# Доступ к веб-ресурсам с использованием JaCarta PKI по протоколу HTTPS

## Руководство по настройке

Листов: 14

Автор: Dmitry Shuralev

# Аннотация

Настоящий документ содержит сведения о настройке двухфакторной аутентификации по электронным ключам **JaCarta PKI** к информационным ресурсам на веб-сервере IIS.

# Оглавление

# Доступ к информационным ресурсам по HTTPS

## Общие сведения

Существует возможность аутентификации с использованием электронного ключа JaCarta при получении доступа к информационным ресурсам по протоколу HTTPS. Данный тип аутентификации может использоваться не только для доступа к защищённому веб-сайту, но и для доступа к различным службам, например, Outlook Web Access, Microsoft Exchange, Шлюз служб терминалов, или к веб-сервисам других вендоров, например, Citrix XenApp/XenDesktop.

> Подробное руководство об установке и настройке **Citrix Xen Desktop** доступно в документе — "**JaCarta для аутентификации в XenDesktop/XenApp 7.x. Руководство по настройке**", который размещён на официальном сайте "Аладдин Р.Д.", в разделе "Интеграционные инструкции" — https://www.aladdin-rd.ru/support/guides.

Внедрение аутентификации пользователя с использованием сертификата в памяти **JaCarta** позволит усилить защищённость указанных служб и предотвратить несанкционированный доступ.

> **Примечание.**
>
> В качестве примера в настоящем документе рассматривается доступ к защищённому сайту.

# Настройка сервера

## Общие рекомендации и последовательность действий

При настройке веб-сервера для исключения несанкционированного доступа к нему рекомендуется максимально ограничить возможности аутентификации пользователя, исключив анонимную аутентификацию, а также другие стандартные способы аутентификации.

> В целях безопасности развертывать центр сертификации на веб-сервере не рекомендуется.

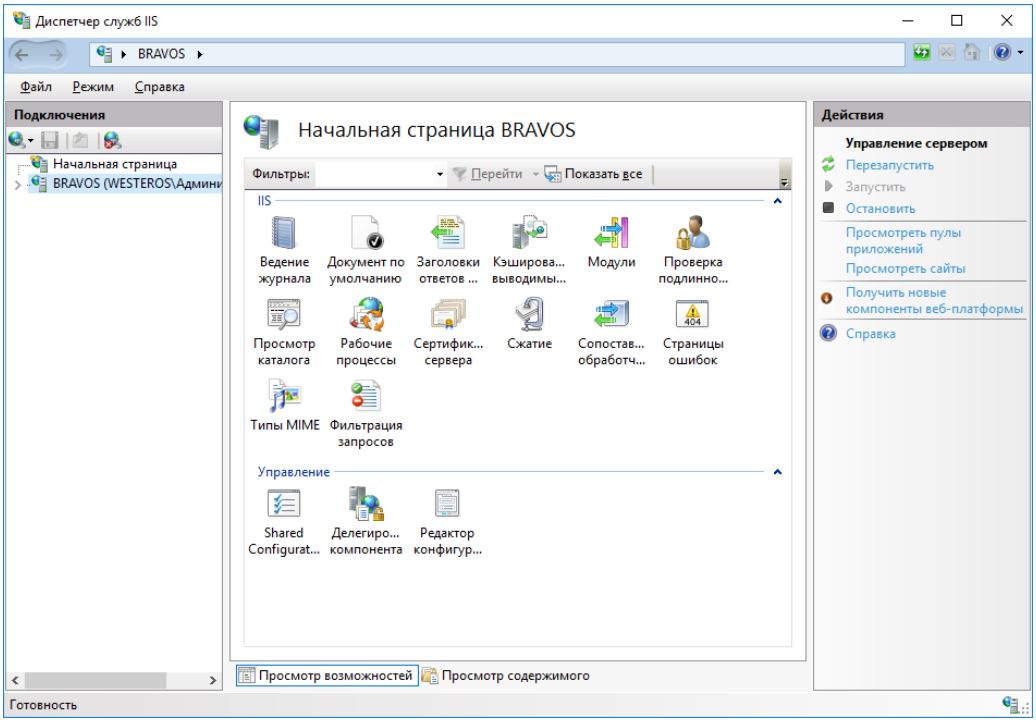
## Общие настройки сервера

Для того чтобы настроить веб-сервер, выполните следующую последовательность действий.

