установленные компоненты JMS, после чего выполните установку новых версий компонентов JMS.

При установке сервера JMS следует обратить внимание на следующие условия:

- если в предыдущей установке служба сервера JMS запускалась от имени **Системная учетная запись** (предлагается по умолчанию, подробнее см. раздел «Настройка служебной учетной записи», с. 89), то сразу после установки сервера следует запустить *мастер первоначальной настройки* (запускается по умолчанию автоматически) и выполнить первоначальную настройку конфигурации, используя вариант **Использовать настройки от предыдущей установки** (см. рис. 79, с. 75);

- если в предыдущей установке служба сервера JMS запускалась от имени служебной учетной записи (**Учётная запись пользователя**, см. раздел «Настройка служебной учетной записи», с. 89), то сразу после установки сервера (отменив выполнение *мастера первоначальной настройки*) следует выполнить действия, описанные в разделе «Настройка запуска службы сервера JMS от имени служебной учётной записи», с. 72, используя служебную учётную запись, применявшуюся в предыдущей установке сервера. После чего следует запустить *мастер первоначальной настройки* (см. «Запуск мастера первоначальной настройки конфигурации», с. 74) и выполнить первоначальную настройку конфигурации, используя вариант **Использовать настройки от предыдущей установки** (см. рис. 79, с. 75).

  **Примечание.** В случае если данные о прежней служебной учётной записи утрачены, сразу после установки сервера JMS (до запуска *мастера первоначальной настройки*) следует выполнить следующие действия:

  1. Подготовить новую служебную учётную запись, руководствуясь разделом «Подготовка служебной учетной записи для запуска сервера JMS», с. 67.

  2. Выполнить создание имени входа на сервере СУБД, руководствуясь разделом «Создание имени входа на сервере базы данных для служебной учетной записи сервера JMS», с. 96.

  3. Если служебная учётная запись использовалась также в качестве агента регистрации (при выпуске сертификатов в MSCA), то на такую учетную запись следует выпустить и зарегистрировать в хранилище соответствующий сертификат (см. разделы «Сертификаты для работы с JMS», с. 24, и «Шаблон сертификата агента регистрации», с. 28).

  4. Запустить *мастер первоначальной настройки* (см. «Запуск мастера первоначальной настройки конфигурации», с. 74) и выполнить первоначальную настройку конфигурации, используя вариант **Дополнительные опции развертывания** (см. рис. 79, с. 75) **-> Подключение к существующей базе данных**.

## 11.1 Восстановление настроек приложений JMS Admin и MaintenancePlanRunner после обновления JMS

В случае если конфигурационные файлы приложений JMS Admin и MaintenancePlanRunner в предыдущих инсталляциях JMS были изменены, то для корректной работы данных приложений сразу после их обновления следует восстановить значения параметров, которые были до обновления JMS (конфигурационных файлов).

**Примечания:**

1. В частности, следует обратить внимание на значения параметров UseDNSSearch и ServerUrl. Так, в случае если в значении параметра ServerUrl до обновления использовался префикс «https» (подключение по SSL), то после обновления «http» следует заменить на «https».
2. Информацию о расположении конфигурационного файла приложения JMS Admin см. в разделе «Конфигурационный файл приложения JMS Admin (Консоли управления JMS)», с. 131.
3. Информацию о расположении конфигурационного файла утилиты MaintenancePlanRunner см. «Руководство администратора. Часть 2» [3] в разделе «Запуск планов обслуживания с помощью утилиты MaintenancePlanRunner» -> «Сведения об утилите».

## 11.2 Порядок работы с подсистемой отчетов при обновлении JMS

В случае, если к JMS подключена система отчетов, перед обновлением JMS данную подсистему следует отключить (отключить от БД JMS) с помощью мастера конфигурирования подсистемы отчётов.

**Важно!** Подсистему отчетов следует включить (подключить к БД JMS) сразу после обновления JMS, в противном случае, возможна рассинхронизация данных в подсистеме отчетов с данными в БД JMS.

# 12. Меню управления сервером JMS в области уведомлений

Чтобы открыть меню управления JMS Server, щелкните правой кнопкой на значке (Сервер JMS) в области уведомлений.

Меню будет иметь следующий вид.

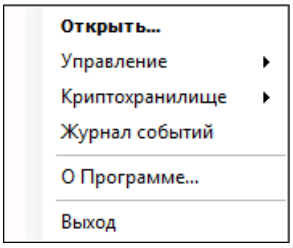



*Рис. 165 – Меню управления JMS Server*

Меню предоставляет доступ к следующим настройкам (см. табл. 32).

*Табл. 32 - Меню быстрого запуска*

| Пункт меню | Подпункт/описание |
|---|---|
| **Открыть** | Открывает окно управления сервером JMS (см. «Окно управления сервером JMS» н стр. 151). |
| **Управление** | Содержит следующие подпункты:<br>• **Старт** – запускает сервер JMS;<br>• **Стоп** – останавливает работу сервера JMS;<br>• **Пауза** – приостанавливает работу сервера JMS;<br>• **Продолжить** – возобновляет работу сервера JMS после приостановки;<br>• **Рестарт** – перезапускает сервер JMS. |
| **Криптохранилище** | Содержит следующие подпункты:<br>• **Смонтировать** – монтирует криптохранилище (например, если оно не было смонтировано во время первоначальной настройки конфигурации);<br>• **Демонтировать** – демонтирует криптохранилище. |
| **Журнал событий**<br>(Журнал приложений и служб Windows) | Открывает журнал приложений и служб ОС Windows. |
| **О Программе** | Отображает сведения о JMS. |
| **Выход** | Скрывает значок (Сервер JMS) из области уведомлений. Чтобы вновь отобразить значок, в меню **Пуск** выберите **JaCarta Management System -> Сервер JMS**. |

# 13. Окно управления сервером JMS (серверный агент)

Чтобы открыть окно управления сервером JMS, щелкните правой кнопкой на значке (Сервер JMS) в области уведомлений и выберите **Открыть**. Отобразившееся окно будет иметь семь вкладок (см. табл. 33).

*Табл. 33 - Вкладки окна управления сервером JMS*

| Вкладка | Описание и ссылка на соответствующий подраздел |
|---|---|
| **Статус** | Отображает статус сервера JMS и статус криптохранилища JMS, а также позволяет останавливать и перезапускать сервер JMS и монтировать/демонтировать криптохранилище (подробнее см. «Статус», с. 152). |
| **Мастер-ключ БД** | Позволяет производить операции с мастер-ключом базы данных, такие как резервное копирование, восстановление, отзыв и замена мастер-ключа БД (подробнее см. «Мастер-ключ БД», с. 153). |
| **Криптография** | Отображает список поставщиков криптографии, которые можно использовать для шифрования криптохранилища JMS, а также позволяет добавить новые поставщики криптографии (подробнее см. «Криптография», с. 167). |
| **Лицензии** | Отображает список установленных лицензий, а также позволяет добавить новые лицензии или удалить существующие (подробнее см. «Лицензии», с. 173). |
| **Каталоги учетных записей** | Отображает список используемых каталогов учетных записей, а также позволяет зарегистрировать новый каталог учетных записей или настроить параметры уже используемого (подробнее см. «Каталоги учетных записей», с. 179). |
| **Привязки каталогов** | Отображает действующие привязки каталогов учетных записей, а также позволяет зарегистрировать новую привязку каталога учетных записей (подробнее см. «Привязки каталогов учетных записей», с. 180). |
| **Настройка** | Позволяет выполнить первоначальную настройку конфигурации, а также позволяет настроить параметры:<br>• серверной службы **Aladdin EAP Engine Service**;<br>• службы аутентификации JMS;<br>• рассылки уведомлений по электронной почте.<br>Подробнее см. «Настройка», с. 184. |
| **Безопасность** | Позволяет выполнить настройки:<br>• параметров сервиса аутентификации («Настройки сервиса аутентификации JMS», с. 194);<br>• поддерживаемых версий протоколов SSL/TLS («Настройки использования SSL/TLS», с. 191) |
| **Коннекторы** | На этой вкладке отображаются зарегистрированные в JMS коннекторы. Коннектор – программный компонент, расширяющий функциональность JMS. Подробнее см. «Коннекторы», с. 196. |
| **Настройки JAS** | Отображает статус подключения к серверу JAS, а также позволяет выполнить настройки такого подключения. Подробнее см. «Настройки JAS», с. 197. |

## 13.1 Статус

Вкладка **Статус** окна управления сервером JMS выглядит следующим образом (см. рис. 166).

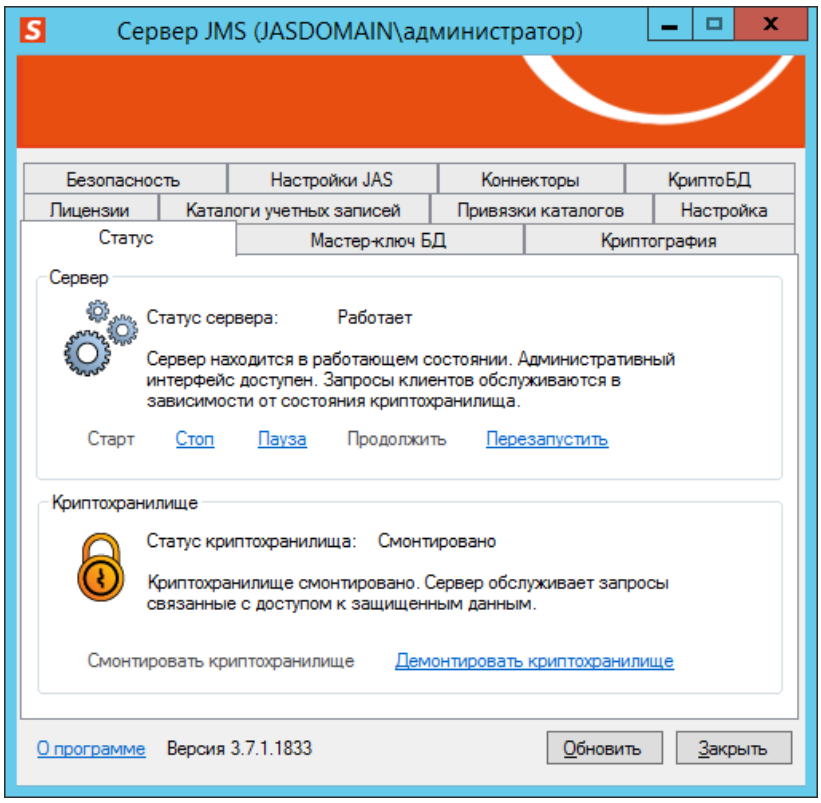



*Рис. 166 – Вкладка **Статус***

Вкладка **Статус** содержит следующие элементы (см. табл. 34).

*Табл. 34 – Вкладка Статус*

| Секция | Элемент | Описание |
|---|---|---|
| **Сервер** | **Статус сервера** | Отображает состояние сервера JMS на текущий момент. |
| | **Старт** | Запускает сервер JMS (впервые или после остановки). |
| | **Стоп** | Останавливает работу сервера JMS. |
| | **Пауза** | Приостанавливает работу сервера JMS. |
| | **Продолжить** | Возобновляет работу сервера JMS (после приостановки). |
| | **Перезапустить** | Перезапускает сервер JMS. |
| **Криптохранилище** | **Статус криптохранилища** | Отображает текущий статус криптохранилища. |
| | **Смонтировать криптохранилище** | Монтирует (подключает) криптохранилище. |
| | **Демонтировать криптохранилище** | Демонтирует (отключает) криптохранилище. |

Для обновления отображаемых сведений щелкните на кнопке **Обновить**.

## 13.2 Мастер-ключ БД

Вкладка **Мастер-ключ БД** выглядит следующим образом (см. рис. 167).

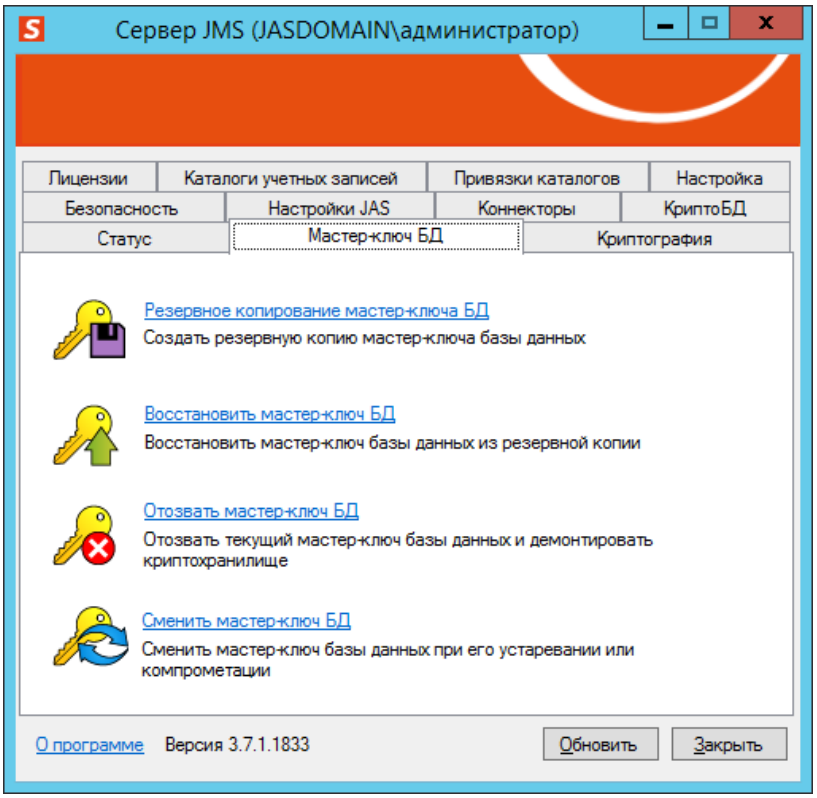



*Рис. 167 – Вкладка Мастер-ключ БД*

Эта вкладка содержит ссылки, которые позволяют выполнять операции с мастер-ключом БД (см. табл. 35).

*Табл. 35 – Вкладка Мастер-ключ БД*

| Ссылка | Описание |
|---|---|
| **Резервное копирование мастер-ключа БД** | Запускает процедуру создания резервной копии мастер-ключа БД (см. «Резервное копирование мастер-ключа БД», с. 153). |
| **Восстановить мастер-ключ БД** | Запускает процедуру восстановления мастер-ключа БД (см. «Восстановление мастер-ключа БД», с. 157). |
| **Отозвать мастер-ключ БД** | Запускает процедуру отзыва мастер ключа БД (см. «Отзыв мастер-ключа БД», с. 160). |
| **Сменить мастер-ключ БД** | Запускает процедуру смены мастер-ключа БД (см. «Смена мастер-ключа БД», с. 163). |

Для обновления отображаемых сведений щелкните на кнопке **Обновить**.

### 13.2.1 Резервное копирование мастер-ключа БД

Для успешного выполнения резервного копирования мастер-ключа БД электронный ключ оператора JMS должен быть подсоединен к компьютеру.

Окно приветствия мастера резервного копирования мастер-ключа БД выглядит следующим образом (см. рис. 168).

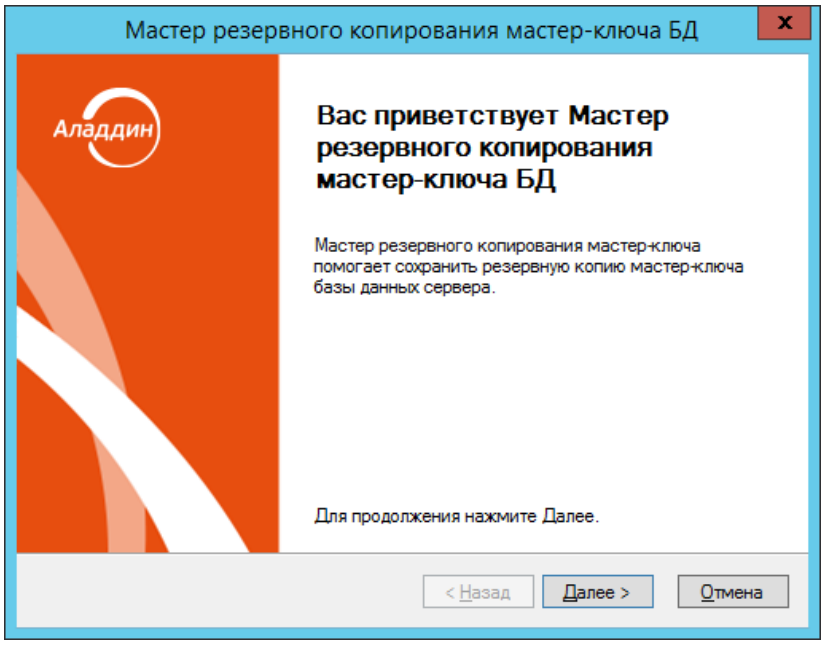



*Рис. 168 – Окно приветствия мастера резервного копирования мастер-ключа БД*

1. Нажмите **Далее**.

Для успешного выполнения процедуры необходимо, чтобы электронный ключ оператора JMS был подсоединен к компьютеру.

Отобразится следующее окно.

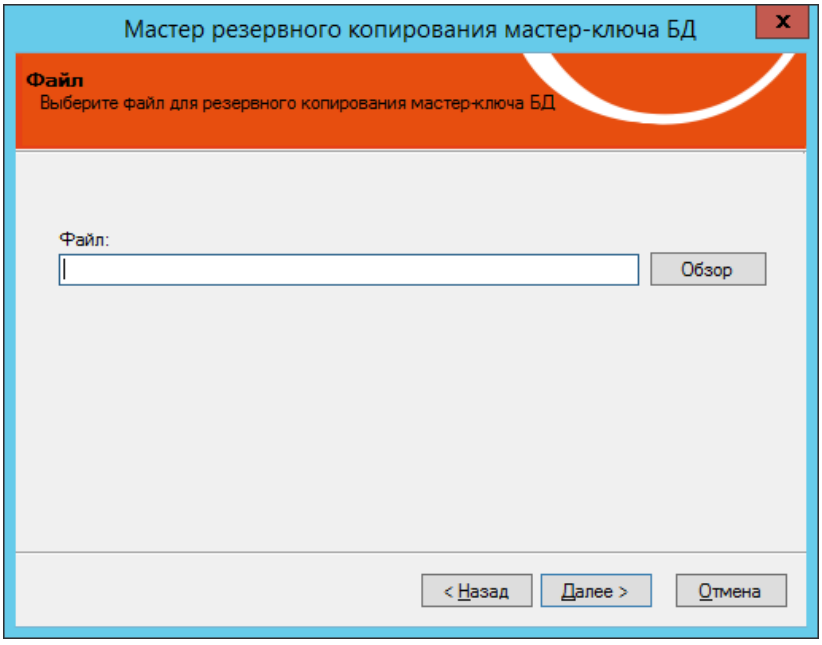



*Рис. 169 – Задание пути сохранения файла резервной копии мастер-ключа БД*

2. Воспользовавшись кнопкой **Обзор**, задайте путь сохранения и имя файла резервной копии мастер-ключа БД, после чего нажмите **Далее**.

Отобразится следующее окно.

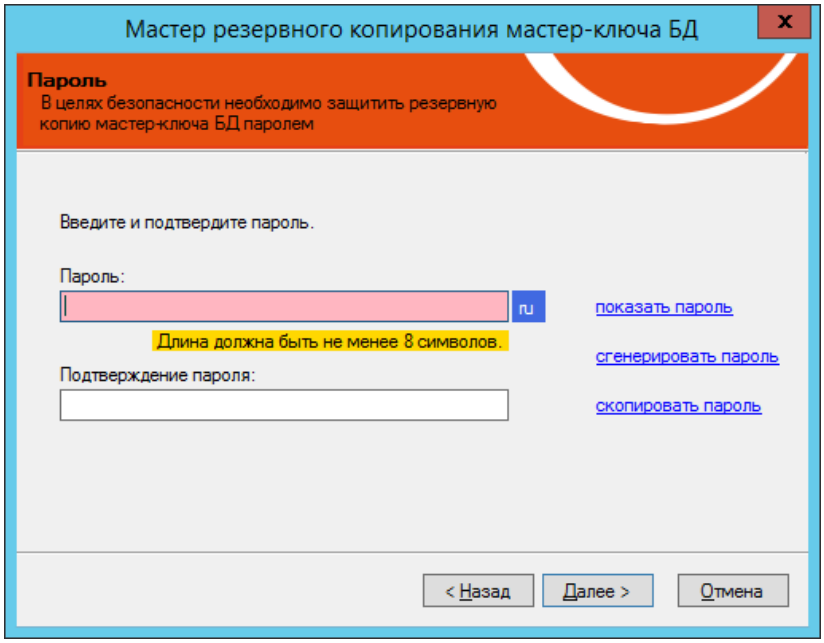



*Рис. 170 – Окно задания пароля для файла резервной копии мастер-ключа БД*

3. В полях **Пароль** и **Подтверждение пароля** задайте пароль для файла резервной копии мастер-ключа БД и введите подтверждение соответственно (пароль должен содержать не менее восьми символов), после чего нажмите **Далее**.
   Отобразится следующее окно.

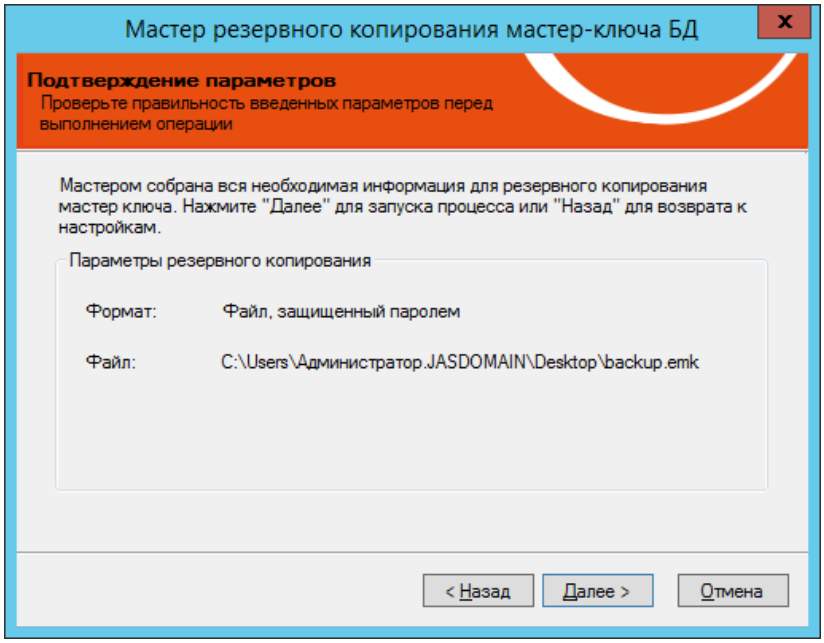



*Рис. 171 – Окно подтверждения параметров сохранения файла резервной копии мастер-ключа БД*

4. Нажмите **Далее**.
5. Если появится окно **Ввод PIN-кода** (см. рис. 172), введите PIN-код пользователя для электронного ключа оператора JMS, после чего нажмите **ОК**.

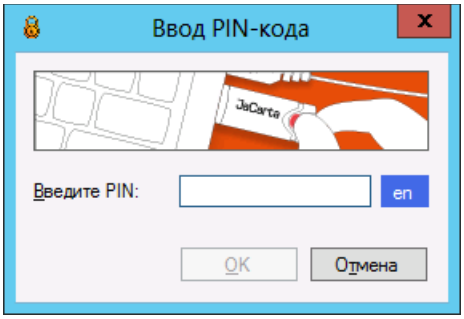



*Рис. 172 – Окно **Ввод PIN-кода***

6. Отобразится следующее окно.

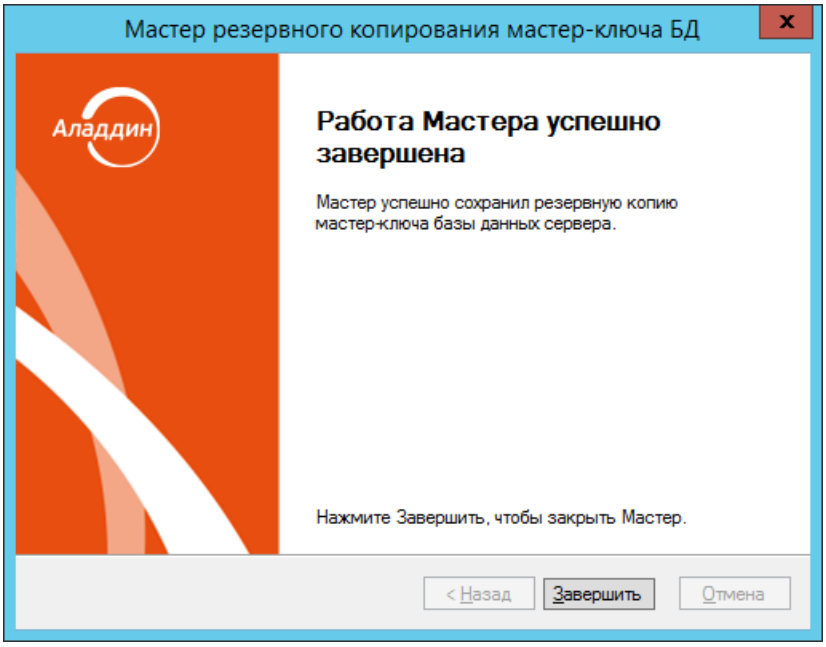



*Рис. 173 – Окно завершения работы мастера создания резервной копии мастер-ключа БД*

7. Нажмите **Завершить** – резервная копия мастер-ключа БД сохранена.

### 13.2.2 Восстановление мастер-ключа БД

Окно приветствия мастера восстановления мастер-ключа БД выглядит следующим образом.

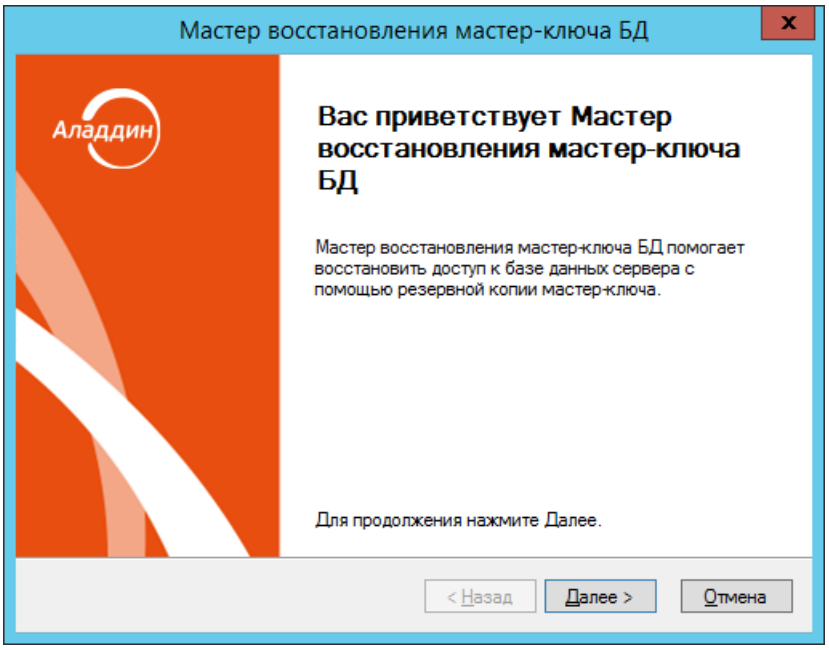



*Рис. 174 – Окно приветствия мастера восстановления мастер-ключа БД*

1. Нажмите **Далее**.
   Отобразится следующее окно.

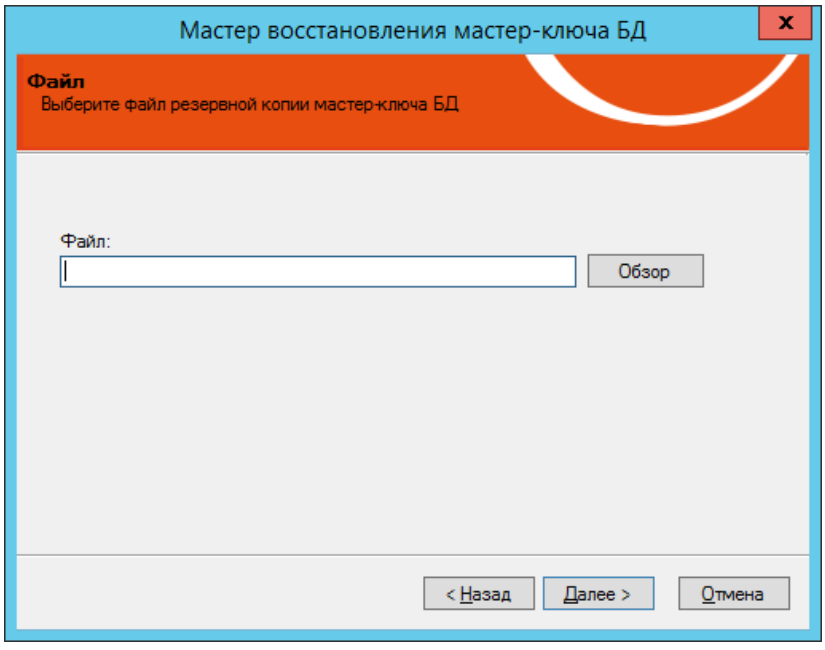



*Рис. 175 – Окно выбора файла резервной копии мастер-ключа*

2. Воспользуйтесь кнопкой **Обзор**, чтобы указать путь к файлу резервной копии мастер-ключа БД, после чего нажмите **Далее**.

Отобразится следующее окно.

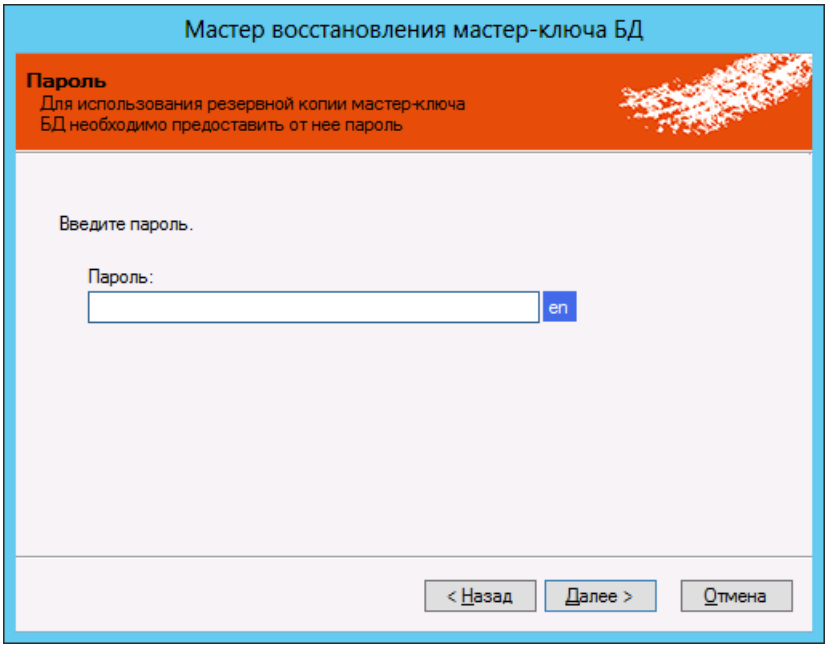



*Рис. 176 – Окно ввода пароля для файла резервной копии мастер-ключа*

3. В поле **Пароль** введите пароль, защищающий файл резервной копии мастер-ключа, после чего нажмите **Далее**.
   Отобразится следующее окно.

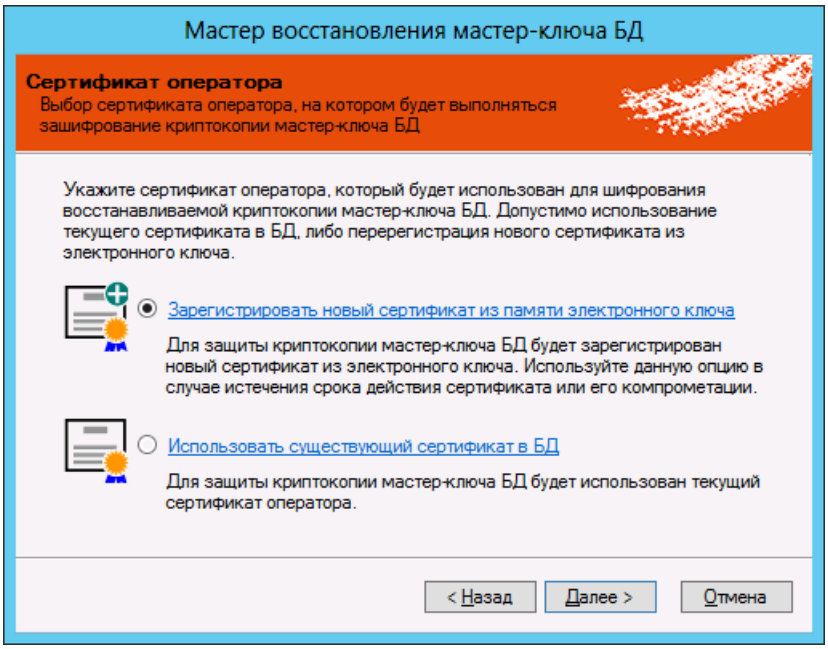



*Рис. 177 – Окно выбора сертификата оператора*

4. Выберите подходящий вам вариант:

   – Зарегистрировать новый сертификат из памяти электронного ключа;
   – Использовать существующий сертификат в БД.

В настоящей процедуре для примера используется пункт **Зарегистрировать новый сертификат из памяти электронного ключа** – в этом случае электронный ключ оператора JMS должен быть подсоединен к компьютеру.

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

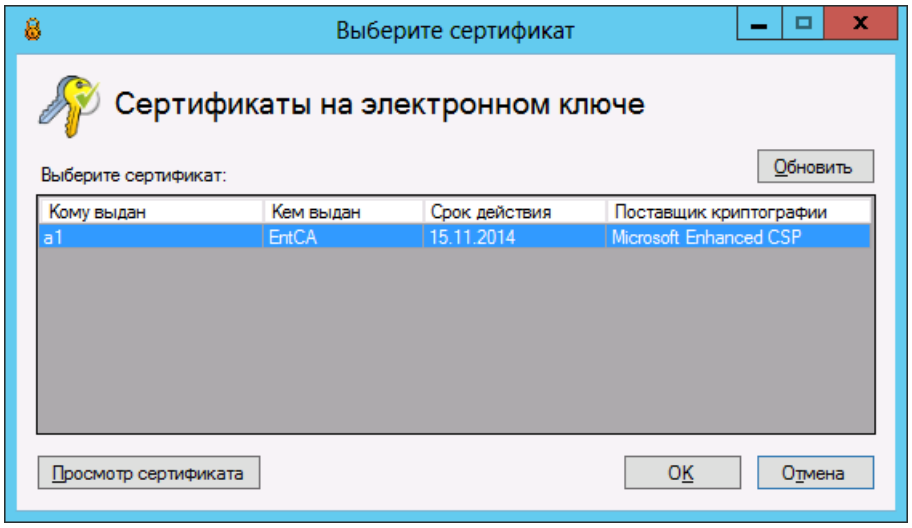



*Рис. 178 – Выбор сертификата в памяти электронного ключа*

6. Выберите нужный сертификат и нажмите **OK**.
   Отобразится следующее окно.

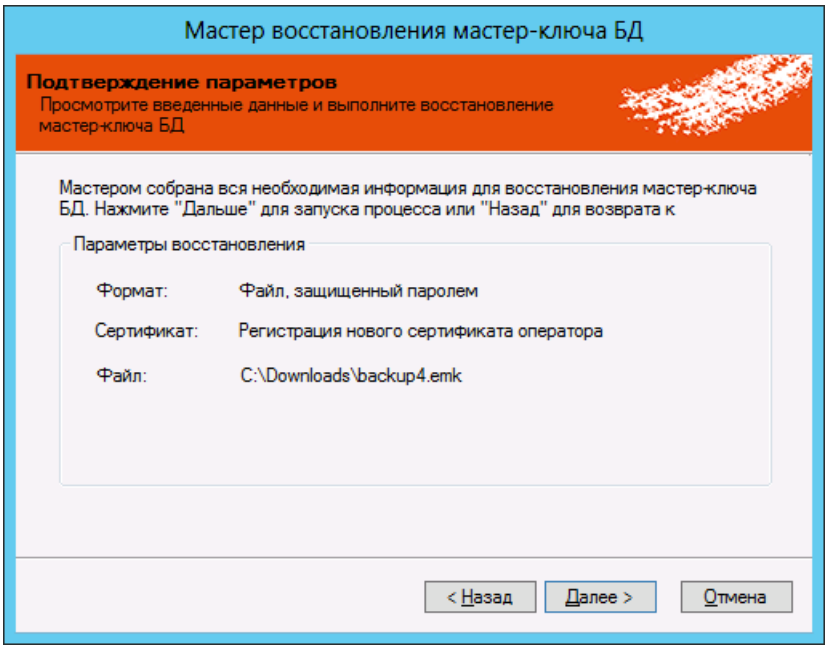



*Рис. 179 – Окно подтверждения параметров перед восстановлением мастер-ключа*

7. Нажмите **Далее**.
8. Введите PIN-код пользователя электронного ключа оператора JMS, если отобразится соответствующее окно.

Окно ввода PIN-кода может не появиться, если PIN-код был введен заранее и в настройках JC-Client/eToken PKI Client/Единого клиента JaCarta установлена настройка кеширования PIN-код пользователя.

По завершении восстановления мастер-ключа БД отобразится следующее окно.

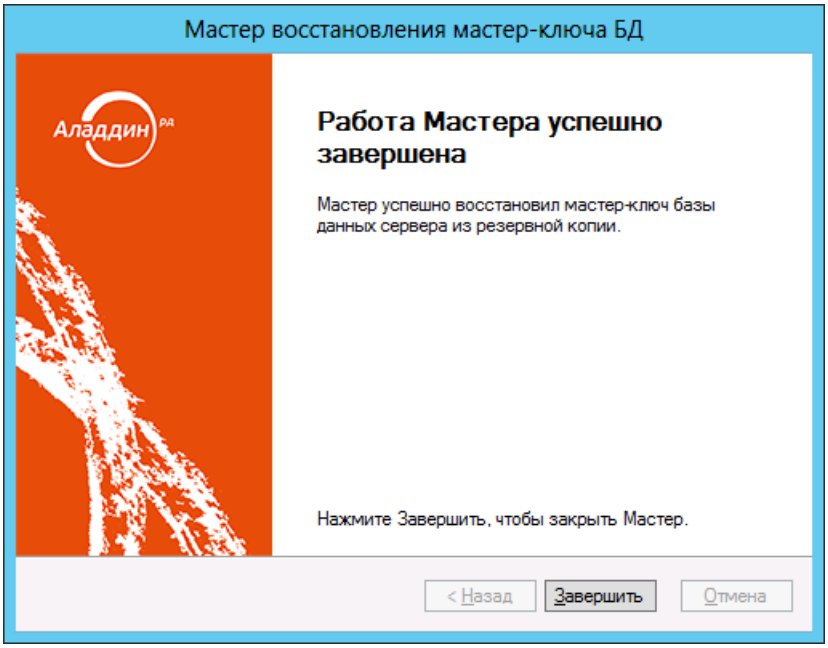



*Рис. 180 – Окно завершения процедуры восстановления мастер-ключа*

9. Нажмите **Завершить** для завершения процедуры.

### 13.2.3 Отзыв мастер-ключа БД

Окно приветствия мастера отзыва мастер-ключа выглядит следующим образом.

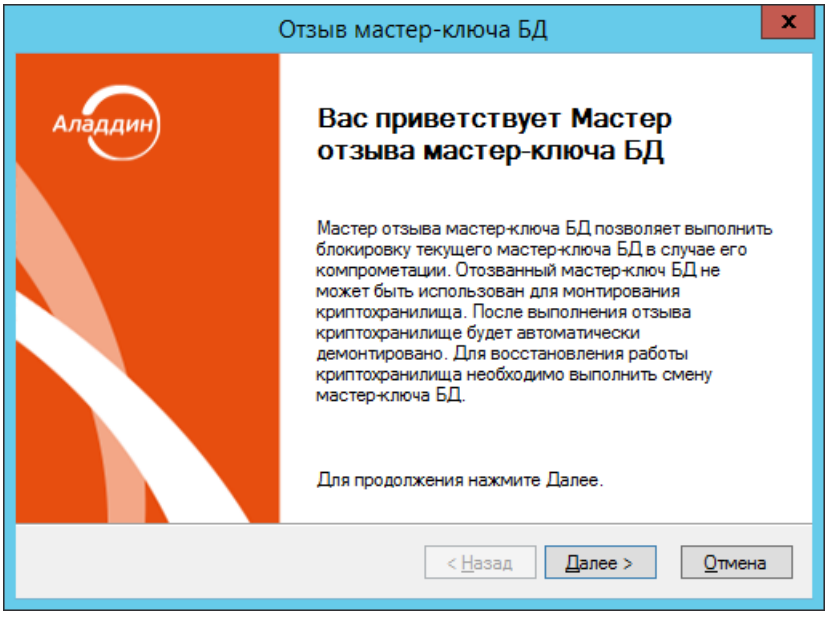



*Рис. 181 – Окно приветствия мастера отзыва мастер-ключа БД*

1. Нажмите **Далее**.

Отобразится следующее окно.

