ИНСТРУКЦИЯ
по системе защиты
«1С-Рарус»

rarus.ru

Оглавление

Защита решения 2

1.1. Что такое система лицензирования 2

1.2. Программные ключи защиты 5

1.3. Установка системы лицензирования 7

1.4. Настройка адреса сервера лицензирования 11

1.5. Активация программного ключа 15

1.5.1. Автоматическая активация через Интернет 19

1.5.2. Активация через файловый запрос 20

1.5.3. Активация по телефону 22

1.5.4. Активация через веб-форму сервера лицензирования 25

1.6. Активация пакета лицензий 26

1.6.1. Активация через веб-форму сервера лицензирования 33

1.7. Сервер лицензирования 34

1.7.1. Windows версия 35

1.7.2. Linux версия 37

1.8. Web-сервер лицензирования 38

1.8.1. Подключения 39

1.8.2. Список ключей 41

1.8.3. Функции 43

1.8.4. Настройка 45

1.8.5. Активация ключа 46

ЗАЩИТА РЕШЕНИЯ

В этом разделе приводится информация о защите решения.

1.1. ЧТО ТАКОЕ СИСТЕМА ЛИЦЕНЗИРОВАНИЯ

Система лицензирования – это набор аппаратных (ключи защиты) и / или программных (сервер лицензирования) средств, совокупность которых позволяет ограничить нелицензионное использование программного продукта. Для работы решения необходимо взаимодействие сервера лицензирования и ключа защиты.

Лицензионные ограничения на использование программного продукта задаются в ключе защиты.

Возможны два вида ключей защиты: программные и аппаратные.

- Программный ключ требует активации для своего создания. Процесс активации создает программный ключ на конкретном сервере лицензирования. В результате активации программный ключ привязывается к

уникальным аппаратным параметрам компьютера, на котором запущен сервер лицензирования.

- Аппаратные ключи выполнены в форм-факторе и по технологии USB. На каждом ключе имеется наклейка, которая содержит следующую информацию:
  - название решения, для которого ключ предназначен;
  - уникальный номер (s/n) ключа защиты и его штрих-код.

Решение всегда использует программу «сервер лицензирования». Связь между компонентой защиты и сервером лицензирования осуществляется по протоколу TCP/IP. По умолчанию сервер лицензирования использует порт 15200 для лицензирования и 15201 для веб-сервера управления.

Система лицензирования состоит из трех частей. Первая часть – это **компонента защиты**. Она загружается в рамках серверного контекста конфигурации. Для получения лицензии на работу компонента защиты подключается по протоколу TCP/IP ко второй части системы лицензирования – **серверу лицензирования**. Сервер лицензирования представляет собой службу Windows (демон Linux), установленную на том же компьютере, на котором и запускается приложение, или на любом компьютере в рамках сети. В свою очередь сервер лицензирования обращается к третьей части системы лицензирования – **ключам защиты**, установленным на том же компьютере, что и сервер лицензирования, для того чтобы найти нужный для работы программы ключ. Если такой ключ будет найден, то сервер лицензирования выдаст компоненте защиты лицензию на работу (при условии, что в ключе есть свободные лицензии).

Для установки системы лицензирования используются:

- в Windows файл **Setup.exe** в папке **Protect** из комплекта поставки решения;
- в Linux файл **setup.sh** в папке **protect** из комплекта поставки решения;
- отдельно установочные файлы защиты в Windows msi и в Linux RPM пакеты для CentOS и Red Hat , DEB пакеты для Ubuntu, Debian и их производных, доступные для скачивания по ссылке https://rarus.ru/downloads/2553/.

Если решение работает локально, только на одном компьютере, то именно на этом компьютере и устанавливается сервер лицензирования. Если же несколько пользователей решения работают в общей сети по протоколу TCP/IP, то используется единый общий сервер – один из компьютеров сети, на котором устанавливается сервер лицензирования. Все остальные компьютеры сети подключаются к этому серверу лицензирования.

Примечание

Также решение может работать на терминальном сервере без каких-либо дополнительных настроек. В этом случае программа «сервер лицензирования» может быть установлена как на сам терминальный сервер, так и на любой другой компьютер в сети терминального сервера. Необходимо, чтобы компьютер, на который установлен сервер лицензирования, был включен и доступен на протяжении всей работы программы на терминальном сервере

Система лицензирования доступна для платформ Windows и Linux x32 и x64, т.е. работа защищенного решения в серверном режиме возможна только на сервере 1С-Предприятия под указанными платформами.

При настройке параметров защиты смена экранов настройки управляется стандартными кнопками:

- «Далее» – переход к следующему экрану мастера (после того, как выполнены требуемые действия).
- «Назад» – переход к предыдущему экрану мастера для исправления ранее принятых решений.
- «Отмена» – прекращение установки (после подтверждения).

1.2. ПРОГРАММНЫЕ КЛЮЧИ ЗАЩИТЫ

В качестве альтернативы аппаратным ключам защиты могут использоваться программные ключи защиты. По сути, программный ключ представляет собой специально сформированный файл. В нем содержатся лицензионные ограничения и критерии аппаратной привязки; ключ, созданный на одном компьютере, не будет работать на другом.

Физически файлы ключей хранятся в папке:

- для Windows: %CommonAppData%\Protect\RarusSoftKey;
- для Linux: /home/licserver/.config/Protect/RarusSoftKey.

Эти файлы имеют имя, соответствующее номеру ключа, и расширение **.dongle**. Ключ имеет текстовый формат; в начале файла ключа расположена описательная секция, из которой можно узнать, что это за ключ и для какого продукта.

Установка программного ключа выполняется в интерактивном режиме из запущенной программы. Для этого нужно в мастере управления лицензированием выбрать пункт «Активировать программный ключ» (см. «Активация программного ключа»). Каждый ключ имеет свой уникальный серийный номер и набор пин-кодов для активации. Количество этих пин-кодов определяется для

каждой программы индивидуально. Ключ разрешено устанавливать только на одном компьютере.

> **Важно!**
>
> Дополнительные пин-коды предназначены для переактивации программного ключа на этом компьютере в случае изменения аппаратной составляющей. Запрещено использовать несколько ключей защиты от одной поставки решения за счет активации дополнительных пин-кодов на других компьютерах.

Для установки ключа на определенный компьютер на этом компьютере следует первоначально установить сервер лицензирования.

> **Важно!**
>
> После активации программный ключ не переносится на другой компьютер/станцию. Поэтому следует быть внимательным при выборе компьютера для установки сервера лицензирования. Впоследствии именно к его аппаратным частям будет привязываться ключ.