Убедитесь в том, что сервер удовлетворяет системным требованиям. В частности, на нём должна быть установлена роль **Веб-сервер (IIS)**.

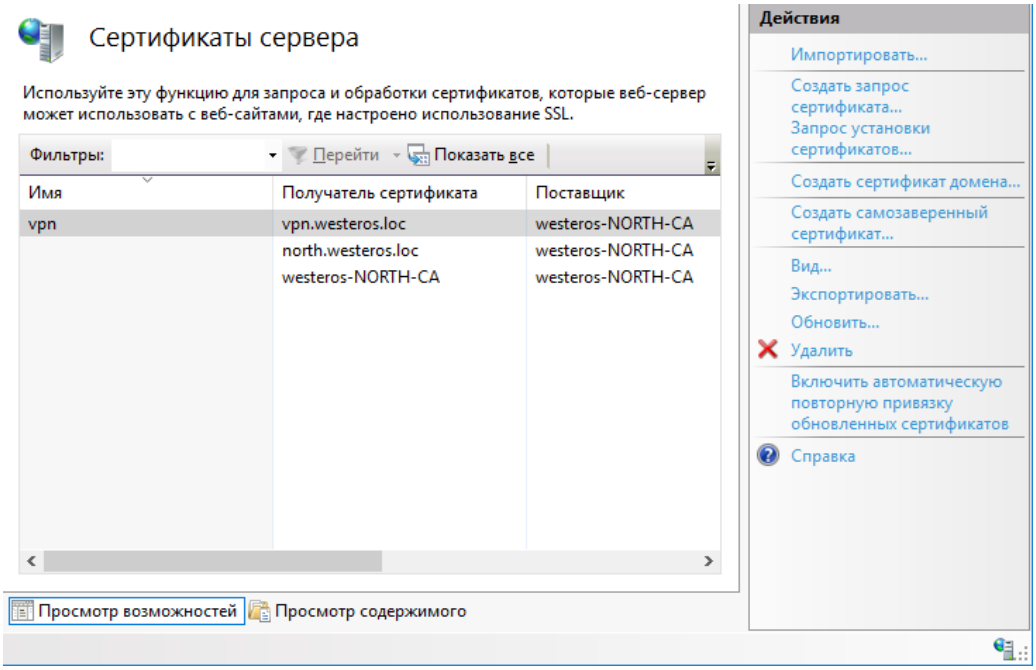
Запустите **Диспетчер служб IIS**.

В дереве консоли выберите имя сервера – в центральной части окна отобразятся доступные возможности.




В секции **IIS** сделайте двойной щелчок на **Сертификаты сервера**.

Центральная область окна будет выглядеть следующим образом.




В колонке **Действия** справа щёлкните на ссылке **Создать сертификат домена**.

Отобразится окно мастера создания сертификата.

В окне мастера создания сертификата заполните необходимые поля и нажмите **Далее**.

> **Примечание.**
>
> Значение в поле **Полное имя** должно совпадать с адресом сайта, который пользователь будет вводить в браузере.

На следующей странице мастера создания сертификата, в поле **Локальный центр сертификации**, выберите используемый центр сертификации (при необходимости воспользуйтесь кнопкой **Обзор**), в поле **Понятное имя** введите дополнительное имя сертификата.

Нажмите **Готово**, чтобы закрыть окно мастера создания сертификата.

Снова выберите веб-сервер, щёлкнув на его имени в окне диспетчера служб IIS.

В центральной части окна в секции **IIS** сделайте двойной щелчок на значке **Проверка подлинности**.