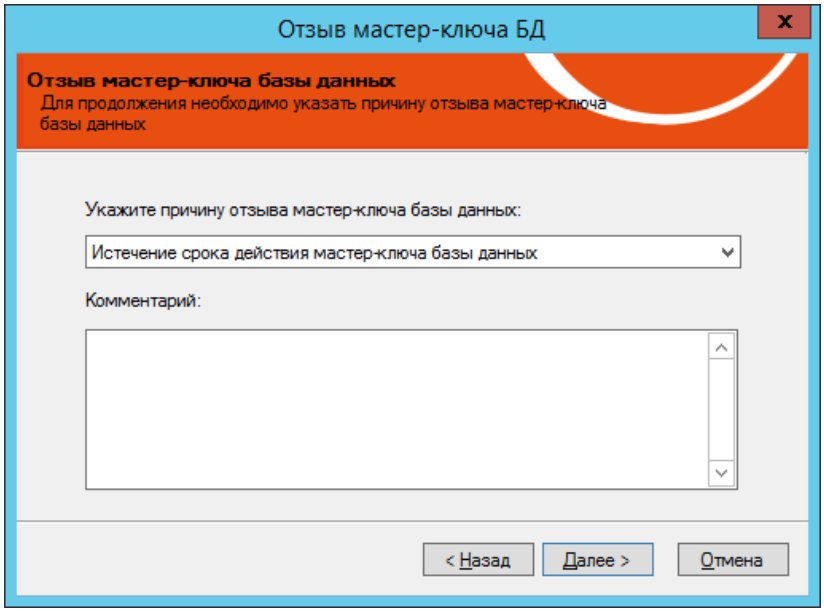



*Рис. 182 – Окно указания причины отзыва мастер-ключа БД*

2. В раскрывающемся списке укажите причину отзыва мастер-ключа базы данных (см. рис. 183).

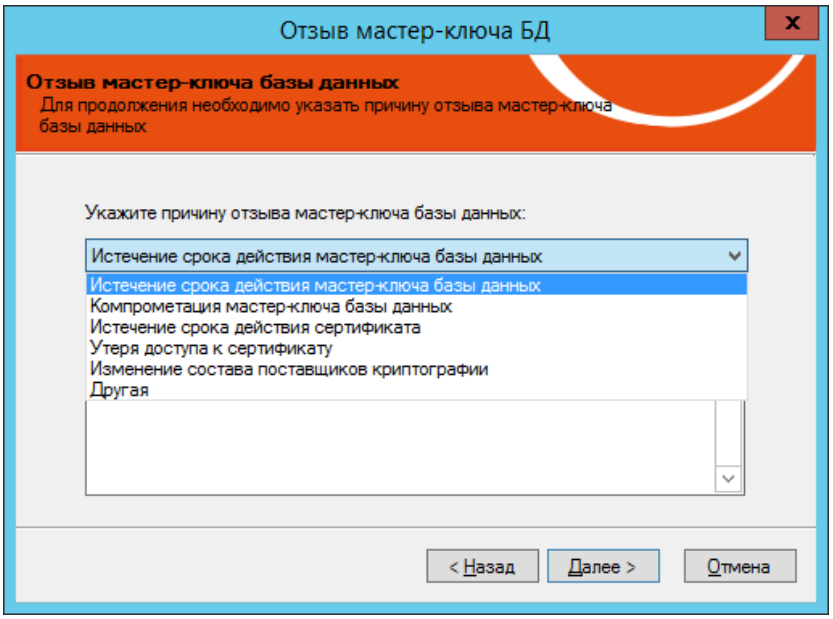



*Рис. 183 – Список причин отзыва мастер-ключа БД*

3. В поле **Комментарий** введите развернутый комментарий и нажмите **Далее**.

Отобразится следующее окно.

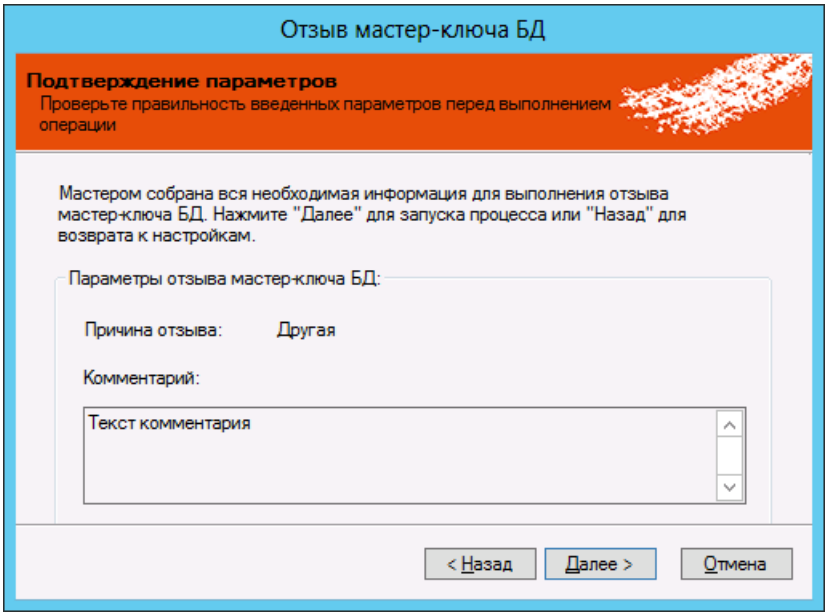



*Рис. 184 – Окно подтверждения параметров отзыва мастер-ключа БД*

4. Нажмите **Далее**.
   По завершении отзыва мастер-ключа БД отобразится следующее окно.

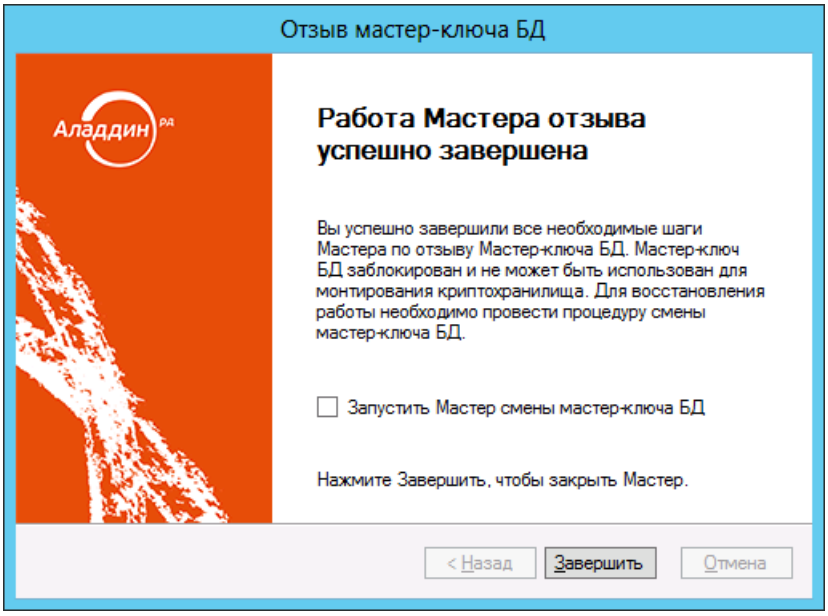



*Рис. 185 – Окно завершения процедуры отзыва мастер-ключа БД*

5. При необходимости установите флаг **Запустить Мастер смены мастер-ключа БД**.

В этом случае по завершении процедуры отзыва мастер-ключа БД отобразится окно мастера приветствия смены мастер-ключа БД (см пункт «Смена мастер-ключа БД»).

6. Нажмите **Завершить**.

### 13.2.4 Смена мастер-ключа БД

Окно приветствия мастера смены мастер-ключа БД выглядит следующим образом.

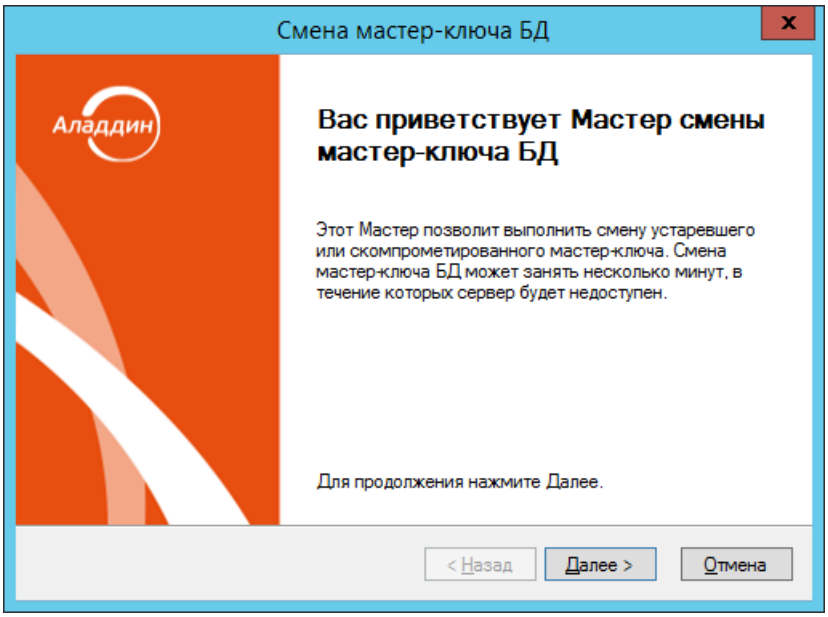



*Рис. 186 – Окно приветствия мастера смены мастер-ключа БД*

1. Нажмите **Далее**.

Для успешного выполнения процедуры необходимо, чтобы электронный ключ оператора JMS был подсоединен к компьютеру.

Отобразится следующее окно.

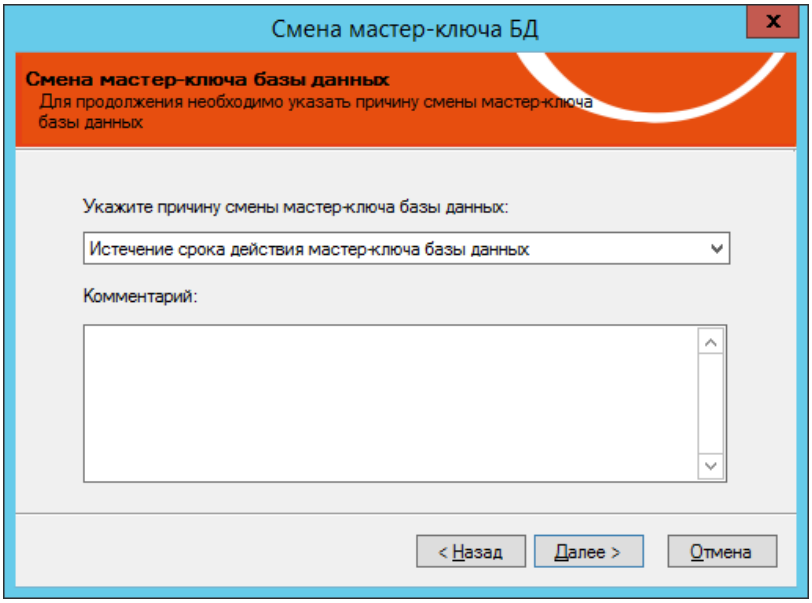



*Рис. 187 – Окно указания причины смены мастер-ключа БД*

2. В раскрывающемся списке укажите причину отзыва мастер-ключа базы данных (см. Рис. 188).

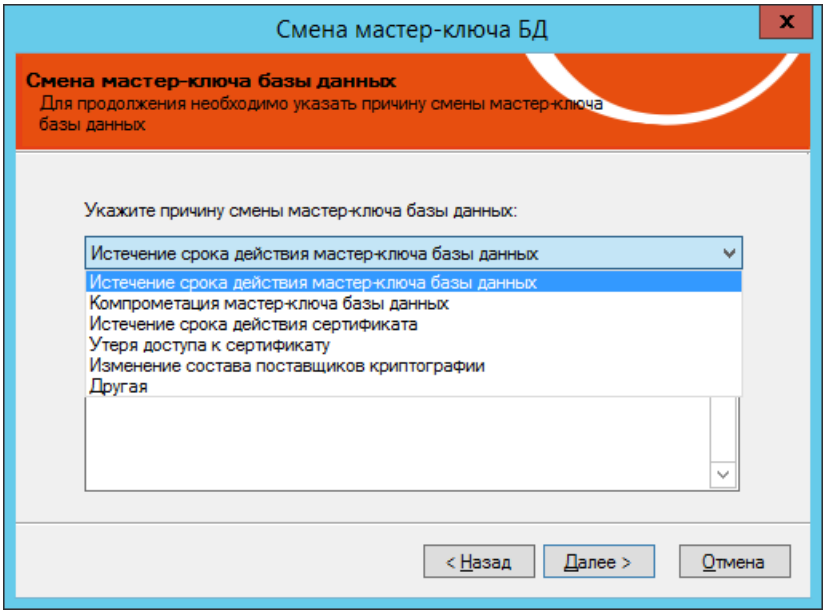



*Рис. 188 – Список причин смены мастер-ключа БД*

3. В поле **Комментарий** введите развернутый комментарий и нажмите **Далее**. Отобразится следующее окно.

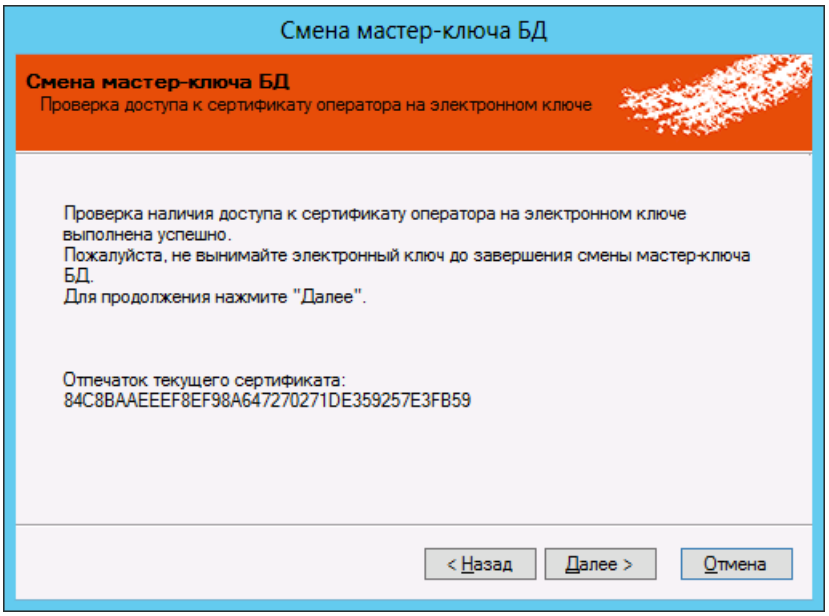



*Рис. 189 – Окно проверки доступа к сертификату оператора JMS в памяти электронного ключа*

4. Нажмите **Далее**.

Отобразится следующее окно.

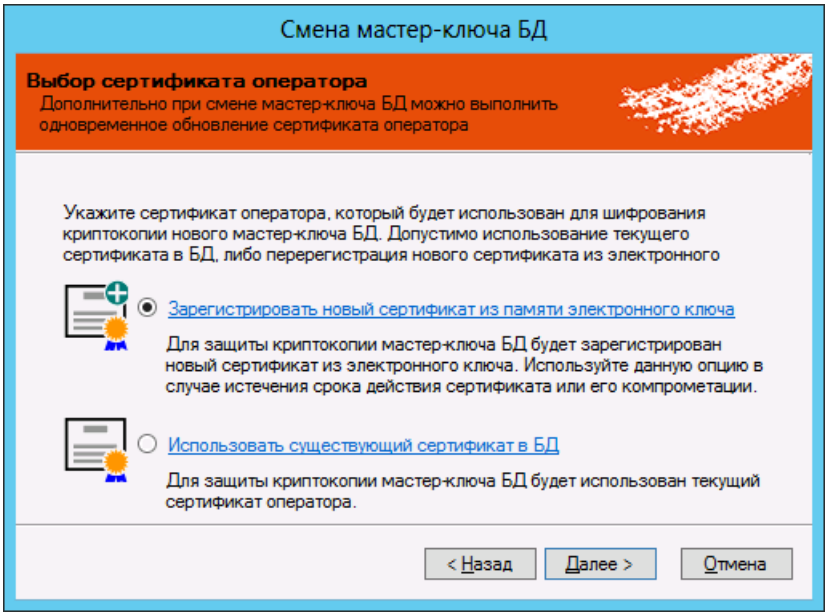



*Рис. 190 – Окно выбора сертификата оператора JMS*

5. Выберите подходящий вам вариант:

   - **Зарегистрировать новый сертификат из памяти электронного ключа**;
   - **Использовать существующий сертификат в БД**.

В настоящей процедуре для примера используется пункт **Зарегистрировать новый сертификат из памяти электронного ключа**.

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

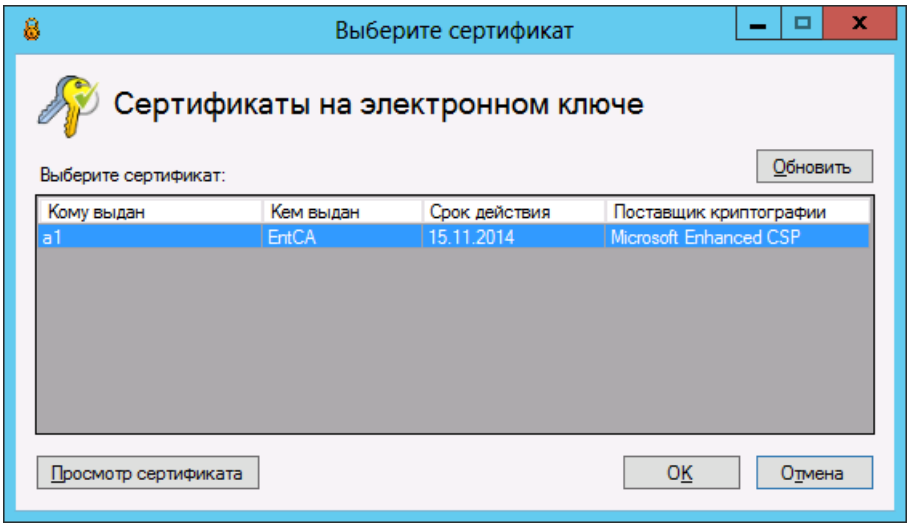



*Рис. 191 – Выбор сертификата оператора JMS*

7. Выберите нужный сертификат и нажмите **OK**.

Отобразится следующее окно.

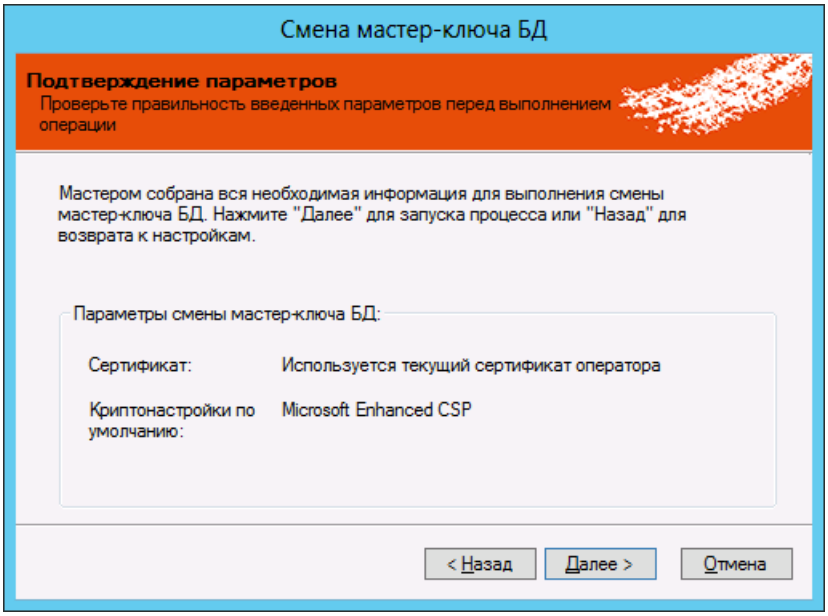



*Рис. 192 – Окно подтверждения параметров*

8. Нажмите **Далее**.
9. В соответствующем окне введите PIN-код пользователя электронного ключа оператора JMS и подтвердите ввод, нажав **ОК**.
   При успешной смене мастер-ключа БД отобразится следующее окно.

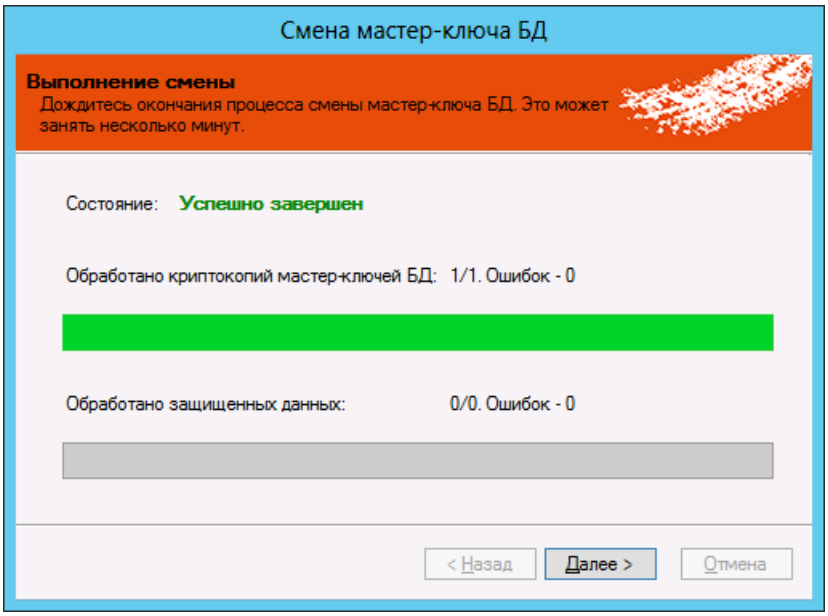



*Рис. 193 – Успешное завершение смены мастер-ключа БД*

10. Нажмите **Далее**.

Отобразится окно завершения процедуры смены мастер-ключа БД.

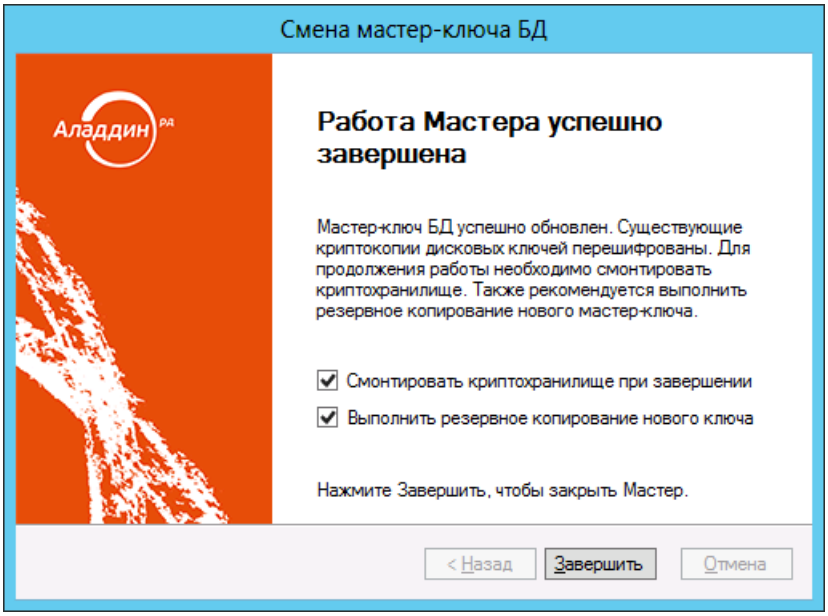



*Рис. 194 – Окно завершения процедуры смены мастер-ключа БД*

11. При необходимости установите флаги:

    - **Смонтировать криптохранилище при завершении**;
    - **Выполнить резервное копирование нового ключа** – в этом случае после нажатия кнопки **Завершить** отобразится окно приветствия мастера резервного копирования созданного мастер-ключа БД (см. пункт «Резервное копирование мастер-ключа БД»).

12. Нажмите **Завершить**.

## 13.3 Криптография

Вкладка **Криптография** отображает список установленных поставщиков криптографии, которые можно использовать для шифрования криптохранилища JMS. Настройки на этой вкладке не имеют отношения к возможности использования поставщика криптографии для выпуска электронных ключей.

### 13.3.1 Общий вид вкладки Криптография

Вкладка **Криптография** выглядит следующим образом.

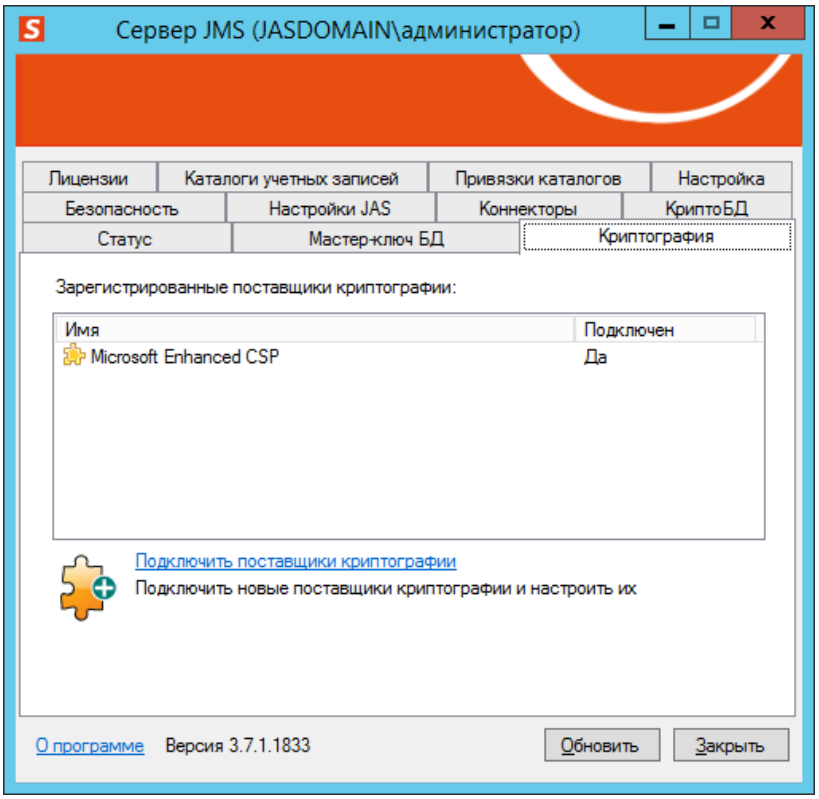



*Рис. 195 – Вкладка Криптография*

Ссылка **Подключить поставщики криптографии** позволяет запустить процедуру подключения нового поставщика криптографии (см. «Подключение поставщика криптографии» ниже).

### 13.3.2 Подключение поставщика криптографии

Процедура подключения нового поставщика криптографии приведена на примере КриптоПро CSP.

Окно приветствия мастера подключения поставщика криптографии выглядит следующим образом.

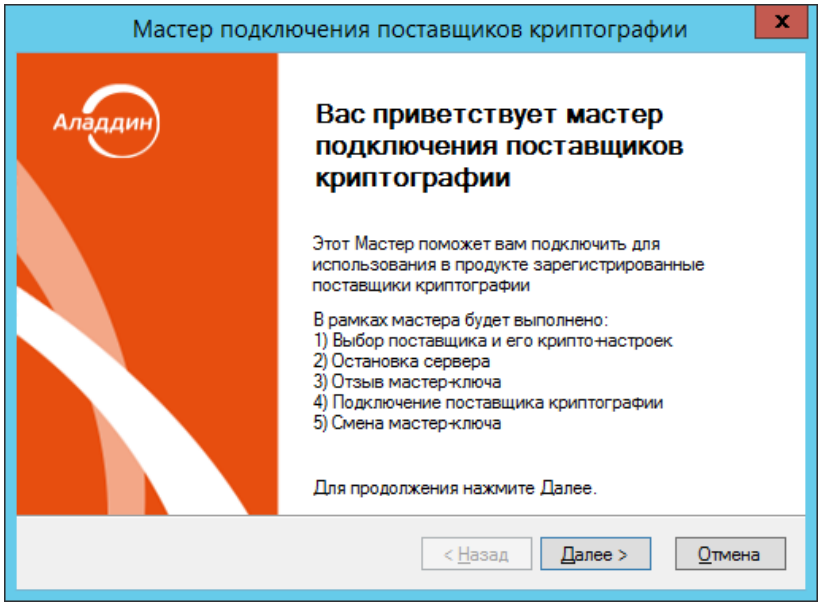



*Рис. 196 – Окно приветствия мастера подключения поставщика криптографии*

1. Нажмите **Далее**.
   Отобразится следующее окно.

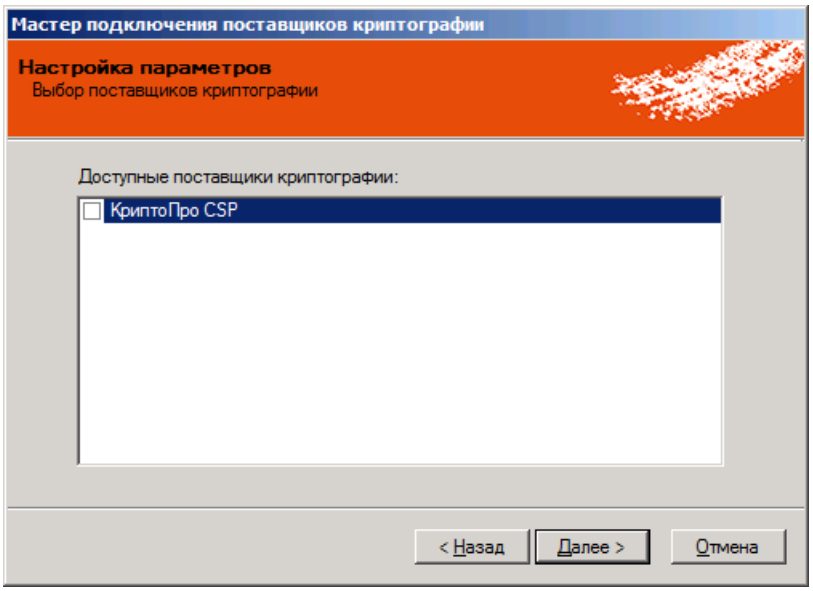



*Рис. 197 – Выбор доступных поставщиков криптографии*

2. Выберите нужный поставщик криптографии и нажмите **Далее**.

Отобразится следующее окно.

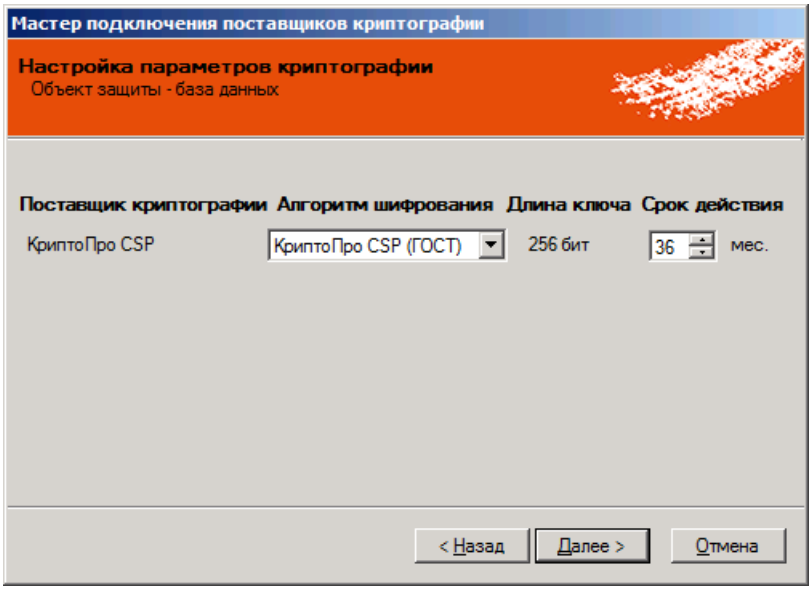



*Рис. 198 – Настройка параметров криптографии*

3. Выполните необходимые настройки и нажмите **Далее**.
   Отобразится следующее окно.

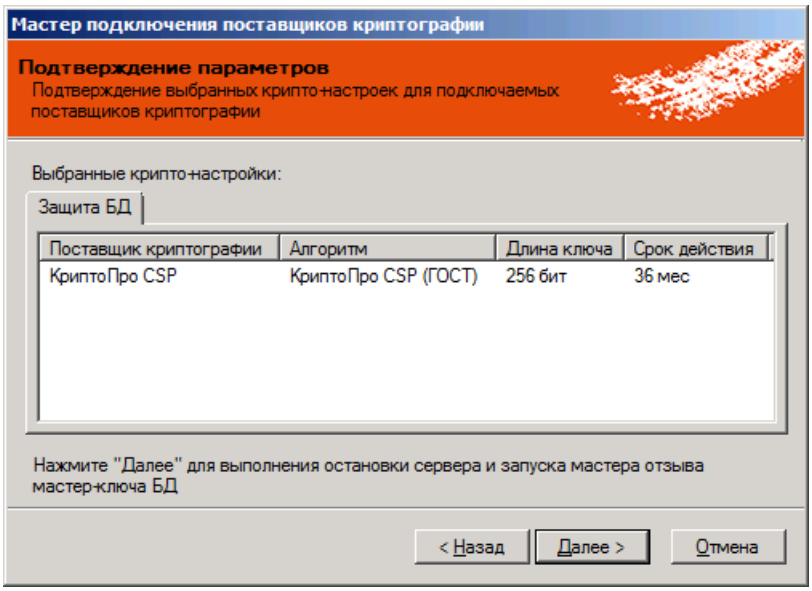



*Рис. 199 – Подтверждение параметров криптографии*

4. Нажмите **Далее**.
   Отобразится окно приветствия мастера отзыва мастер-ключа БД.
5. Выполните процедуру отзыва мастер-ключа БД (см. «Отзыв мастер-ключа БД»).

По завершении отзыва мастер-ключа БД произойдет перезапуск сервера управления JMS.

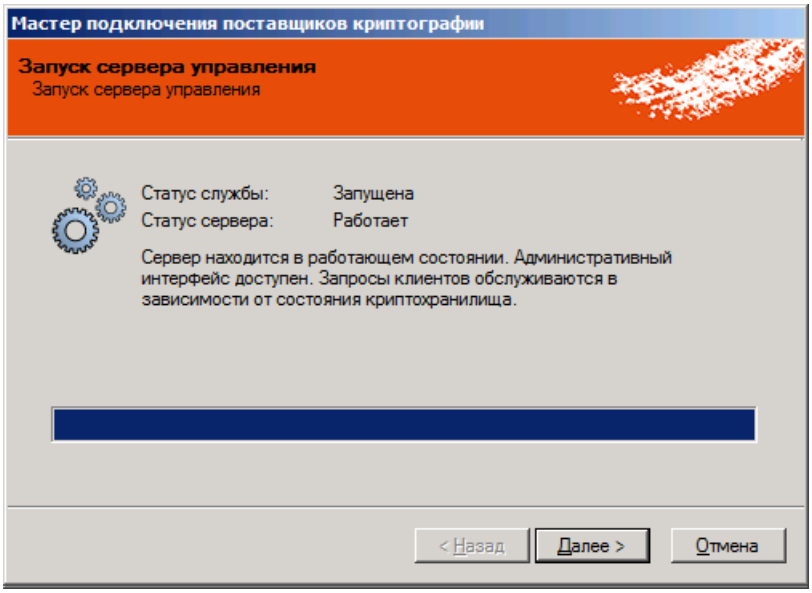



*Рис. 200 – Перезапуск сервера управления*

6. Нажмите **Далее**.
   После перезапуска сервера управления JMS отобразится следующее окно.

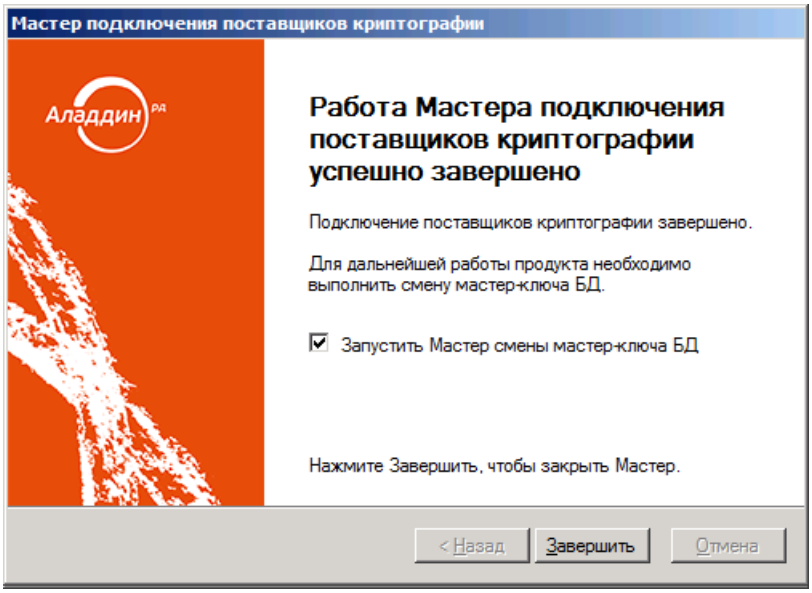



*Рис. 201 – Завершение процедуры подключения поставщика криптографии*

7. Нажмите **Завершить** для завершения процедуры.
8. Если вы оставили отмеченным флаг **Запустить Мастер смены мастер-ключа БД**, отобразится окно соответствующего мастера – выполните необходимые действия, руководствуясь сведениями, представленными в пункте «Смена мастер-ключа БД», с. 163.

После смены мастер-ключа БД вам будет предложено выполнить резервное копирование нового мастер-ключа БД – выполните необходимые действия, руководствуясь представленными в пункте «Резервное копирование мастер-ключа БД», с. 153.

По завершении всех необходимых процедур новый поставщик криптографии отобразится на вкладке **Криптография**.

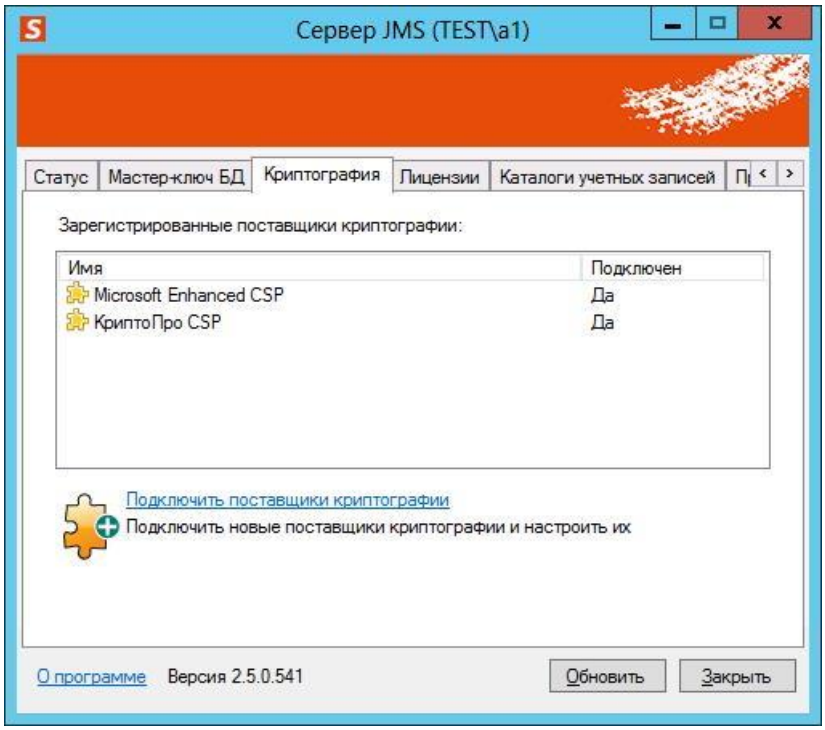



*Рис. 202 – Новый поставщик криптографии отображен в списке **Зарегистрированные поставщики криптографии***

## 13.4 Лицензии (установка лицензии на JMS/JAS)

Вкладка **Лицензии** содержит сведения об установленных лицензиях и выглядит следующим образом.

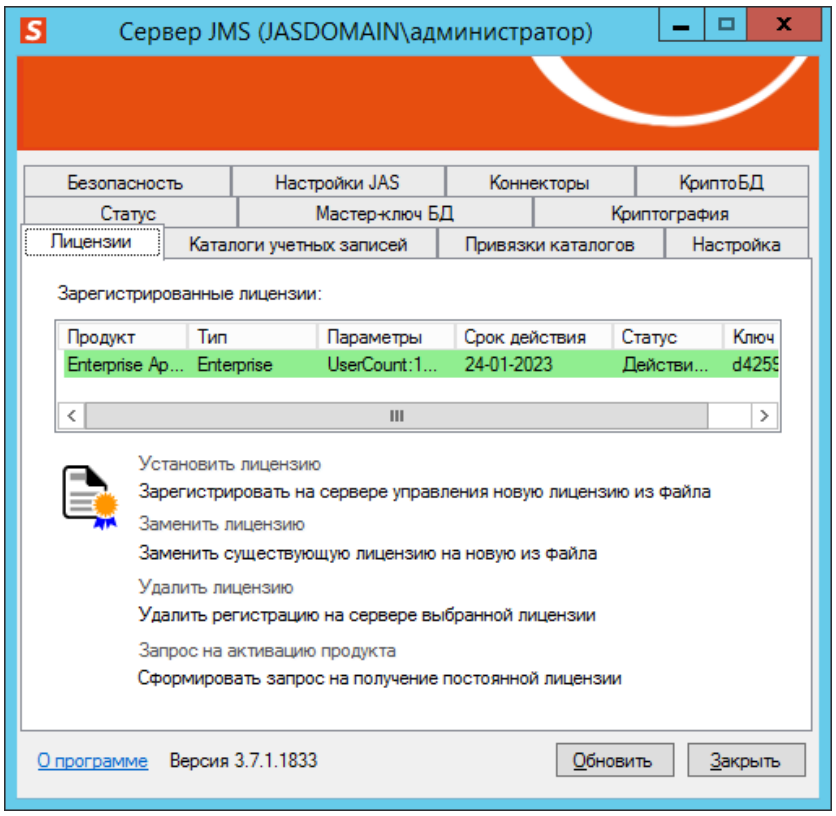



*Рис. 203 – Общий вид вкладки **Лицензии***

Вкладка содержит следующие элементы (см. табл. 36).