В процессе активации ключ привязывается к следующим аппаратным частям:

1. К жесткому диску, на котором находится системный раздел.
2. К сетевой карте (если их несколько, то к первой найденной).
3. К операционной системе, ее серийному номеру и имени компьютера.
4. К материнской плате.

В случае изменения хотя бы одного параметра программный ключ теряет работоспособность. Восстановить ее можно с

помощью реактивации ключа с использованием дополнительных пин-кодов. Если пин-коды закончились, то следует обратиться на линию консультации по данному программному продукту.

1.3. УСТАНОВКА СИСТЕМЫ ЛИЦЕНЗИРОВАНИЯ

Система лицензирования предназначена для работы в операционных системах Windows и Linux. Минимально поддерживаемая версия Windows XP SP3. Для Linux поддерживается работа в версиях с менеджерами пакетов DEB и RPM. Для всех современных операционных систем доступна работа как в x32, так и в x64.

Важно!

Установка системы лицензирования на каждой рабочей станции должна производиться пользователем, обладающим администраторскими правами в операционной системе.

Если установка происходит в операционной системе Windows Vista или Windows 7 (и пользователь обладает правами администратора), то система запросит у пользователя подтверждение для продолжения установки.

Если пользователь не обладает правами администратора, то система предложит указать новую учетную запись пользователя, у которой есть права администратора. Программа установки будет запущена от имени этой новой учетной записи.

Если установка происходит в операционной системе Linux, то она выполняется через sudo под текущим пользователем или от лица пользователя root.

Важно!

Перед тем как устанавливать систему лицензирования, следует остановить программы, использующие ключ

защиты.

Если используются другие программные продукты фирмы 1С-Рарус, то, возможно, на компьютере установлена и работает старая версия Сервера защиты **keyserver.exe** (в службах она имеет имя "Сервер защиты"), которую следует остановить перед установкой сервера лицензирования.

При подключении ключа защиты к USB-порту компьютера, если система лицензирования еще не установлена, некоторые операционные системы могут предложить начать установку драйвера ключа. В этом случае следует нажать кнопку «Отмена» [1]. Ключ USB нужно подключать после установки системы лицензирования.

Установка системы лицензирования возможна как из самого решения, так и из отдельного инсталлятора. Для Linux установка возможна только через установочные deb rpm пакеты. Если решение будет использоваться на нескольких компьютерах, то систему лицензирования нужно установить на сервере, который и будет раздавать лицензии. В этом случае нужно использовать отдельный инсталлятор системы лицензирования:

- для Windows файл **setup.exe** в папке **Protect**;
- для Linux файл **setup.sh** в папке **protect**.

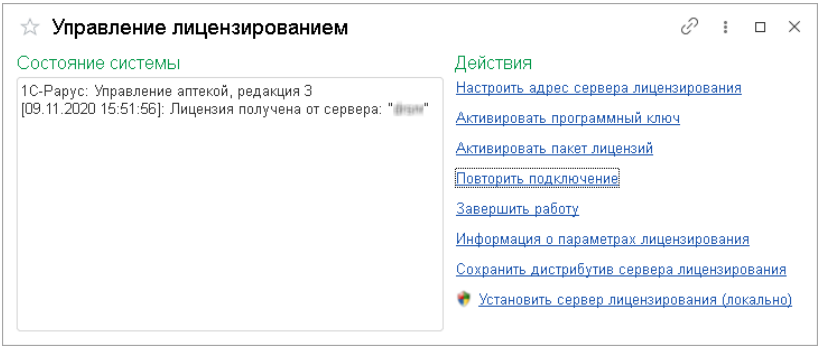
Если же решение будет использоваться на одном компьютере, то для установки системы лицензирования в Windows следует запустить решение.

1 По умолчанию Windows не знает о ключе и не имеет на борту соответствующего драйвера. Поэтому установка ключа невозможна. После установки системы лицензирования драйвер будет добавлен в Windows и установка ключа будет возможна. Если после установки ключа Windows будет искать драйвер в Windows Update, то эту операцию можно смело пропустить, так как нужный драйвер уже доступен в системе.

alfa@rarus.ru

Если рабочей системой является Linux, то перед запуском решения требуется сначала установить сервер лицензирования, как это описано далее.

Если защита ранее не была установлена (для Windows), то автоматически откроется окно «Управление лицензированием».



При помощи формы «Управление лицензированием» следует установить и настроить сервер лицензирования.

В данном диалоговом окне присутствуют следующие команды:

- «Настроить адрес сервера лицензирования».
- «Активировать программный ключ».
- «Активировать пакет лицензий».
- «Повторить подключение».
- «Завершить работу».
- «Информация о параметрах лицензирования».
- «Сохранить дистрибутив сервера лицензирования».

- «Установить сервер лицензирования (локально)» (доступно только для Windows) [2].

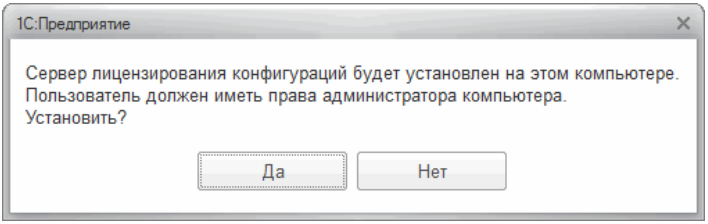
Для работы программного продукта необходимо установить сервер лицензирования.

Место установки сервера лицензирования зависит от варианта работы решения.

- В локальном варианте работы вся работа производится на одном рабочем месте (компьютере). Именно на этот компьютер и следует установить сервер лицензирования.
- В сетевом варианте работы сервер лицензирования устанавливается только на компьютер-сервер, а остальные компьютеры подключаются к серверу. **Этот вариант является рекомендуемым**.

Для установки сервера лицензирования на компьютере Windows следует выбрать пункт «Установить сервер лицензирования».

Перед тем как начать установку, система уточнит, обладает ли текущий пользователь компьютера правами администратора.

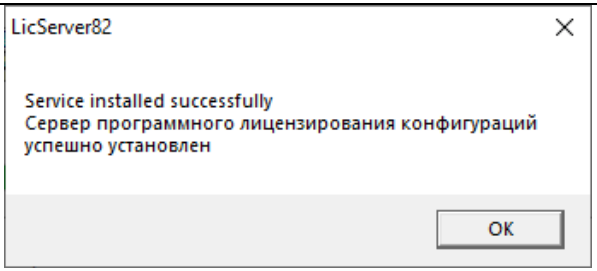


Нажатие кнопки «Да» начинает установку сервера лицензирования на данный компьютер.

После завершения установки появляется сообщение об этом.