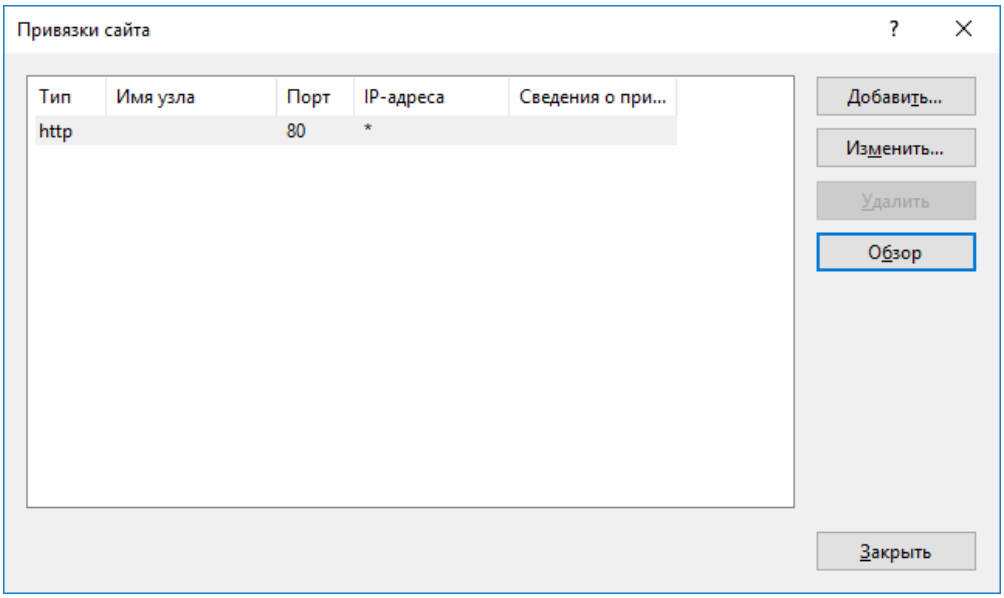
Отключите все способы проверки подлинности, кроме **Проверка подлинности клиента Active Directory с помощью сертификата**. Для этого, выбрав способ проверки подлинности, в колонке **Действия** щёлкните на ссылке **Отключить** или **Включить**.

# Настройка сайта

В окне диспетчера служб IIS разверните ветвь с именем сервера и выберите **сайты** > **Default Web Site**.

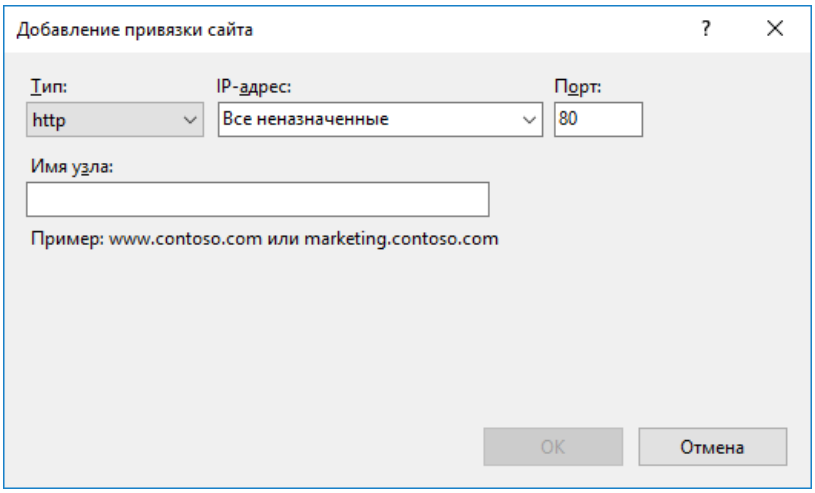
В правой части окна щёлкните на ссылке **Привязка**.

Отобразится следующее окно.




Нажмите **Добавить**.

Отобразится следующее окно.