*Табл. 36 – Элементы вкладки Лицензии*

| Элемент интерфейса | | Описание |
|---|---|---|
| Таблица **Зарегистрированные лицензии** | Столбец **Продукт** | Отображает компонент JMS, к которому применяется лицензия. |
| | Столбец **Тип** | Отображает версию поставки продукта (тип лицензии):<br>• **Enterprise** – JaCarta Management System Enterprise Edition<br>• **CA Edition** – JaCarta Management System CA Edition |
| | Столбец **Параметры** | Отображает дополнительные параметры лицензии. |
| | Столбец **Срок действия** | Отображает срок действия лицензии. |
| | Столбец **Статус** | Отображает статус лицензии. |
| | Столбец **Ключ** | Отображает ключ лицензии |

| Элемент интерфейса | Описание |
|---|---|
| Ссылка **Установить лицензию** | Позволяет указать путь к файлу лицензии. |
| Ссылка **Заменить лицензию** | Позволяет заменить текущую лицензию на выбранную пользователем. |
| Ссылка **Удалить лицензию** | Позволяет удалить выбранную лицензию. |
| Ссылка **Запрос на активацию продукта** | Позволяет выполнить запрос на получение лицензии (ссылка активна при использовании активационной лицензии, см. раздел «Активация продукта», с. 176). |

Кнопка **Обновить** позволяет обновить сведения, отображающиеся в таблице **Зарегистрированные лицензии**.

**Примечание.** После установки постоянной лицензии отображается окно **Уведомление об активации продукта**, отображающее сроки действия лицензии, имя контактного лица компании и запрос на подтверждение о прочтении данного уведомления. Для окончания процедуры установки лицензии следует отметить данный флаг и нажать кнопку **Принять**.

### 13.4.1 Версии поставки продукта и лицензионные опции

JMS может поставляться в нескольких версиях (Табл. 37), отличающихся набором функций.

Версия поставки продукта определяется устанавливаемым файлом лицензии. Кроме того, специально сконфигурированная лицензия (файл лицензии) может определять подключение/отключение отдельных возможностей продукта (подробная конфигурация опций определяется частным соглашением с заказчиком).

**Важно!**

1. Параметры лицензии отображаются в разделе **Настройки -> Лицензии** консоли управления JMS.
2. Каждая лицензия обеспечивает функционирование продукта только в течение указанного в ней срока (параметры **Дата начала действия** и **Дата окончания действия** в разделе **Настройки -> Лицензии**). По окончании срока действия лицензии ключевые функции JMS блокируются (продукт перестает работать). Для продления нормального функционирования продукта необходимо приобрести и установить лицензию на очередной срок эксплуатации.
3. Лицензия JMS обычно поставляется с условием привязки к домену Active Directory (параметр **Домен** в раздел **Настройки** -> **Лицензии** консоли управления JMS). В случае если сервер JMS развернут вне этого домена (или его поддомена), функции JMS блокируются.

*Табл. 37 – Версии поставки продукта и лицензионные опции*

| Версия поставки продукта / опция лицензии | Описание |
|---|---|
| **JaCarta Management System Enterprise Edition**<br>(Версия продукта, определяется лицензией. Краткое название версии – **Enterprise.** Версия отображается в параметре **Тип** в раздел **Настройки** -> **Лицензии** консоли управления JMS) | Полнофункциональная версия продукта, обеспечивающая автоматизацию администрирования электронных ключей на предприятии с использованием ПО Клиент JMS на рабочих станциях. |
| **JaCarta Management System CA Edition** | Версия предназначена для заказчиков, использующих JMS для выпуска большого числа электронных ключей без необходимости автоматически администрировать электронные ключи посредством ПО |

| Версия поставки продукта / опция лицензии | Описание |
|---|---|
| (Версия продукта, определяется лицензией. Краткие названия версии – **CA**, **CA Edition.** Версия отображается в параметре **Тип** в раздел **Настройки** -> **Лицензии** консоли управления JMS) | Клиент JMS (типичные заказчики такой конфигурации – удостоверяющие центры).<br><br>В данной версии отключена возможность использования компонента JMS Client на рабочих станциях, с чем связаны следующие особенности пользовательского интерфейса:<br>• в *Консоли управления JMS* отсутствует раздел **Рабочие станции**, а также все управляющие элементы, связанные с настройками ПО *Клиент JMS*;<br>• в серверном агенте *Сервер JMS* отсутствуют настройки сервиса аутентификации для ПО *Клиент JMS* и другие связанные с ним настройки. |
| **Лицензия на право использования ПО «Учет СКЗИ»**<br><br>(Опция в рамках файла лицензии для поставляемой версии продукта) | Лицензия обеспечивает включение функции «Учет СКЗИ». Лицензия регулирует число экземпляров СКЗИ, которые могут быть зарегистрированы и администрироваться посредством JMS (подробнее порядок регулирования системе см. «Руководство администратора. Часть 2» [3], раздел «Консоль управления JMS» -> «Учет СКЗИ»). |
| **Лицензия на право использования функции «Поддержка USB-токенов и смарт-карт сторонних производителей»**<br><br>(Опция в рамках файла лицензии для поставляемой версии продукта) | Лицензия обеспечивает поддержку электронных ключей сторонних производителей, а именно компаний: ISBC GROUP, «Актив» и SafeNet.<br><br>Лицензия регулирует число поддерживаемых электронных ключей сторонних производителей. При превышении числа зарегистрированных электронных ключей функции регистрация новых электронных ключей становится недоступна.<br><br>Число доступных для регистрации электронных ключей уменьшается в момент регистрации электронного ключа в JMS и увеличивается в момент его удаления из JMS (см. «Руководство администратора. Часть 2» [3], раздел «Жизненный цикл электронного ключа») |
| **Лицензия на право использования ПО «Поддержка внешних УЦ» продукта JaCarta Management System на 1 пользователя**<br><br>(Опция в рамках файла лицензии для поставляемой версии продукта) | Лицензия позволяет использовать коннекторы JMS к внешним УЦ:<br>• УЦ КриптоПро 1.5<br>• УЦ КриптоПро 2.0<br>• УЦ ViPNet 4.6<br>• УЦ Notary-Pro 2.7<br>для выпуска сертификатов.<br><br>Лицензия на использование конкретного удостоверяющего центра регулирует число пользователей, для которых доступен выпуск сертификата в УЦ указанного производителя/версии. (В случае если пользователь, для которого выпущен сертификат, заблокирован, или действие его сертификата прекращено, лицензия для данного пользователя возвращается в пул лицензий данного типа.) |
| **Лицензия на право использования опции "Поддержка JaCarta Authentication Server" ПО JaCarta Management System**<br><br>(Опция в рамках файла лицензии для поставляемой версии продукта) | Лицензия обеспечивает возможность использования функций сервера аутентификации JAS (JaCarta Authentication Server) рамках поставленной версии JMS. Об установке и настройке сервера JAS см. часть 3 руководства администратора [4]. |

**Примечание.** Настоящая таблица описывает только лицензионные опции, связанные с операциями конфигурирования продукта из ПО *Консоль управления JMS* и *Сервер JMS*. Подробную актуальную информацию о правилах лицензирования с описанием всех лицензионных опций следует запрашивать у производителя продукта

### 13.4.2 Активация продукта

С операцией установки файла лицензии связана процедура активации продукта.

Изначально продукт поставляется с «активационной» лицензией. После установки такой лицензии работа продукта в полнофункциональном режиме возможна лишь на протяжении «активационного» периода, определённого в такой лицензии (обычно 2 недели, Рис. 204).

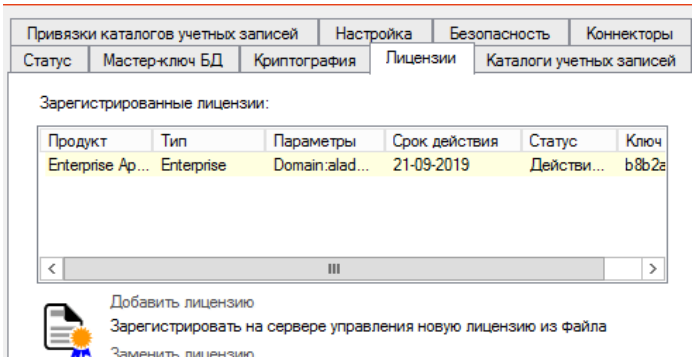



*Рис. 204 – Отображение активационной лицензии*

По окончании активационного периода все основные функции продукта (кроме возможности замены/установки лицензии) блокируются до момента установки постоянной лицензии, Рис. 205.

**Примечание.** Активационный период обеспечивает функционирование продукта в тестовом режиме и не входит в фактически оплаченный период действия пользовательской лицензии на продукт.

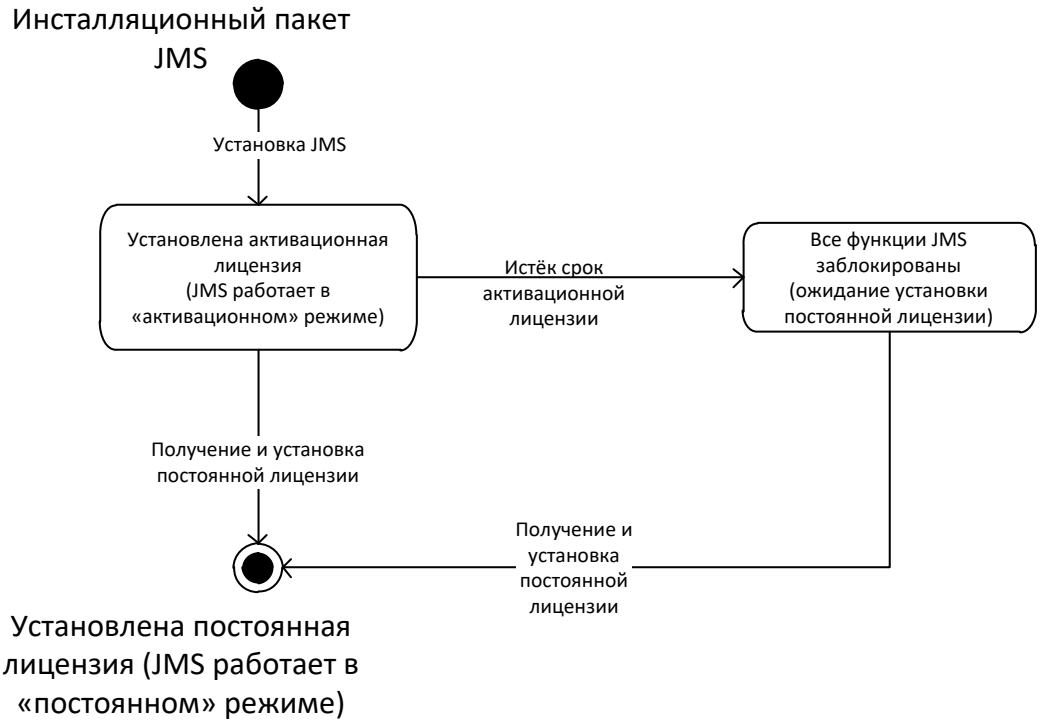



*Рис. 205 – Диаграмма переходов для процедуры активации JMS*

Для перевода продукта в режим обычной работы («постоянный» режим), следует установить постоянную лицензию (выдается производителем пользователю JMS после создания им файла «Запрос на активацию», который генерируется в интерактивном режиме из программ **Сервер JMS** или **Консоль управления JMS**).

В момент установки активационной лицензии пользователю выводится уведомление о необходимости активации продукта (Рис. 206)

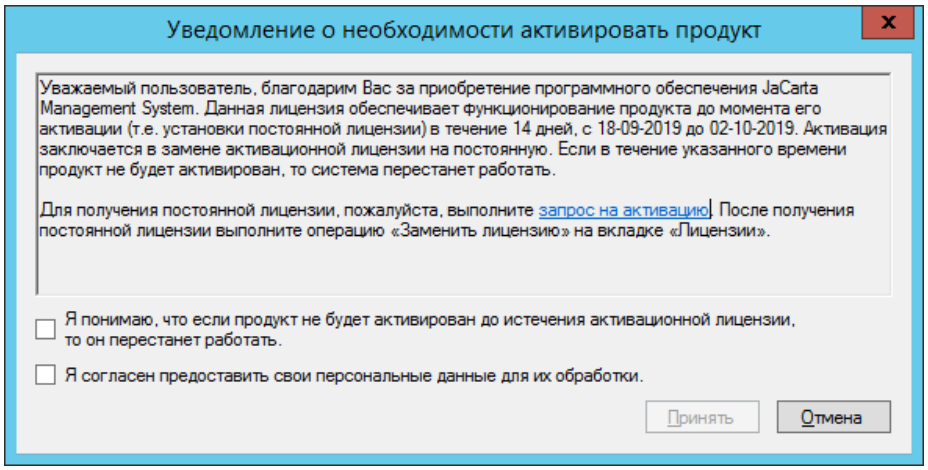



*Рис. 206 – Уведомление о необходимости активации продукта*

В этом окне пользователь должен ввести подтверждения о том, что ознакомлен с данным уведомлением, а также может запустить процедуру составления запроса на получение постоянной лицензии.

Для формирования запроса на получение постоянной лицензии следует нажать на ссылку **запрос на активацию**. При этом отобразится окно следующего вида (Рис. 207).

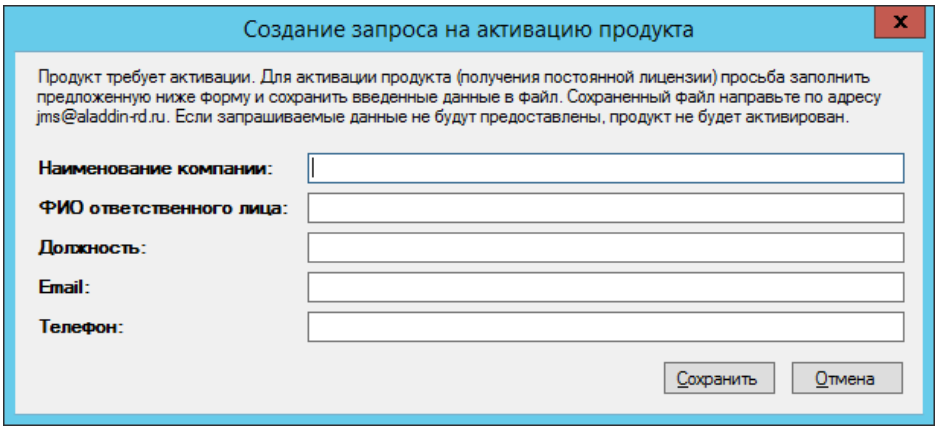



*Рис. 207 – Форма запроса учетных данных пользователя JMS*

**Примечания:**

Запрос на активацию можно сформировать позже из консоли управления следующими способами.

1. Из справочного окна **О программе** консоли управления JMS. Для этого в консоли управления JMS в верхней панели любого раздела нажмите **О программе** и в появившемся окне (Рис. 208) нажмите на ссылку **Активация продукта**.
2. В течение действия активационной лицензии при вызове Консоли управления JMS также выдается предупреждение о необходимости активации продукта и предлагается сформировать запрос на активацию.

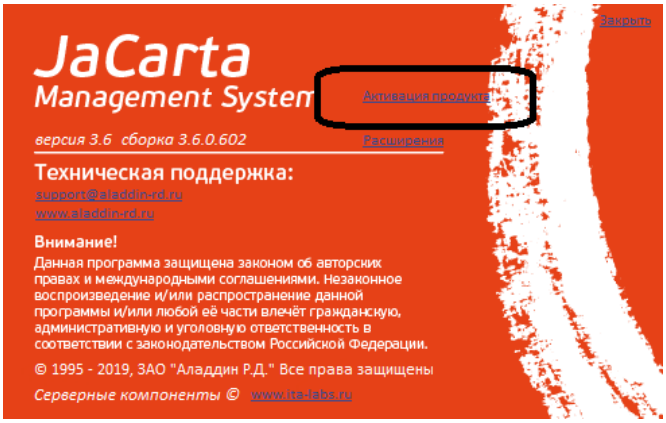



*Рис. 208 – Вызов формы запроса на активацию через окно **О программе***

Заполните поля формы создания запроса на активацию, сохраните запрос в виде PDF-файла и отправьте на указанный адрес электронной почты. По получении ответа следует установить в JMS постоянную лицензию, используя ссылку **Заменить лицензию** на вкладке **Лицензии** серверного агента (Рис. 203, с. 173).

После установки постоянная лицензия будет выглядеть следующим образом (Рис. 209).

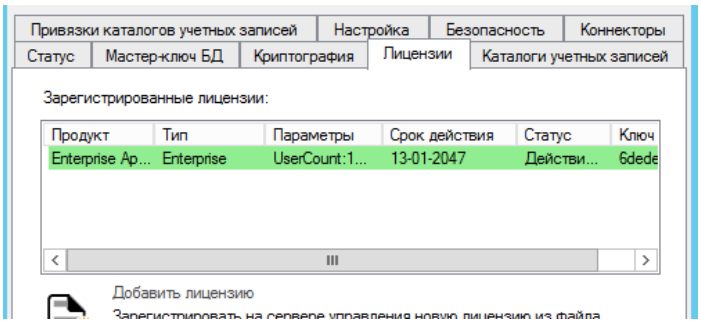



*Рис. 209 – Отображение постоянной лицензии*

## 13.5 Каталоги учетных записей

Вкладка **Каталоги учетных записей** содержит сведения о зарегистрированных каталогах учетных записей и выглядит следующим образом.

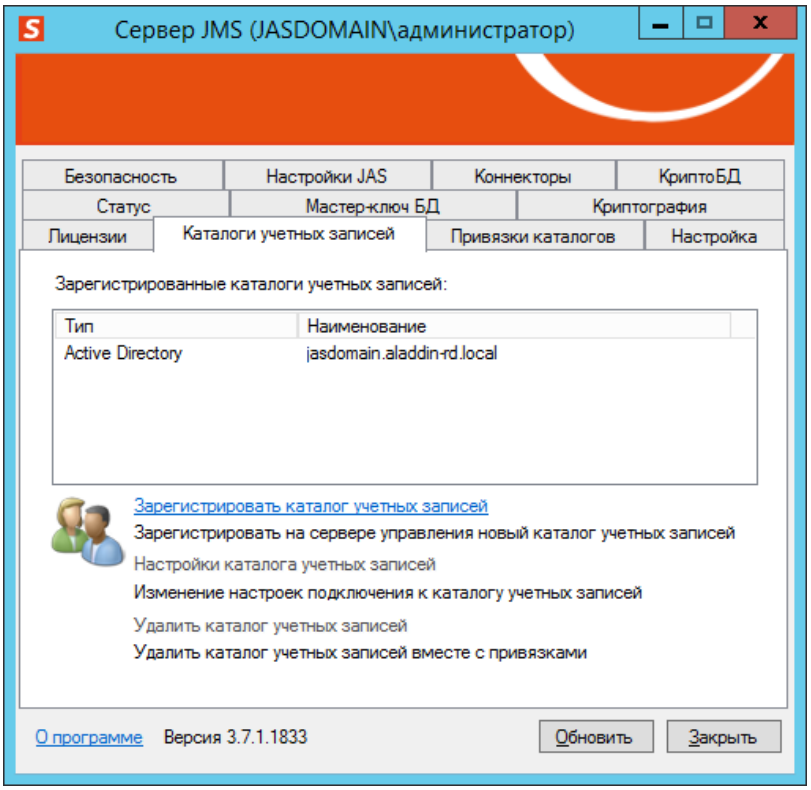



*Рис. 210 – Вкладка Каталоги учетных записей*

Вкладка содержит следующие элементы (см. табл. 38)

*Табл. 38 – Элементы вкладки Каталоги учетных записей*

| Элемент интерфейса | | Описание |
|---|---|---|
| Таблица **Зарегистрированные каталоги учетных записей** | Столбец **Тип** | Отображает тип зарегистрированного каталога учетных записей. |
| | Столбец **Наименование** | Отображает имя зарегистрированного каталога учетных записей. |
| Ссылка **Зарегистрировать каталог учетных записей** | | Позволяет зарегистрировать новый каталог учетных записей (для Active Directory аналогично процедуре первоначальной конфигурации – подробнее см. «Настройка каталога учетных записей», с. 77). |
| Ссылка **Настройка каталога учетных записей** | | Позволяет изменить настройку выбранного каталога учетных записей (например, изменить служебную учетную запись или изменить список используемых атрибутов учетных записей пользователей). |

| Элемент интерфейса | Описание |
|---|---|
| Ссылка **Удалить каталог учетных записей** | Позволяет удалить выбранный каталог учетных записей<br><br>**Важно!**<br>1. Перед выполнением данной операции следует сделать резервную копию БД JMS.<br>2. В случае если данная операция выполняется в кластерной конфигурации JMS на одном из узлов NLB-кластера, то следует остановить все остальные узлы кластера JMS.<br><br>**Примечание.** Операция доступна только для дополнительных каталогов учетных записей. Операция недоступна для основного каталога учетных записей (устанавливается первым) |

Кнопка **Обновить** позволяет обновить отображаемые данные.

## 13.6 Привязки каталогов учетных записей

JMS позволяет связать учетные записи пользователей из разных ресурсных систем (например, из Active Directory и из КриптоПро УЦ 2.0) по совпадающему атрибуту - например, по адресу электронной почты. Таким образом, после осуществления привязки две учетные записи в разных ресурсных системах будут восприниматься как одна. Это позволит избежать путаницы при назначении и дальнейшем управлении электронными ключами пользователей.

Чтобы связать учетные записи из разных ресурсных систем, выполните следующие действия.

Связываемые ресурсные системы должны быть уже зарегистрированы в JMS (см. «Каталоги учетных записей» выше).

1. Откройте окно управления сервером JMS и перейдите на вкладку Привязки каталогов учетных записей.
   Окно будет иметь следующий вид.

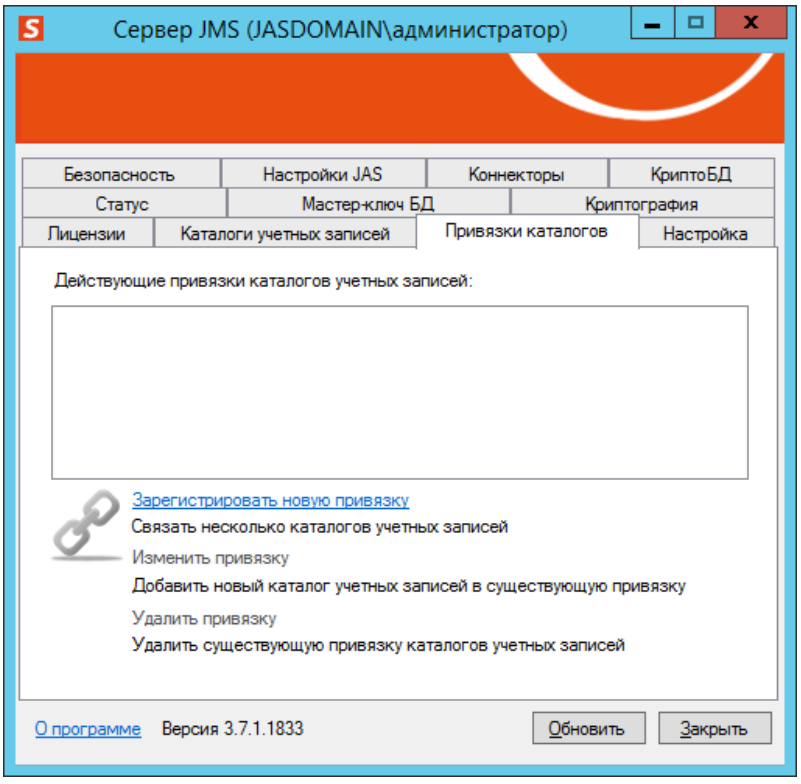



*Рис. 211 – Вкладка **Привязки каталогов учетных записей***

2. Щелкните на ссылке **Зарегистрировать новую привязку**.

Действие необратимо. После создания привязки к каталогу учетных записей удалить такую привязку невозможно.

Отобразится следующее окно.

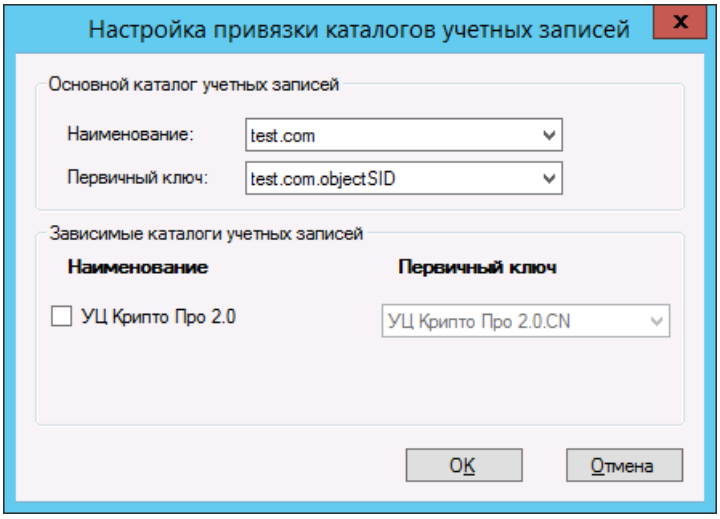



*Рис. 212 – Настройка привязки каталогов учетных записей*

3. Выполните настройку, руководствуясь табл. 39.

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

*Табл. 39 - Настройка привязки каталогов учетных записей*

| Секция | Настройка | Описание |
|---|---|---|
| **Основной каталог учетных записей** | **Наименование** | Имя основного каталога учетных записей. |
| | **Первичный ключ** | Атрибута учетной записи из основного каталога, по которому будет происходить сопоставление учетных записей из разных каталогов. В настоящем документе для примера будет использоваться атрибут **mail** (адрес электронной почты). |
| **Зависимые каталоги учетных записей** | **Наименование** | Имя зависимого каталога учетных записей. |
| | **Первичный ключ** | Атрибут учетной записи из зависимого каталога, по значению которого учетные записи из зависимого каталога будут сопоставляться с учетными записями из основного каталога. Например, в КриптоПро УЦ 2.0 атрибут, содержащий адрес электронной почты пользователя, называется **E**. Таким образом, для примера связывания учетных записей в настоящем документе будет использоваться сопоставление значений атрибуте **mail** из Active Directory и атрибута **E** из КриптоПро УЦ 2.0. |

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

Отобразится следующее сообщение.

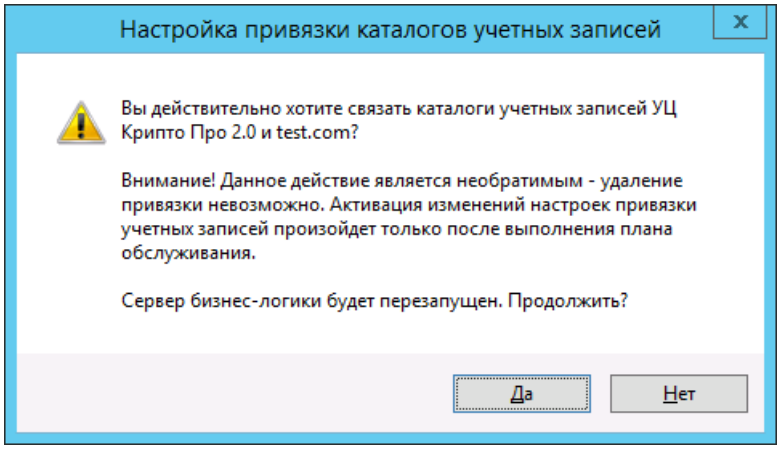



*Рис. 213 – Предупреждение о необратимости привязки*

5. Нажмите **Да**.
   Отобразится следующее окно.

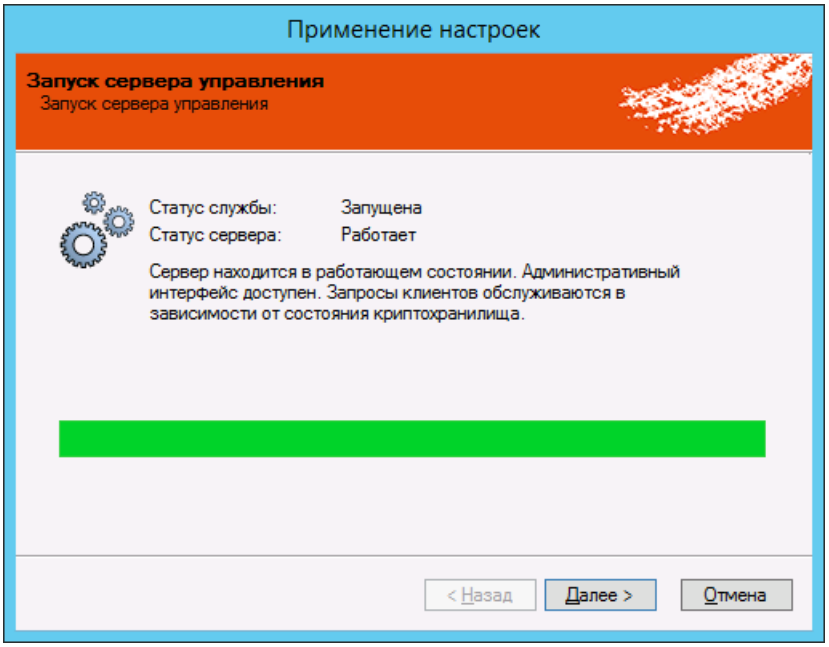



*Рис. 214 – Запуск сервера управления*

6. Нажмите **Далее**.

Отобразится следующее окно.

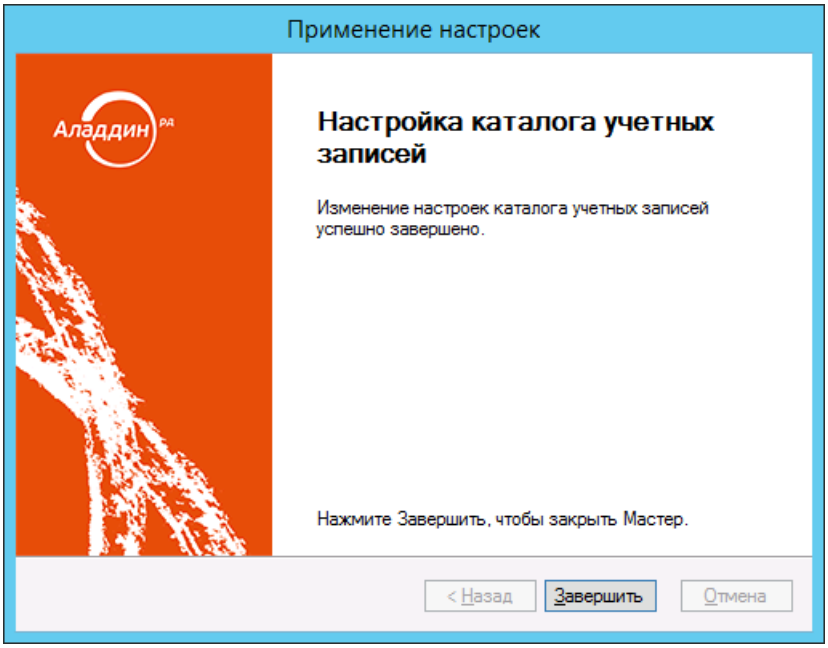



*Рис. 215 – Окно завершения процедуры привязки каталога учетных записей*

Привязка отобразится в окне управления сервером JMS.

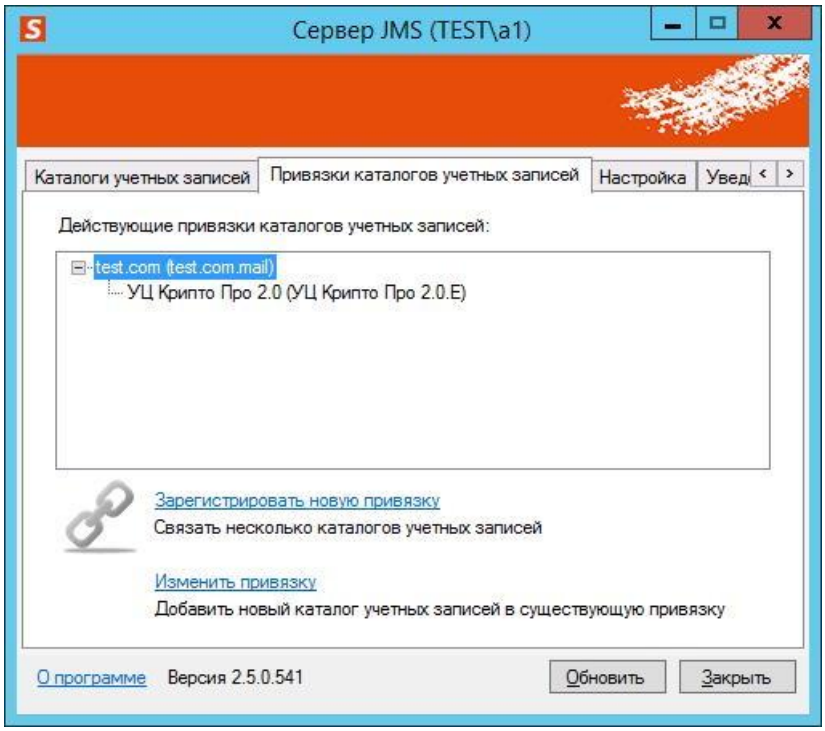



*Рис. 216 – Действующие привязки каталогов учетных записей*

Чтобы зарегистрировать пользователей из связанных ресурсных систем (каталогов учетных записей), выполните действия, приведенные в документе «Руководство администратора. Часть 2» [3], раздел «Регистрация пользователей из связанных каталогов учетных записей».

## 13.7 Настройка

### 13.7.1 Общий вид вкладки Настройка

Вкладка **Настройка** выглядит следующим образом.

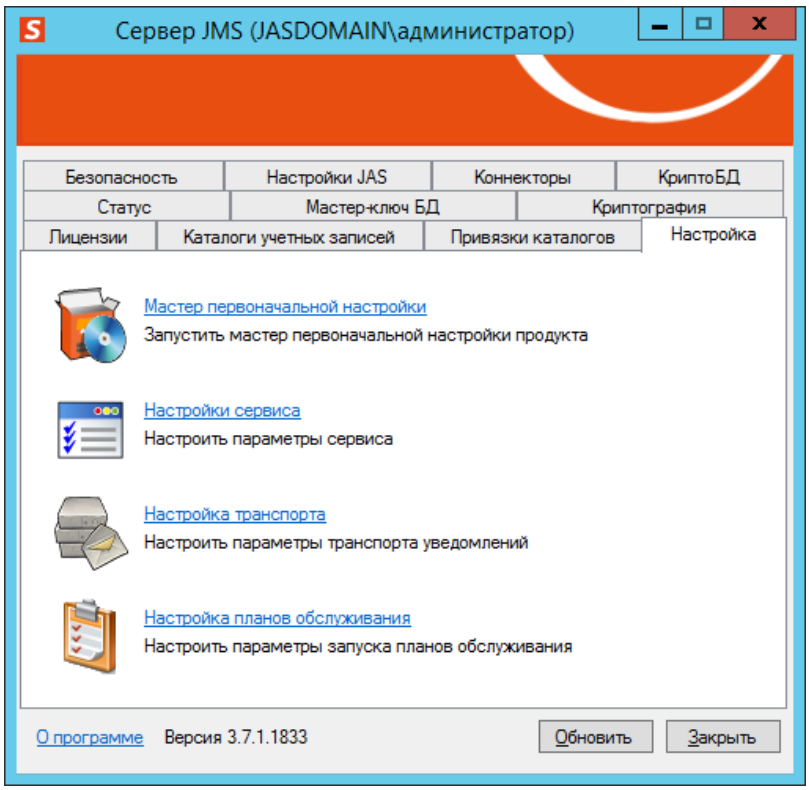



*Рис. 217 – Вкладка Настройка*

Вкладка содержит следующие элементы (см. табл. 40).

*Табл. 40 – Элементы вкладки Настройка*

| Элемент интерфейса | Описание |
|---|---|
| Ссылка **Мастер первоначальной настройки** | Запускает мастер первоначальной настройки конфигурации JMS – подробнее см. «Начало процедуры и выбор конфигурации», с. 75. |
| Ссылка **Настройки сервиса** | Отображает окно настройки серверной службы Aladdin EAP Engine Service – подробнее см. «Настройки сервиса (службы) Aladdin EAP Engine Service», с. 185. |
| Ссылка **Настройка транспорта** | Позволяет указать параметры SMTP- и/или Syslog-сервера для отправки уведомлений – подробнее см. «Настройка транспорта», с. 186. |
| Ссылка **Настройка планов обслуживания** | Позволяет отключить выполнение планов обслуживание на данном сервере JMS – подробнее см. «Настройка планов обслуживания», с. 189. |

### 13.7.2 Настройки сервиса (службы) Aladdin EAP Engine Service

Окно настройки серверной службы Aladdin EAP Engine Service выглядит следующим образом.

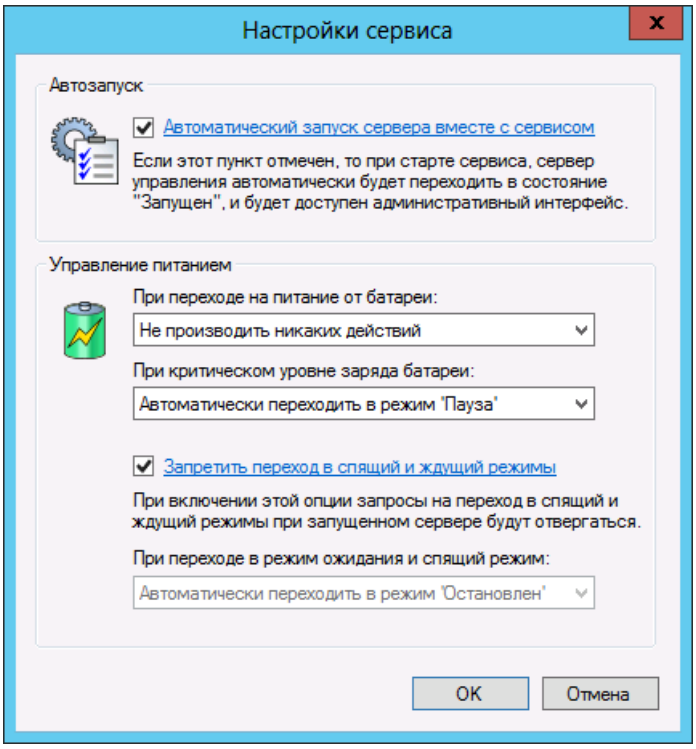



*Рис. 218 – Окно настройки серверной службы Aladdin EAP Engine Service*

Доступны следующие настройки (см. табл. 41).

*Табл. 41 – Настройки серверной службы Aladdin EAP Engine Service*

| Настройка | Описание |
|---|---|
| Флаг **Автоматический запуск сервера вместе с сервисом** | Если флаг установлен, при запуске службы автоматически будет запускаться сервер управления JMS, предоставляя доступ к административному интерфейсу. |
| Список **При переходе на питание от батареи** | Позволяет настроить параметры работы серверной службы при переходе на питание от батареи. Список содержит следующие пункты:<br>• **Не производить никаких действий**;<br>• **Автоматически переходить в режим 'Пауза'**;<br>• **Автоматически переходить в режим 'Остановлен'**. |
| Список **При критическом уровне заряда батареи** | Позволяет настроить параметры работы серверной службы при критическом уровне заряда батареи. Список содержит следующие пункты:<br>• **Не производить никаких действий**;<br>• **Автоматически переходить в режим 'Пауза'**;<br>• **Автоматически переходить в режим 'Остановлен'**. |
| Флаг **Запретить переход в спящий и ждущий режимы** | Если флаг установлен, запросы на переход в спящий и ждущий режимы при запущенном сервере будут отвергаться. |

| Настройка | Описание |
|---|---|
| Список **При переходе в режим ожидания и спящий режим** | Список активен, только если снят флаг **Запретить переход в спящий и ждущий режим**. Список содержит следующие пункты:<br>• **Не производить никаких действий**;<br>• **Автоматически переходить в режим 'Пауза'**;<br>• **Автоматически переходить в режим 'Остановлен'**. |

### 13.7.3 Настройка транспорта

Чтобы включить возможность рассылки уведомлений по электронной почте и настроить параметры соединения с почтовым сервером, выполните следующие действия.

1. В окне управления сервером JMS перейдите на вкладку **Настройка** и щелкните на ссылке **Настройка транспорта**.
   Отобразится следующее окно.