2 При запуске решения на сервере 1С-Предприятия этот пункт будет запрещен. Используйте отдельный инсталлятор системы лицензирования.

alfa@rarus.ru



Нажатие кнопки «OK» завершает установку сервера лицензирования.

По окончанию установки в браузере, выбранном на данном компьютере по умолчанию (например, Internet Explorer), откроется web-сервер лицензирования, предназначенный для более детального контроля ключей и лицензий (см. раздел «Web-сервер лицензирования» на стр. 38).

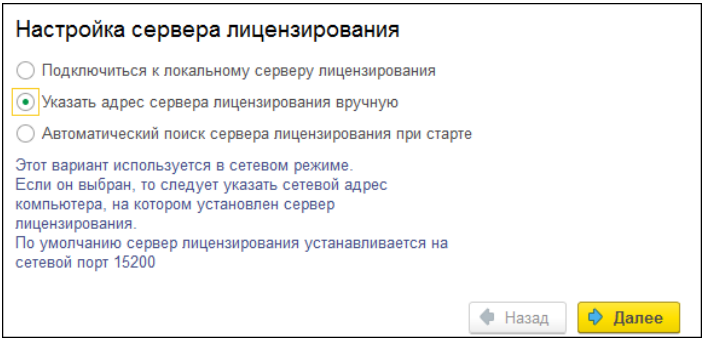
Если используется аппаратный ключ защиты в Windows, то необходимо подключить этот ключ к USB-порту компьютера, на котором установлен сервер лицензирования. После этого следует убедиться, что ключ доступен для использования. Для этого в web-сервере следует перейти на закладку «Ключи защиты» и убедиться, что данный ключ отображается в списке ключей защиты и имеет статус «Активен».

1.4. НАСТРОЙКА АДРЕСА СЕРВЕРА ЛИЦЕНЗИРОВАНИЯ

После того как сервер лицензирования установлен, на всех компьютерах, работающих с решением, следует настроить адрес этого сервера.

Для этого в окне «Управление лицензированием» следует выбрать пункт «Настроить адрес сервера лицензирования».

Откроется следующая форма.



В этом окне следует выбрать один из трех вариантов подключения и нажать «Далее».

- «Подключиться к локальному серверу лицензирования». Доступно только для Windows. Этот вариант следует выбирать в случае работы в локальном режиме: то есть на одном рабочем месте, без использования сети. Если используется аппаратный ключ защиты, то его следует подключать к этому компьютеру. Если же используется программный ключ защиты, то его следует активировать на данном компьютере. При выборе этого варианта подключения в константу «Сервер лицензирования» записывается значение *LOCAL – в этом режиме компонента защиты проверяет наличие сервера лицензирования на том компьютере, на котором запущено решение. Если сервер лицензирования присутствует, то компонента защиты подключается к нему по протоколу TCP/IP на адрес localhost.

  Внимание!

  Если информационная база размещена на сервере 1С-Предприятия, то компонента запускается на сервере и по умолчанию пытается найти и подключиться к серверу

лицензирования локально (то есть, опять же на сервере). Это поведение можно изменить, выбрав вариант подключения «Указать адрес сервера лицензирования вручную».

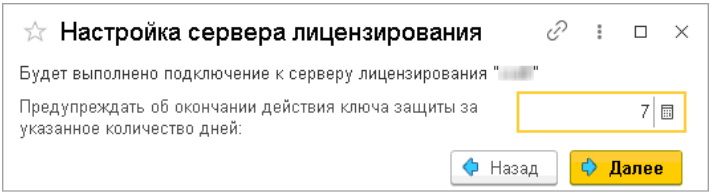
- «Указать адрес сервера лицензирования вручную». Доступно для Windows и Linux. Этот вариант используется в сетевом и локальном режимах, **является рекомендуемым**. Если он выбран, то следует указать сетевой адрес компьютера, на котором установлен сервер лицензирования. По умолчанию сервер лицензирования устанавливается на сетевой порт 15200. При работе в Linux для подключения к локальному серверу лицензирования достаточно в качестве адреса ввести localhost.
- «Автоматический поиск сервера лицензирования при старте». Доступно только для Windows. Этот вариант также используется в сетевом режиме. При использовании данного варианта происходит автоматический поиск настроенных серверов лицензирования в сети. При выборе этого варианта подключения в константу «Сервер лицензирования» записывается значение *AUTO – в этом случае компонента защиты осуществляет поиск сервера лицензирования. Для этого компонента посылает в сеть широковещательный UDP запрос. В ответ сервера лицензирования, доступные в сети, посылают информацию о себе. После этого компонента защиты использует первый ответивший сервер. При каждом запуске операция будет повторяться. В этом режиме старт защиты наиболее долгий; он может занимать несколько секунд.

Во втором диалоговом окне настройки для первых двух вариантов подключения может быть задан код доступа к ключу. Этот код позволяет однозначно указать, какой ключ

защиты будет использовать решение. Использоваться будут только ключи, у которых задан в точности такой же код доступа.

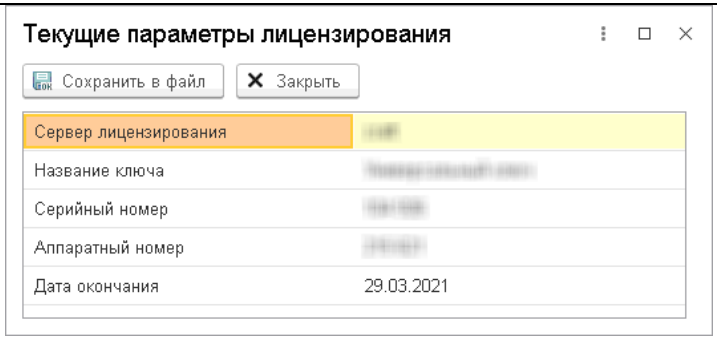
Это может быть удобно, например, если один сервер обслуживает сети нескольких фирм. Для ключей каждой из фирм могут быть заданы свои коды доступа. Таким образом, клиенты из каждой фирмы смогут обращаться только к ключу своей фирмы.

После выбора варианта подключения на следующей форме настройки сервера лицензирования пользователь может настроить предупреждение об окончании действия ключа защиты за указанное количество дней.



В дальнейшем при старте системы выполняется проверка срока действия всех ключей лицензирования. Если для каких-либо ключей до окончания срока действия остается менее указанного количества дней, то выводится соответствующее предупреждение.

При выборе пункта «Информация о параметрах лицензирования» в окне «Управление лицензированием» открывается форма с текущими параметрами лицензирования, в т.ч. с информацией о дате окончания действия ключа.