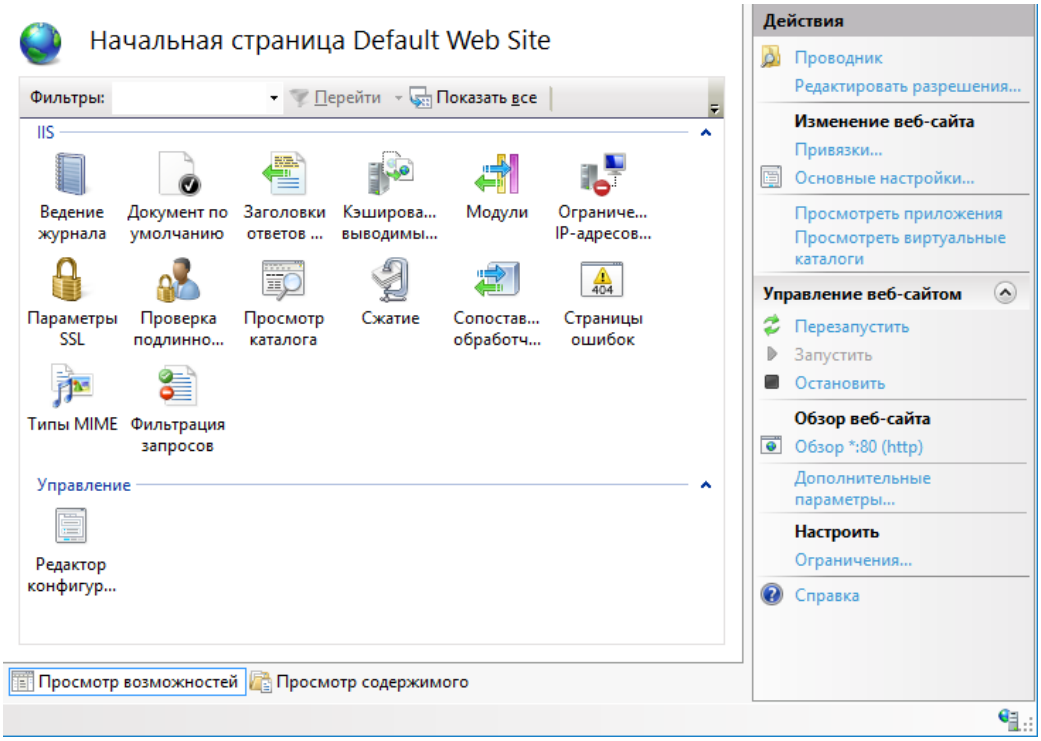



В списке **Тип** выберите **https**, и в списке **Сертификаты SSL** – сертификат сервера.

Нажмите **ОК**.

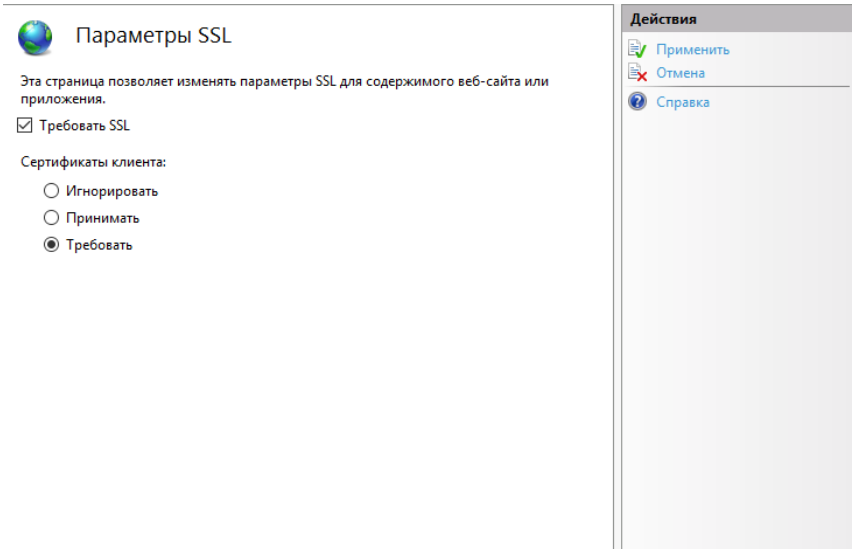
В окне диспетчера служб IIS щёлкните на сайте или виртуальном каталоге, доступ к которому нужно сделать защищённым (например, **сайты** > **Default Web Site** > **site**).