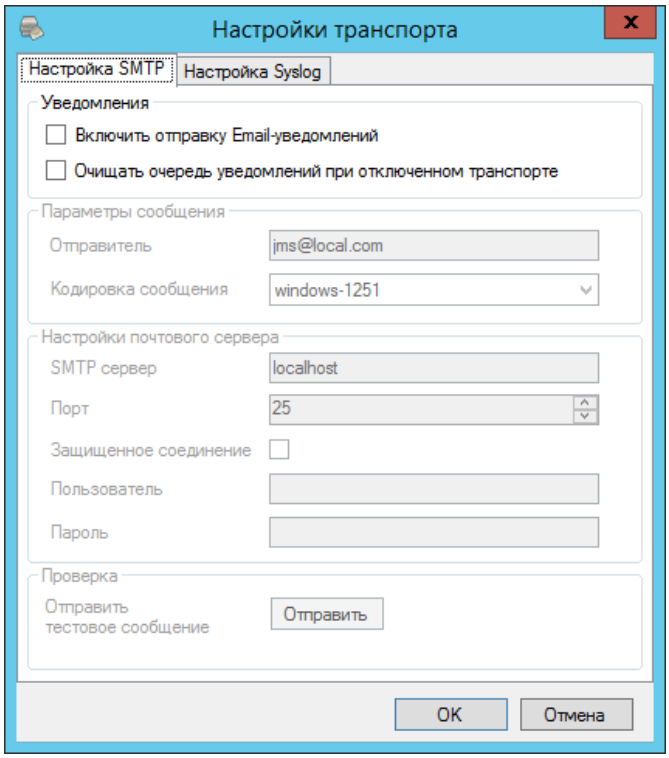



*Рис. 219 – Настройка SMTP*

2. Выполните настройку, руководствуясь табл. 42.

*Табл. 42 – Настройка параметров уведомлений*

| Настройка | Описание |
|---|---|
| <Секция> **Уведомления** | |
| **Включить отправку Email-уведомлений** | После установки этого флага становятся активными настройки соединения с почтовым сервером. |

| Настройка | Описание |
|---|---|
| **Очищать очередь уведомлений при отключении транспорта** | Опция позволяет удалить «зависшие» уведомления в очереди, которые были сформированы некорректными настройками транспорта. |
| <Секция> **Параметры сообщения** | |
| **Отправитель** | Укажите адрес электронной почты, который будет значиться в качестве отправителя в уведомлениях.<br>**Примечание.** Некоторые SMTP-серверы не поддерживают указание отправителя, в этом случае в поле **Отправитель** следует указать фактический адрес почтового аккаунта пользователя (то же, значение что и в поле **Пользователь**) |
| **Кодировка сообщения** | Выберите используемую кодировку, в которой будут рассылаться уведомления (текст письма):<br>• **windows-1251**;<br>• **utf-8**. |
| <Секция> **Настройки почтового сервера** | |
| **SMTP сервер** | Укажите IP-адрес или полное доменное имя (FQDN) почтового сервера (почтового сервера, с которого будет осуществляться рассылка). |
| **Порт** | Выберите порт подключения к почтовому серверу. |
| **Защищенное соединение** | Установите флаг, если для связи с почтовым сервером необходимо использовать защищенное (SSL/TLS) соединение. Для этого почтовый сервер должен поддерживать режим **StartTLS**. |
| **Пользователь** | Введите адрес электронной почты (учетную запись пользователя), с которого осуществляется рассылка уведомлений, например:<br>*your_post@yandex.ru* |
| **Пароль** | Укажите пароль для выбранной учетной записи (адреса электронной почты), указанной в поле **Пользователь**. |
| <Секция> **Проверка** | |
| **Отправить тестовое сообщение** | Нажмите кнопку с целью проверки корректности введенных данных в полях данного окна. При верных данных на адрес, указанный в поле **Пользователь**, будет доставлено письмо с текстом «Проверка настроек SMTP» |

**Примечание.** После применения сделанных настроек SMTP JMS выполнит проверку соединения с почтовым сервером путем отправки тестового сообщения и в случае успеха будет перезапущен. После этого в консоли управления JMS будет разрешена настройка правил рассылки уведомлений по различным событиям системы.

3. Выберите вкладку **Настройка Syslog**.

Отобразится следующее окно.

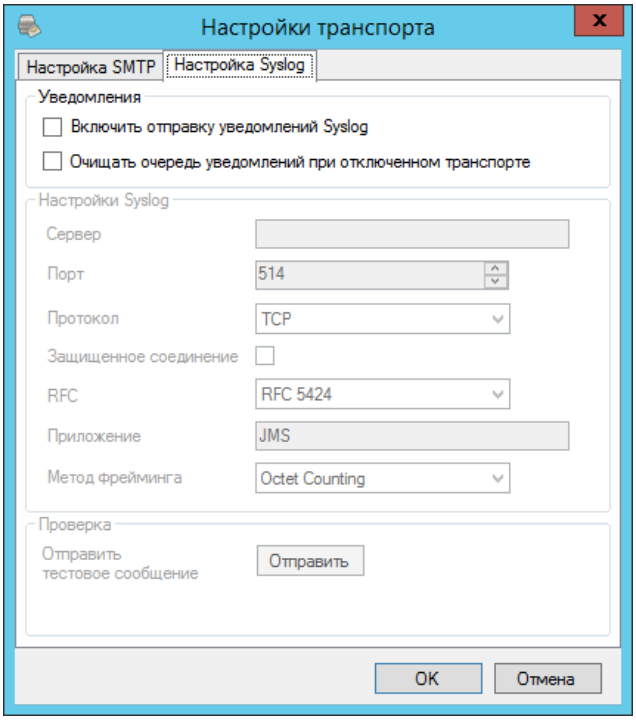



*Рис. 220 – Настройка Syslog*

4. Выполните настройку, руководствуясь Табл. 43.

*Табл. 43 – Настройка параметров взаимодействия с сервером Syslog*

| Настройка | Описание |
|---|---|
| <Секция> **Уведомления** | |
| **Включить отправку уведомлений Syslog** | После установки этого флага становятся активными настройки соединения с Syslog-сервером. |
| **Очищать очередь уведомлений при отключении транспорта** | Опция позволяет удалить «зависшие» уведомления в очереди, которые были сформированы некорректными настройками транспорта. |
| <Секция> **Настройки Syslog** | |
| **Сервер** | Укажите IP-адрес или полное доменное имя (FQDN) Syslog-сервера. |
| **Порт** | Выберите порт подключения к почтовому Syslog-серверу. |
| **Протокол** | Выберите протокол транспортного уровня для работы с Syslog. Возможные варианты:<br>• **TCP** (по умолчанию)<br>• **UDP** |

| Настройка | Описание |
|---|---|
| **Защищенное соединение** | Установите флаг, если для связи с Syslog-сервером необходимо использовать защищенное (SSL/TLS) соединение.<br>Опция доступна только при использовании протокола TCP. |
| **RFC** | Выберите спецификацию Syslog для работы с сервером.<br>Возможные варианты:<br>• **RFC 5424** (по умолчанию)<br>• **RFC 3164**<br>**Примечание.** Рекомендуется использовать RFC5424, т.к. стандарт RF3164 подразумевает, что сообщение может содержать только печатные символы из таблицы ASCII с кодами в диапазоне от 32 до 126. При выборе RFC3164 невозможна передача кириллицы |
| **Приложение** | Текстовый идентификатор приложения (используется в выходных данных Syslog для идентификации приложения)<br>Значение по умолчанию: **JMS** |
| **Метод фрейминга** | Метод определения границ сообщения в случае, если одновременно посылается несколько сообщений<br>Возможные варианты:<br>• **Octet Counting** (по умолчанию) – в начале каждого Syslog-сообщения устанавливается его длина для определения границ сообщения;<br>• **Not-Transparent-Framing** – сообщения могут разделяться следующими символами: ASCII LF, ASCII NUL или последовательностью символов CR и LF |
| <Секция> **Проверка** | |
| **Отправить тестовое сообщение** | Нажмите кнопку с целью проверки корректности введенных данных в полях данного окна. При верных данных на сервер будет отправлено тестовое сообщение. |

5. По завершении настроек нажмите **OK** – в случае корректных настроек сервер JMS будет перезапущен, после чего настройки вступят в силу.

### 13.7.4 Настройка планов обслуживания

Окно планов обслуживания выглядит следующим образом.

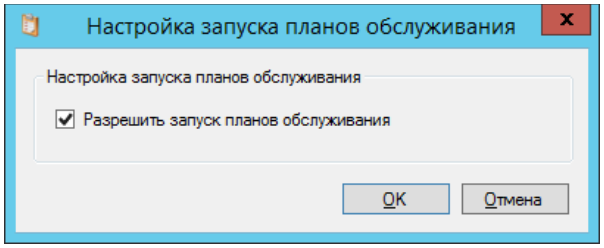



*Рис. 221 – Окно настройки планов обслуживания*

В случае если на сервере JMS необходимо отключить выполнение планов обслуживания сбросьте флаг **Разрешить запуск планов обслуживания**.

**Примечание.** Для того чтобы выполнение планов обслуживания было отключено в кластере JMS следует отключить выполнение планов обслуживание на всех узлах кластера.

## 13.8 Безопасность

### 13.8.1 Общий вид вкладки Безопасность

Вкладка **Безопасность** выглядит следующим образом.

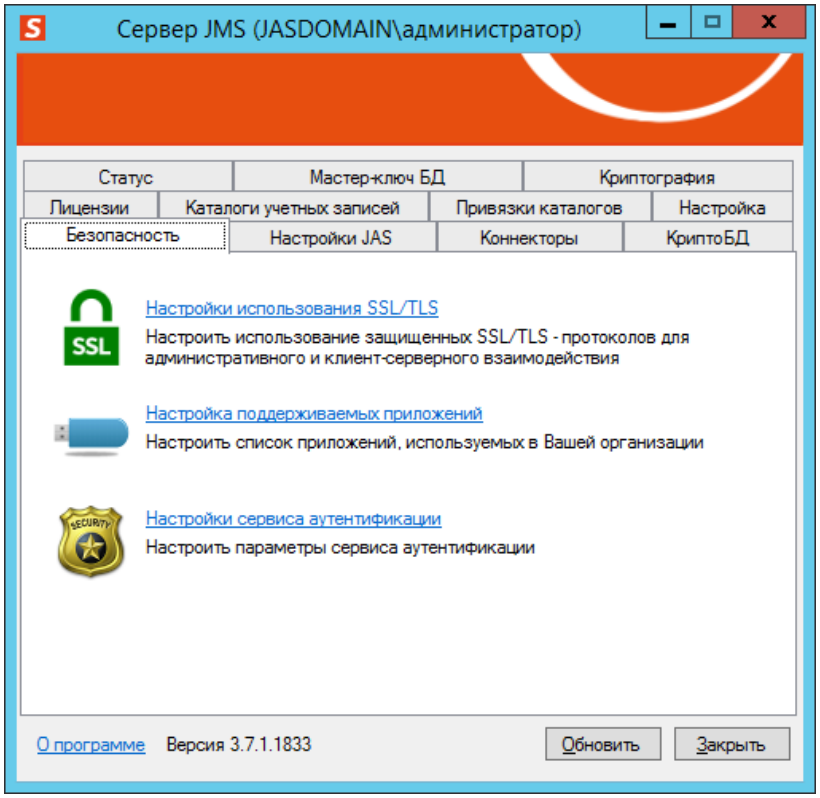



*Рис. 222 – Вкладка Безопасность*

Вкладка содержит следующие элементы (см. Табл. 44).

*Табл. 44 – Элементы вкладки Безопасность*

| Элемент интерфейса | Описание |
|---|---|
| Ссылка **Настройки протокола SSL/TLS** | Позволяет установить/запретить использование протоколов SSL/TLS при исходящих соединениях – подробнее см. «Настройки использования SSL/TLS», с. 191. |

| Элемент интерфейса | Описание |
|---|---|
| Ссылка **Настройка поддерживаемых приложений** | Позволяет скрыть приложения в электронных ключах (апплеты), которые не планируется использовать при эксплуатации JMS – подробнее см. «Настройка поддерживаемых приложений», с. 193. |
| Ссылка **Настройки сервиса аутентификации**<br>(Ссылка отсутствует в версии продукта JMS *CA Edition*) | Позволяет настроить службу аутентификации JMS – подробнее см. «Настройки сервиса аутентификации JMS», с. 194. |

### 13.8.2 Настройки использования SSL/TLS

Перед настройкой SSL-соединения на стороне сервера JMS убедитесь, что в хранилище сертификатов на сервере JMS установлены необходимые сертификаты. Для этого выполните следующие действия.

1. Откройте окно хранилища сертификатов компьютера на сервере JMS.
2. В отобразившемся окне выберите **Сертификаты (локальный компьютер) -> Личное -> Сертификаты**.
   Выпущенный сертификат для поддержки SSL-соединения с сервером JMS (см. «Выпуск сертификата в хранилище сертификатов компьютера», с. 42) отобразится в списке сертификатов компьютера (Рис. 223).

**Важно!** В случае запуска службы сервера JMS от имени служебной учетной записи (см. раздел «Настройка служебной учетной записи», с. 89) SSL-сертификаты сервера следует поместить в личное хранилище пользователя, от имени которого будет запускаться служба сервера.

Для обеспечения возможности SSL-соединения сервера JMS с Консолью управления JMS (JMS Admin) и клиентом JMS (JMS Client) можно использовать как один сертификат, так и два разных сертификата.

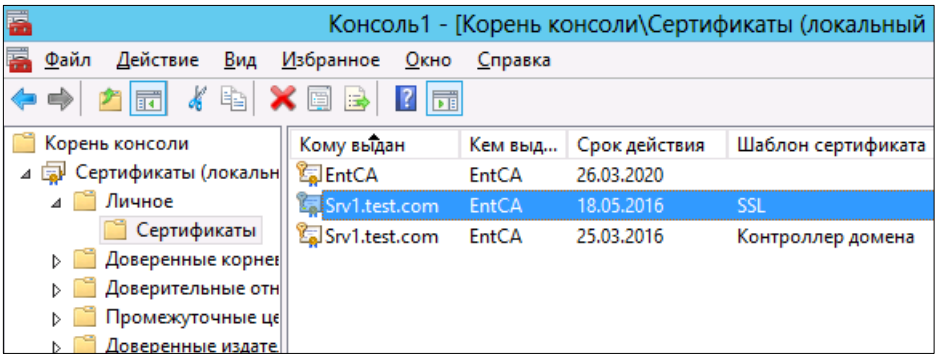



*Рис. 223 – Проверка наличия SSL-сертификата в хранилище «Личное» локального компьютера*

Чтобы настроить протоколы SSL/TLS выполните следующие действия.

1. В окне управления сервером JMS перейдите на вкладку **Безопасность** и нажмите **Настройки использования SSL/TLS**.

Отобразится следующее окно.

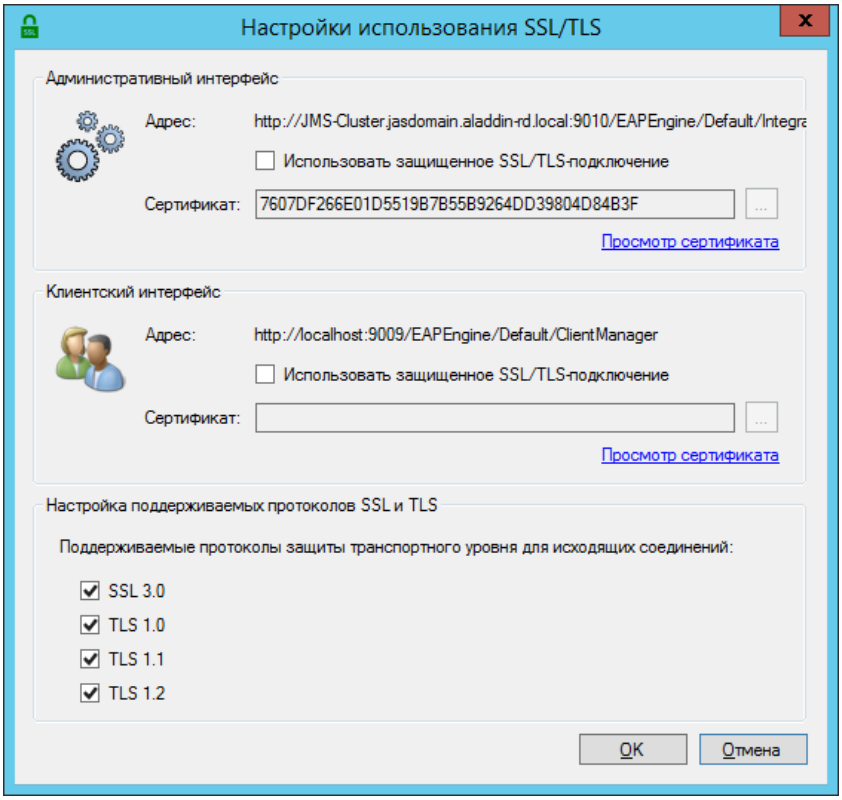



*Рис. 224 – Настройки протокола SSL/TLS*

2. Выполните настройки, руководствуясь Табл. 45.

*Табл. 45 – Настройки использования SSL/TLS*

| Элемент интерфейса | Описание |
|---|---|
| <Секция> **Административный интерфейс**<br>(API-интерфейс сервера JMS для обращения из компонента JMS Admin, или Консоли управления JMS) | |
| **Адрес** | Адрес административного интерфейса (считывается из реестра) |
| **Использовать защищенное SSL/TLS-подключение** | Установите флаг, если соединение должно осуществляться по протоколу SSL/TLS |
| **Сертификат** | Нажмите кнопку … и выберите сертификат, который должен использоваться в протоколах SSL/TLS со стороны сервера JMS<br>(Поле доступно для редактирования только при установленном флаге **Использовать защищенное SSL/TLS-подключение**) |
| Ссылка **Просмотр сертификата** | Нажмите для просмотра свойств установленного сертификата |
| <Секция> **Клиентский интерфейс**<br>(API-интерфейс сервера JMS для обращения из компонента JMS Client, или Клиента JMS) | |
| **Адрес** | Адрес клиентского интерфейса (считывается из реестра) |

| Элемент интерфейса | Описание |
|---|---|
| **Использовать защищенное SSL-соединение** | Установите флаг, если соединение должно осуществляться по протоколу SSL/TLS |
| **Сертификат** | Нажмите кнопку … и выберите сертификат, который должен использоваться в протоколах SSL/TLS со стороны сервера JMS<br>(Поле доступно для редактирования только при установленном флаге **Использовать защищенное SSL/TLS-подключение**) |
| Ссылка **Просмотр сертификата** | Нажмите для просмотра свойств установленного сертификата |
| <Секция> **Настройка поддерживаемых протоколов SSL и TLS** | |
| **Поддерживаемые протоколы защиты транспортного уровня для исходящих соединений** | Данная настройка предназначена для определения списка поддерживаемых протоколов защиты транспортного уровня и распространяется только на исходящие соединения (отправка почтовых уведомлений, соединение с внешними системами и др.). По умолчанию в компоненте JMS Server включены все предусмотренные в нем протоколы защиты транспортного уровня.<br>**Важно!** Данная настройка не распространяется на подключения к СУБД MS SQL Server.<br>При необходимости установите/сбросьте флаги протоколов, которые должны / не должны использоваться при исходящих соединениях с внешними системами. Доступные опции:<br>• **SSL 3.0**<br>• **TLS 1.0**<br>• **TLS 1.1**<br>• **TLS 1.2**<br>**Примечание.** Настройка может быть востребована отдельными организациями, использующими JMS, в которых установлен организационный запрет на применение определенных (например устаревших) протоколов защиты данных. |

3. Нажмите **OK**, чтобы сохранить настройки.
4. При включении SSL-соединений будет произведена автоматическая перезагрузка службы сервера JMS.

### 13.8.3 Настройка поддерживаемых приложений

Данная настройка позволяет скрыть приложения в электронных ключах (апплеты), которые не планируется использовать при эксплуатации JMS.

Настройка позволяет снизить сложность административного интерфейса программы (скрыть неиспользуемые профили настроек и фильтры приложений в профилях, а также целые разделы Консоли управления JMS, например разделы для работы с ридерами смарт-карт).

Чтобы настроить поддерживаемые приложения выполните следующие действия.

1. В окне управления сервером JMS перейдите на вкладку **Безопасность** и нажмите **Настройки поддерживаемых приложений**.

Отобразится окно следующего вида.

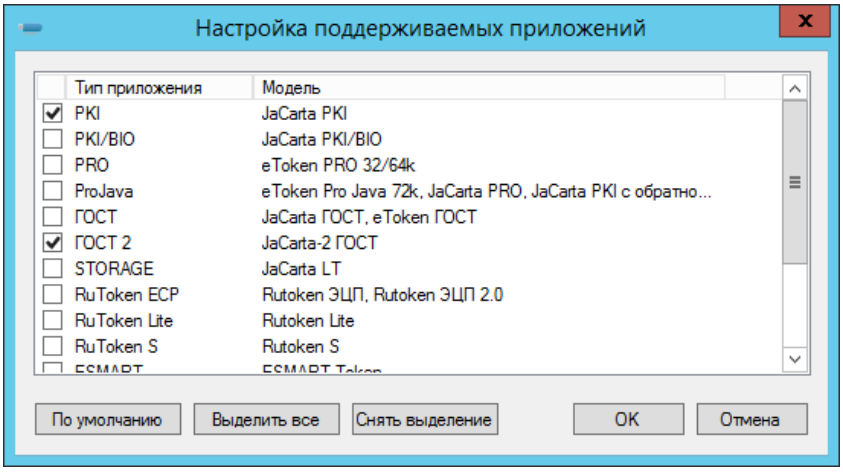



*Рис. 225 – Настройки поддерживаемых приложений*

2. При необходимости установите/сбросьте флаги приложений (апплетов в электронных ключах), которые должны / не должны использоваться в Консоли управления JMS и нажмите **OK**.

**Примечания:**

1. Прежде чем отключить включенное приложение, следует убедиться, что данное приложение (апплет) не был ранее задействован в настройках/профилях JMS, в противном случае отключение флага закончится с ошибкой.
2. Вступление в силу произведенных изменений происходит только после перезапуска сервера JMS (перезапуск производится автоматически с согласия пользователя с отображением соответствующего окна уведомления).

### 13.8.4 Настройки сервиса аутентификации JMS

Исходная настройка сервиса (службы) аутентификации JMS происходит в процессе первоначальной настройки конфигурации. Впоследствии настройки этой службы можно изменить в окне управления сервером JMS.

Чтобы настроить службу аутентификации JMS после первоначальной настройки конфигурации, выполните следующие действия.

1. В окне управления сервером JMS перейдите на вкладку **Безопасность** и щелкните на ссылке **Настройки сервиса аутентификации**.

Отобразится следующее окно.

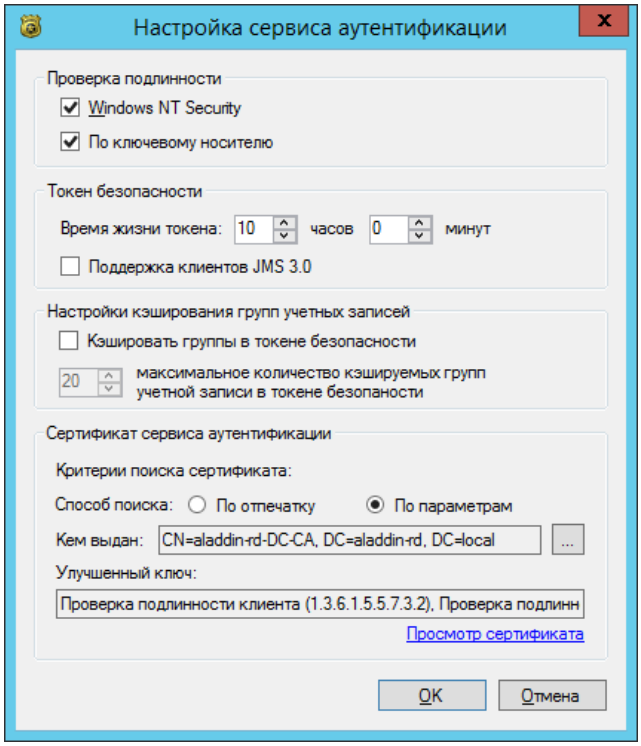



*Рис. 226 – Настройки службы аутентификации JMS*

2. Выполните настройки в секциях **Проверка подлинности**, **Токен безопасности**, **Настройки кэширования групп учетных записей**, руководствуясь Табл. 11, с. 87.
3. В секции **Сертификат сервиса аутентификации** укажите параметры поиска сертификата сервиса аутентификации в режиме **По отпечатку**.
4. Воспользуйтесь кнопкой ..., чтобы выбрать сертификат службы аутентификации JMS.
5. Для сохранения изменений нажмите **ОК** – при этом сервер JMS будет перезапущен, чтобы изменения вступили в силу.

**Важно!** При работе JMS в кластерной конфигурации:

1. После перезапуска сервера JMS настройки службы аутентификации JMS применяются только к текущему узлу. Таким образом, чтобы настройки службы аутентификации JMS применились во всем кластере, необходимо перезапустить все экземпляры сервера JMS (вкладка **Статус** окна управления сервером JMS) - на всех узлах кластера.
2. В случае смены сертификата службы аутентификации JMS на одном узле кластера следует убедиться, что данный сертификат вместе с закрытым ключом установлен также и на остальных узлах кластера.
3. В секции **Сертификат сервиса аутентификации** для поля **Способ поиска** допускается выбор только значения **По отпечатку.**

## 13.9 Коннекторы

Вкладка **Коннекторы** выглядит следующим образом.

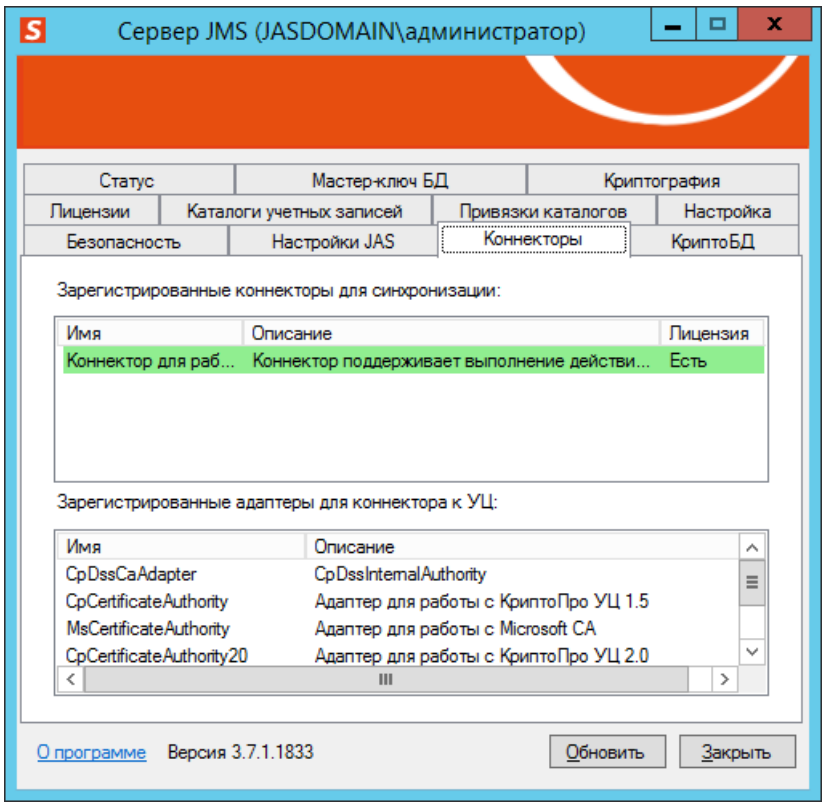



*Рис. 227 – Вкладка **Коннекторы***

На вкладке присутствуют следующие элементы - табл. 46.

*Табл. 46 – Элементы вкладки Коннекторы*

| Элемент | Описание |
|---|---|
| **Зарегистрированные коннекторы** | Список зарегистрированных в JMS коннекторов. |
| **Зарегистрированные адаптеры** | Список установленных адаптеров. (Адаптеры расширяют функциональность установленных коннекторов к удостоверяющим центрам.) |

## 13.10 Настройки JAS

Вкладка **Настройки JAS** выглядит следующим образом.

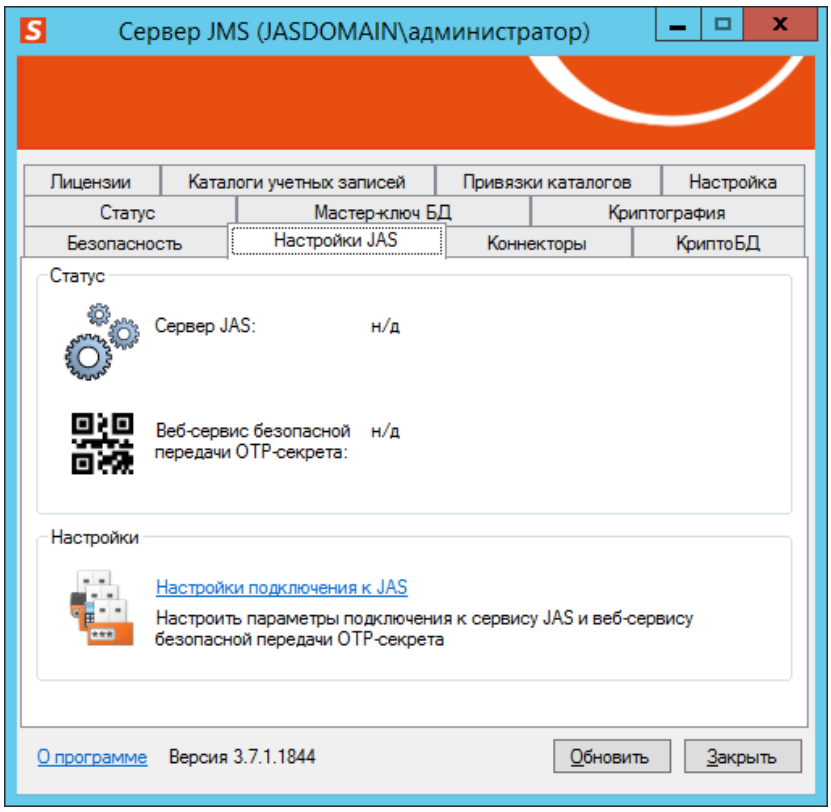



*Рис. 228 – Вкладка **Настройки JAS***

На вкладке присутствуют элементы в соответствии с Табл. 47.

*Табл. 47 – Элементы вкладки Настройки JAS*

| Элемент | Описание |
|---|---|
| **Статус** | Секция с отображением статуса подключения к серверу JAS и web-сервису безопасной передачи OTP-секрета (Aladdin 2FA Service) |
| **Настройки** | Секция с настройками подключения к серверу JAS |

### 13.10.1 Настройка подключения к JAS

Для того чтобы сервер аутентификации JaCarta Authentication Server (JAS) мог нормально функционировать после его установки (см. руководство по установке и настройке JAS [4]) необходимо выполнить подключение к нему сервера JMS.

Для настройки подключения к JAS выполните следующие действия.

1. В приложении Сервер JMS выберите вкладку **Настройки JAS** (Рис. 228, выше) и нажмите **Настройки подключения к JAS**.

Отобразится следующее окно

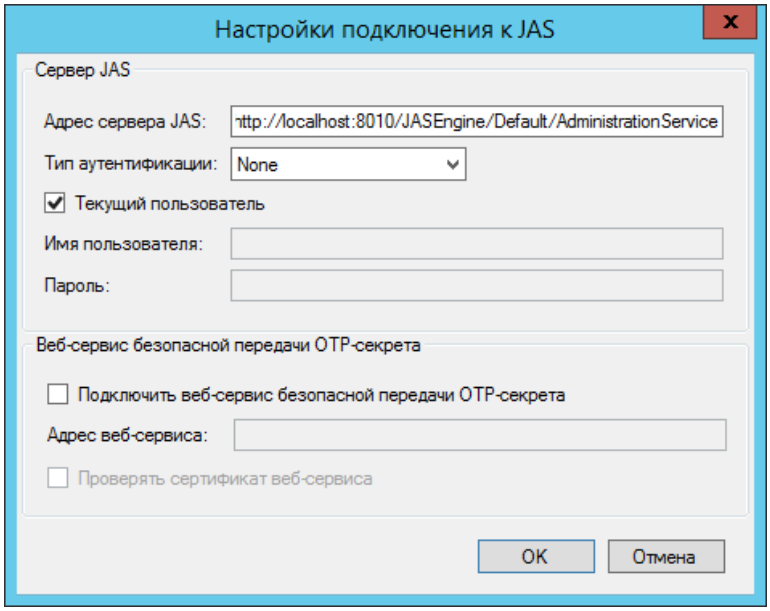



*Рис. 229 – Окно настроек подключения к JAS*

2. Выполните настройку, руководствуясь Табл. 48.

*Табл. 48 – Настройка параметров уведомлений*

| Настройка | Описание |
|---|---|
| <секция> **Сервер JAS** | |
| **Адрес сервера JAS** | Укажите в данном поле адрес в следующем формате<br>`https://<FQDN-имя сервера>:8010/JASEngine/Default/AdministrationService`<br>где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, srv01.test.com<br>Значение по умолчанию:<br>**http://localhost:8010/JASEngine/Default/AdministrationService**<br>**Примечание.** В случае кластерной конфигурации сервера JAS (отказоустойчивого кластера) в качестве параметра <FQDN-имя сервера> должно быть указано DNS-имя роли кластера (отличается от DNS-имени кластера). Подробнее см. настройки для FC-кластера JAS в руководстве по JAS [4]. |
| **Тип аутентификации** | Тип проверки аутентификации.<br>Допустимые значения:<br>• **None** – аутентификация отключена;<br>• **Windows** – используется стандартная аутентификация Windows;<br>• **Basic** – базовая http-аутентификация (пароль и логин передаются в теле запроса);<br>• **NTLM** – используется аутентификация Windows по протоколу NTLM.<br>Выбор значения должен быть согласован с параметром **SecurityType** настроек интерфейса **AdministrationService** сервера JAS (см. |

| Настройка | Описание |
|---|---|
| | руководство по JAS [4] раздел «Настройка сетевых программных интерфейсов JAS Server»).<br><br>Значение по умолчанию: **none** |
| **Текущий пользователь** | Если флаг **Текущий пользователь** установлен, то подключение к серверу JAS будет осуществляться от имени того же пользователя, от чьего имени запущено приложение **Сервер JMS** (серверный агент). В противном случае следует заполнить поля **Имя пользователя** и **Пароль**<br><br>Флаг установлен по умолчанию. |
| **Имя пользователя** | Имя пользователя, от имени которого сервер JMS будет подключаться к серверу JAS (по интерфейсу **AdministrationService**). |
| **Пароль** | В случае если в поле **Имя пользователя** указано соответствующее значение, в поле **Пароль** следует указать пароль этого пользователя в службе Active Directory |
| <секция> **Веб-сервис безопасной передачи OTP-секрета** | |
| **Подключить веб-сервис безопасной передачи OTP-секрета** | Установите флаг, если необходимо подключить web-сервис безопасной передачи OTP-секрета (Aladdin 2FA Service).<br><br>По умолчанию флаг не установлен. |
| **Адрес веб-сервиса** | Задайте адрес web-сервиса безопасной передачи OTP-секрета (Aladdin 2FA Service). Адрес следует получить у компании-оператора web-сервиса. |
| **Проверять сертификат веб-сервиса** | Установите флаг, если для подключения необходимо выполнять автоматическую аутентификацию web-сервиса безопасной передачи OTP-секрета (Aladdin 2FA Service).<br><br>Для обеспечения работы опции следует установить сертификат web-сервиса в хранилище доверенных сертификатов на сервере JMS. |

3. Нажмите **Ок**
   В случае успешного подключения к серверу JAS отобразится следующее окно

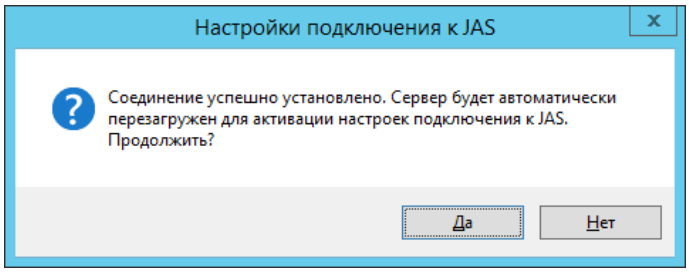



*Рис. 230 – Сообщение об успешном подключении к серверу JAS*

4. Нажмите **Да** и дождитесь окна с результатом применения настроек.

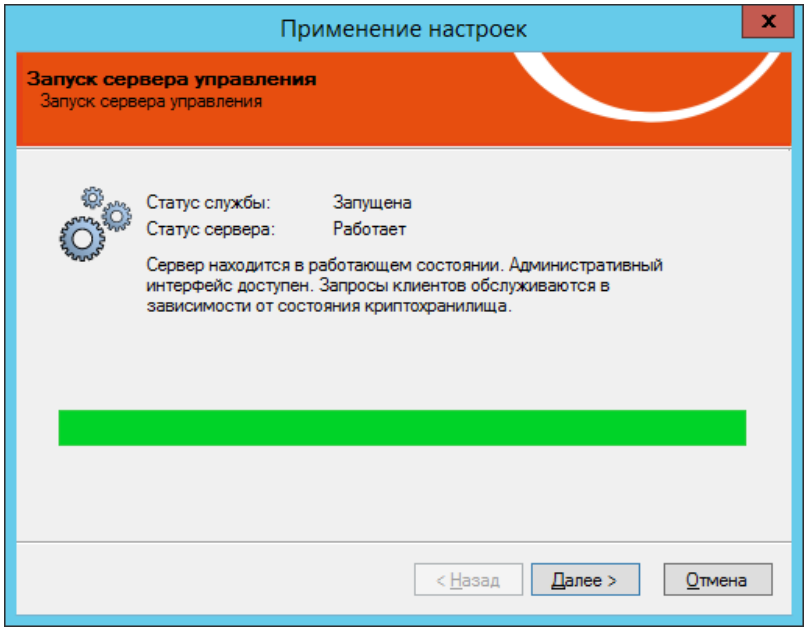



*Рис. 231 – Окно завершения применения настроек подключения к JAS*

5. Следуйте указаниям мастера настройки подключения к JAS до завершения процедуры.

В случае успешного подключения к серверу JAS (а при необходимости и к веб-сервису безопасной передачи OTP-секрета) в полях статуса соответствующих служб будет отображаться значение *Подключено* (Рис. 221)

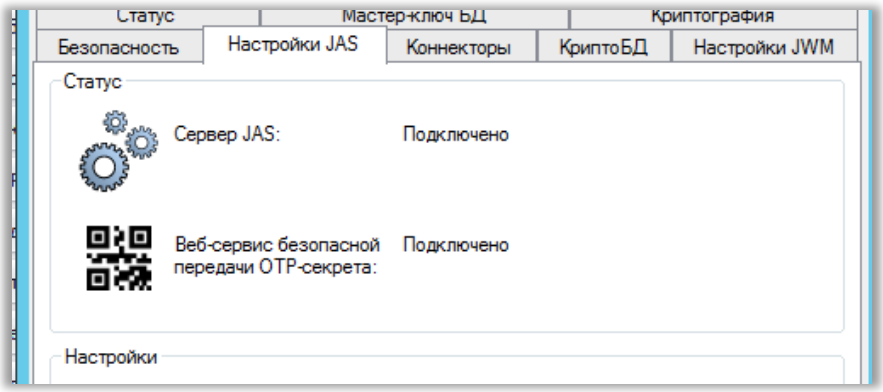



*Рис. 232 – Корректные статусы служб на вкладке Настройки JAS*

## 13.11 Настройки JWM

**Примечание.** Вкладка **Настройки JWM** становится доступна только после установки JWM-коннектора для JMS, подробнее см. раздел «JWM-коннектор для JMS», с. 218.

Вкладка **Настройки JWM** выглядит следующим образом.

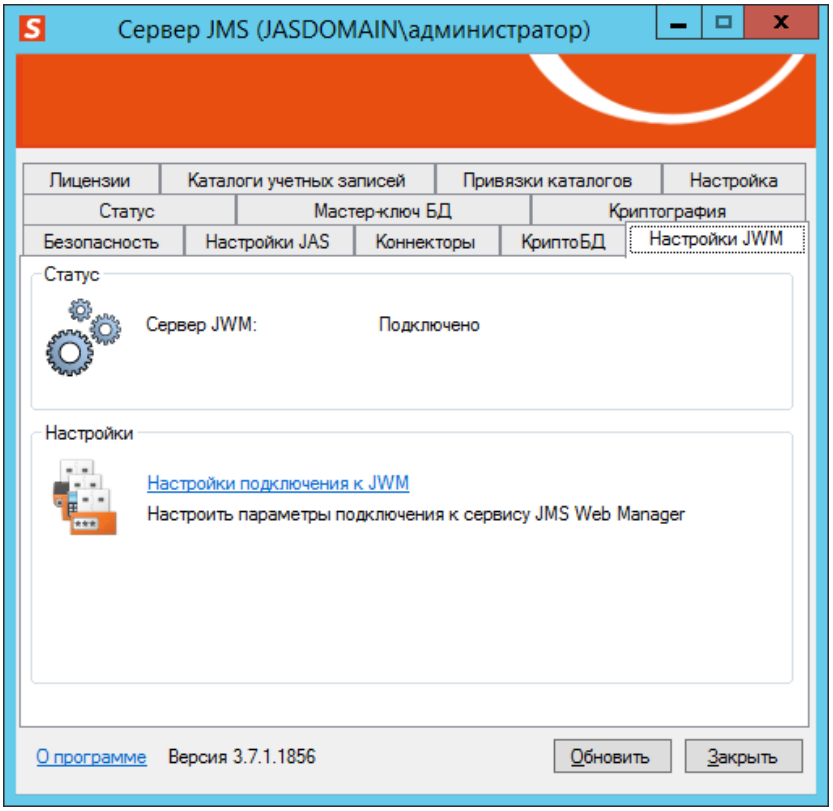



*Рис. 233 – Вкладка **Настройки JWM***

Подробнее порядок выполнения настроек на вкладке описан в разделе «Настройка подключения к JWM на сервере JMS», с. 222.

# 14. Смена языка пользовательского интерфейса JMS

В случае если после инсталляции JMS возникла необходимость изменить язык пользовательского интерфейса (в текущей версии поддерживаются русский и английский языки), это можно сделать путем редактирования параметров реестра, руководствуясь настоящим разделом.