1.5. АКТИВАЦИЯ ПРОГРАММНОГО КЛЮЧА

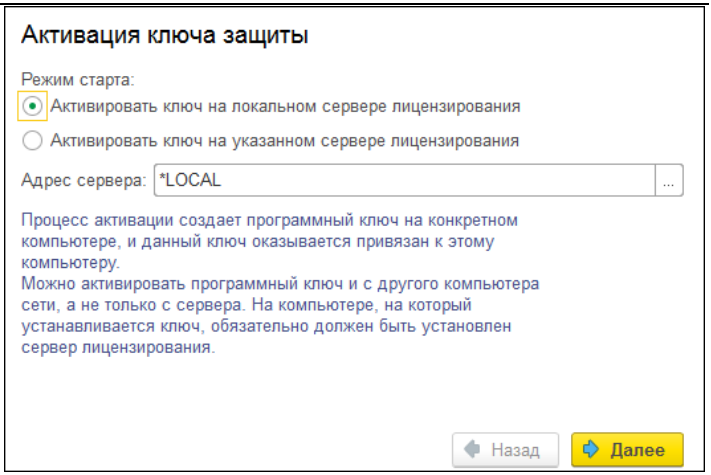
Как говорилось выше, система лицензирования может использовать два вида ключей: аппаратные и программные.

Аппаратные ключи подключаются к USB-разъему компьютера, на котором установлен сервер лицензирования.

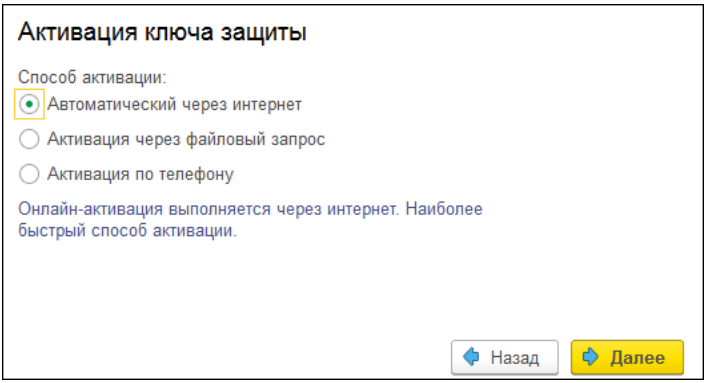
Программные ключи требуют активации. Процесс активации создает программный ключ на конкретном компьютере, и данный ключ оказывается привязан к этому конкретному компьютеру. Можно активировать программный ключ и с другого компьютера сети, а не только с сервера. Но на компьютере, на который устанавливается ключ, обязательно должен быть установлен сервер лицензирования.

Для активации ключа защиты следует в окне «Управление лицензированием» выбрать пункт «Активировать программный ключ».

Откроется окно выбора режима работы.



Здесь следует выбрать локальный либо сетевой режим и нажать «Далее».



На этой форме следует выбрать способ активации ключа.

- «Автоматический через интернет». Онлайн-активация выполняется по Интернету. Наиболее быстрый способ активации.
- «Активация через файловый запрос». В этом способе работы программой создается файл запроса активации.

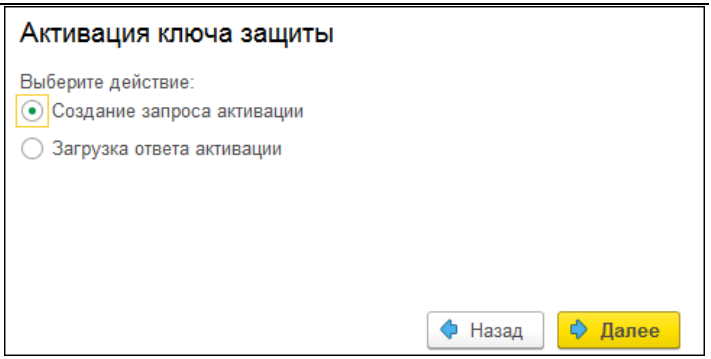
Этот файл каким-либо способом – например, по электронной почте – передается в центр лицензирования (почтовый адрес указан в сообщении, которое появится на экране сразу после создания файла запроса). На основании данного файла запроса в центре лицензирования создается файл активации, который передается обратно. После загрузки файла активации пользователь в соответствующей форме указывает путь к файлу активации и активирует программный ключ.

- «Активация по телефону». В этом способе работы пользователь звонит по телефону в центр лицензирования и зачитывает цифровой код, отображенный программой. В ответ из центра сообщают цифровой код для активации. Пользователь вводит этот код в соответствующее поле и активирует программный ключ. Данный способ удобен, если есть только телефонная связь, а связь по Интернету отсутствует.

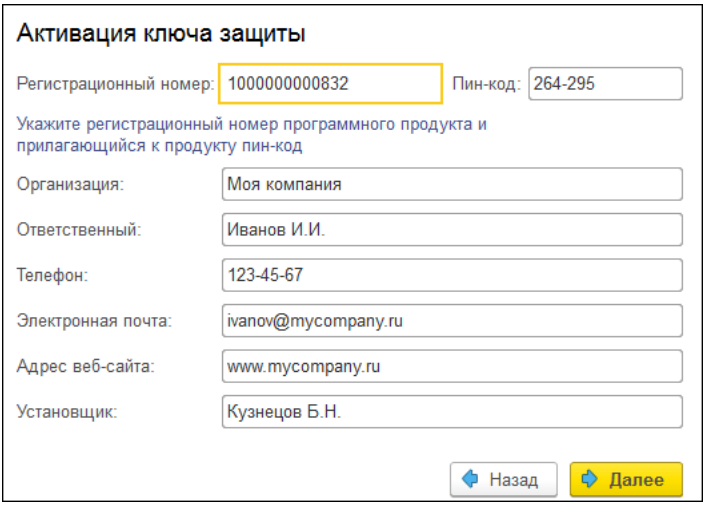
Рассмотрим эти способы подробнее.

При выборе способа активации «Автоматический через интернет» либо «Активация по телефону» открывается экран ввода параметров пользователя (см. ниже).

Если выбран способ активации через файловый запрос, то следует указать, какое именно действие выполняется: создание файла запроса или загрузка файла активации.



Далее открывается экран ввода параметров пользователя (в двух других способах активации эта форма открывается сразу).



На этом экране пользователь вводит регистрационный номер программного продукта и прилагающийся к продукту пин-код. Пин-коды, входящие в комплект поставки программного продукта, предназначены для активации и, при необходимости, последующей реактивации одного и

того же программного ключа. Реактивация используется для восстановления работоспособности программного ключа в случае изменения аппаратной составляющей сервера. К программному продукту прилагаются несколько пин-кодов – например, на случай, если изменилась аппаратная составляющая компьютера, на котором установлен сервер лицензирования и активирован программный ключ. С помощью дополнительных пин-кодов в этом случае можно восстановить работоспособность решения.