В центральной части окна станут доступны настройки данного сайта.




Сделайте двойной щелчок на иконке **Параметры SSL**.

Страница примет следующий вид.




Установите флажок **Требовать SSL** и в секции **Сертификаты клиента**, выберите **Требовать**.

В колонке **Действия** нажмите **Применить**.

# Действия пользователя

Для получения доступа к защищённому сайту выполните следующее.

Запустите **Microsoft Internet Explorer.**

Убедитесь в том, что ваш электронный ключ JaCarta с сертификатом, дающим право на доступ к сайту, подсоединен к компьютеру.

Введите адрес защищённого сайта, начинающийся с https.

В окне Безопасность Windows выберите сертификат пользователя и нажмите OK.

При необходимости введите PIN-код пользователя **JaCarta.**

Признаком установления защищённого соединения служит появление значка  рядом с адресной строкой Internet Explorer.

# Настройка Mozilla Firefox и проверка входа на защищённый веб-сайт

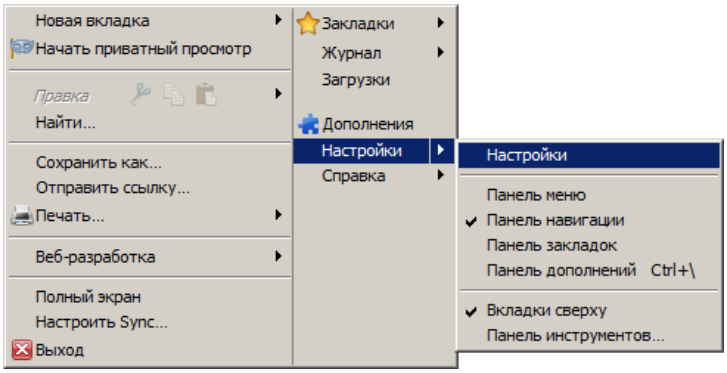
Помимо браузера **Internet Explorer**, для доступа к защищённому веб-сайту существует возможность использовать браузер **Mozilla Firefox**, для этого потребуется небольшая настройка.

Чтобы использовать электронные ключи **JaCarta** с **Mozilla Firefox**, в настройках браузера необходимо указать путь к библиотеке **PKCS11** из состава **Единый клиент JaCarta**. Если браузер **Mozilla Firefox** был установлен на компьютер до установки **Единый клиент JaCarta,** и если при установке **Единый клиент JaCarta** была отмечена соответствующая опция, путь к библиотеке прописывается в настройках **Mozilla Firefox** автоматически.

Чтобы указать путь к **PKCS11** из состава **Единый клиент JaCarta** вручную, выполните следующие действия.

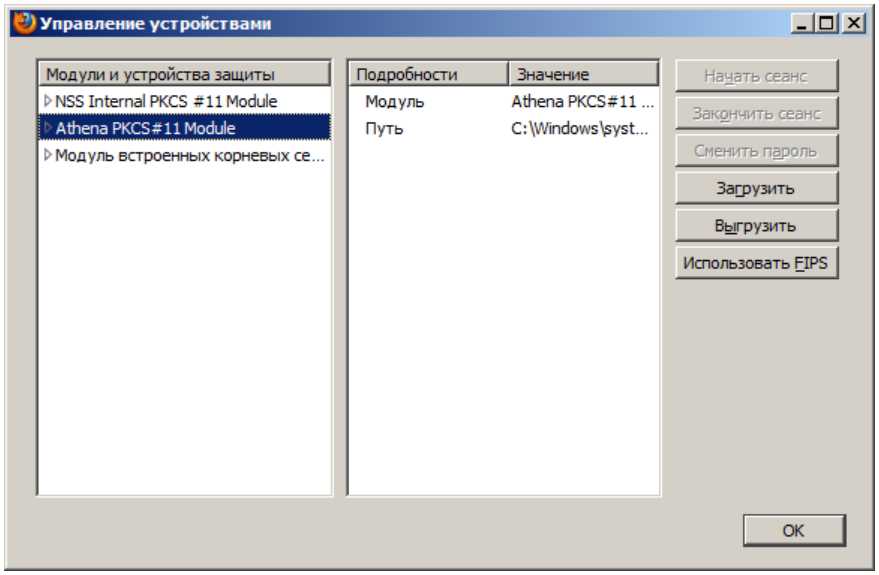
Запустите **Mozilla Firefox,** щёлкните на значке 

и выберите **Настройки > Настройки**, как показано на изображении ниже.