Смена языка в компонентах управляется с помощью строкового параметра реестра Culture:

- `Culture=ru` – установка для русского языка;
- `Culture=en` – установка для английского языка;

Язык устанавливается каждого модуля JMS в отдельности в соответствующих ветках реестра, подробнее смотри в разделах:

- «Установка языка интерфейса для модуля JMS Admin и административных утилит»;
- «Установка языка интерфейса для модуля JMS Client»;
- «Установка языка интерфейса для модуля JMS Server и утилиты MaintenancePlanRunner»;
- «Установка языка интерфейса для утилиты сбора диагностической информации»;

В случае задания некорректного языкового параметра или отсутствия соответствующих языковых ресурсов используется язык по умолчанию – русский.

Параметр может быть задан как для компьютера в целом (в разделе реестра `HKEY_LOCAL_MACHINE`), так и для конкретного пользователя (в разделе реестра `HKEY_CURRENT_USER`). Приоритет у

параметра из раздела HKEY_CURRENT_USER. Т.е. приложение сначала ищет в разделе HKCU, затем в разделе HKLM.

**Примечание.** В случае обновления JMS (см. «Обновление JMS», с. 148) путем установки инсталляционного пакета с языком, отличным от ранее установленного, в обновленной версии будет сохранен язык первоначальной установки, если параметр `Culture` был указан в реестре явно (т.е. инсталлятор проверяет ранее установленный в реестре Windows язык интерфейса для конкретного модуля JMS).

### 14.1 Установка языка интерфейса для модуля JMS Admin и административных утилит

Установите необходимое значение строкового параметра `Culture` (`ru` или `en`) в следующих разделах реестра Windows:

- **Для конкретного пользователя:** HKEY_CURRENT_USER\SOFTWARE\Aladdin\EAP Administrative Client\Settings
- **Для компьютера в целом:** HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\EAP Administrative Client\Settings

### 14.2 Установка языка интерфейса для модуля JMS Client

Установите необходимое значение строкового параметра `Culture` (`ru` или `en`) в следующих разделах реестра Windows:

- **Для конкретного пользователя:** HKEY_CURRENT_USER\SOFTWARE\Aladdin\Enterprise Application Platform Client\Settings
- **Для компьютера в целом:** HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Client\Settings

### 14.3 Установка языка интерфейса для модуля JMS Server и утилиты MaintenancePlanRunner

Установите необходимое значение строкового параметра `Culture` (`ru` или `en`) в следующих разделах реестра Windows:

- **Для конкретного пользователя:** HKEY_CURRENT_USER\SOFTWARE\Aladdin\Enterprise Application Platform Server\Settings
- **Для компьютера в целом:** HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Server\Settings

### 14.4 Установка языка интерфейса для утилиты сбора диагностической информации

Установите необходимое значение строкового параметра `Culture` (`ru` или `en`) в следующих разделах реестра Windows:

- **Для конкретного пользователя:** HKEY_CURRENT_USER\SOFTWARE\Aladdin\Enterprise Application Platform Common\Settings
- **Для компьютера в целом:** HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\Enterprise Application Platform Common\Settings

# 15. Компонент 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.

JWM включает в себя следующие основные web-сервисы:

- **web-портал удаленного управления JMS**, представляющий собой web-модификацию консоли управления JMS (подробнее см. вторую часть руководства администратора [3]);
- **внутренний web-портал самообслуживания пользователей**, представляющий собой web-модификацию JMS-клиента и предназначенный для использования внутри корпоративной сети;
- **внешний web-портал самообслуживания пользователей** – то же, но для подключения из публичной сети (Интернет).

Все прикладные функции (административные и пользовательские, а также функции аутентификации) компонент JWM выполняет путем обращения к серверным компонентам JMS (JMS Server) и JAS (JaCarta Authentication Server) посредством соответствующих API-интерфейсов.

Компонент JWM может устанавливаться и функционировать на одном из компьютеров того же домена Windows, которому принадлежит сервер JMS.

## 15.1 Дистрибутив

Дистрибутив компонента JWM состоит из одного файла *AladdinJMS.Web.Manager_x.x.x.xxxx_x64.msi*.

## 15.2 Системные требования для компонента JWM

*Табл. 49 – Системные требования для установки компонента JWM*

| 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 JWM |
| **Место на диске** | Для нормального функционирования компонента JWM требуется минимум 500 Мбайт свободного дискового пространства |
| **Операционная система** | • Microsoft Windows Server 2008 R2 SP1;<br>• Microsoft Windows Server 2012;<br>• Microsoft Windows Server 2012 R2;<br>• Microsoft Windows Server 2016;<br>• Microsoft Windows Server 2019 |
| **База данных** | • Microsoft SQL Server 2008;<br>• Microsoft SQL Server 2008 R2;<br>• Microsoft SQL Server 2012;<br>• Microsoft SQL Server 2014;<br>• Microsoft SQL Server 2016;<br>• Microsoft SQL Server 2017;<br>• Microsoft SQL Server 2019;<br>(При использовании СУБД Microsoft SQL Server необходимым компонентом является *SQL Server Database Engine*)<br>• PostgreSQL версии 12 или более поздних версий |

| Компонент среды функционирования | Требование |
|---|---|
| **Дополнительное ПО** | • Internet Information Server версии 7.0 или более поздней (в составе серверной ОС Windows)<br>  **Примечание.** При установке/настройке роли веб-сервера (IIS) в перечне служб ролей следует установить **Проверка подлинности Windows** в добавление к установленным по умолчанию.<br>• Распространяемый пакет Visual C++ для Visual Studio 2015 версии 14.0.24215 или более поздней (Visual C++ Redistributable for Visual Studio 2015)<br>• .NET Core Runtime 3.1.22 Hosting Bundle Installer или более поздняя версия данного ПО<br>• Microsoft .NET Framework 4.8 или более поздние версии данного ПО<br>  **Примечание.** Перед установкой дополнительного ПО убедитесь в том, что выполнено обновление ОС Window |
| **Другие требования** | Установка должна осуществляться от имени учётной записи с правами администратора |
| | Компонент JWM должен устанавливаться на сервере, принадлежащем тому же домену Windows, что и сервер JMS, к которому JWM будет подключен после настройки |
| | Для обеспечения связи с web-порталами JWM через web-браузер по протоколу https необходимо выполнить установку и привязку сертификата SSL на сервер IIS в соответствии с документацией Microsoft |
| | В целях служебной (внутренней) аутентификации JWM для компьютера, на котором функционирует сервер IIS, следует выпустить сертификат по шаблону, описанному в разделе «Шаблон сертификата службы аутентификации JMS и серверов JMS/SQL», с. 28. |

## 15.3 Установка компонента JWM

Чтобы установить компонент JWM, выполните следующие действия.

1. Запустите на выполнение файл дистрибутива (см. «Дистрибутив», с. 203).

Отобразится следующее окно.

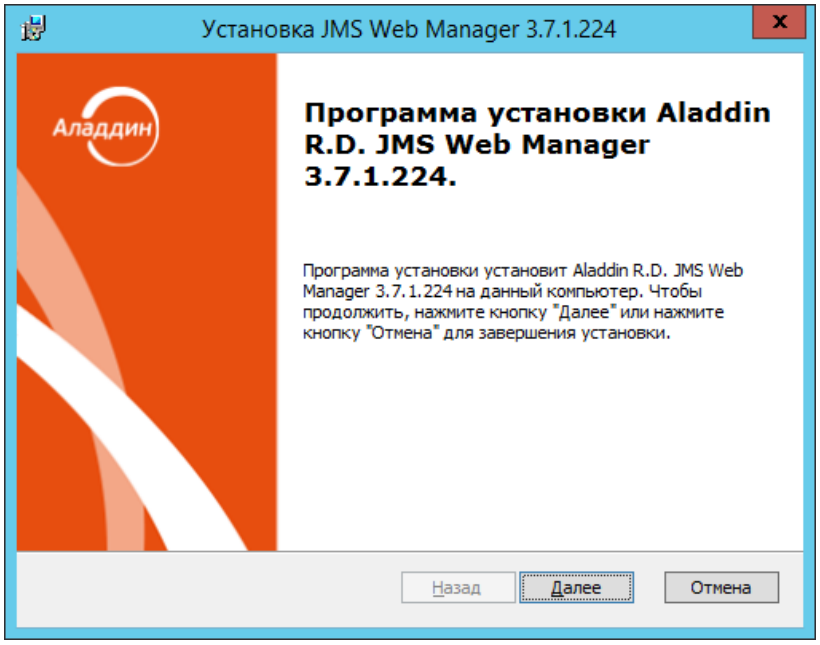



*Рис. 234 – Окно приветствия мастера установки компонента JWM*

2. Нажмите **Далее**.
   Отобразится следующее окно.

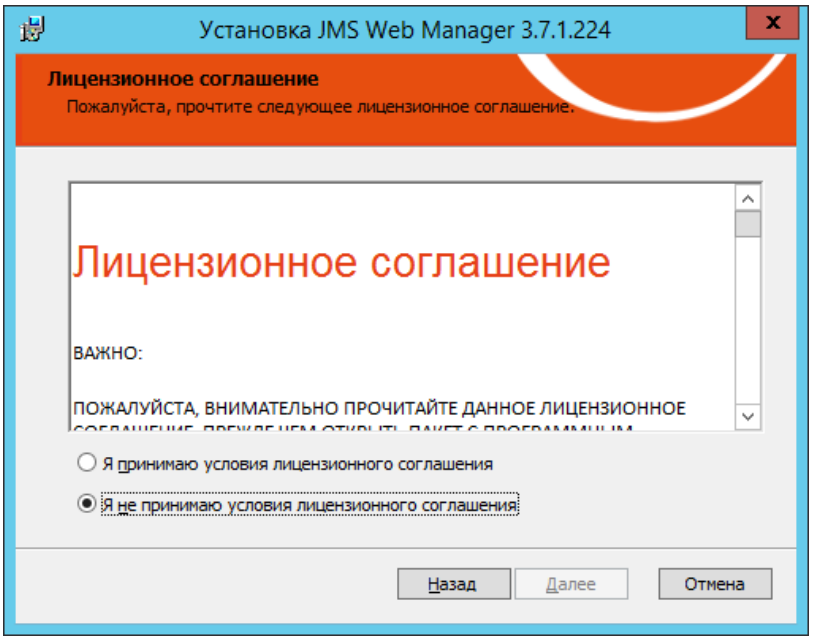



*Рис. 235 – Окно лицензионного соглашения*

3. Выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.

Отобразится следующее окно.

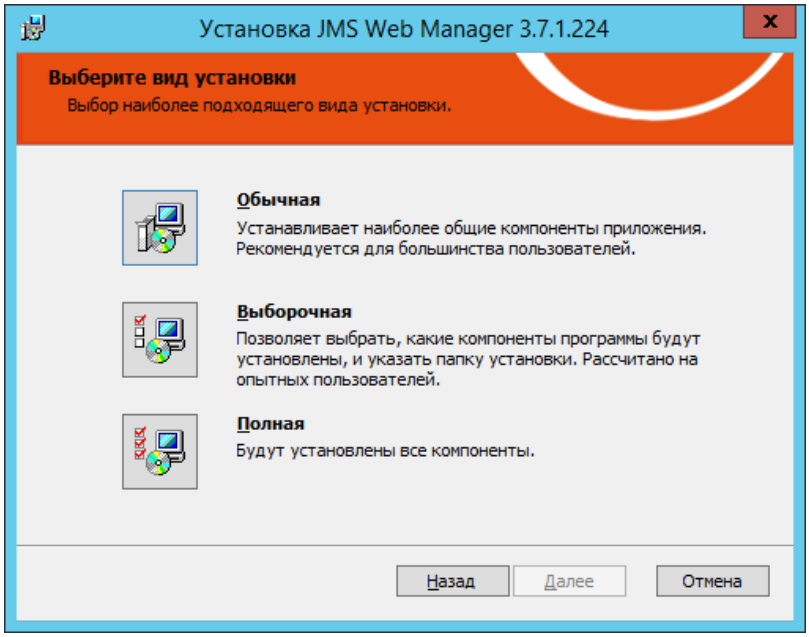



*Рис. 236 – Окно выбора варианта установки*

4. Выберите пункт **Полная**.

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

Отобразится следующее окно.

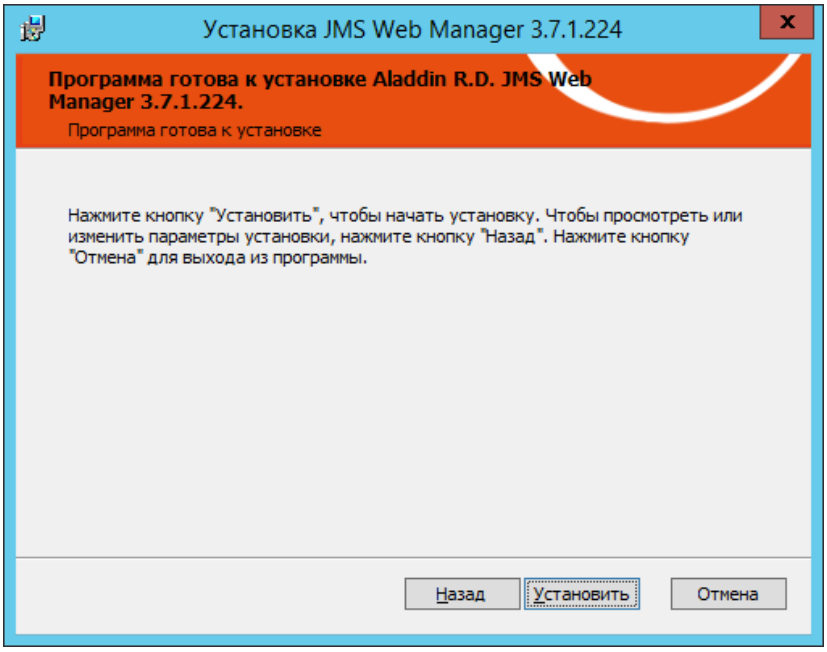



*Рис. 237 – Окно готовности к установке*

5. Нажмите **Установить**.

По завершении установки отобразится следующее окно.

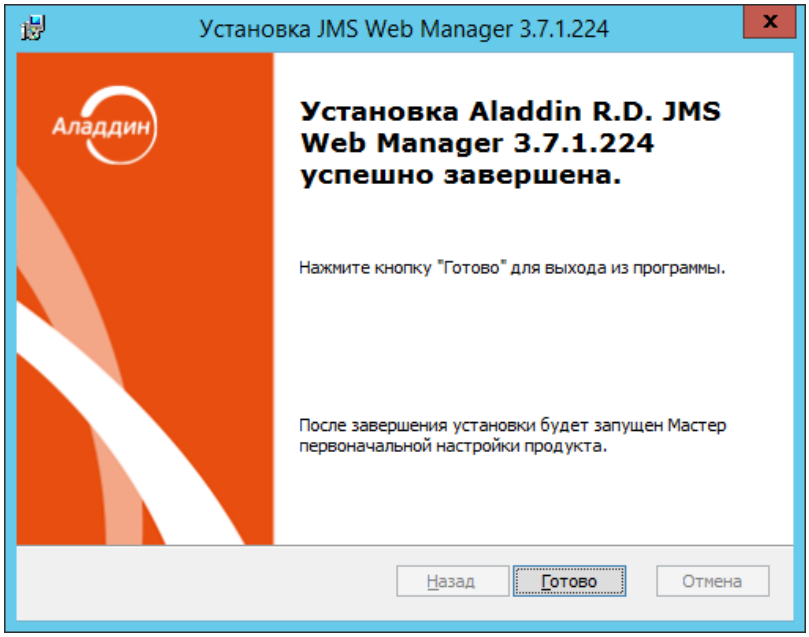



*Рис. 238 – Окно завершения установки*

6. Нажмите **Готово** для завершения процедуры.

После установки компонента JWM автоматически откроется окно мастера настройки JWM (см. «Настройка компонента JWM», ниже)

## 15.4 Настройка компонента JWM

Окно мастера настройки JWM открывается автоматически после установки компонента JWM.

Если вы закрыли окно мастера настройки JWM, к нему можно вернуться самостоятельно, запустив приложение **JMS Web Manager Настройка** (значок W) в разделе **JaCarta Management System** списка пользовательских приложений соответствующей версии операционной системы Windows Server.

Окно приветствия мастера настройки компонента JWM выглядит следующим образом.

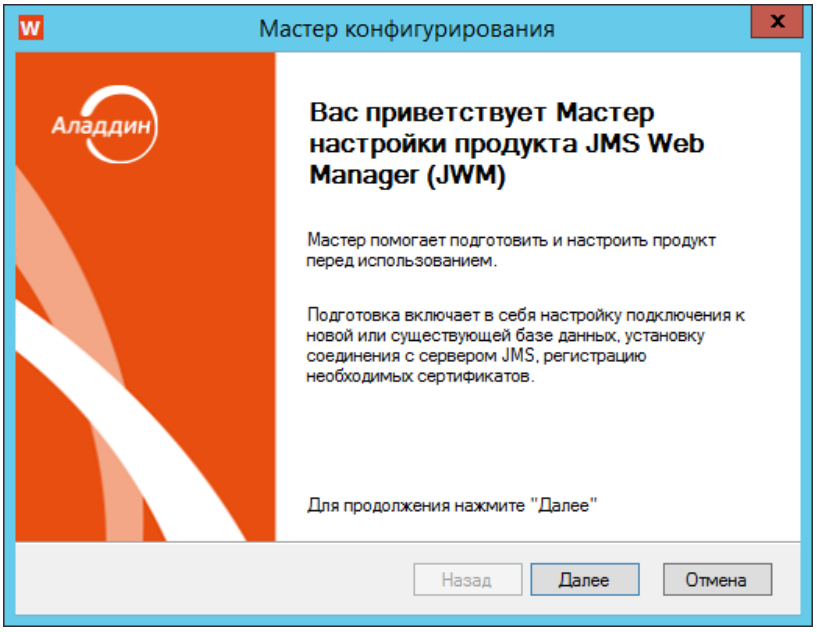



*Рис. 239 – Окно приветствия мастера настройки JWM*

**Примечание.** В случае повторной настройки, мастер позволяет воспользоваться установленной ранее конфигурацией, при этом на стартовом экране появляется флаг Использовать конфигурацию от прошлой установки (Рис. 240).

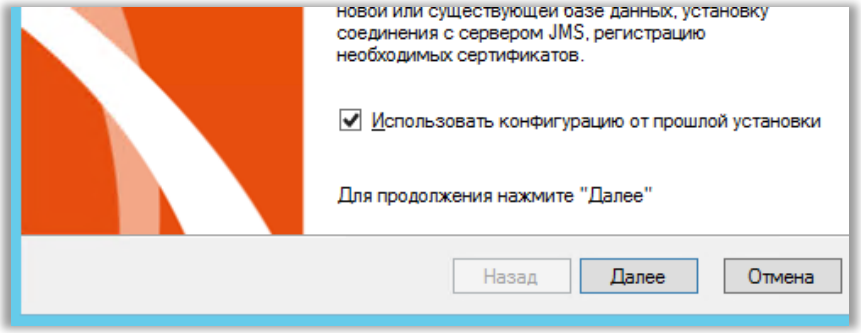



*Рис. 240 – Флаг использование прежних параметров при повторном запуске настройки JWM*

1. Нажмите **Далее**.

Отобразится следующее окно.

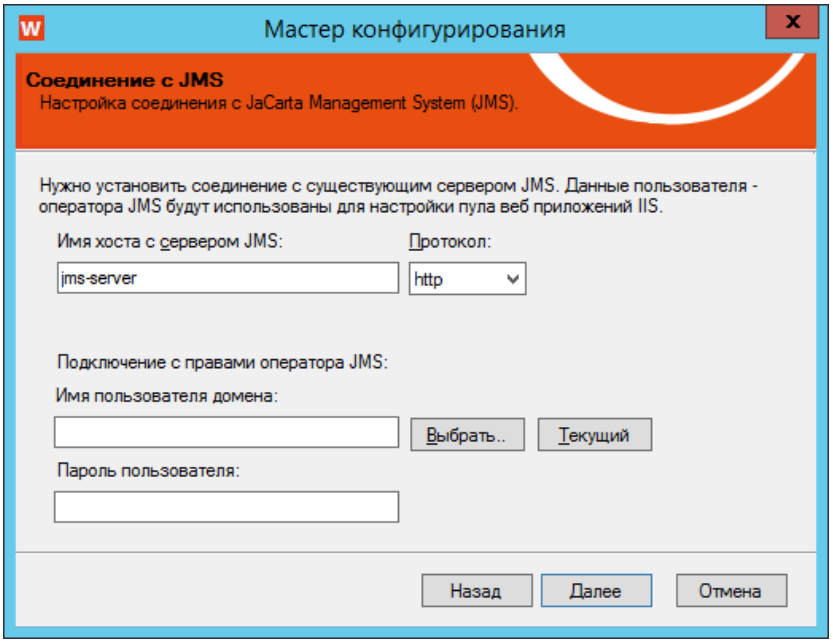



*Рис. 241 – Окно настройки соединения с сервером JMS*

2. Выполните настройку, руководствуясь Табл. 50.

*Табл. 50 – 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*)<br><br>**Примечания:**<br>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.<br>2. В случае использования протокола http допускается указать NetBIOS-имя сервера JMS (при этом, если компонент JWM установлен на одном хосте с сервером JMS, в качестве имени можно указать *localhost*) |
| **Протокол** | Выберите протокол подключения к серверу JMS. Возможные значения:<br>• **http** (значение по умолчанию)<br>• **https**<br><br>**Примечание.** Для выбора протокола https на сервере JMS должна быть настроена поддержка SSL в части, касающейся связи JMS по SSL с административным агентом из состава JMS Admin (см. раздел «Настройка SSL-соединения на стороне сервера JMS», с. 126) |
| **Имя пользователя домена** | Введите имя пользователя в формате **DOMAIN\username**.<br><br>**Важно!** Указанному пользователю должна быть назначена роль **Оператор** в JMS.<br><br>**Примечания:**<br>**1.** Допускается указание имени пользователя в формате UPN (например *username@domain.com*) |

| Настройка | Описание |
|---|---|
| | 2. От имени данного пользователя будет запускаться **План обслуживания жизненного цикла OTP-токенов** при самостоятельном выпуске таких токенов пользователями через web-портал самообслуживания. Поэтому данный пользователь должен быть зарегистрирован с правами Оператора в JMS (т.е. роли, обладающей правом **Запуск плана обслуживания**) |
| **Пароль пользователя** | Введите пароль пользователя |

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

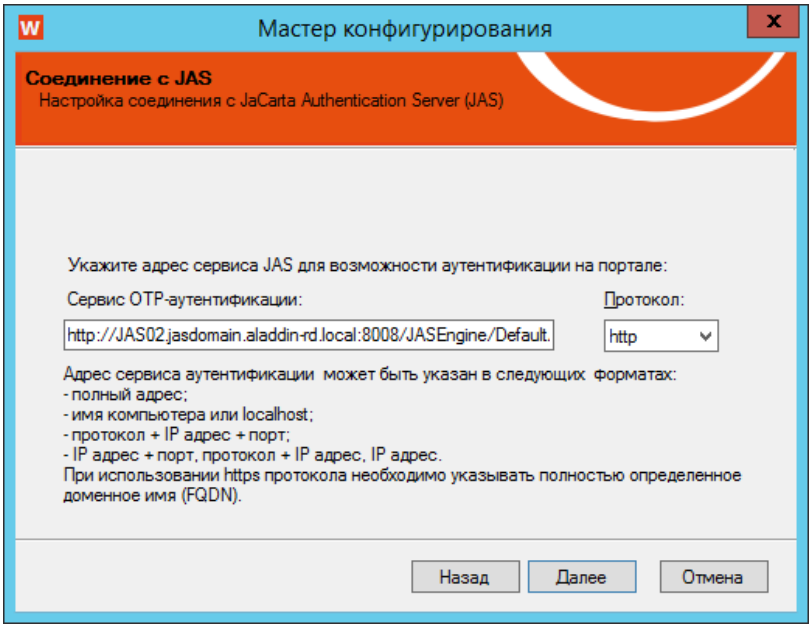



*Рис. 242 – Окно настройки подключения к серверу JAS*

4. Выполните настройку, руководствуясь Табл. 51.

*Табл. 51 – Настройки подключения к серверу JAS*

| Настройка | Описание |
|---|---|
| **Сервис OTP-аутентификации** | Введите адрес подключения к сервису OTP-аутентификации JAS в формате:<br>`http://<FQDN-имя сервера JAS>:8008/JASEngine/Default/AuthenticationService/rest/Authenticate`<br>где <FQDN-имя сервера> – полное доменное имя (FQDN) сервера JAS, например, srv01.test.com; либо, в случае кластерной конфигурации JAS, полное доменное имя (FQDN) *кластерной роли*, созданной на этапе настройки отказоустойчивого кластера (подробнее см. в части 3 руководства администратора [4], раздел «Настройка отказоустойчивого кластера JAS»).<br>Допустимые форматы ввода имени для разных условий см. в подсказке диалогового окна. |
| **Протокол** | Выберите протокол подключения к серверу JAS. Возможные значения:<br>• **http** (значение по умолчанию)<br>• **https** |

| Настройка | Описание |
|---|---|
| | **Примечание.** Для выбора протокола https на сервере JAS должна быть настроена поддержка SSL (см. в части 3 руководства администратора [4], раздел «Настройка в JAS протоколов SSL/TLS»). |

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

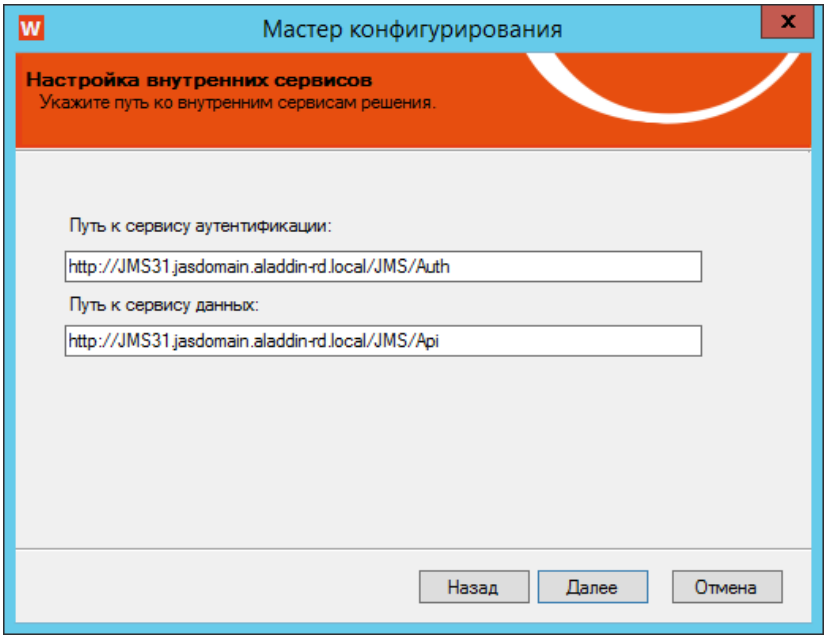



*Рис. 243 – Окно настройки соединения с сервером JMS*

6. Выполните настройку, руководствуясь Табл. 52.

*Табл. 52 – Настройка адресов внутренних сервисов JMS*

| Настройка | Описание |
|---|---|
| **Путь к сервису аутентификации** | Поле заполняется автоматически. При необходимости отредактируйте. |
| **Путь к сервису данных** | Поле заполняется автоматически. При необходимости отредактируйте. |

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

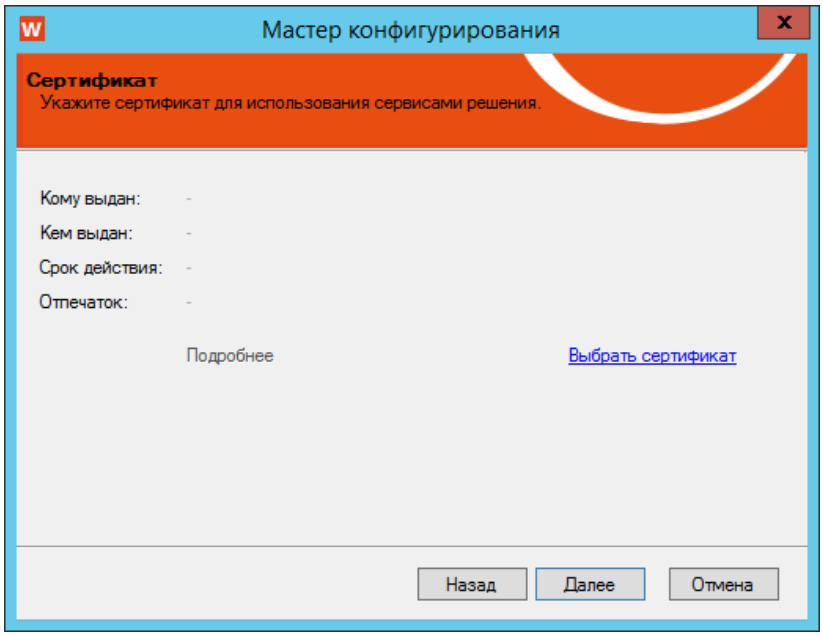



*Рис. 244 – Окно выбора сертификата для JWM*

8. Выберите сертификат, выпущенный заблаговременно для целей внутренней аутентификации JWM в соответствии с рекомендациями из Табл. 49, с. 203.
9. Нажмите **Далее**.
   Отобразится следующее окно.

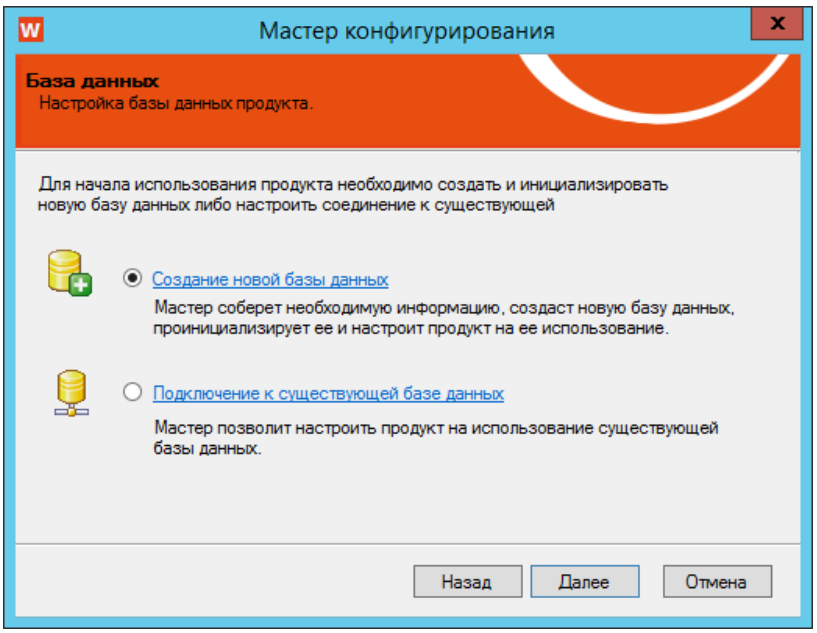



*Рис. 245 – Окно выбора подключения к серверу СУБД*

10. Для создания новой базы данных выполните следующий шаг процедуры.
(В противном случае, т.е. для обновления или восстановления JWM выберите опцию **Подключение к существующей базе данных** и следуйте указаниям мастера до завершшния подключения).

**Примечание.** База данных JWM предназначена для хранения служебных данных самого компонента JWM и устанавливается и работает независимо от базы данных JMS.

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

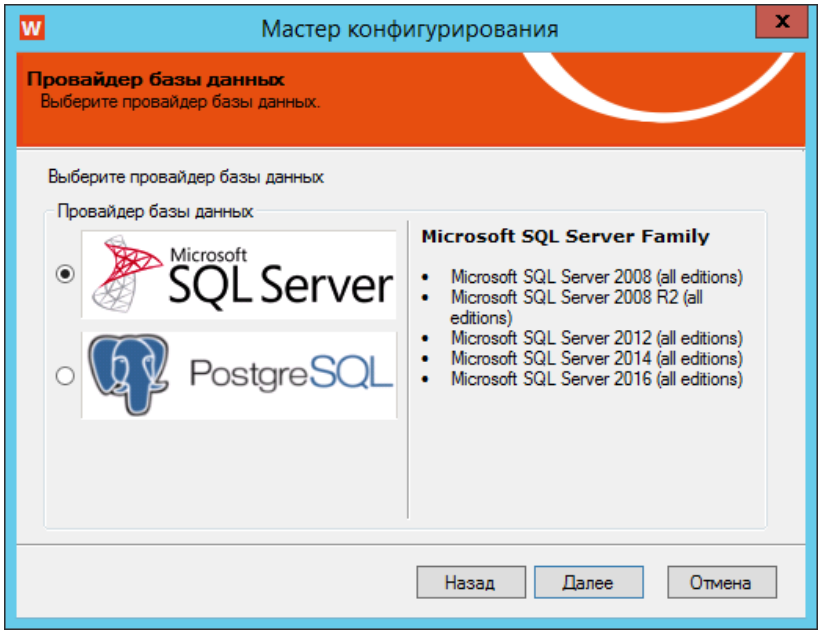



*Рис. 246 – Окно выбора провайдера базы данных*

12. Выберите тип СУБД (MS SQL Server или PostgreSQL), в которой планируется размещать БД JMS и нажмите **Далее**.
13. В зависимости от выбранного на предыдущем шаге типа СУБД отобразится одно из окон подключения к БД JMS (см. Рис. 247 – случай расположения БД в СУБД MS SQL Server, Рис. 248 – случай расположения БД в СУБД PostgreSQL).

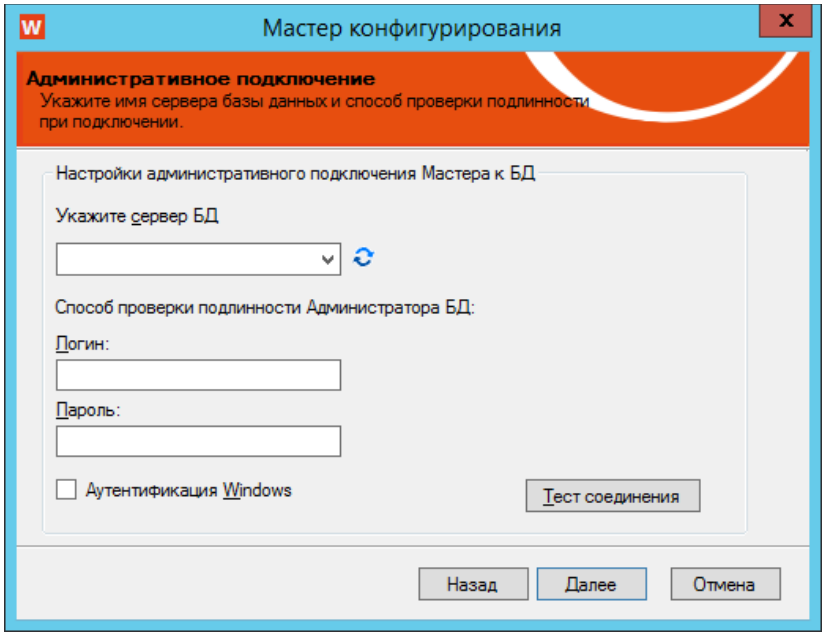



*Рис. 247 – Окно настройки подключения к базе данных в СУБД MS SQL Server*

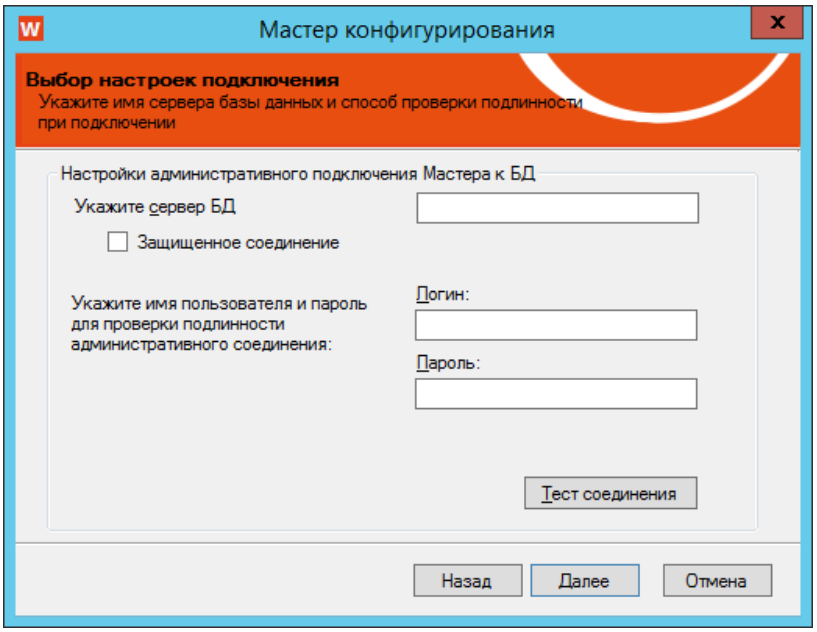



*Рис. 248 – Окно настройки подключения к базе данных в СУБД PostgreSQL*

14. Выполните необходимые настройки, руководствуясь табл. 13.

*Табл. 53 – Настройки подключения к серверу БД*

| Настройка | Описание |
|---|---|
| **Укажите сервер БД** | В случае использования СУБД MS SQL Server 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.<br><br>В случае использования СУБД PostgreSQL введите IP-адрес хоста, на котором функционирует SQL-сервер. |

| Настройка | Описание |
|---|---|
| **Защищенное соединение**<br>(Только для PostgreSQL) | Установите этот флаг, если хотите использовать для подключения к базе данных SSL-соединение. |
| **Аутентификация Windows**<br>(Только для MS SQL) | 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.<br>При выборе пункта **Аутентификация Windows** (проверка подлинности Windows) убедитесь, что пользователю, от имени которого выполняется мастер настройки, предоставлены права на администрирование SQL-сервера. |
| **Логин, Пароль** | Введите логин и пароль пользователя, от имени которого выполняется подключение серверу СУБД (в случае MS SQL требуется только в случае отключенного флага **Аутентификация Windows**) |

В настоящем документе для примера настройки подключения к серверу базы данных MS SQL Server используется проверка подлинности Windows.

15. Чтобы проверить корректность настроек, нажмите **Тест соединения**.
    Если соединение настроено верно, отобразится следующее сообщение.

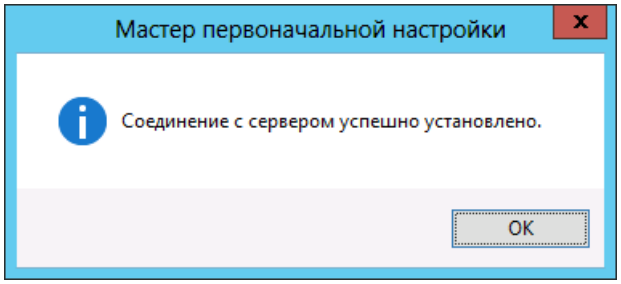



*Рис. 249 – Сообщение об успешной установке соединения с сервером*

16. Нажмите **OK** и в окне мастера первоначальной настройки конфигурации нажмите **Далее**.

Отобразится следующее окно.

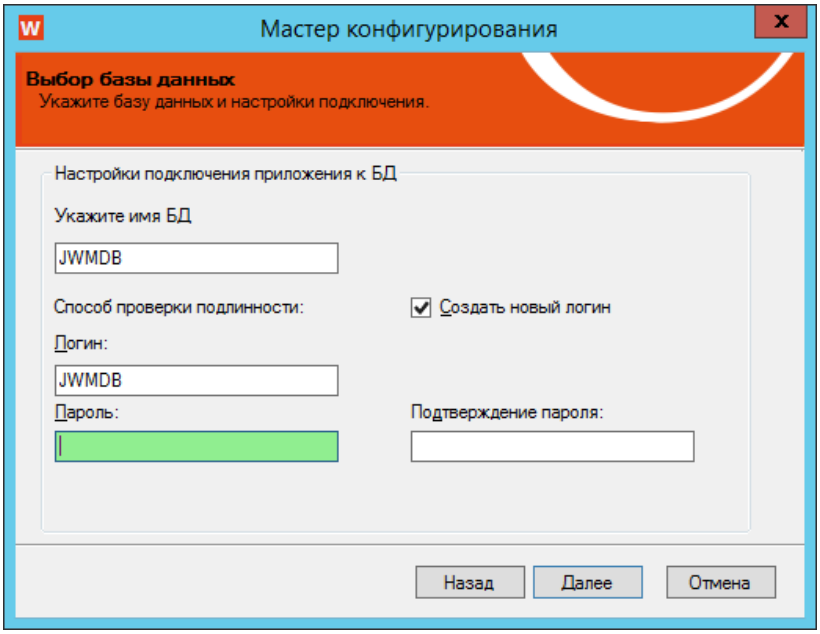



*Рис. 250 – Окно создания или выбора БД JMS при использовании СУБД MS SQL Server*

17. Выполните настройки в соответствии с Табл. 14.

*Табл. 54 – Настройки подключения к базе данных*

| Настройка | Описание |
|---|---|
| **Укажите имя БД** | В зависимости от необходимости отредактируйте или оставьте без изменения предложенное имя БД по умолчанию. |
| **Создать новый логин** | В случае необходимости использовать уже имеющуюся пару логин—пароль отключите флаг. |
| **Логин** | В зависимости от необходимости отредактируйте или оставьте без изменения предложенный логин по умолчанию. |
| **Пароль**<br>**Подтверждение пароля** | Укажите пароль и его подтверждение, если создается новая пара логин—пароль, либо просто укажите пароль, если используется ранее созданный логин. |

18. Нажмите **Далее**.