Также в этом диалоговом окне пользователю следует указать параметры своей компании.

Дальнейшие действия различны для разных способов активации; поэтому далее мы рассмотрим эти способы по отдельности.

1.5.1. Автоматическая активация через Интернет

Важно!

Для автоматической активации необходимо иметь доступ в Интернет.

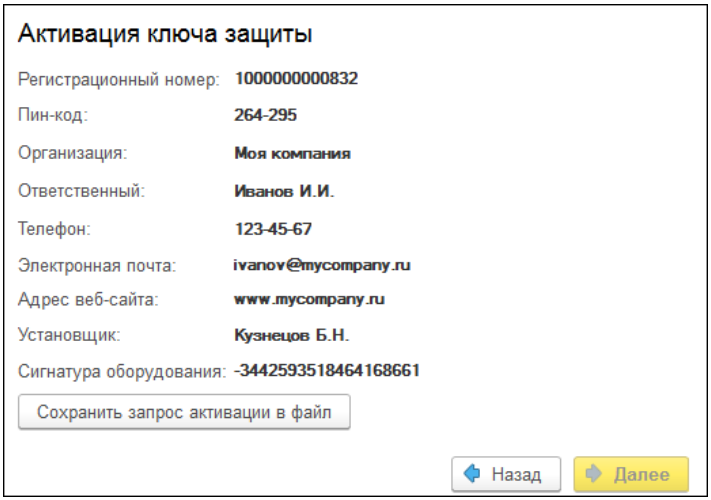
После того как введены регистрационный номер программного продукта, пин-код и параметры пользователя, следует нажать кнопку «Далее». Ключ защиты будет автоматически активирован.

Важно!

В случае, если по какой-либо причине автоматическая активация ключа не была произведена, обратитесь к Вашему системному администратору. Сервер активации имеет адрес https:// support.rarus.ru/activation/

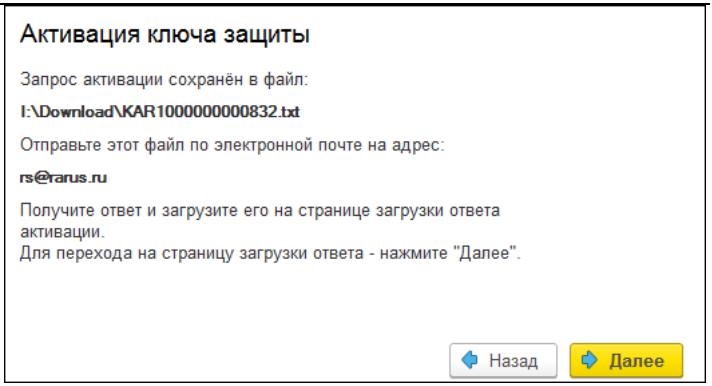
1.5.2. Активация через файловый запрос

После того как введены регистрационный номер программного продукта, пин-код и параметры пользователя, следует нажать кнопку «Далее». В результате откроется форма, на которой будут отображаться введенные сведения.



На этом экране следует нажать кнопку «Сохранить запрос активации в файл». Программа предложит выбрать место сохранения файла запроса.

После сохранения файла запроса на следующем экране будет указано место его сохранения на компьютере и адрес электронной почты, по которому этот файл следует отправить.

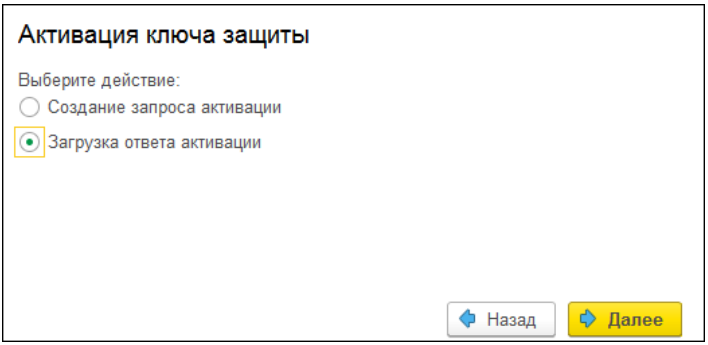


Сохраненный файл запроса следует отправить по указанному адресу электронной почты. С ответом будет прислан файл активации.

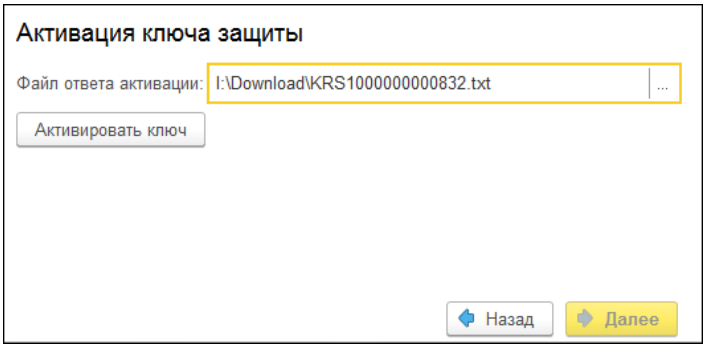
Для загрузки файла активации следует, как и при создании файла загрузки, выбрать пункт «Активация через файловый запрос». В следующем диалоговом окне следует выбрать пункт «Загрузка ответа активации».

Внимание!

Загружать файл активации ключа необходимо на тот же сервер лицензирования, на котором создавался файл запроса активации. В противном случае активация ключа невозможна и ключ будет недоступен.



В следующей форме следует указать путь к файлу активации и нажать кнопку «Активировать ключ».

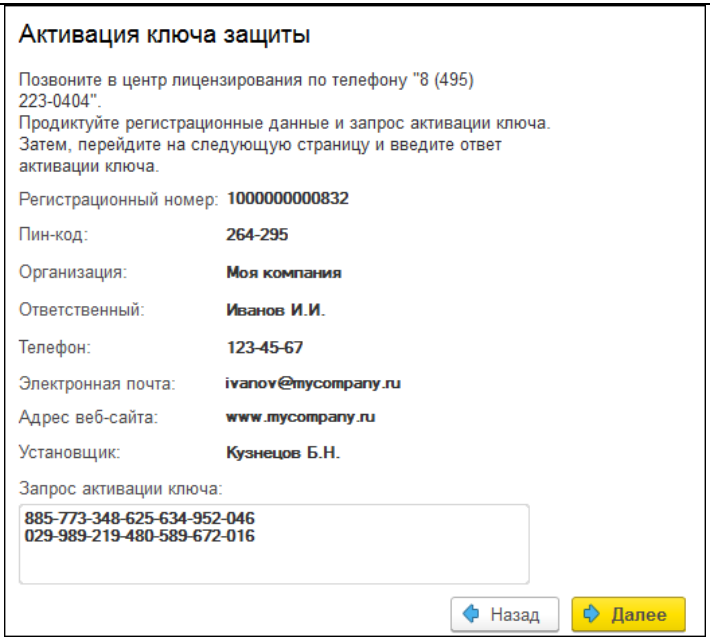


После этого ключ будет активирован.