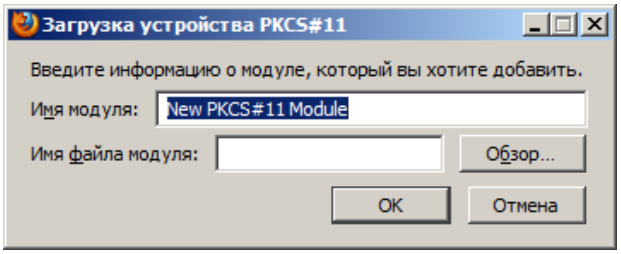

В отобразившемся окне щёлкните на значке  (**Дополнительные**), выберите вкладку **Шифрование** и нажмите **Устройства защиты**.

Отобразится следующее окно.




Если путь к библиотеке PKCS11 был прописан автоматически в процессе установки **Единый клиент JaCarta**, в списке **Модули и устройства защиты** будет значиться **Athena PKCS#11 Module**. В противном случае нажмите **Загрузить**.

Отобразится следующее окно.



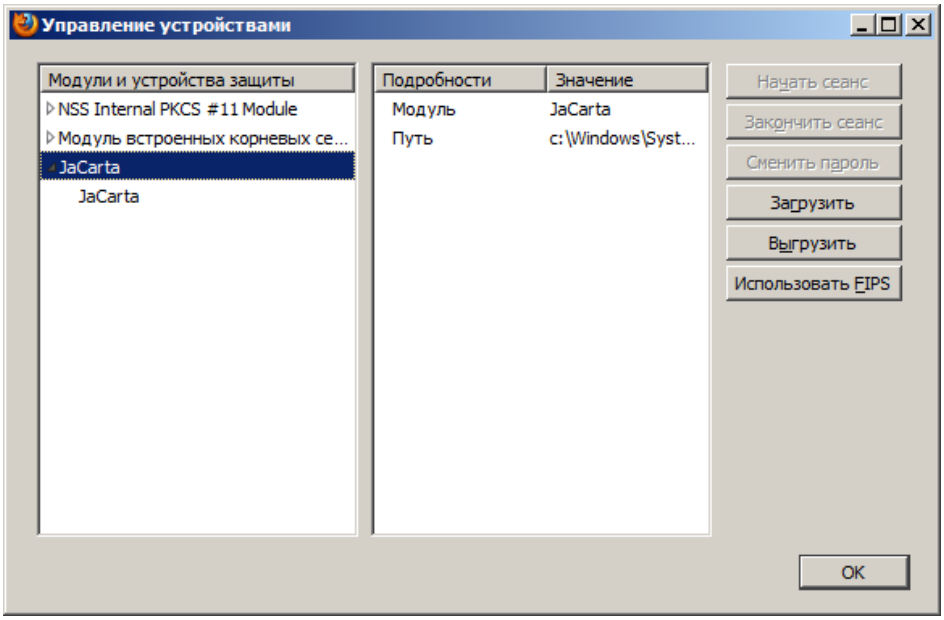

В поле **Имя модуля** введите имя нового модуля **(например, JaCarta),** в поле **Имя файла модуля** укажите путь к библиотеке **PKCS11** из состава **Единый клиент JaCarta** (при необходимости воспользуйтесь кнопкой **Обзор**).

Файл библиотеки **PKCS11** из состава **Единый клиент JaCarta** находится по следующему пути:

`C:\Windows\System32\asepkcs.dll`

Нажмите **OK**.

Добавленная библиотека отобразится в списке **Модули и устройства защиты**.