Отобразится окно следующего вида.

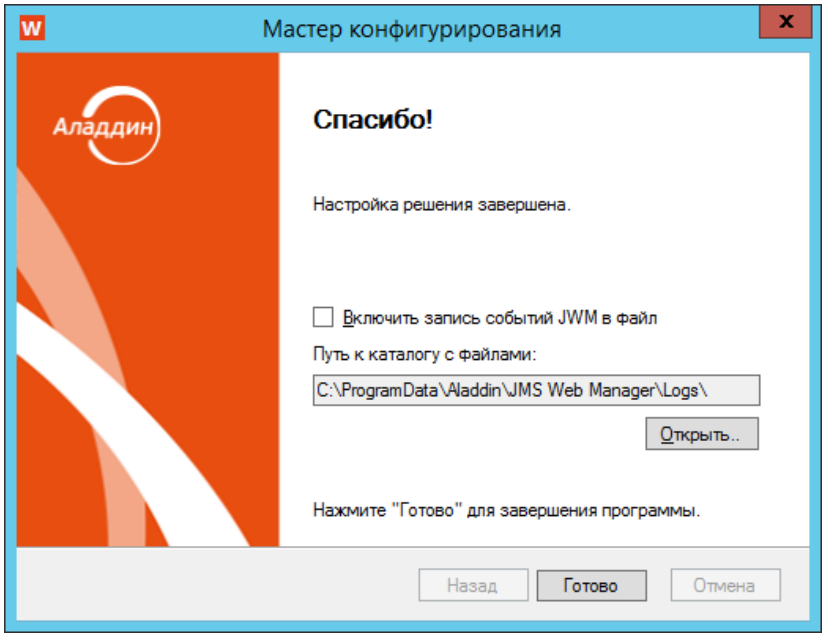



*Рис. 251 – Окно завершения работы мастера настройки JWM*

19. Чтобы включить журналирование работы web-сервисов, входящих в состав JWM установите флаг **Включить запись событий JWM в файл**.

**Примечание.** Файлы журналов располагаются в папке *%ProgramData%\Aladdin\JMS Web Manager\Logs*. Имена файлов журналов начинаются с названия соответствующих web-сервисов, входящих в состав JWM, таких как auth, data, admin, private. Пути к файлам журналов задаются в конфигурационных файлах соответствующих web-сервисов (файлы web.config). Уровень детализации указывается в файлах appsettings.json соответствующих web-сервисов.

20. Нажмите **Готово** для окончания процедуры.

## 15.5 Подготовительные действия для самостоятельной установки JWA пользователями

Для того чтобы обеспечить возможность установки пользователями клиентского агента (JWA) на своих рабочих компьютерах по подсказке из web-клиента следует выполнить следующие действия.

После развертывания и настройки на сервере JWM в каждом из автоматически созданных каталогов:

- для публичного портала JWM (папка по умолчанию «`C:\Program Files\JMS Web Manager\UserPlacePrivate`»)
- для закрытого портала JWM (папка по умолчанию «`C:\Program Files\JMS Web Manager\UserPlacePublic`»)

следует создать вложенную папку следующего формата:

`\wwwroot\Modules\<платформа>`

где вместо <*платформа*> - следует подставить "Win64", "Linux" или "MacOs" в зависимости от используемых клиентских операционных систем.

В каждый из созданных вложенных каталогов следует скопировать дистрибутивы JWA для соответствующих платформ.

**Примечания:**

1. В текущей версии продукта реализованы дистрибутивы JWA только для 32- и 64-раздрядных платформ Windows (см. раздел «Компонент JMS Web Agent (JWA)», с. 225).
2. В зависимости от планирующегося к использованию дистрибутива JWA (32- или 64-раздрядного) в папку `...\Win64` следует поместить один из этих дистрибутивов.

# 16. JWM-коннектор для JMS

JWM-коннектор для JMS представляет собой набор дополнительных компонентов для Сервера JMS и Консоли управления JMS, позволяющий управлять объектами JWM и правами пользователей по отношении к объектам JWM, доступным из личного кабинета пользователя.

JWM-коннектор включает в себя два компонента:

- модуль коннектора для сервера JMS, устанавливается на машину с компонентом JMS Server;
- модуль расширения для консоли управления JMS, устанавливается на машину с компонентом JMS Admin.

**Важно!** Модуль расширения для консоли управления JMS требует установки на каждом хосте, на котором функционирует приложение *Консоль управления JMS*.

Инсталлятор коннектора автоматически определяет наличие на хосте того типа приложения (сервера JMS или консоли управления), для которого требуется установить соответствующий компонент коннектора.

## 16.1 Дистрибутив

Дистрибутив JWM-коннектора для JMS представлен следующими файлами:

- *AladdinJMS.Web.Connector_x.x.x.xxxx_x64.msi* – инсталлятор для 64-битных платформ Windows.

## 16.2 Системные требования JWM-коннектора для JMS

Системные требования JWM-коннектора:

- для установки серверного компонента JWM на сервере JMS необходимо обеспечить минимум 10 Мбайт дискового пространства, в остальном системные требования совпадают (не требуют дополнительных ресурсов) с системными требованиями к установке компонента JMS Server (см. разделы 4.1 и 4.3);
- для установки компонента, предназначенного для консоли управления JMS, необходимо обеспечить минимум 10 Мбайт дискового пространства, в остальном системные требования совпадают (не требуют дополнительных ресурсов) с системными требованиями к установке компонента JMS Admin (см. разделы 4.2 и 4.3).

## 16.3 Установка JWM-коннектора для JMS

Чтобы установить JWM-коннектор, выполните следующие действия.

1. Запустите на выполнение файл дистрибутива JWM-коннектора (см. «Дистрибутив», с. 218).

Отобразится следующее окно.

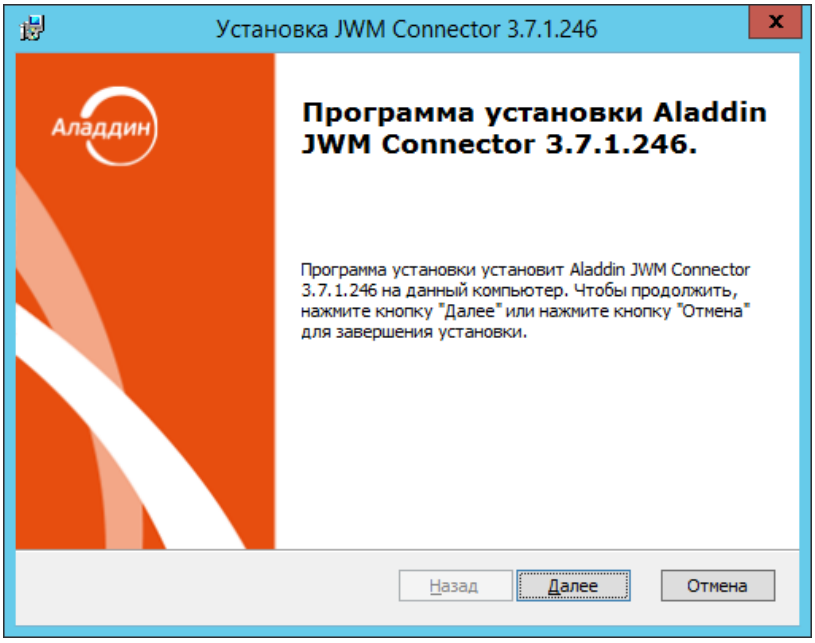



*Рис. 252 – Окно приветствия мастера установки JWM-коннектора*

2. Нажмите **Далее**.
   Отобразится следующее окно.

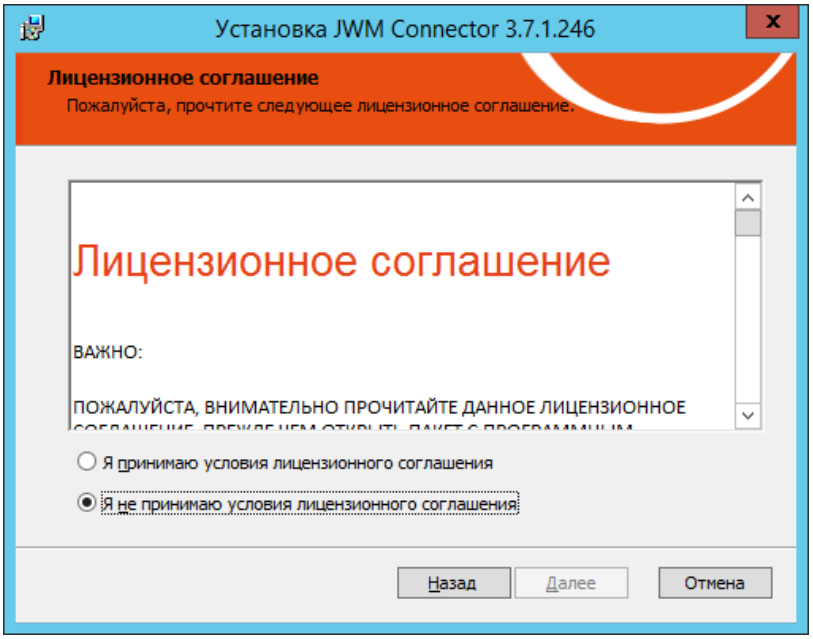



*Рис. 253 – Окно лицензионного соглашения*

3. Выберите **Я принимаю условия лицензионного соглашения** и нажмите **Далее**.

Отобразится следующее окно.

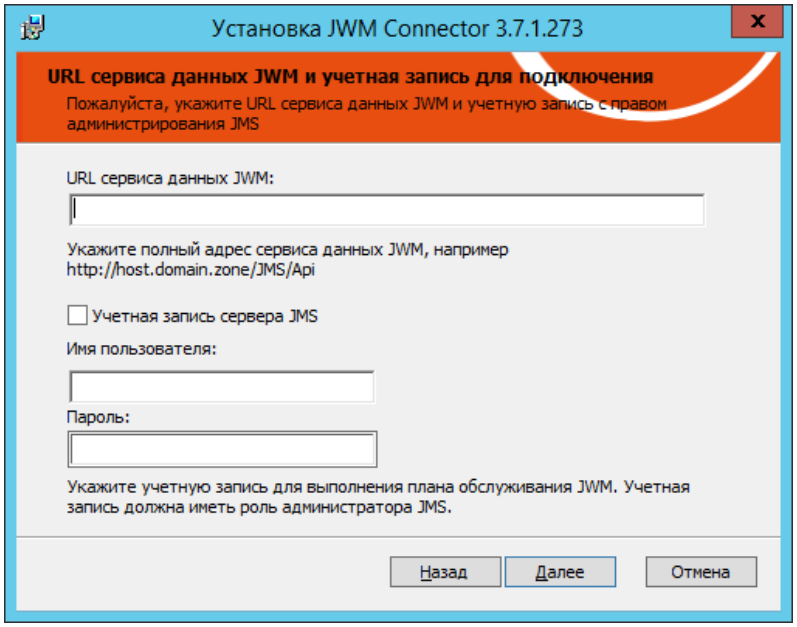



*Рис. 254 – Окно настройки подключения к JWM*

4. Выполните настройку, руководствуясь Табл. 55.

*Табл. 55 – Настройка подключения к JWM*

| Настройка | Описание |
|---|---|
| **URL сервиса данных JWM** | Введите URL сервиса данных, как это было сделано при настройке компонента JWM в поле **Путь к сервису данных** (Рис. 243, с. 211, раздел «Настройка компонента JWM»). |
| **Учетная запись сервера JMS** | При установке флага подключение к серверу JWM будет осуществляться от имени той же учетной записи, от которой запускается служба сервера JMS Настройка работает только в случае, если служба запускается от имени пользователя.<br>Для корректной работы коннектора убедитесь, что у этой учетной записи в JMS назначена роль *Администратор ИБ*. В противном случае введите необходимые данные в полях **Имя пользователя** и **Пароль**, как это указано в описании данных полей |
| **Имя пользователя**<br>**Пароль** | Введите **Имя пользователя** (доменное имя в формате DOMAIN\username) , которому в JMS назначена роль *Администратор ИБ*. В поле **Пароль** введите пароль данного доменного пользователя. |

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

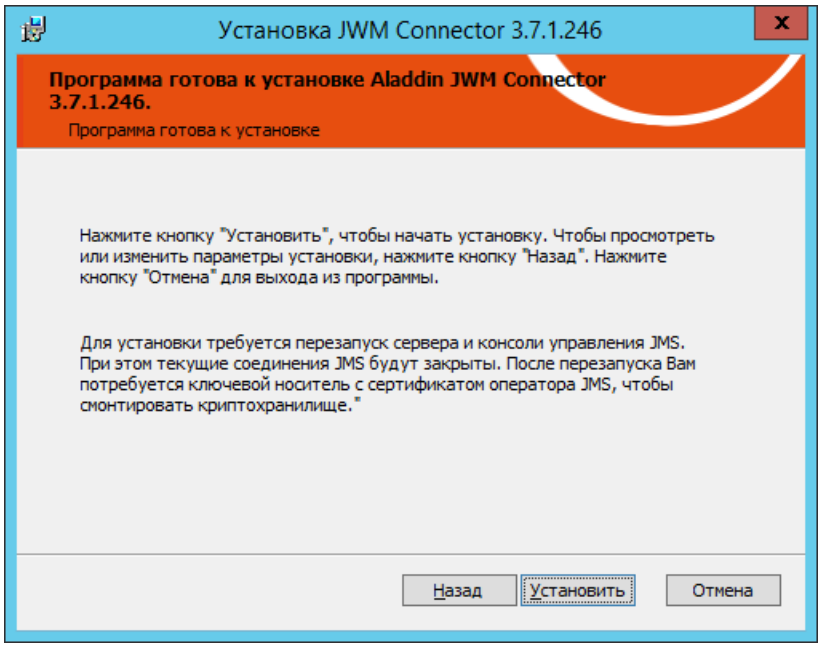



*Рис. 255 – Окно готовности к установке*

6. Нажмите **Установить**.
   По окончании установки отобразится запрос на перезагрузку компонентов JMS.

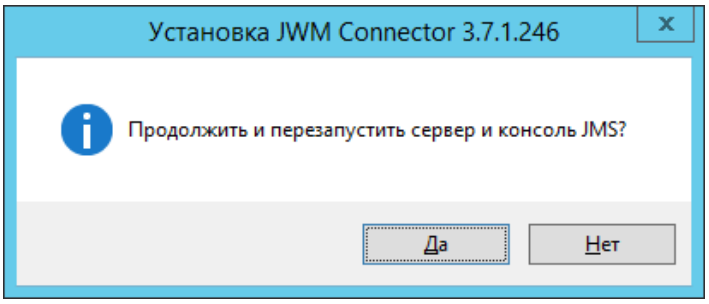



*Рис. 256 – Окно запроса на перезагрузку компонентов JMS*

7. Нажмите **Да**.

По завершении перезагрузки отобразится следующее окно.

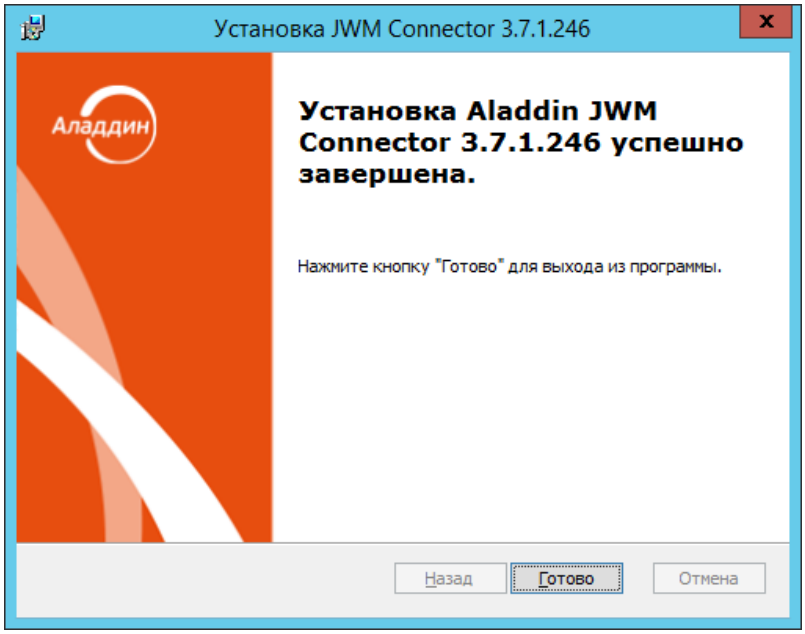



*Рис. 257 – Окно завершения установки*

8. Нажмите **Готово** для завершения процедуры.

Для изменения настроек подключения к JMW можно воспользоваться соответствующей вкладкой серверного агента (см. раздел «Настройка подключения к JWM на сервере JMS», below).

## 16.4 Настройка подключения к JWM на сервере JMS

После установки JWM-коннектора на сервере JMS в серверном агенте (приложение Сервер JMS) добавится вкладка **Настройки JWM** (Рис. 258, ниже), на которой можно проверить статус подключения к JMW, а также выполнить необходимую настройку подключения, если была допущена ошибка на этапе установки JWM-коннектора.

Для изменения начальных настроек подключения к JWM выполните следующие действия.

1. Запустите приложение Сервер JMS и откройте вкладку **Настройки JWM**.

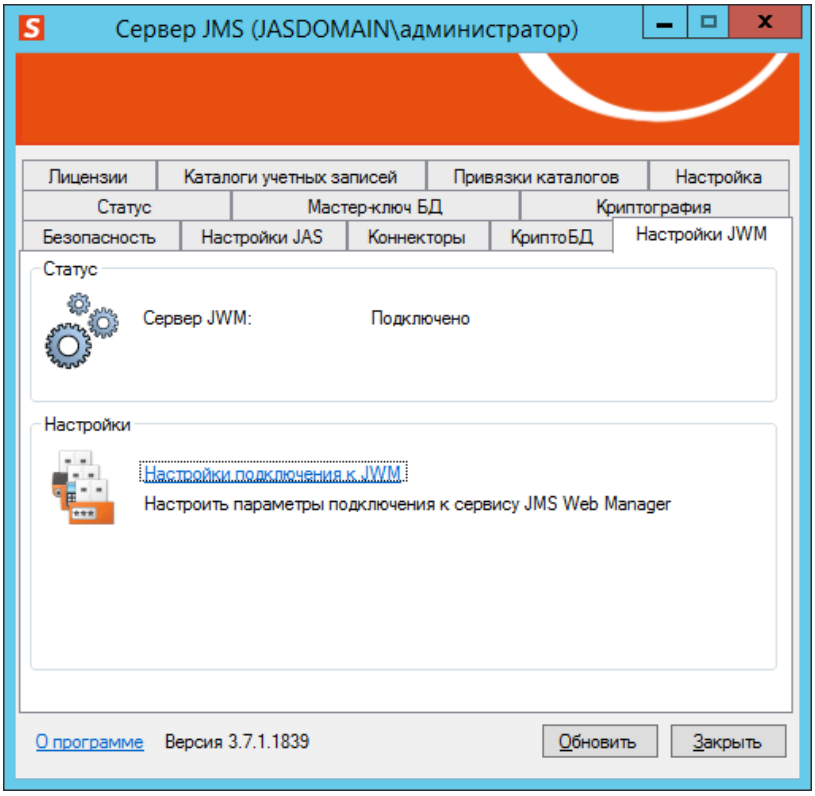



*Рис. 258 – Вкладка серверного агента Настройки JWM*

2. Нажмите **Настройки подключения к JWM**.
   Отобразится следующее окно.

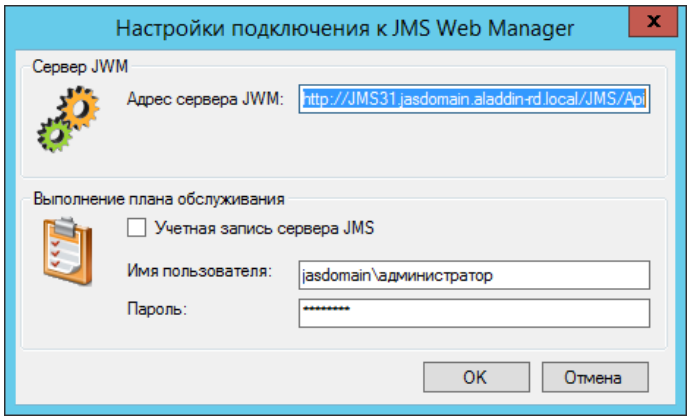



*Рис. 259 – Окно настроек подключения к JMW*

3. Выполните настройку, руководствуясь Табл. 55, с. 220 (поле **Адрес сервера JWM** соответствует параметру **URL сервиса данных JWM** в указанной таблице).

При правильном выполнении настроек подключения к JWM в секции **Статус** на вкладке **Настройки JMW** (Рис. 258, выше), в поле **Сервер JWM** должно отображаться значение *Подключено*.

# 17. Настройка подключения к JWM из web-клиента JMS

Настоящий раздел описывает параметры подключения к JWM из web-клиента JMS для случая, если компонент JMS Web Manager (см. раздел «Компонент JMS Web Manager (JWM)», с. 202), а именно та часть JWM, на которой запущены пулы приложений DataService и Auth, установлен на сервере, отличном от сервера JMS.

Для подключения к JWM с клиентской машины JMS из web-браузера через внутренний портал в режиме аутентификации (т.е. на вкладке) **Текущий пользователь** (Рис. 260, подробнее см. руководство пользователя [1]) выполните следующие действия.

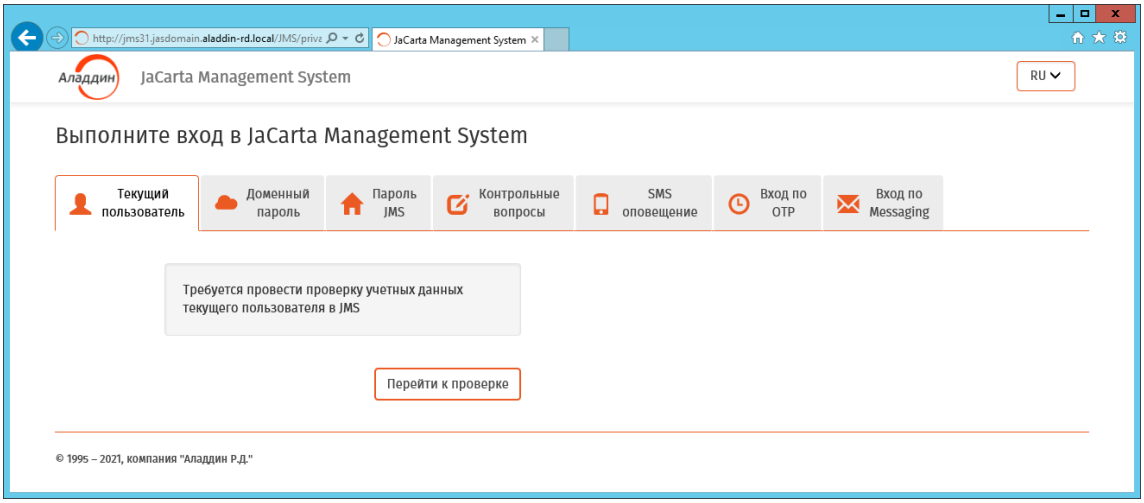



*Рис. 260 – Страница аутентификации пользователя на внутреннем портале самообслуживания*

1. На компьютере с Web-клиентом JMS в зависимости от используемого браузера в реестр добавьте следующие элементы:

1.1. В случае использования на клиентском компьютере браузера Google Chrome

1.1.1. Создайте в реестре на клиентском компьютере раздел **[HKEY_LOCAL_MACHINE\Software\Policies\Google\Chrome]**

1.1.2. В созданном разделе добавьте строковый параметр **AuthNegotiateDelegateAllowlist** со значением *<FQDN_домена_JMS>*
где <FQDN_домена_JMS> — полное доменное имя AD-домена, в котором работает сервер JMS, например, domain.test.com;
(допускается также указание символа подстановки «*» вместо имени нижнего уровня домена, например *.test.com)

1.2. В случае использования браузера Microsoft Edge

1.2.1. Создайте в реестре на клиентском компьютере раздел **[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Edge]**

1.2.2. В созданном разделе добавьте строковый параметр **AuthNegotiateDelegateAllowlist** со значением *<FQDN_домена_JMS>*
где <FQDN_домена_JMS> — полное доменное имя AD-домена, в котором работает сервер JMS, например, domain.test.com;
(допускается также указание символа подстановки «*» вместо имени нижнего уровня домена, например *.test.com)

2. После применения изменений в реестре перезапустите браузер.

Для массовой настройки подключения клиентских компьютеров к серверу JWM воспользуйтесь механизмом групповых политик Active Directory.

# 18. Компонент JMS Web Agent (JWA)

Компонент JMS Web Agent (JWA) устанавливается на тех клиентских компьютерах с web-клиентом JMS (приложением Личный кабинет) под управлением ОС Windows, на которых должно выполняться физическое обращение к электронным ключам JaCarta (PKI/ГОСТ/ГОСТ2/LT/SF ГОСТ/ALO и др.).

## 18.1 Дистрибутив

Дистрибутив компонента JWM включает в себя следующие файлы:

- *AladdinJMS.WebAgent_x.x.x.xxx_x64.msi* – для 64-разрадных ОС Windows;
- *AladdinJMS.WebAgent_x.x.x.xxx_x86.msi* – для 32-разрадных ОС Windows.

## 18.2 Системные требования компонента JWA

Системные требования компонента JMS Web Agent приведены в документе RU.АЛДЕ.03.16.001-04 30 01-1 «Программное обеспечение JaCarta Management System v3.7. Формуляр».

## 18.3 Порядок самостоятельной установки JWA пользователями

Порядок самостоятельной установки JWA пользователями web-клиента JMS приведен в руководстве пользователя [1], в разделе «Первый вход в личный кабинет и самостоятельная установка JWA».

## 18.4 Команда для автоматизированного развертывания JWA на компьютерах пользователей

**Примечание.** JMS предполагает самостоятельную установку JWA пользователями по подсказке из web-клиента. Подсказка появится только в случае выполнения необходимых предварительных действий (копирования дистрибутива JWA в установленную папку на сервере JWM, подробнее см. раздел «Подготовительные действия для самостоятельной установки JWA пользователями», с. 217).

Настоящий раздел описывает альтернативный способ установки JWA, который можно использовать для развертывания JWA на клиентских компьютерах путем настройки групповых политик Windows.

Для установки JWA из командной строки используется стандартный установщик Windows `msiexec`, например:

```
msiexec /i Aladdin.JMS.WebAgent_x.x.x.xxx_x64.msi /quiet INSTALL_TYPE="WindowsService"
PORTAL_URI="https://jms.server/jms/private" USE_SSL="1" SSL_CREATE_CERTIFICATE="1"
```

Подробное описание параметров команды приведено в Табл. 56.

*Табл. 56 – Параметры (PROPERTY) команды msiexec /i AladdinJMS.WebAgent_x.x.x.xxx_x64.msi*

| Свойство/PROPERTY | Значение / PropertyValue |
|---|---|
| **INSTALL_TYPE** | Тип установки JWA.<br><br>Допустимые значения:<br>• **INSTALL_TYPE="App"** – установка в качестве приложения Windows;<br>• **INSTALL_TYPE="WindowsService"** – установка в качестве службы Windows |

| Свойство/PROPERTY | Значение / PropertyValue |
|---|---|
| **PORTAL_URI** | Путь к сервису портала JWM (внутреннего – private; или внешнего—public).<br>Например:<br>**PORTAL_URI="https://jms.server/jms/private"** |
| **USE_SSL** | Флаг использования SSL для JWA.<br>Допустимые значения:<br>• **USE_SSL="0"** – SSL не используется;<br>• **USE_SSL="1"** – SSL используется.<br>Значение по умолчанию: **USE_SSL="1"** |
| **SSL_CREATE_CERTIFICATE** | Флаг создания самоподписанного сертификата и использования его для SSL-соединения.<br>Допустимые значения:<br>• **SSL_CREATE_CERTIFICATE ="0"** – не генерировать сертификат;<br>• **SSL_CREATE_CERTIFICATE ="1"** – сгенерировать сертификат.<br>Значение по умолчанию: **SSL_CREATE_CERTIFICATE ="1"**<br>**Важно!** Генерация сертификата доступна только при указании свойства **USE_SSL="1"** |
| **CERTIFICATE_THUMBPRINT** | Отпечаток сертификата, который следует использовать. Данный сертификат должен быть заблаговременно установлен в хранилище (хранилище компьютера).<br>Например:<br>**CERTIFICATE_THUMBPRINT="b696f465af65b503d6e69d9ca47c4568bac50f38"**<br>**Важно!** При использовании параметра **CERTIFICATE_THUMBPRINT** следует явным образом отключить создание самоподписанного сертификата, указав параметр **SSL_CREATE_CERTIFICATE="0"**<br>Например:<br>`msiexec /i Aladdin.JMS.WebAgent.x64.msi /quiet INSTALL_TYPE="WindowsService" PORTAL_URI="https://jms.server/jms/private" USE_SSL="1" SSL_CREATE_CERTIFICATE="0" CERTIFICATE_THUMBPRINT="b696f465af65b503d6e69d9ca47c4568bac50f38"` |

# 19. Коннектор КриптоПро DSS

Коннектор КриптоПро DSS представляет собой компонент JMS, обеспечивающий интеграцию с продуктом «Сервер электронной подписи „КриптоПро DSS“» компании КриптоПро.

Коннектор КриптоПро DSS включает в себя два компонента:

- модуль коннектора для сервера JMS (название компонента в мастере установки — «Поддержка Сервера JMS»), устанавливается на машину с компонентом JMS Server;
- модуль расширения для консоли управления JMS (название компонента в мастере установки — «Поддержка Консоли управления JMS»), устанавливается на машину с компонентом JMS Admin.

**Важно!** Компонент «Поддержка консоли управления JMS» требует установки на каждом хосте, на котором функционирует приложение *Консоль управления JMS*.

Инсталлятор коннектора способен автоматически определять наличие на хосте того типа приложения (сервера JMS или консоли управления), для которого требуется установить соответствующий компонент коннектора. Нужный компонент коннектора можно также выбрать вручную в режиме выборочной установки.

## 19.1 Дистрибутив

Дистрибутив коннектора КриптоПро DSS состоит из одного файла *Aladdin.EMS.CPDSS.Setup.msi*.

Файл дистрибутива содержит в себе оба компонента: как модуль коннектора для сервера JMS, так и модуль расширения для консоли управления JMS.

## 19.2 Системные требования коннектора КриптоПро DSS

Системные требования коннектора КриптоПро DSS при установке:

- его серверного компонента на сервере JMS совпадают (не требуют дополнительных ресурсов) с системными требованиями к установке компонента JMS Server (см. разделы 4.1 и 4.3);
- его компонента, предназначенного для консоли управления JMS, совпадают (не требуют дополнительных ресурсов) с системными требованиями к установке компонента JMS Admin (см. разделы 4.2 и 4.3).

## 19.3 Установка коннектора КриптоПро DSS

**Примечание.** В случае если компоненты JMS Server и JMS Admin устанавливаются раздельно (например, когда они установлены на разных компьютерах), то установку коннектора КриптоПро DSS надо выполнить в следующем порядке:

1. Запустить инсталлятор на машине с компонентом JMS Server (т.е. на сервере JMS).
2. Запустить инсталлятор на машине с компонентом JMS Admin (т.е. на консоли управления JMS).

Чтобы установить коннектор КриптоПро DSS, выполните следующие действия.

1. Запустите на выполнение файл инсталлятора.

Отобразится следующее окно.

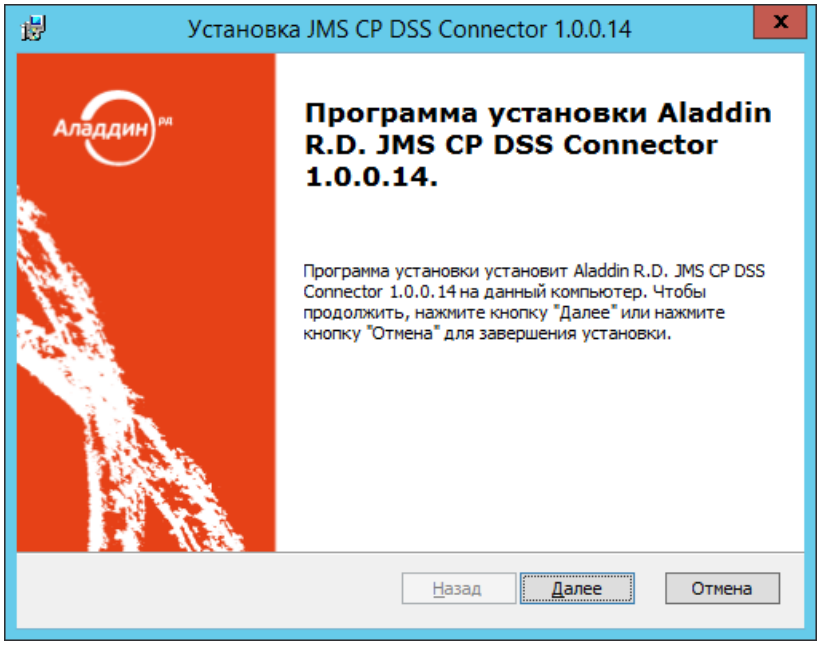



*Рис. 261 – Окно приветствия мастера установки коннектора КриптоПро DSS*

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

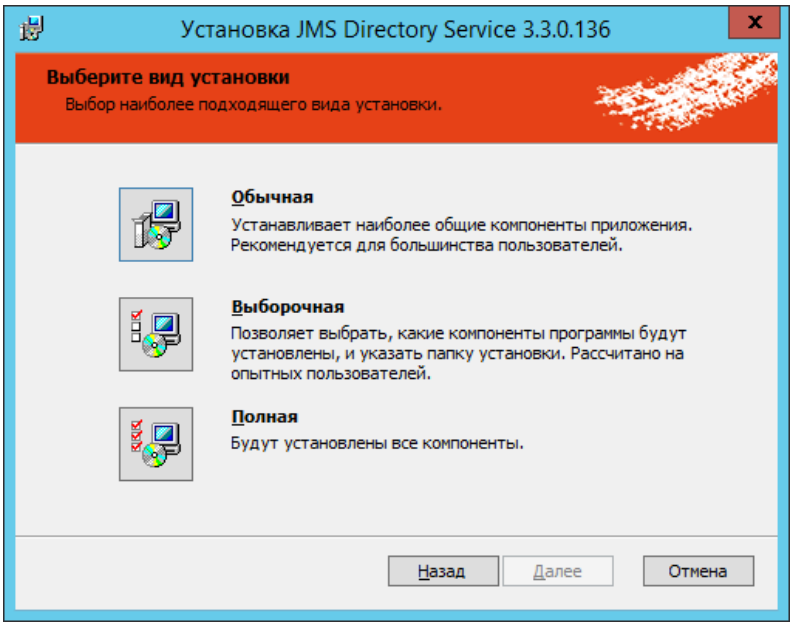



*Рис. 262 – Окно выбора варианта установки*

3. Если на компьютере установлены оба компонента – JMS Server и JMS Admin – выберите пункт **Полная**; на компьютере будут автоматически установлены как модуль коннектора для сервера JMS, так и модуль расширения для административной консоли JMS. Далее следуйте указаниям мастера до завершения процесса установки.
   В противном случае выберите пункт **Выборочная**.

Отобразится следующее окно.

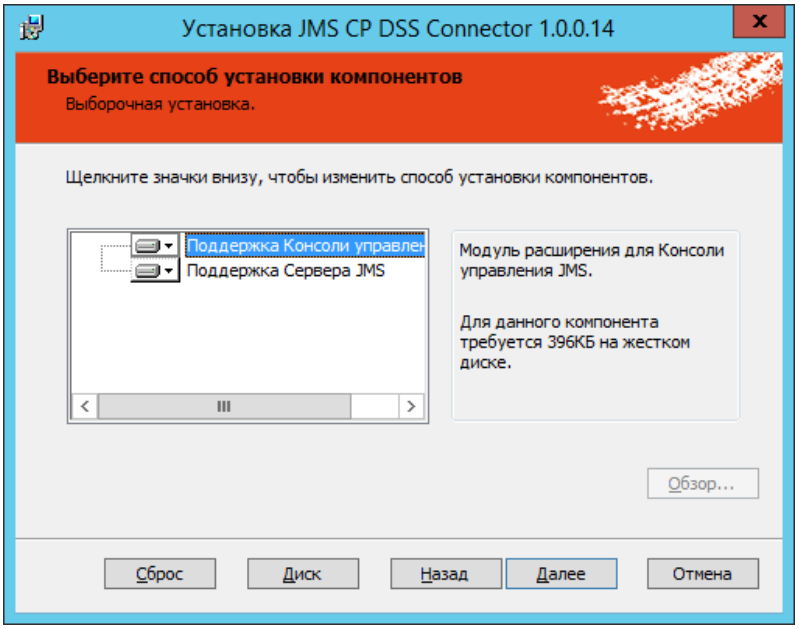



*Рис. 263 – Окно выбора компонентов коннектора КриптоПро DSS*

Выполните настройки установки каждого компонента в отдельности.

**Примечания:**

1. Чтобы задать путь установки, отличный от пути по умолчанию, напротив поля **Расположение** нажмите **Обзор** и внесите необходимые изменения.
2. Если необходимо установить компоненты коннектора выборочно, отключите лишние компоненты, в противном случае автоматически будут установлены все компоненты коннектора, применимые к данному хосту (например, если на данном хосте установлено только приложение *Консоль управления JMS*, то из всего инсталляционного комплекта будут установлен компонент «Поддержка Консоли управления JMS»).

4. Нажмите **Далее**.

Отобразится следующее окно.

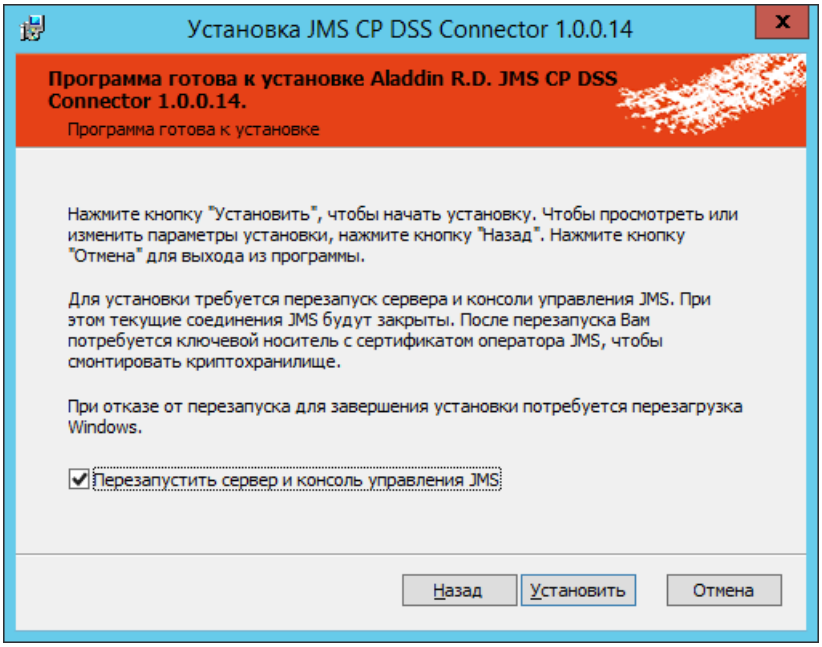



*Рис. 264 – Окно готовности к установке*

5. 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).
6. Нажмите **Установить**.
7. В случае установленного флага **Перезапустить сервер и консоль управления JMS** (см. выше) отобразится окно запроса на перезагрузку сервера и консоли управления JMS (Рис. 265). (Если флаг не был установлен перейдите к следующему шагу.)

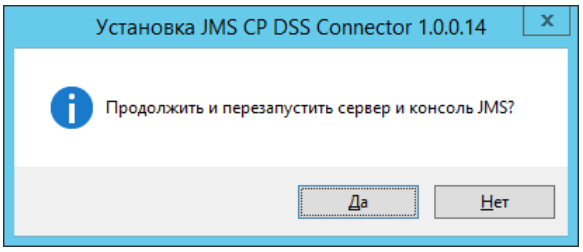



*Рис. 265 – Окно запроса перезагрузки сервера*

Нажмите **Да** для продолжения установки коннектора.

8. По окончанию установки отобразится следующее окно.

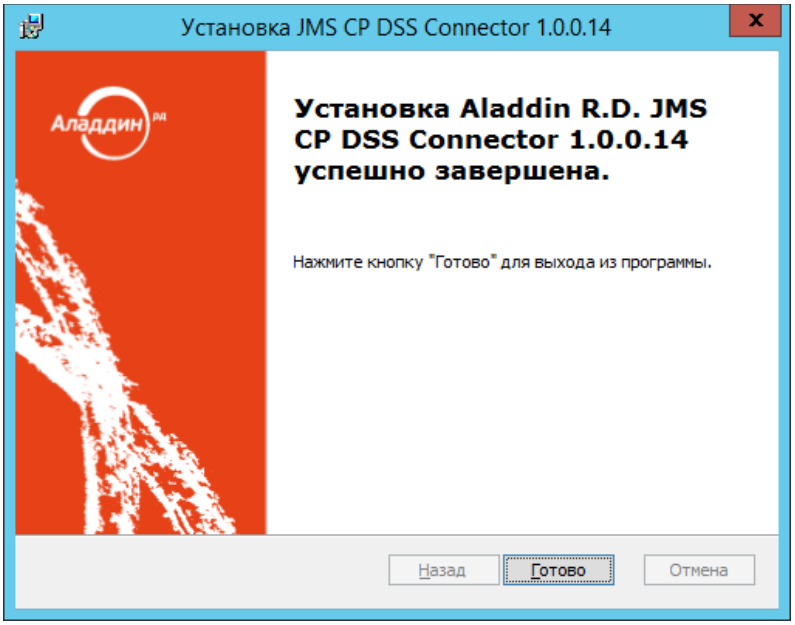



*Рис. 266 – Окно завершения процедуры установки*

9. Для завершения установки нажмите **Готово**.