1.5.3. Активация по телефону[3]

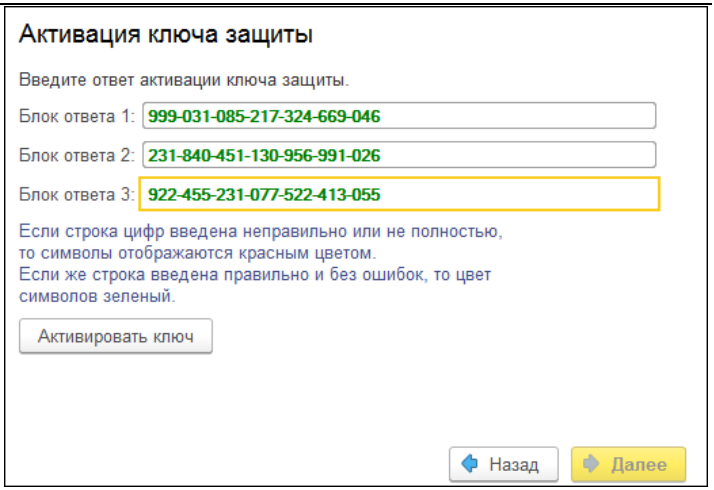
После того как введены регистрационный номер программного продукта, пин-код и параметры пользователя, следует нажать кнопку «Далее». В результате откроется диалоговое окно, в котором будут отображаться введенные сведения.

[3] Резервный вариант. Может быть использован при отсутствии доступа к сети Интернет.



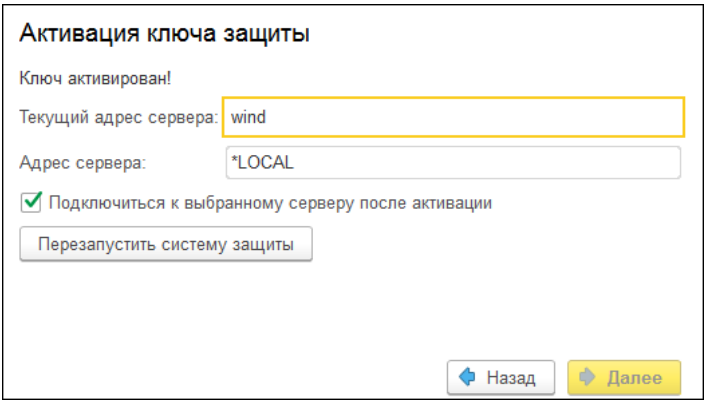
Также на этом экране указан телефон для активации ключа. Следует позвонить по этому телефону и продиктовать цифровой код, указанный в нижней части формы, в поле «Запрос активации ключа». После того как код продиктован и принят, следует нажать «Далее».

Сотрудник центра лицензирования продиктует Вам ответ активации ключа защиты. Этот ответ, состоящий из трех блоков, следует ввести на следующем экране.



В программе проверяется корректность ввода. Если строка цифр введена неправильно или не полностью, то символы отображаются красным шрифтом. Если же строка введена правильно и без ошибок, то цвет символов зеленый.

После того как все три цифровых блока введены, следует нажать кнопку «Активировать ключ».

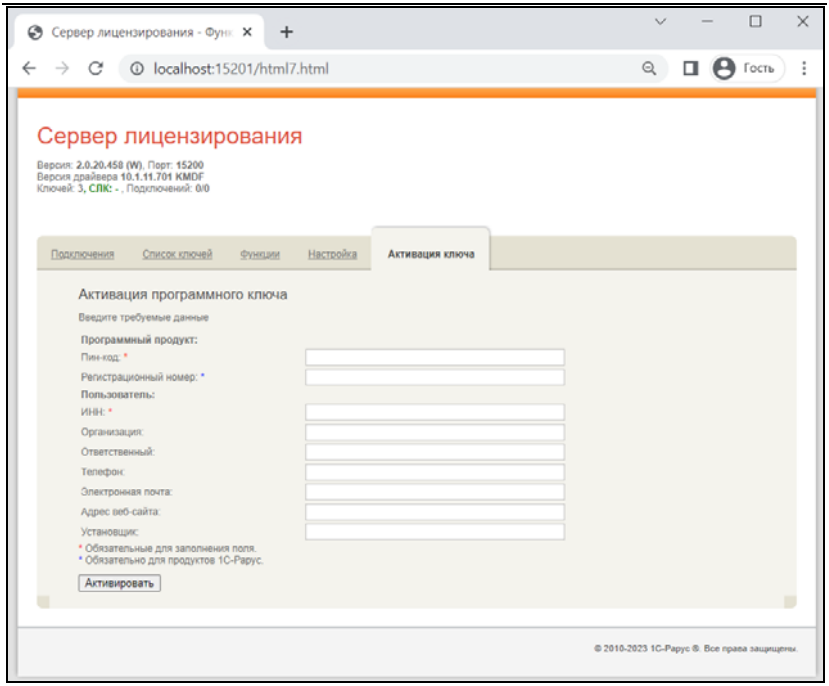


После этого ключ будет активирован.

1.5.4. Активация через веб-форму сервера лицензирования

Данная активация выполняется через Интернет. Для ее выполнения нужно в браузере вызвать форму сервера лицензирования, набрав в адресной строке http://localhost:15201. Если сервер лицензирования установлен на другом компьютере, то нужно вместо localhost ввести его адрес.

В открывшейся странице «Сервер лицензирования» браузера следует выбрать закладку «Активация ключа». На данной странице нужно ввести регистрационный номер программного продукта, пин-код и параметры пользователя. Для завершения процесса следует нажать кнопку «Активировать». В случае ввода неправильных данных будет выведено соответствующее сообщение. Если все данные введены корректно, то на закладке «Список ключей» добавится новый ключ.



1.6. АКТИВАЦИЯ ПАКЕТА ЛИЦЕНЗИЙ

Пакет лицензий предназначен для изменения лицензионных ограничений, заданных в уже существующем ключе защиты. Например, если нужно расширить количество пользователей, работающих с решением, компания может приобрести и активировать дополнительные лицензии.

Приобретая пакет лицензий, пользователь получает идентификатор и пароль для установки лицензий.