# Настройка конфигурации Mozilla Firefox

Чтобы обеспечить SSL-доступ к защищённому сайту с использованием цифрового сертификата в памяти **JaCarta**, необходимо включить соответствующую настройку в конфигурации **Mozilla Firefox.** Для этого выполните следующие действия.

> **Примечание.**
>
> Данные действия необязательны для Firefox версий до 4.0.

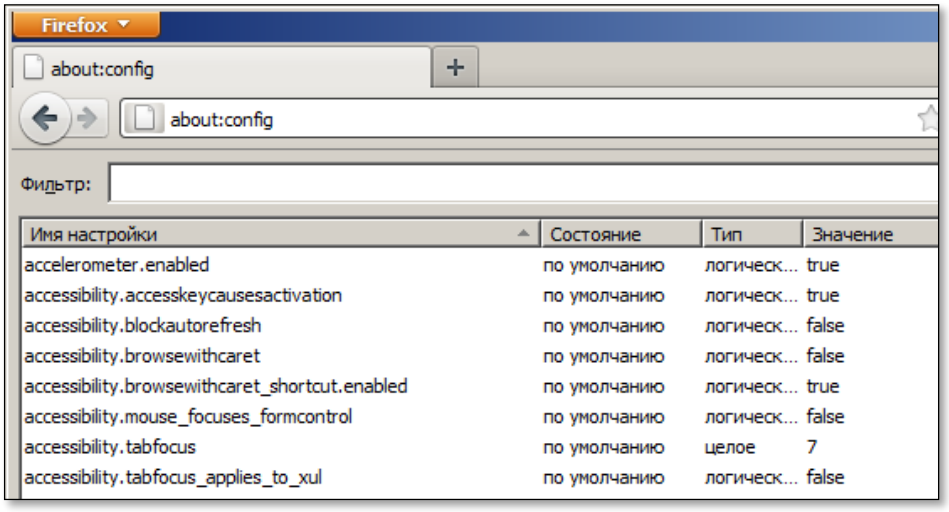
Запустите Mozilla Firefox.

В адресной строке наберите `about:config` и нажмите клавишу **Enter.**

В окне браузера отобразится предупреждающее сообщение.

Нажмите **Я обещаю, что буду осторожен**.

Окно браузера примет следующий вид:




Двойным щелчком измените значение настройки

security.ssl.allow_unrestricted_renego_everywhere__temporarily_available_pref

на **true** (истина).

Для быстрого поиска настройки введите или скопируйте ее в поле **Фильтр**.

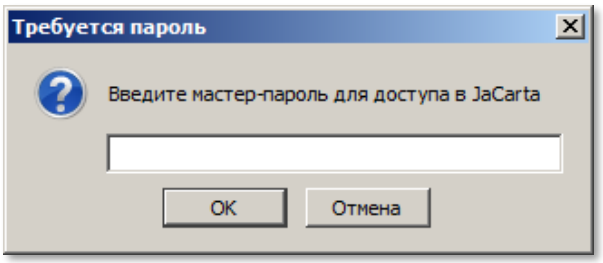
# Действия пользователя

Чтобы получить доступ к защищённому сайту с использованием браузера Mozilla Firefox и электронного ключа JaCarta, выполните следующие действия.

Убедитесь в том, что к компьютеру подключен электронный ключ JaCarta. На USB-токене JaCarta должен гореть световой индикатор.

Запустите браузер Mozilla Firefox, в адресной строке введите адрес защищённого сайта (адрес должен начинаться с `https://`) и нажмите клавишу ВВОД.

Отобразится следующее окно.




Введите пароль пользователя JaCarta и нажмите **OK**.

После этого вы попадете на защищённый сайт.

# 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-rd.ru (общий)

Web: www.aladdin-rd.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 Web-сайт:

**www.aladdin-rd.ru/support/index.php**

Для оперативного решения Вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

# Регистрация изменений

| Версия | Изменения |
|---|---|
| 1.0 | Исходная версия документа |
| | |
| | |

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, №3442 от 10.11.17
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 стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Apple Developer



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