После установки компонента коннектора на сервере JMS, выполните установку соответствующего компонента (повторите шаги 1—9) на всех компьютерах с консолью управления JMS.

# 20. Коннектор к Offline Certification Authority

Коннектор к Offline Certification Authority представляет собой компонент JMS, который позволяет выполнять выпуск сертификатов пользователей в аккредитованных удостоверяющих центрах, не имеющих сетевого подключения к телекоммуникационным сетям общего пользования.

Коннектор к Offline Certification Authority включает в себя два компонента:

- компонент коннектора для сервера JMS, устанавливается на компьютер с компонентом JMS Server;
- модуль расширения для консоли управления JMS, устанавливается на компьютер с компонентом JMS Admin.

**Важно!** Модуль расширения для консоли управления JMS требует установки на каждом хосте, на котором функционирует приложение *Консоль управления JMS*.

## 20.1 Дистрибутив

Дистрибутив коннектора к Offline Certification Authority состоит из двух компонентов:

- *Aladdin.EMS.OfflineCA.Server.X.X.X.XX-x64.msi / Aladdin.EMS.OfflineCA.Server.X.X.X.XX-x86.msi* – инсталлятор для установки на сервере JMS (соответственно для 32- / 64-битных платформ);
- *Aladdin.EMS.OfflineCA.Admin.X.X.X.XX-x64.msi / Aladdin.EMS.OfflineCA.Admin.X.X.X.XX-x86.msi* – инсталлятор для установки на компьютере с консолью управления JMS (соответственно для 32- / 64-битных платформ).

## 20.2 Системные требования коннектора к Offline Certification Authority

Для установки серверного компонента, входящего в состав коннектора к Offline Certification Authority, требуется не менее 10 Мбайт свободной дисковой памяти на компьютере. Остальные требования совпадают с требованиями к среде функционирования компонента JMS Server (см. разделы 4.1 и 4.3).

Для установки модуля расширения для консоли управления JMS, входящего в состав коннектора к Offline Certification Authority, требуется не менее 10 Мбайт свободной дисковой памяти на компьютере. Остальные требования совпадают с требованиями к среде функционирования компонента JMS Admin (см. разделы 4.2 и 4.3).

## 20.3 Установка коннектора к Offline Certification Authority

### 20.3.1 Установка серверного компонента коннектора к Offline Certification Authority

Чтобы установить компонент коннектора, предназначенный для компьютера с сервером JMS, выполните следующие действия.

1. Запустите на выполнение файл инсталлятора:

- *Aladdin.EMS.OfflineCA.Server.X.X.X.XX-x64.msi* – в случае 64-битной платформы;
- *Aladdin.EMS.OfflineCA.Server.X.X.X.XX-x86.msi* – в случае 32-битной платформы.

Отобразится следующее окно.

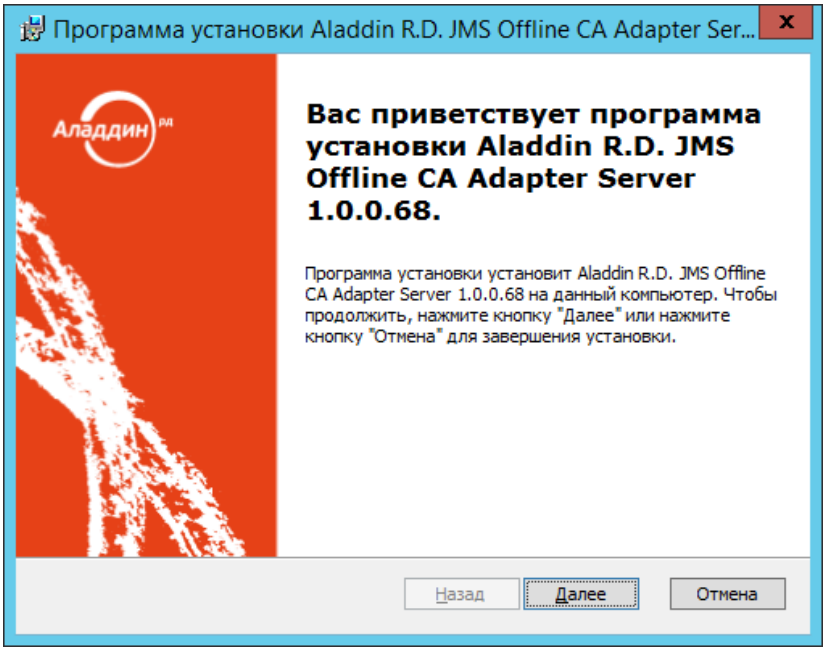



*Рис. 267 – Окно приветствия мастера установки коннектора к Offline Certification Authority*

2. Нажмите **Далее**. Отобразится окно лицензионного соглашения.
   Выберите **Я принимаю условия лицензионного соглашения**, нажмите **Далее** и следуйте указаниям мастера до полной установки серверного компонента коннектора к Offline Certification Authority.

   По завершении установки отобразится следующее окно.

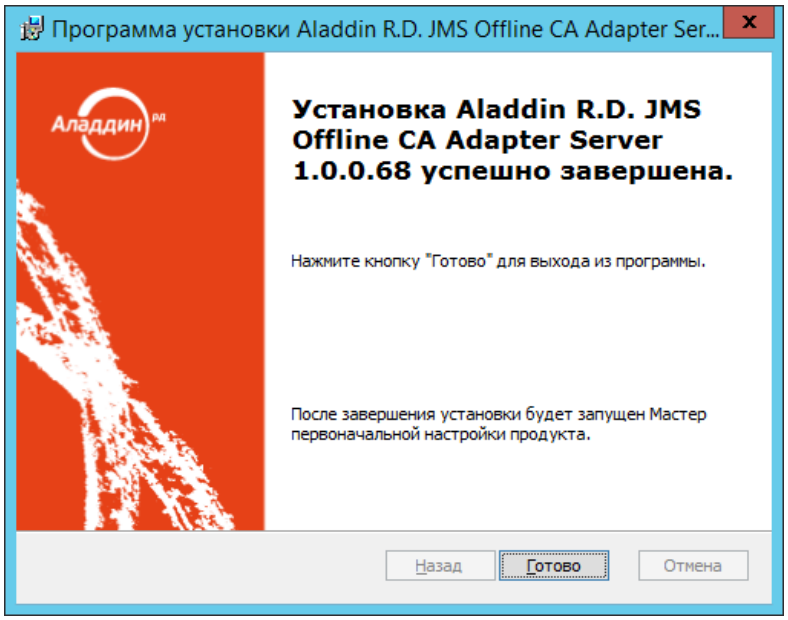



*Рис. 268 – Окно завершения процедуры установки*

По окончании установки серверного компонента коннектора автоматически запустится мастер его настройки.

### 20.3.2 Настройка коннектора к Offline Certification Authority (выполнение мастера настройки)

**Примечание.** Если вы закрыли окно мастера настройки коннектора к Offline Certification Authority после его автоматического запуска, то можете вновь открыть его, запустив вручную на выполнение файл *AladdinJMS.OfflineCertAuthority.Wizards.exe* (устанавливается на компьютер при установке серверного компонента коннектора и располагается в папке сервера JMS, по умолчанию C:\Program Files\Enterprise Management System Server\). Ручной запуск мастера настройки требует полномочий администратора в локальной операционной системе.

Окно приветствия мастера настройки коннектора выглядит следующим образом.

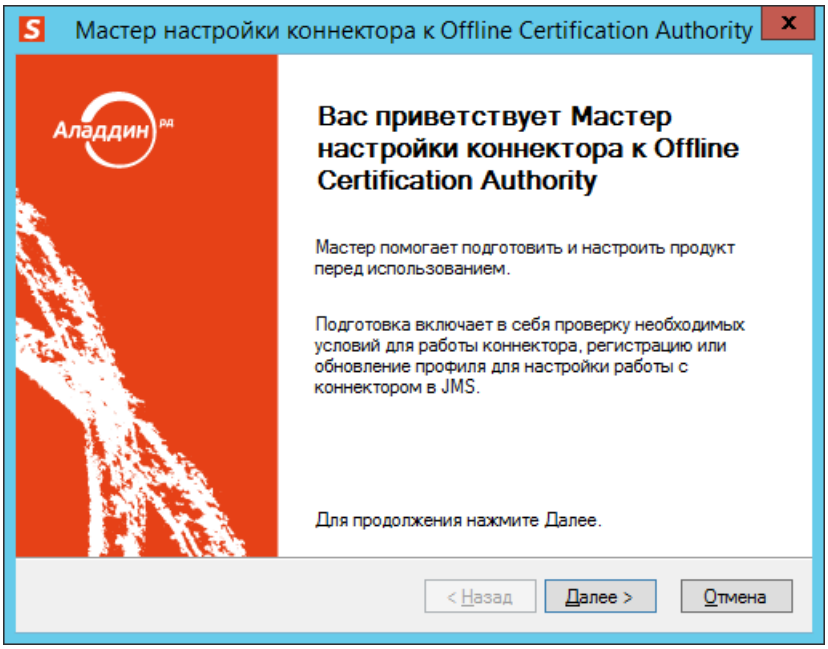



*Рис. 269 – Окно приветствия мастера настройки коннектора к Offline Certification Authority*

1. Нажмите **Далее**.
   Отобразится следующее окно.

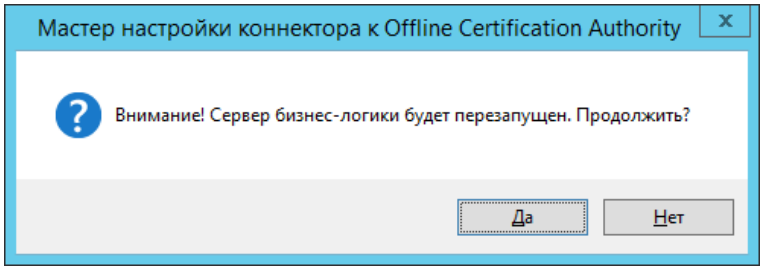



*Рис. 270 – Окно запроса на перезапуск службы сервера JMS*

2. Нажмите **Да** и дождитесь перезапуска службы сервера JMS. Если появится окно **Ввод PIN-кода** (см. рис. 172), введите PIN-код пользователя для электронного ключа оператора JMS, после чего нажмите **ОК**.

3. В случае если требуется обновление профиля коннектора в БД JMS, отобразится окно следующего вида.

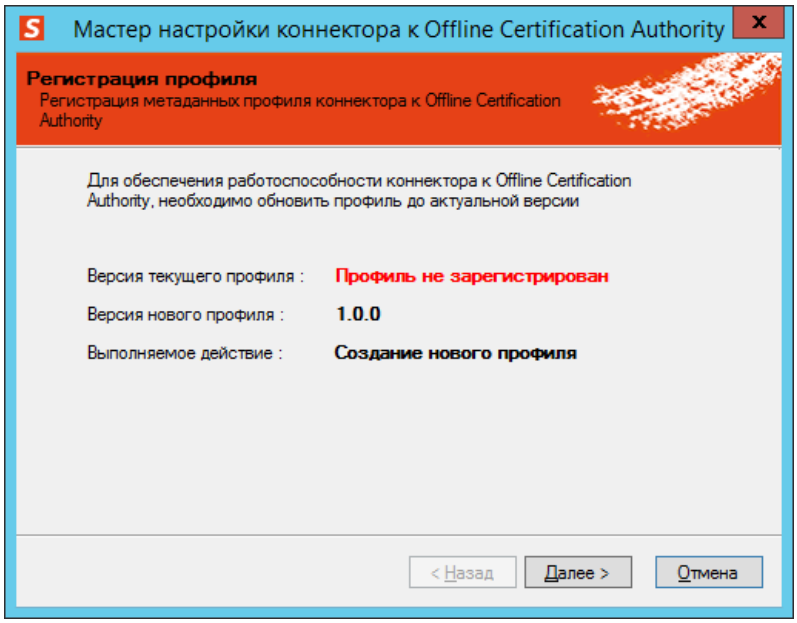



*Рис. 271 – Окно запроса на обновление профиля коннектора*

4. Нажмите **Далее**.
Отобразится окно завершения настройки коннектора.

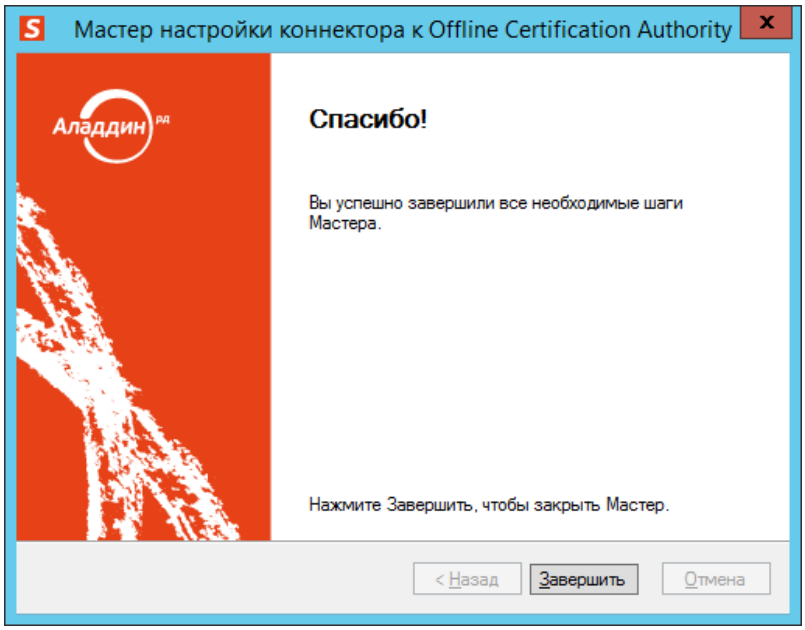



*Рис. 272 – Окно завершения настройки коннектора*

### 20.3.3 Установка модуля расширения для консоли управления JMS

Чтобы установить компонент коннектора к Offline Certification Authority, предназначенный для консоли управления JMS, выполните следующие действия.

1. Запустите на выполнение файл инсталлятора:

- *Aladdin.EMS.OfflineCA.Admin.X.X.X.XX-x64.msi* – в случае 64-битной платформы;
- *Aladdin.EMS.OfflineCA.Admin.X.X.X.XX-x86.msi* – в случае 32-битной платформы.

Отобразится следующее окно.

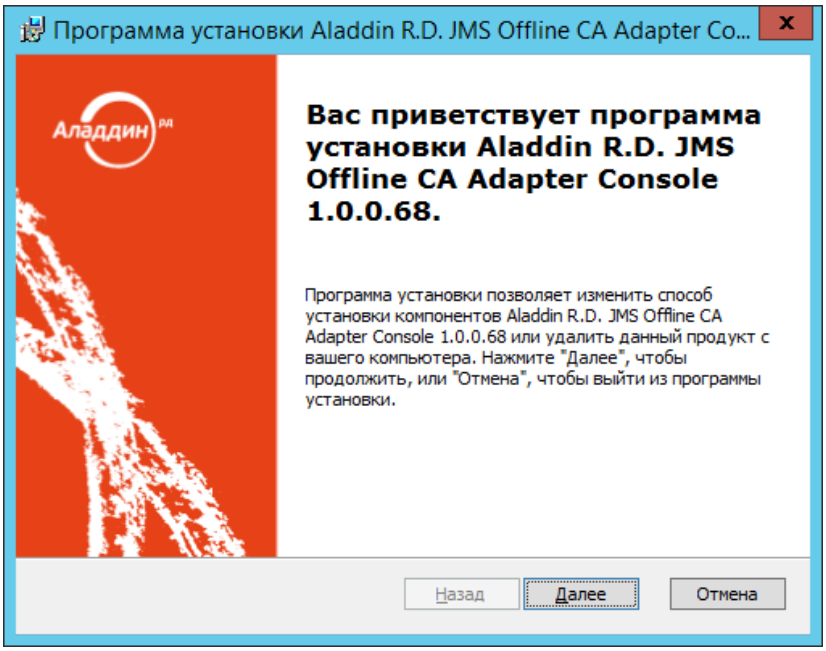



*Рис. 273 – Окно приветствия мастера установки модуля расширения для консоли управления JMS*

2. Нажмите **Далее**. Отобразится окно лицензионного соглашения.
Выберите **Я принимаю условия лицензионного соглашения**, нажмите **Далее** и следуйте указаниям мастера до полной установки компонента коннектора для консоли управления JMS.

   По завершении установки отобразится следующее окно.

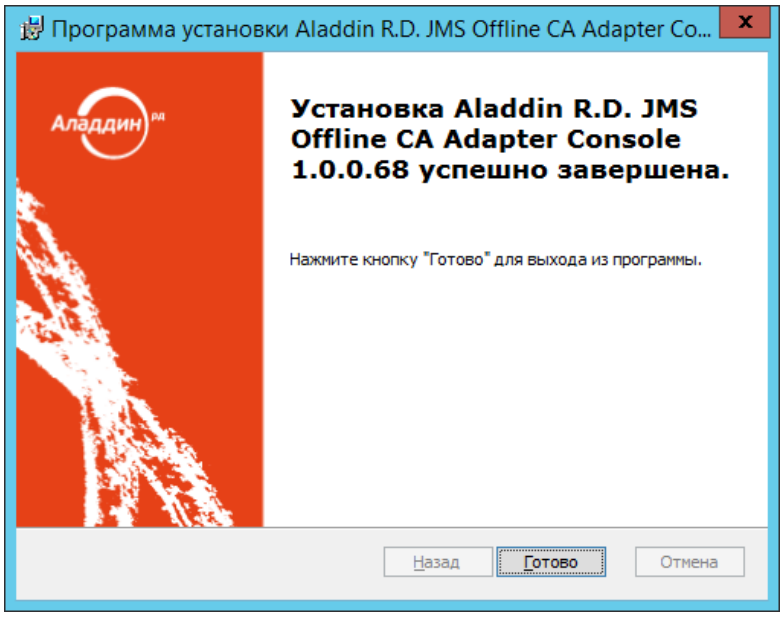



*Рис. 274 – Окно завершения процедуры установки*

# 21. Установка и настройка плагина СКЗИ «Крипто БД» для JMS и JAS

СКЗИ «Крипто БД» предназначено для обеспечения конфиденциальности и контроля целостности информации, хранящейся в таблицах баз данных СУБД Microsoft SQL, посредством криптографического преобразования и имитозащиты.

Использование наложенного сертифицированного СКЗИ «Крипто БД» для защиты таблиц БД JMS является обязательным для сертифицированной версии ПО JMS v3.7.

Для интеграции ПО JMS с СКЗИ «Крипто БД» необходимо выполнить следующие шаги:

1. Выполнить подготовительные действия для развертывания и настройки продукта (см. раздел «Подготовительные действия», с. 237);
2. Выполнить установку плагина «Крипто БД» на всех серверах JMS (см. раздел «Установка плагина «Крипто БД» на сервер JMS», с. 238);
3. Выполнить установку плагина «Крипто БД» на всех серверах JAS (см. раздел «Установка плагина «Крипто БД» на сервер JAS», с. 240);
4. Экспортировать файл конфигурации «Крипто БД» для работы с БД JMS (см. раздел «Процедура создания конфигурации СКЗИ «Крипто БД» для БД JMS», с. 240);
5. Установить СКЗИ «Крипто БД» (см. раздел «Установка СКЗИ «Крипто БД»», с. 244);
6. Выполнить автоматизированное конфигурирование «Крипто БД» (см. раздел «Конфигурирование СКЗИ «Крипто БД» для работы с БД JMS», с. 244);
7. Настроить роли администратора безопасности «Крипто БД» (см. раздел «Настройка ролей в БД для администратора безопасности СКЗИ «Крипто БД»», с. 248);
8. Включить сервер ключей «Крипто БД» (см. раздел «Ввод «Крипто БД» в эксплуатацию (запуск сервера ключей)», с. 249);

## 21.1 Подготовительные действия

Перед установкой и настройкой СКЗИ «Крипто БД» и его интеграцией с ПО JMS необходимо обеспечить следующие условия.

9. Должен быть развернут комплекс компонентов ПО JMS, готовый к работе в версии без защиты с помощью внешнего наложенного СКЗИ («Крипто БД»).
10. Должны быть выполнены предварительные действия, изложенные в разделе 21.1.1 (ниже).

### 21.1.1 Подготовительные действия на сервере СУБД (Microsoft SQL Server)

Действия производятся на сервере СУБД, на котором уже развернута БД JMS без наложенного СКЗИ, готовая к работе или уже эксплуатирующаяся.

#### 21.1.1.1 Конфигурирование сервера СУБД

Для установки «Крипто БД» и преобразования таблиц (шифрования) требуется предварительная конфигурация сервера СУБД. Для установки параметров выполните в консоли MSSQL (isql.exe, или в любой графической консоли для работы с SQL, например *Microsoft SQL Server Management Studio*, Рис. 275) от имени администратора БД (пользователь sa) сценарий, приведенный в документе «Приложение 1. Сценарий конфигурирования сервера СУБД для поддержки СКЗИ «Крипто БД»», с. 255.

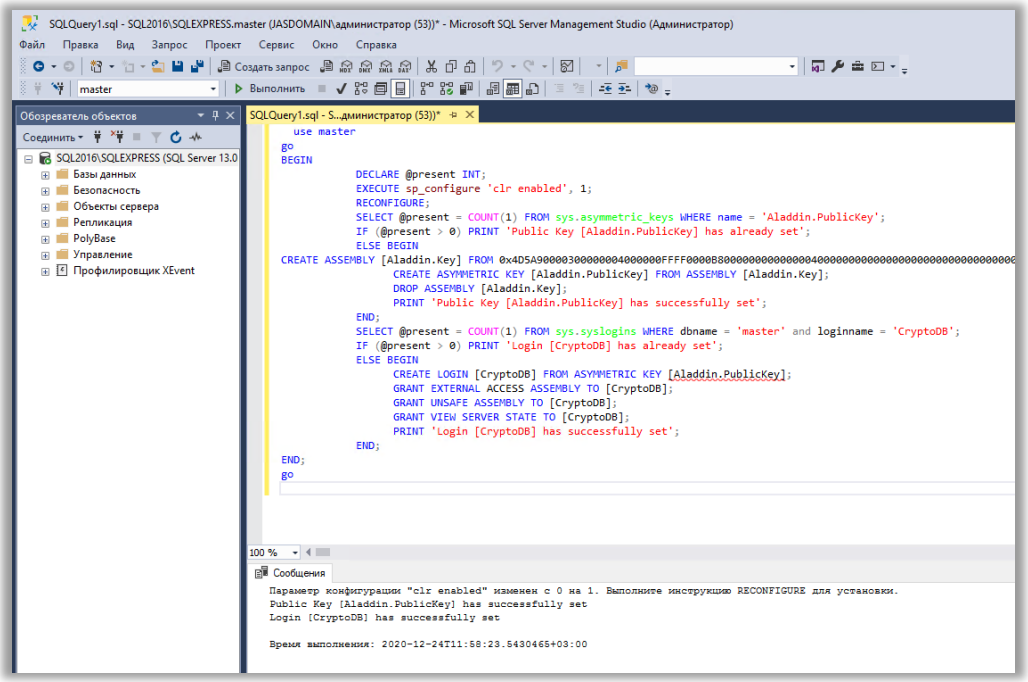



*Рис. 275 – Выполнение сценария конфигурирования сервера СУБД для работы с СКЗИ «Крипто БД»*

#### 21.1.1.2 Создание имени входа для администратора безопасности «Крипто БД»

В консоли MSSQL (isql.exe, или в любой графической консоли для работы с SQL, например *Microsoft SQL Server Management Studio*) от имени администратора БД (пользователь sa) создайте имя входа, которое будет в дальнейшем использоваться для администратора безопасности СКЗИ «Крипто БД».

**Примечание.** В текущем документе в качестве такого имени входа используется *cdbadmin*.

## 21.2 Установка плагинов «Крипто БД»

### 21.2.1 Дистрибутив

Дистрибутив плагинов СКЗИ «Крипто БД» состоит из двух файлов

- *Aladdin.JMS.CryptoDB.Server.Plugin.msi* – установочный пакет для сервера JMS;
- *Aladdin.JAS.CryptoDB.Server.Plugin.msi* – установочный пакет для сервера JAS.

### 21.2.2 Установка плагина «Крипто БД» на сервер JMS

На компьютер с установленным и настроенным компонентом JMS Server (в случае кластера – на все компьютеры с узлами кластера JMS) следует установите соответствующий плагин СКЗИ «Крипто БД».

Для этого выполните следующие действия.

11. Запустите на выполнение файл инсталлятора *Aladdin.JMS.CryptoDB.Server.Plugin.msi*.

Отобразится следующее окно.

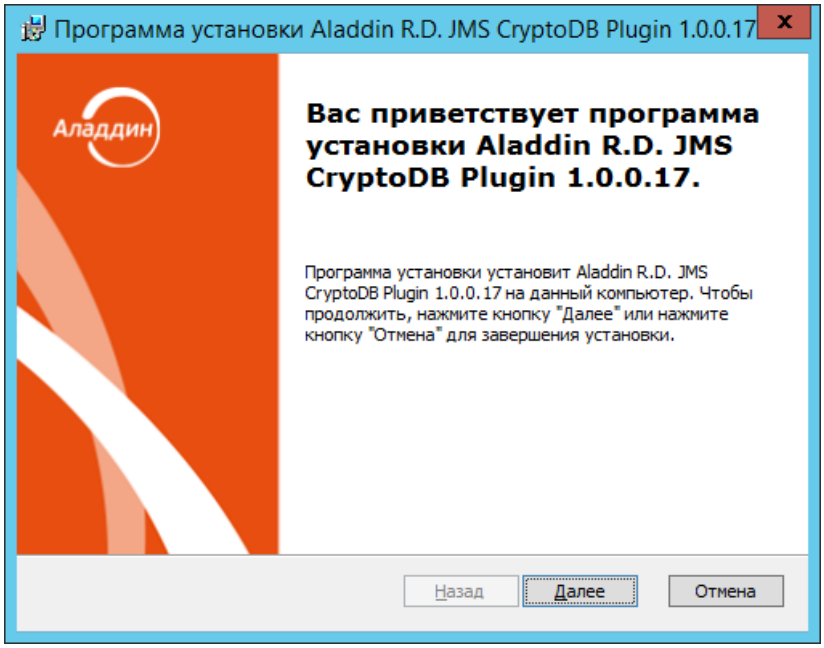



*Рис. 276 – Окно приветствия мастера установки плагина СКЗИ «Крипто БД» для сервера JMS*

12. Нажмите **Далее**. Отобразится окно лицензионного соглашения.
Выберите **Я принимаю условия лицензионного соглашения**, нажмите **Далее** и следуйте указаниям мастера до полной установки плагина.
По завершении установки отобразится следующее окно.

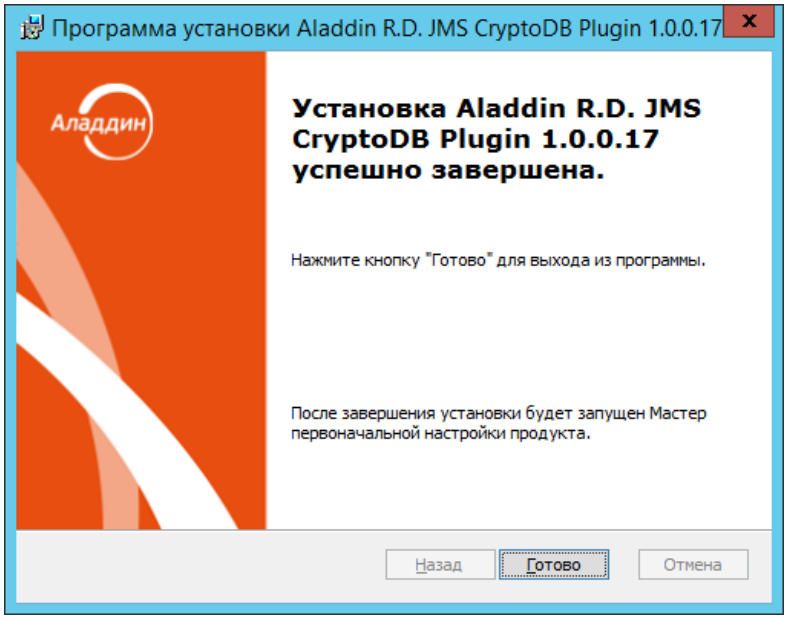



*Рис. 277 – Окно завершения процедуры установки*

В случае необходимости введите PIN-код для монтирования криптохранилища JMS.

По окончании установки в приложении Сервер JMS (серверный агент JMS) добавится вкладка **КриптоБД** (Рис. 278).

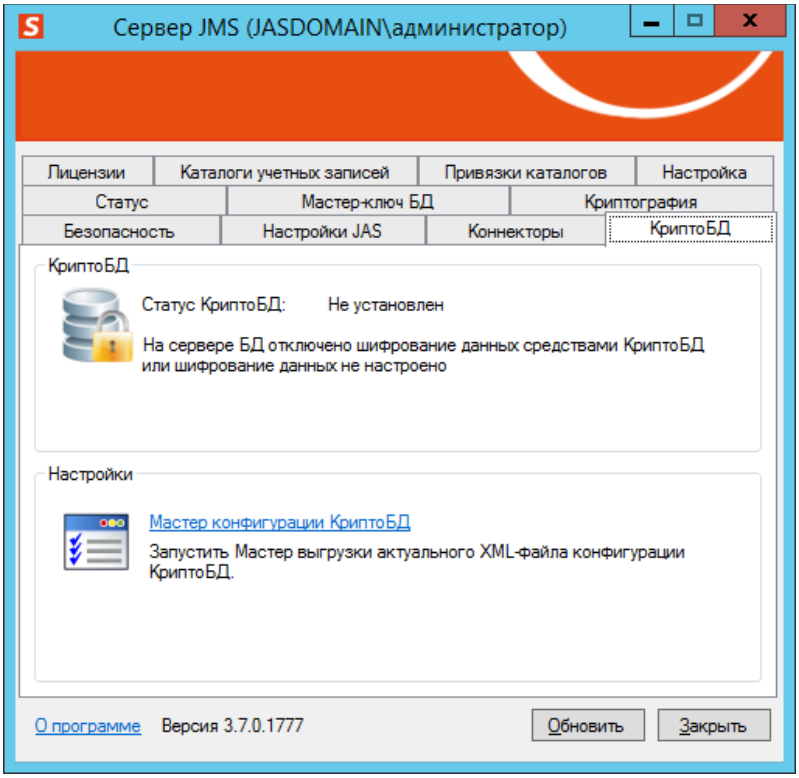



*Рис. 278 – Добавление вкладки **КриптоБД** в серверном агенте JMS*

### 21.2.3 Установка плагина «Крипто БД» на сервер JAS

На компьютер с установленным и настроенным компонентом JAS (в случае кластера – на все компьютеры с узлами кластера JAS) следует установить компонент *Aladdin.JAS.CryptoDB.Server.Plugin.msi*.

Подробное описание установки плагина на сервер приведено в части 3 руководства администратора [4] (раздел «Установка плагина «Крипто БД» на сервер JAS»).

## 21.3 Процедура создания конфигурации СКЗИ «Крипто БД» для БД JMS

Для получения конфигурационного файла СКЗИ «Крипто БД» для используемой БД JMS следует выполнить следующие действия.

1. На сервере JMS (в случае кластера на – на одном из узлов кластера) в приложении *Сервер JMS* (серверный агент) на вкладке **КриптоБД** (Рис. 278, выше) нажмите **Мастер конфигурации КриптоБД**.

Отобразится окно следующего вида.

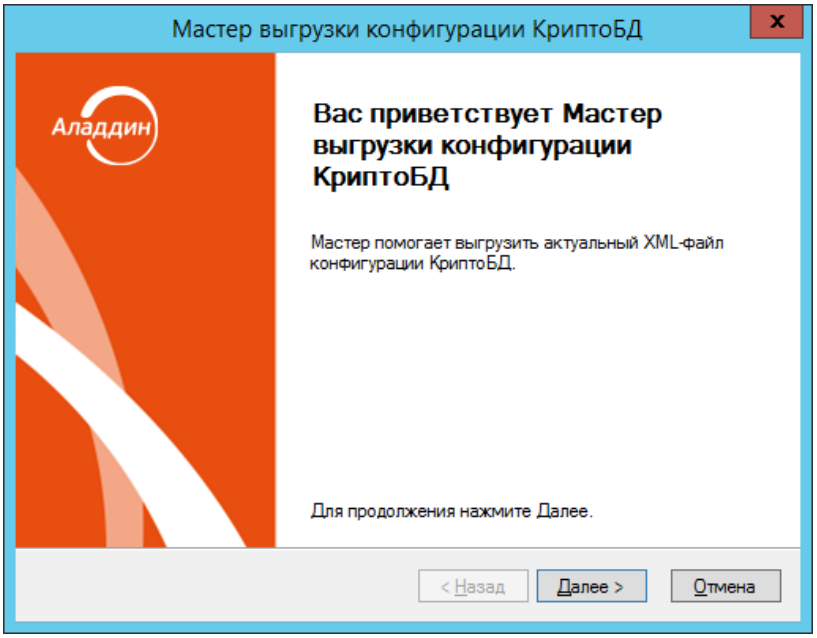



*Рис. 279 – Мастер выгрузки конфигурации СКЗИ «Крипто БД» для БД JMS*

2. Нажмите **Далее**.

   Отобразится окно следующего вида.

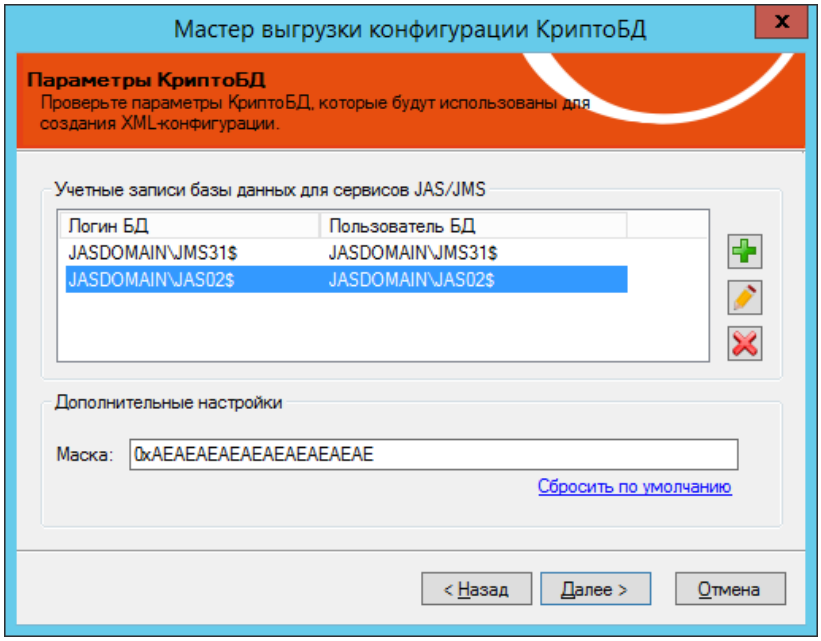



*Рис. 280 – Окно задания учетных записей для работы СКЗИ «Крипто БД» с БД JMS*

3. Выполните настройки в соответствии с Табл. 57.

*Табл. 57 – Заполнение параметров конфигурации СКЗИ «Крипто БД»*

| Настройка | Описание |
|---|---|
| **Учетные записи базы данных для сервисов JAS/JMS** | В строках таблицы (поля **Логин БД** и **Пользователь БД**) следует перечислить все учетные записи (для всех серверов JMS и JAS или соответствующих узлов кластеров), от имени которых выполняется подключение к серверу СУБД (**Логин БД**) и обращение к БД JMS (**Пользователь БД**), т.е. те учетные записи, которым в процессе эксплуатации JMS должен быть предоставлен доступ к таблицам, защищаемым с помощью СКЗИ «Крипто БД».<br>• Значение **Логин БД** соответствует значению, вводимому в мастере первоначальной настройки (Рис. 101, с. 91) в поле **Логин** (либо соответствующая учетная запись Windows NT Security).<br>• Значение **Пользователь БД** соответствует значению, вводимому в мастере первоначальной настройки (Рис. 105, с 94) в поле **Логин** (либо соответствующая учетная запись Windows NT Security)<br>(В отношении сервера JAS аналогичные соответствия см. в настройках подключения сервера JAS к БД JMS: часть 3 руководства администратора [4], раздел «Подключение JAS к базе данных JMS».)<br>Полный перечень учетных записей (имен входа и пользователей БД), используемых серверами JMS и JAS для работы с БД JMS, можно также проверить в консоли SQL Server Management Studio. (Рис. 281 и Рис. 282, ниже).<br>Часть учетных записей заполняется в таблице автоматически (например, учетные записи для серверов или узлов кластера JAS). Учетные записи, используемые другими узлами кластеров JMS (по отношению к узлу, на котором запущен *Мастер выгрузки конфигурации КриптоБД*), следует заполнить вручную (для добавления строк учетных записей используйте значок  , для редактирования –  , для удаления –  ). |
| **Маска** | В данном поле устанавливается условное шестнадцатеричное значение, которое будет отображаться в зашифрованных полях таблиц, защищаемых с помощью СКЗИ «Крипто БД».<br>Значение по умолчанию: *0xAEAEAEAEAEAEAEAEAEAE* |

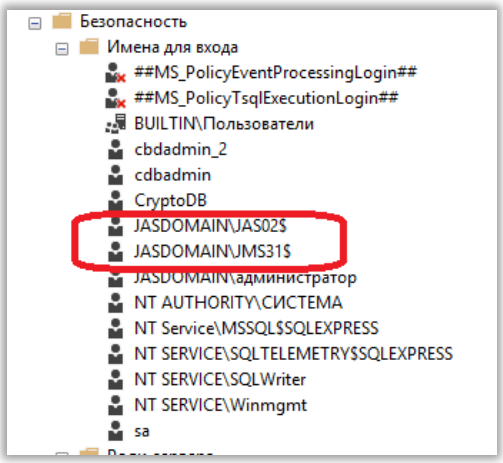



*Рис. 281 – Имена входа типа **Логин БД** для СУБД Microsoft SQL*

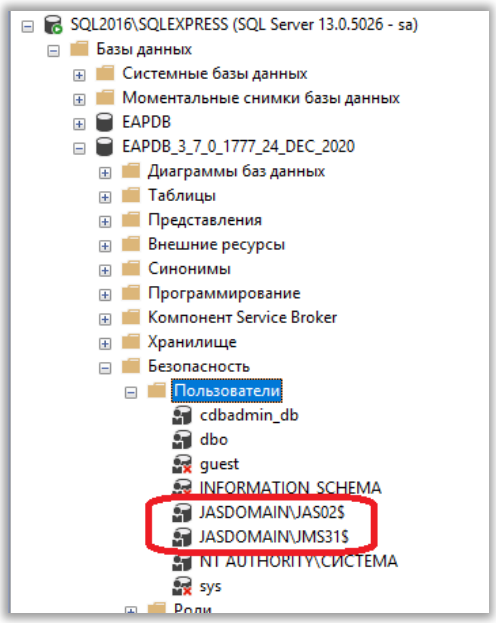



*Рис. 282 – Учетные записи типа **Пользователь БД** для БД JMS*

4. Нажмите **Далее**.

   Отобразится окно следующего вида.

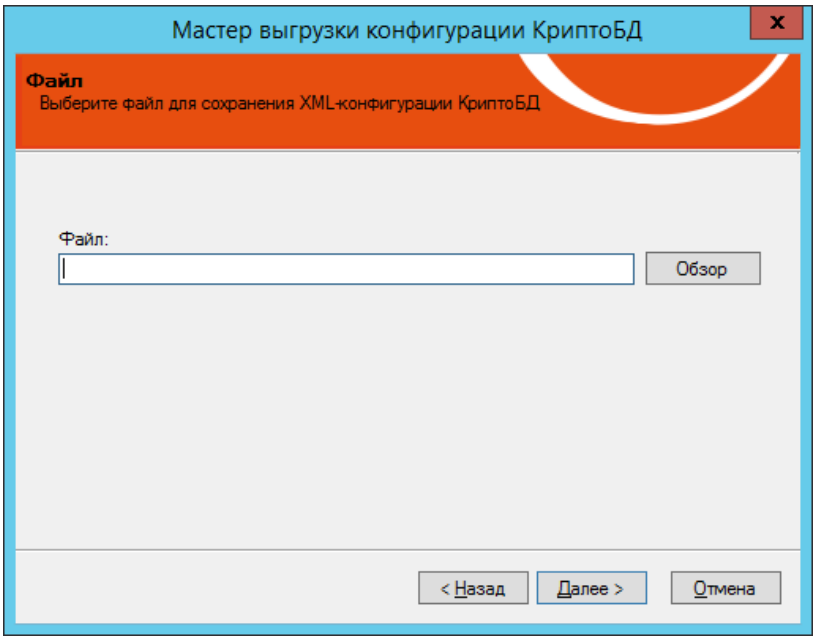



*Рис. 283 – Окно сохранения XML-файла конфигурации СКЗИ «Крипто БД» для БД JMS*

5. Введите имя файла и нажмите **Далее**.

Отобразится окно следующего вида.