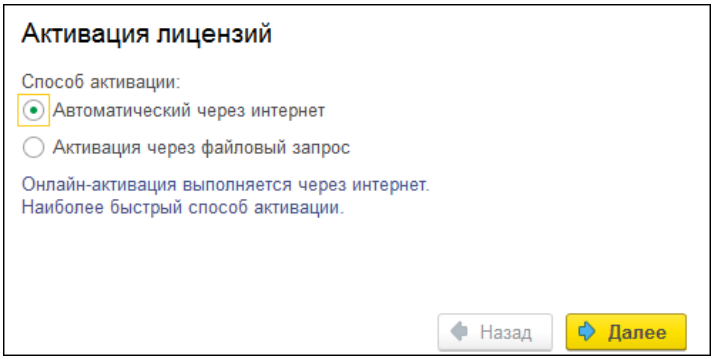
Для того чтобы была возможность активировать новую лицензию, необходимо выполнение следующих условий:

- решение должно быть запущено,

- лицензия с сервера лицензирования должна быть получена.

Только при выполнении этих условий возможна активация нового пакета лицензий (иначе соответствующий пункт в окне «Управление лицензированием» будет недоступен).

Для того чтобы активировать пакет лицензий, в окне «Управление лицензированием» следует выбрать пункт «Активировать пакет лицензий» (как открывать это окно, описано выше в разделе 1.3, «Установка системы лицензирования» на стр. 7).



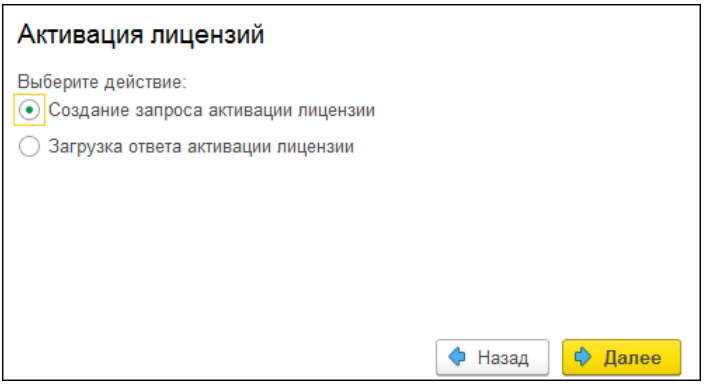
В открывшемся окне следует выбрать способ активации лицензий:

- «Автоматический через интернет». Онлайн-активация выполняется по интернету. Наиболее быстрый способ активации.
- «Активация через файловый запрос». В этом способе работы программой создается файл запроса активации. Этот файл каким-либо способом – например, по электронной почте – передается в центр лицензирования. На основании данного файла запроса в центре лицензирования создается файл активации лицензии,

который передается обратно. Этот файл активации следует загрузить в систему лицензирования. В результате этой загрузки новая лицензия будет активирована.

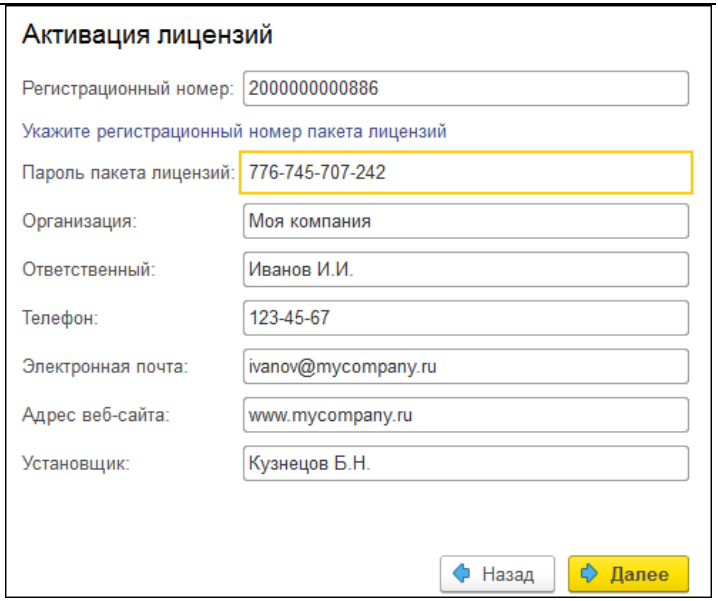
Рассмотрим подробнее активацию лицензий посредством файлового запроса.

При выборе этого способа открывается следующий экран.



В этом диалоговом окне следует указать, какое именно действие выполняется: создание файла запроса или загрузка файла активации.

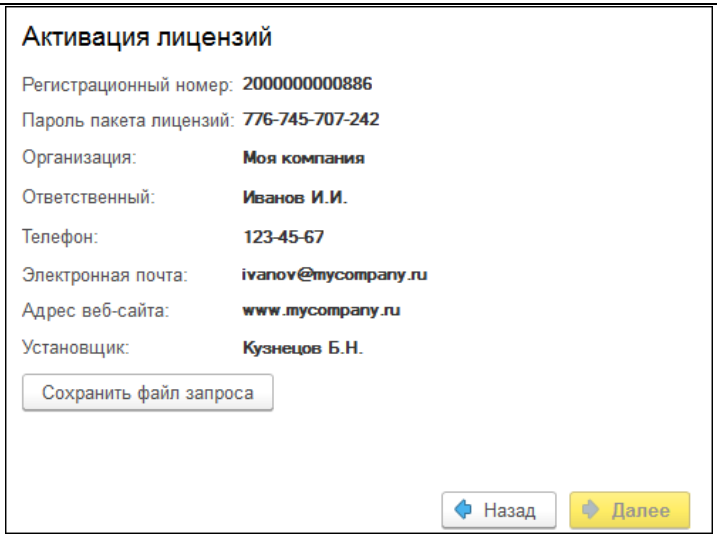
Далее открывается форма ввода параметров пользователя.



Здесь пользователь вводит регистрационный номер программного продукта и пароль пакета лицензий, полученный при приобретении данного пакета.

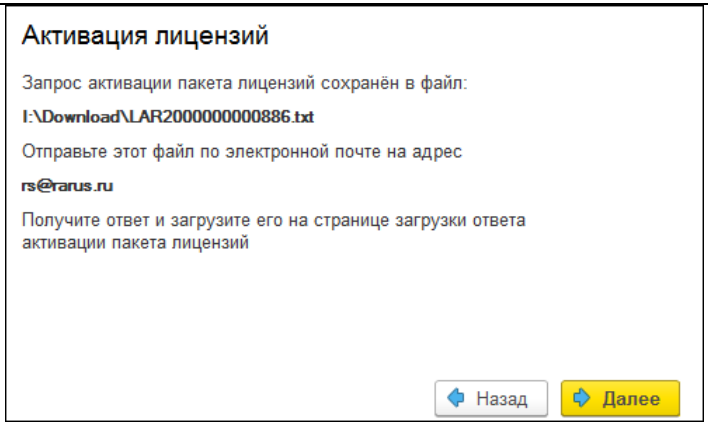
Также на этом экране пользователю следует указать параметры своей компании.