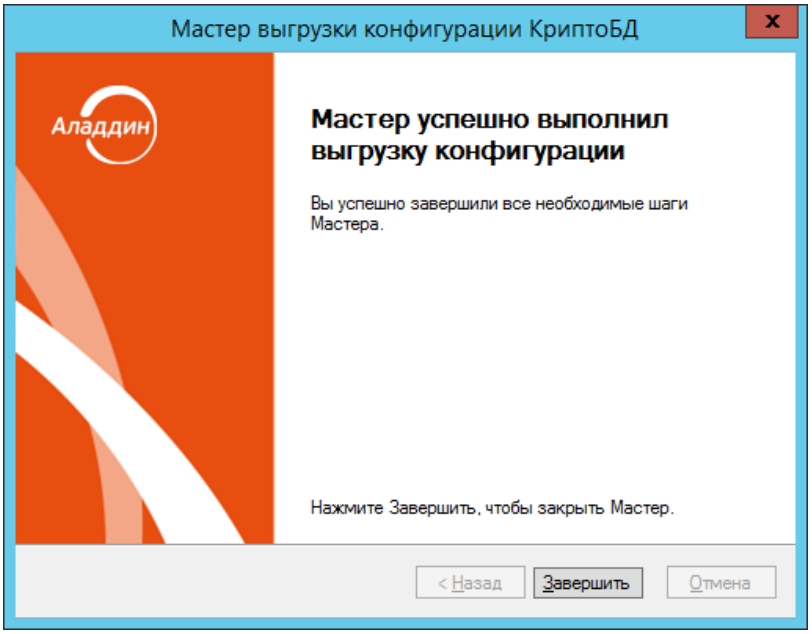



*Рис. 284 – Окно завершения процедуры*

Процедура создания конфигурации СКЗИ «Крипто БД» для БД JMS завершена. Сохраните полученный XML-файл для использования на дальнейших шагах интеграции ПО JMS с «Крипто БД».

## 21.4 Установка СКЗИ «Крипто БД»

Выполните установку СКЗИ «Крипто БД» на компьютере, входящем в один домен AD с сервером JMS (либо кластером JMS).

Для установки используйте следующие инсталляционные пакеты

- *Aladdin.CryptoDB.Admin.MSSQL.GOST_7.0.0.64_x64_Release.msi* – для 64-разрадных ОС Windows;
- *Aladdin.CryptoDB.Admin.MSSQL.GOST_7.0.0.64_x86_Release.msi* – для 32-разрадных ОС Windows.

Для уточнения процедуры установки следует использовать документацию СКЗИ «Крипто БД» [7].

## 21.5 Конфигурирование СКЗИ «Крипто БД» для работы с БД JMS

Для конфигурирования СКЗИ «Крипто БД» для работы с БД JMS выполните следующие действия.

1. Запустите на выполнение *Мастер конфигурирования КриптоБД*: **Пуск** -> **Аладдин** -> **Конфигурирование КриптоБД**

Отобразится окно следующего вида.

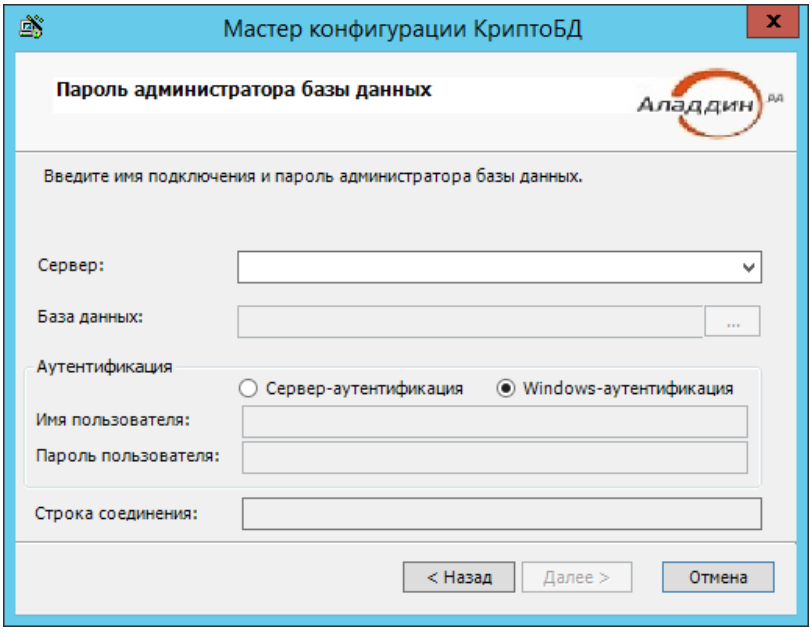



*Рис. 285 – Мастер конфигурирования СКЗИ «Крипто БД»*

2. Выполните настройки в соответствии с Табл. 58.

*Табл. 58 –Параметры подключения к БД JMS*

| Настройка | Описание |
|---|---|
| **Сервер** | Введите имя сервера СУБД в формате <имя_хоста>\<имя_SQL-сервера>, например:<br>SQL2016\SQLEXPRESS. |
| **База данных** | Введите имя базы данных JMS на SQL-сервере, указанном в поле **Сервер**. |
| **Сервер-аутентификация** | Выберите этот пункт для подключения к базе данных с использованием стандартной аутентификации на сервере СУБД. В полях **Имя пользователя** и **Пароль пользователя** необходимо указать соответственно имя входа и его пароль для подключения к серверу СУБД. |
| **Windows-аутентификация** | Выберите этот пункт для подключения к базе данных с использованием аутентификации типа «проверка подлинности Windows».<br>(В этом случае аутентификация будет выполняться от имени пользователя, запустившего на выполнение *Мастер конфигурации Крипто БД*. Для успешной аутентификации следует на сервере СУБД предварительно создать имя входя для такого пользователя). |
| **Строка соединения** | (Нередактируемое поле)<br>Динамически отображает параметры подключения к серверу СУБД по мере заполнения остальных полей |

3. Нажмите **Далее**.

Отобразится окно следующего вида.

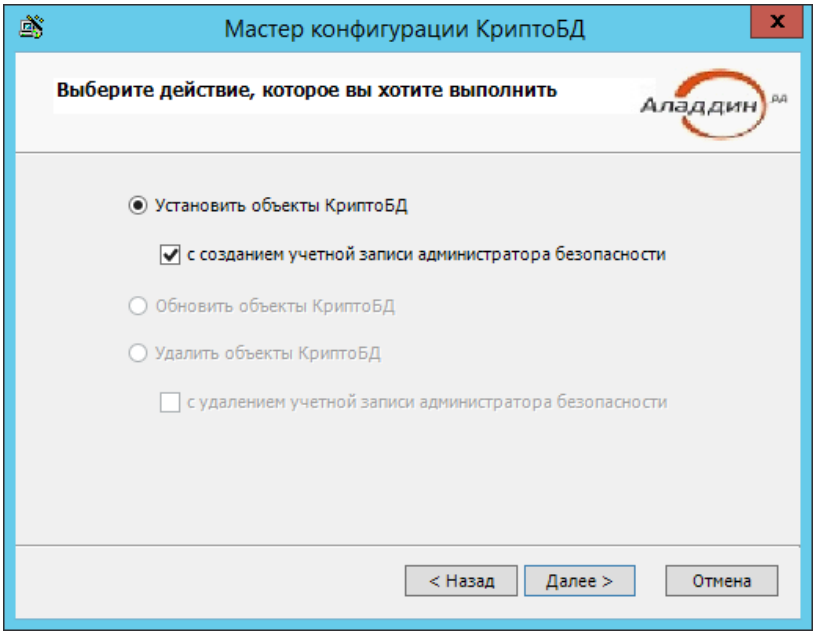



*Рис. 286 – Окно выбора действия в конфигураторе СКЗИ «Крипто БД»*

4. Установите (если не установлен) флаг «**с созданием учетной записи администратора безопасности**» и нажмите **Далее**.

   Отобразится окно следующего вида.

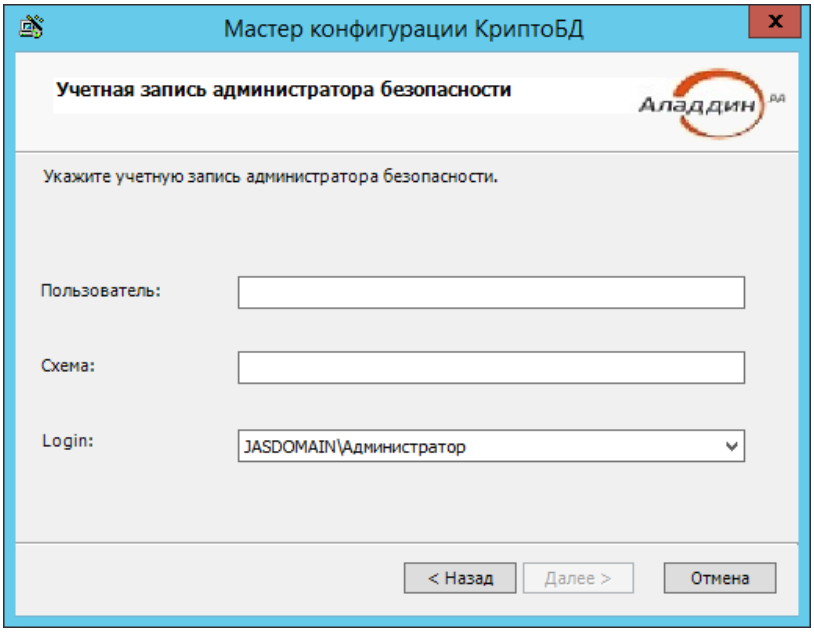



*Рис. 287 – Окно создания учетной записи администратора безопасности СКЗИ «Крипто БД»*

5. Выполните настройки в соответствии с Табл. 59.

*Табл. 59 –Параметры учетной записи администратора безопасности СКЗИ «Крипто БД»*

| Настройка | Описание |
|---|---|
| **Пользователь** | Введите имя пользователя, который будет автоматически создан в составе учётной записи администратора безопасности СКЗИ «Крипто БД», для работы с БД JMS. |
| **Схема** | Введите имя схемы, которая будет автоматически создана в составе учётной записи администратора безопасности СКЗИ «Крипто БД», для работы с БД JMS. |
| **Логин** | Укажите имя входа для администратора безопасности СКЗИ «Крипто БД», созданное на шаге 21.1.1.2 (см. раздел «Создание имени входа для администратора безопасности «Крипто БД»», с. 238). |

6. Нажмите **Далее**.

   Отобразится окно следующего вида.

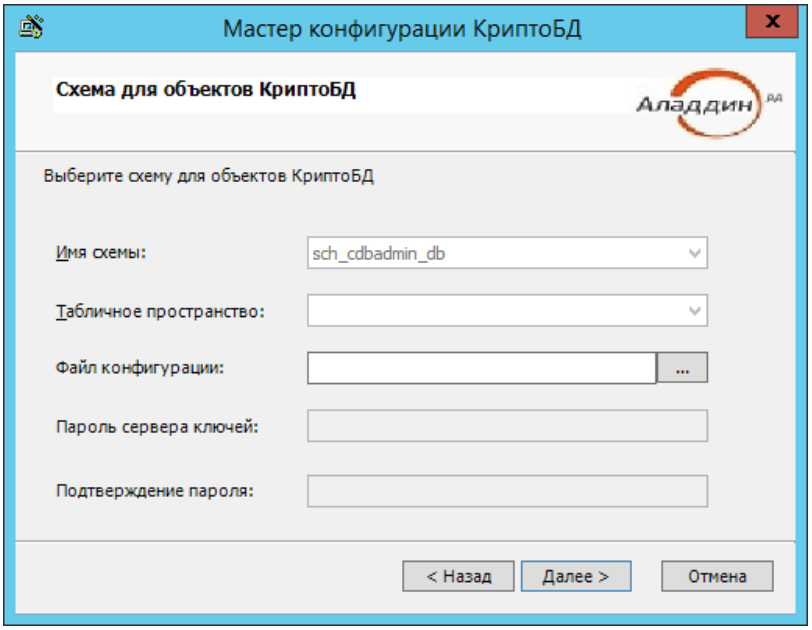



*Рис. 288 – Окно формирования схемы объектов СКЗИ «Крипто БД» для БД JMS*

7. Выполните настройки в соответствии с Табл. 60.

*Табл. 60 –Параметры схемы для объектов СКЗИ «Крипто БД»*

| Настройка | Описание |
|---|---|
| **Имя схемы** | (Нередактируемое поле).<br>Отображается введённое ранее имя схемы |
| **Табличное пространство** | (Нередактируемое поле).<br>Не используется |

| Настройка | Описание |
|---|---|
| **Файл конфигурации** | Выберите XML-файл конфигурации СКЗИ «Крипто БД», сгенерированный на шаге 21.3 (см. раздел «Процедура создания конфигурации СКЗИ «Крипто БД» для БД JMS», с. 240). |
| **Пароль сервера ключей** | Установите пароль сервера ключей СКЗИ «Крипто БД». |
| **Подтверждение пароля** | Подтвердите пароль. |

8. Нажмите **Далее** и следуйте указаниям мастера до появления окна следующего вида.

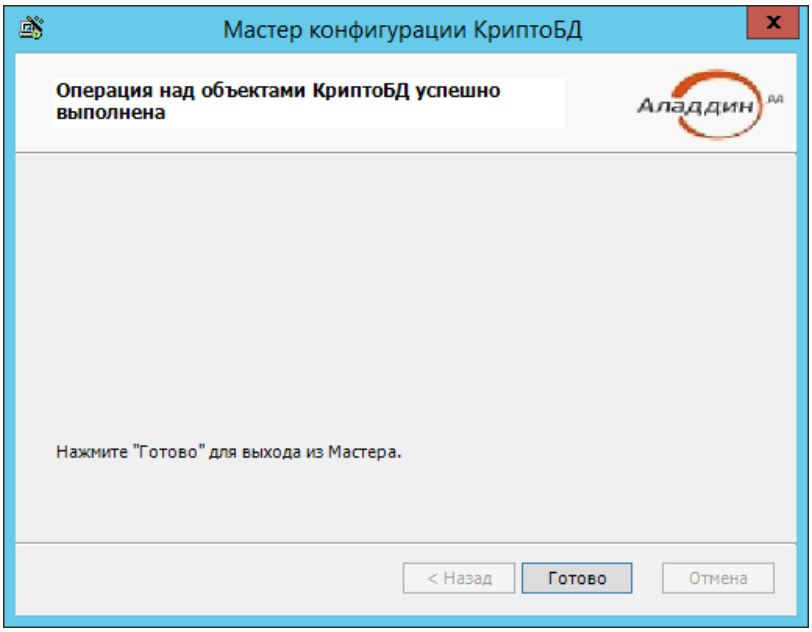



*Рис. 289 – Окно завершения конфигурирования СКЗИ «Крипто БД»*

9. Нажмите **Готово**.

По окончании работы *мастера* СКЗИ «Крипто БД» готово к подключению к БД JMS.

## 21.6 Настройка ролей в БД для администратора безопасности СКЗИ «Крипто БД»

Созданному в результате работы мастера конфигурирования пользователю БД JMS (администратору безопасности СКЗИ «Крипто БД», см. поле Пользователь на Рис. 287, с. 246) следует назначить установленные роли при помощи следующего сценария:

```
exec sp_addrolemember db_datareader, [%ADMIN%]
go
exec sp_addrolemember db_datawriter, [%ADMIN%]
go
exec sp_addrolemember db_ddladmin, [%ADMIN%]
go
exec sp_addrolemember db_securityadmin, [%ADMIN%]
go
```

или из графического интерфейса *Microsoft SQL Server Management Studio* (Рис. 290):

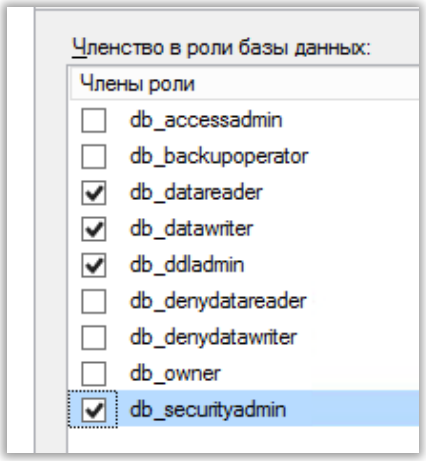



*Рис. 290 – Назначение ролей администратору безопасности СКЗИ «Крипто БД» для БД JMS*

## 21.7 Ввод «Крипто БД» в эксплуатацию (запуск сервера ключей)

Для запуска сервера ключей СКЗИ «Крипто БД» и включения криптографической защиты БД JMS выполните следующие действия.

1. Запустите на выполнение консоль администрирования «Крипто БД»: **Пуск** –> **Аладдин** –> **Консоль администрирования.**

   Отобразится окно следующего вида.

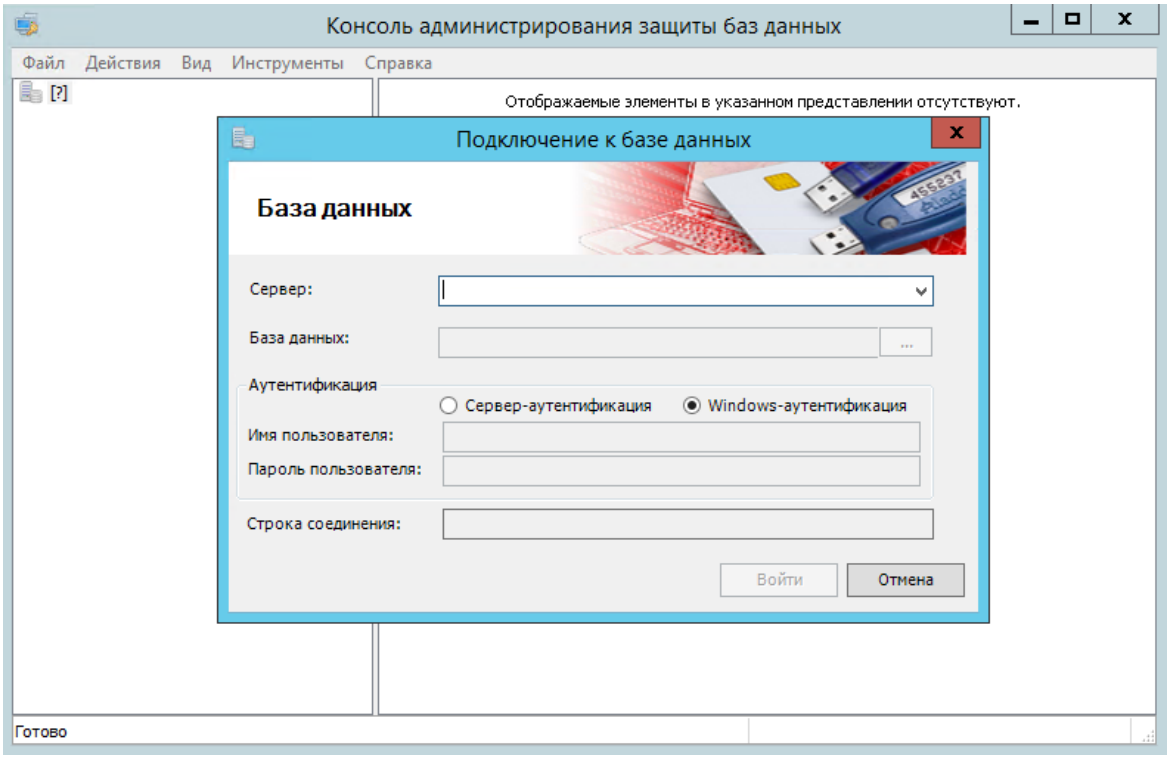



*Рис. 291 – Окно выбора БД JMS*

2. Введите имена сервера СУБД и БД JMS по аналогии с этапом конфигурирования (см. раздел «Конфигурирование СКЗИ «Крипто БД» для работы с БД JMS», с. 244)

**Важно!** Для аутентификации необходимо выбрать опцию **Сервер-аутентификация**, а в поле **Имя пользователя** ввести имя входа для администратора безопасности СКЗИ «Крипто БД», созданное на шаге 21.1.1.2 (см. раздел «Создание имени входа для администратора безопасности «Крипто БД»», с. 238) и соответствующий ему пароль в поле пароля.

3. Нажмите **Войти**.

   Отобразится окно следующего вида.

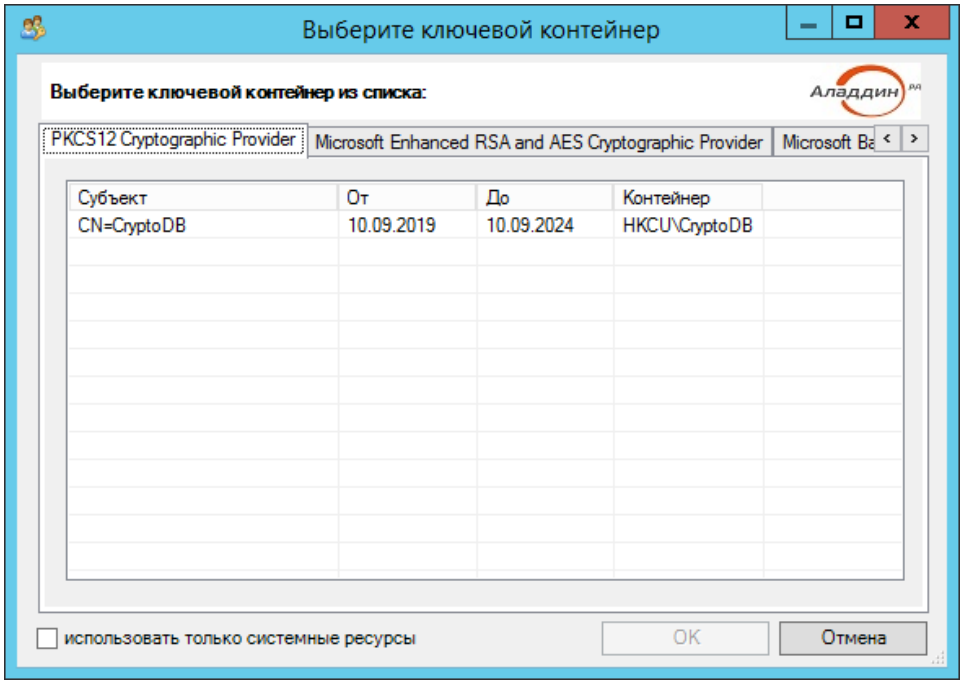



*Рис. 292 – Окно выбора действия в конфигураторе СКЗИ «Крипто БД»*

4. Выберите ключевой контейнер CryptoDB и нажмите **OK**.

   Откроется окно ввода пароля.

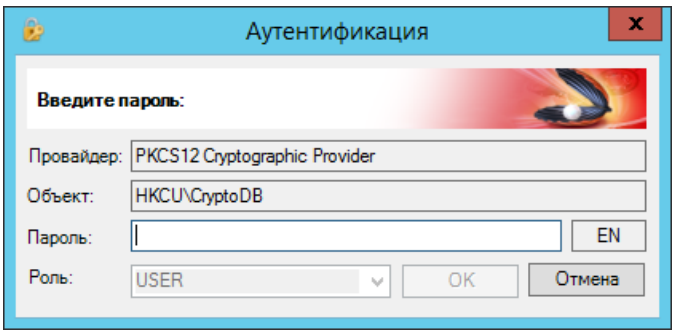



*Рис. 293 – Окно аутентификации в консоли администрирования СКЗИ «Крипто БД»*

5. Введите значение пароля по умолчанию (1234567890) для контейнера CryptoDB и нажмите **OK**.

Отобразится окно следующего вида.

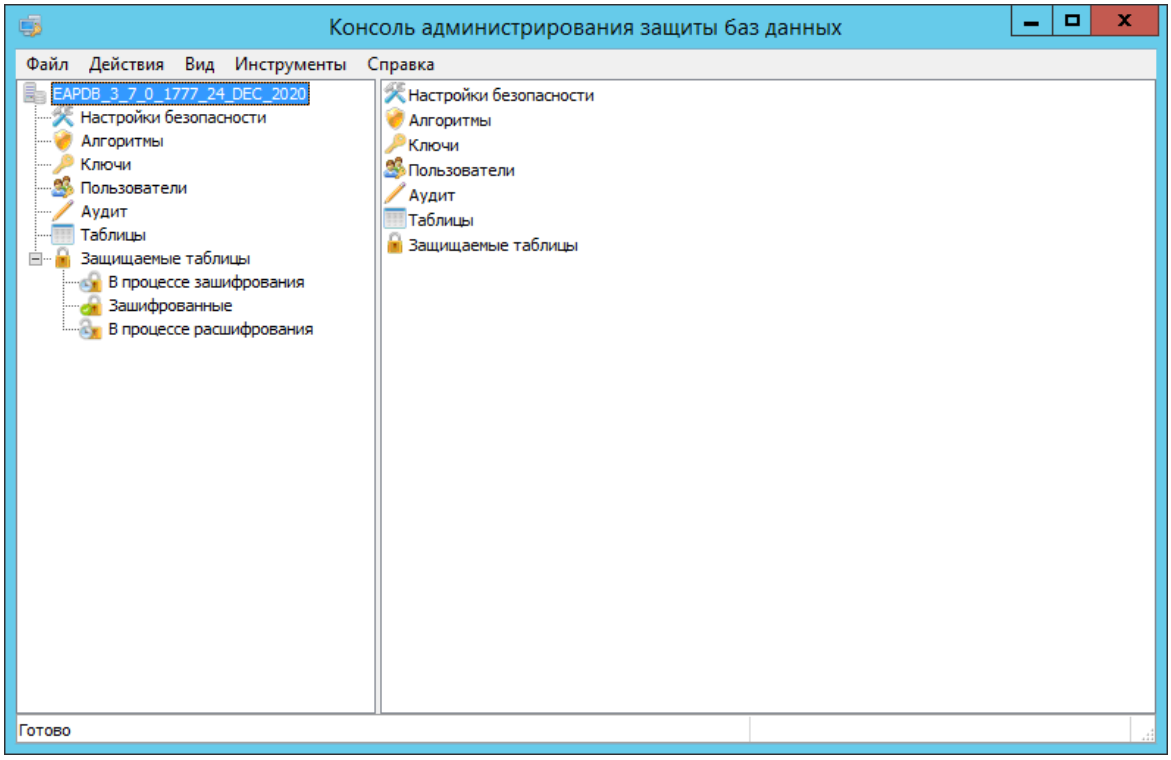



*Рис. 294 – Консоль администрирования СКЗИ «Крипто БД»*

6. В разделе **Защищаемые таблицы** в левой части окна выберите папку **В процессе зашифрования**.
7. Для каждой таблицы из папки **В процессе зашифрования** выполните следующие действия (в случае если раздел пуст, переходите к шагу 8).

7.1. По нажатию правой кнопкой мыши выберите **Зашифровать...**

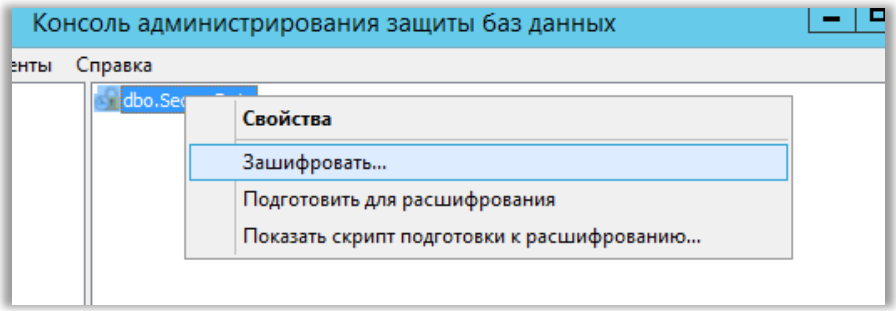



*Рис. 295 – Зашифрование таблиц из папки **В процессе зашифрования***

Отобразится окно следующего вида.

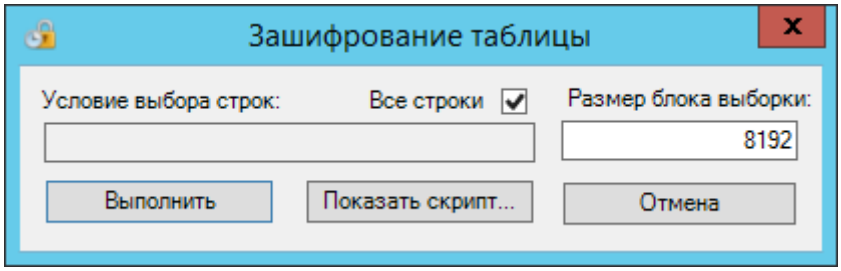



*Рис. 296 – Запрос на выполнения шифрования*

7.2. Нажмите **Выполнить**.

Отобразится окно с уведомлением о зашифровании.

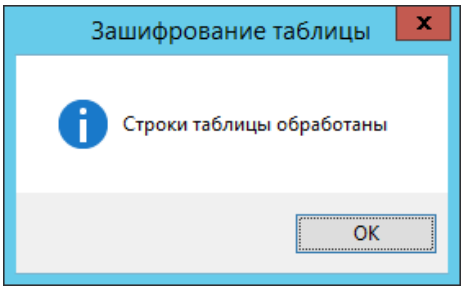



*Рис. 297 – Уведомление о зашифровании таблицы*

7.3. Нажмите **OK**

8. В папке **Зашифрованные** должны отображаться следующие таблицы (Рис. 298).

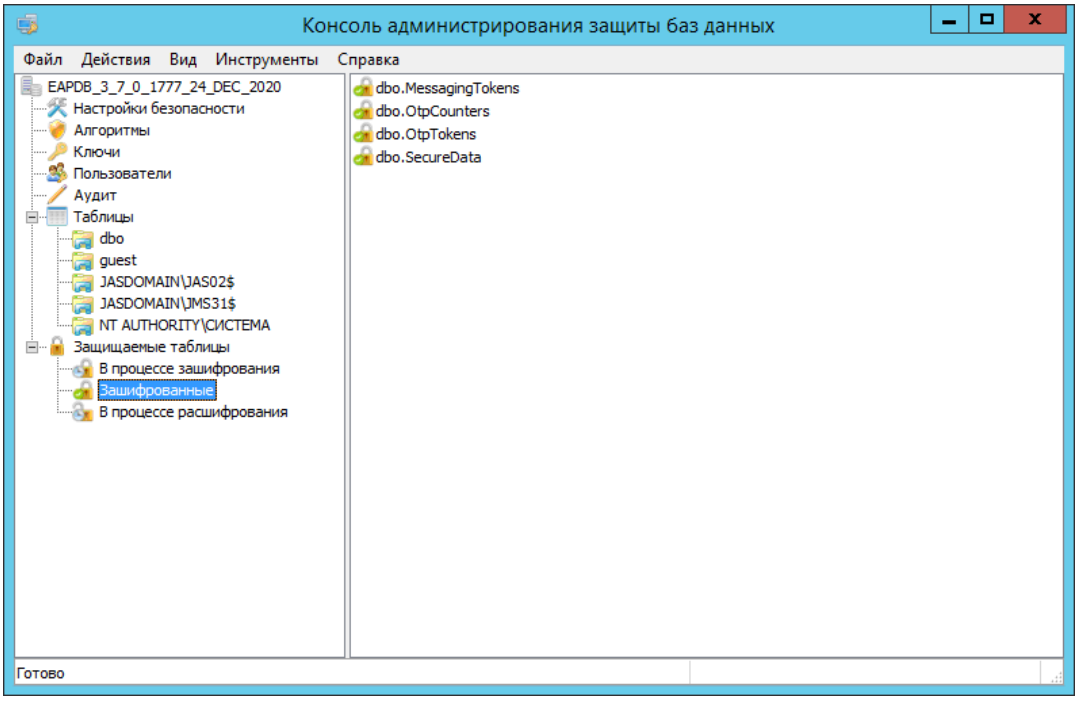



*Рис. 298 – Зашифрованные таблицы БД JMS*

9. В разделе **Настройки безопасности** выберите **Сервер ключей** и нажмите **Запустить** (Рис. 299)

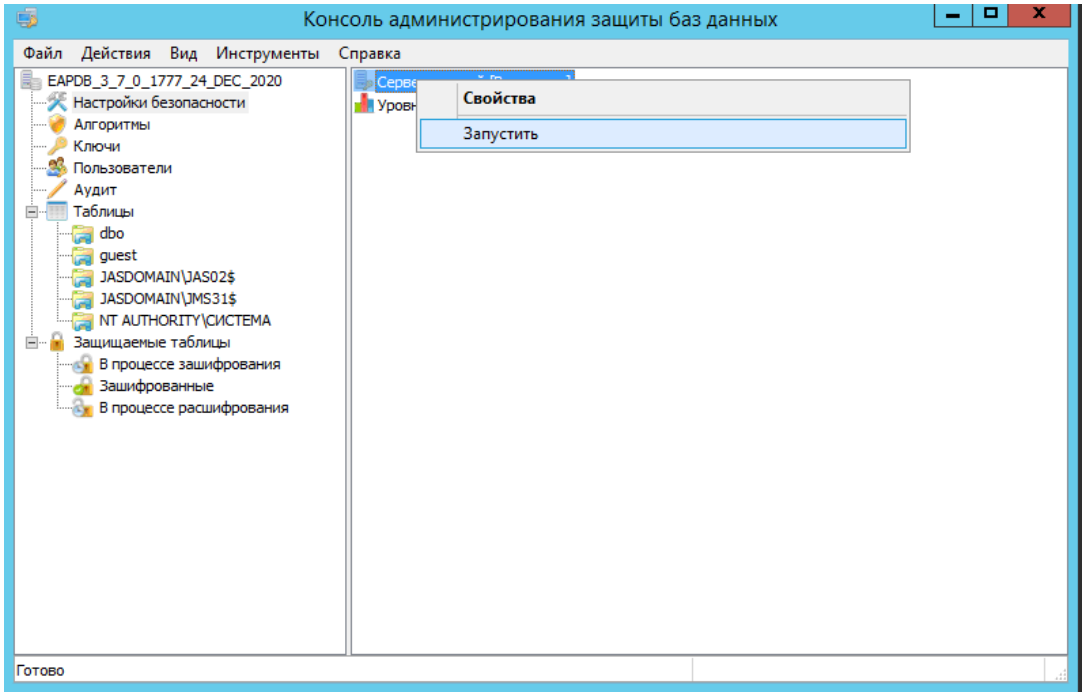



*Рис. 299 – Запуск сервера ключей СКЗИ «Крипто БД»*

10. Отобразится окно ввода пароля.

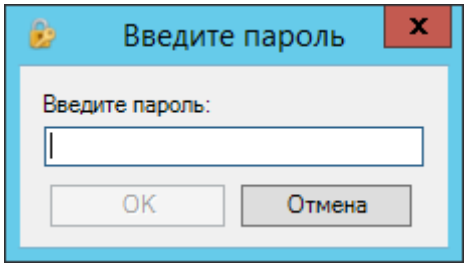



*Рис. 300 – Окно ввода пароля сервера ключей*

11. Введите пароль сервера ключей, заданный на этапе конфигурирования «Крипто БД» (Рис. 288, с. 247) и нажмите **OK**.

12. Сервер ключей перейдет в состояние активен (Рис. 301).

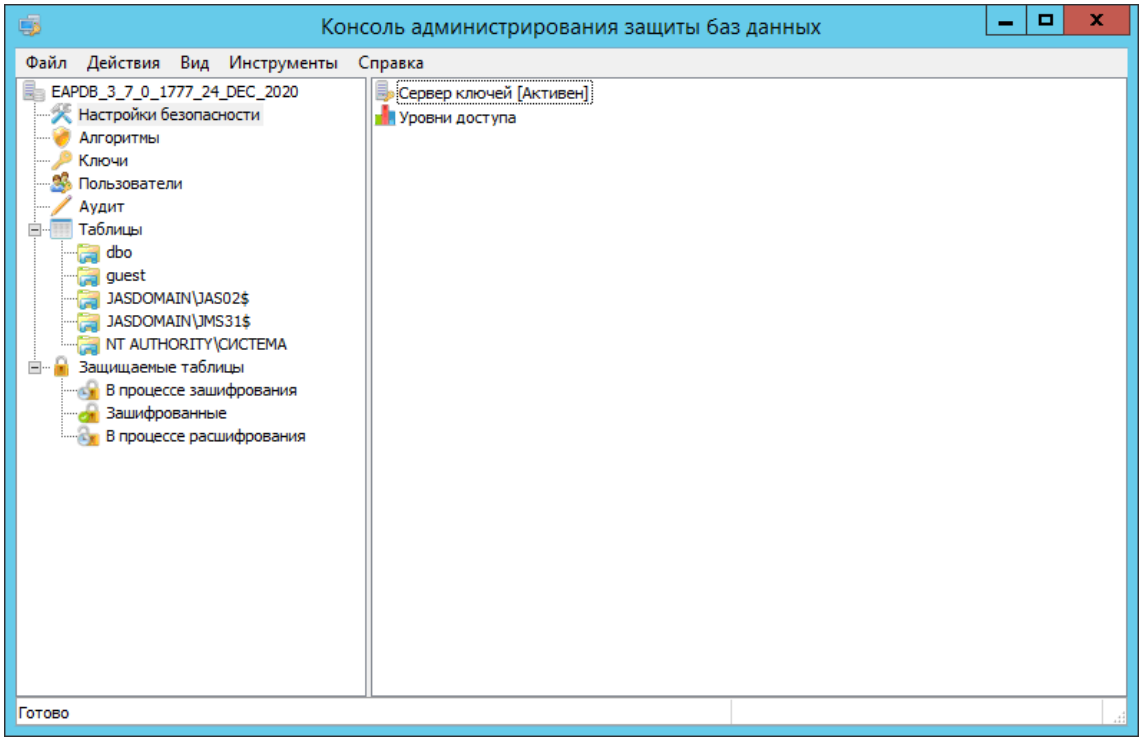



*Рис. 301 – Переход сервера ключей в состояние **Активен***

13. В серверном агенте JMS отобразится соответствующий статус (Запущен) для СКЗИ «Крипто БД» (Рис. 302).

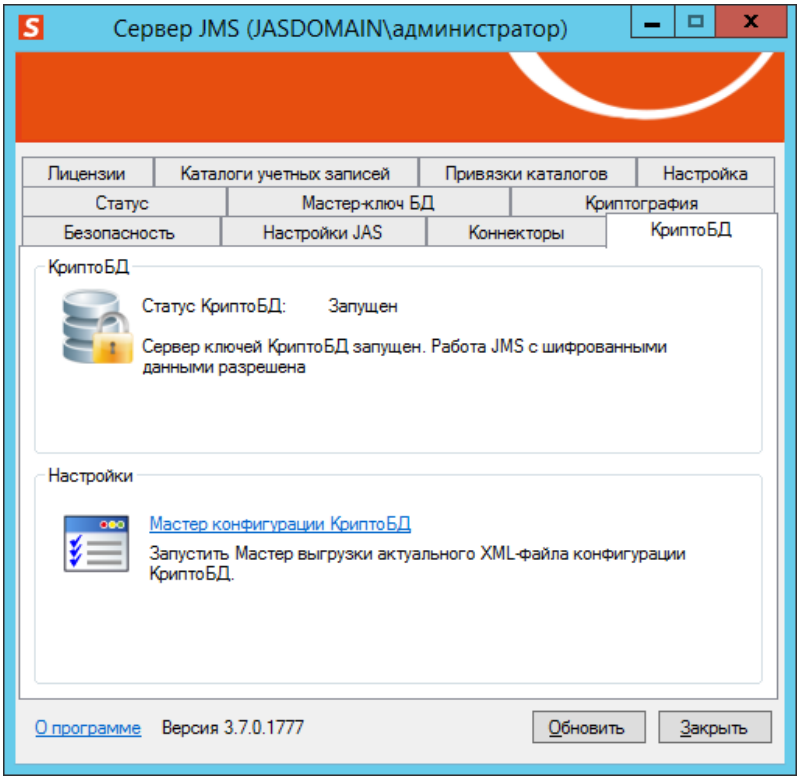



*Рис. 302 – Отображение статуса Запущен для СКЗИ «Крипто БД» в серверном агенте JMS*

На данном шаге интеграция ПО JMS с СКЗИ «Крипт БД» завершена.

# Приложение 1. Сценарий конфигурирования сервера СУБД для поддержки СКЗИ «Крипто БД»

Приложение поставляется в виде отдельного документа [2] (см. список литературы, с. 257).

# 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. Приложение 1 [Текст]. — «Аладдин Р.Д.». — Файл JMS_x.x_AdminGuide_(Part1)_Appx_1.docx

3 JaCarta Management System. Руководство администратора. Часть 2. Функции управления [Текст]. — «Аладдин Р.Д.». — Файл JMS_x.x_AdminGuide_(Part2)_Management_RU.docx

4 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

5 JaCarta Management System. Требования для развертывания продукта [Текст]. — «Аладдин Р.Д.». — Файл JMS-3.7_Requirements.docx

6 JaCarta Management System. Развертывание кластерной конфигурации [Текст]. — «Аладдин Р.Д.». — Файл JMS_ClusteringGuide.docx

7 Комплект документации СКЗИ "Крипто БД"

RU.46538383.50 1430 005-01 92 03. Средство криптографической защиты информации Крипто БД. Версия 2.0. Руководство администратора базы данных MSSQL [Текст]

RU.46538383.50 1430 005-01 92 01-1. Средство криптографической защиты информации Крипто БД. Версия 2.0. Руководство администратора безопасности. Часть I [Текст]

RU.46538383.50 1430 005-01 32 01-2. Средство криптографической защиты информации Крипто БД. Версия 1.0. Руководство администратора безопасности. Часть II [Текст]

RU.46538383.50 1430 005-01. Средство криптографической защиты информации Крипто БД. Версия 2.0. Описание реализации [Текст]

# 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