После нажатия кнопки «Далее» открывается форма, на которой отображаются введенные сведения.



На этом экране следует нажать кнопку «Сохранить файл запроса». Программа предложит выбрать место сохранения файла запроса.

После сохранения файла запроса на следующей форме будет указано место его сохранения на компьютере и адрес электронной почты, по которому этот файл следует отправить.

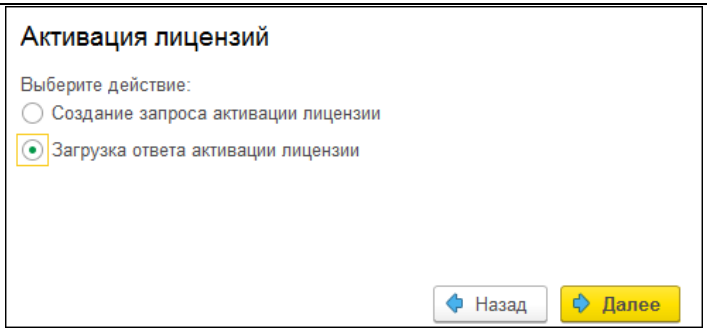


Сохраненный файл запроса следует отправить по указанному адресу электронной почты. С ответом будет прислан файл активации.

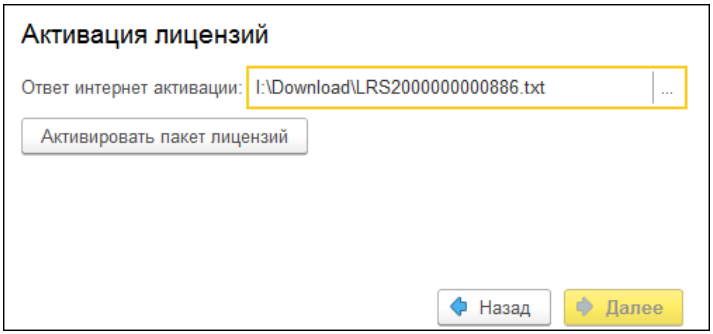
> **Внимание!**
>
> Загружать файл активации пакета лицензий необходимо на тот же сервер лицензирования, на котором создавался файл запроса активации. При этом на этом сервере должен быть установлен тот же ключ защиты, что и во время создания файла запроса. В противном случае активация пакета лицензий невозможна.

Для загрузки файла активации следует, как и при создании файла загрузки, выбрать пункт «Активация через файловый запрос».

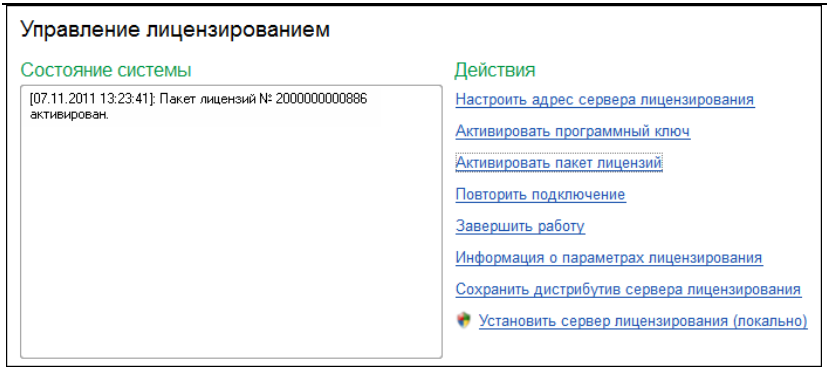
В следующем диалоговом окне следует выбрать пункт «Загрузка ответа активации лицензии».



В следующей форме следует указать путь к файлу активации и нажать кнопку «Активировать пакет лицензий».



После этого пакет лицензий будет активирован. В информационной области окна «Управление лицензированием» об этом будет выведено сообщение.



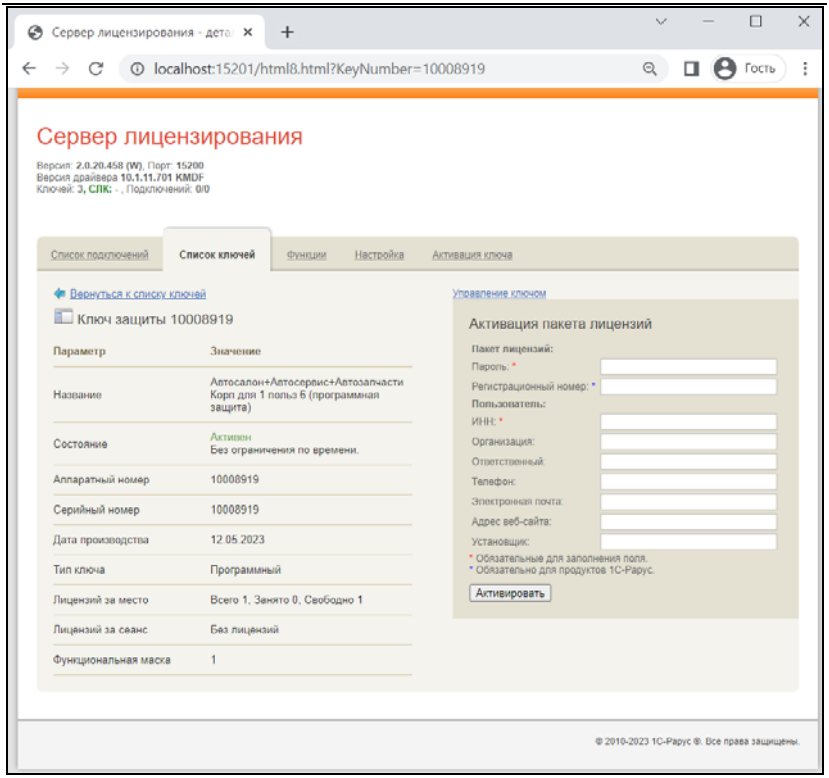
Общее количество активированных лицензий можно увидеть на закладке «Подключения» web-сервера лицензирования, нажав на номер нужного ключа защиты (см. раздел «Web-сервер лицензирования» на стр. 38).

1.6.1. Активация через веб-форму сервера лицензирования

Данная активация выполняется по Интернету. Форма сервера лицензирования в браузере открывается аналогично активации ключа.

Для активации пакета лицензий следует выбрать закладку «Список ключей». В данном списке нужно выбрать требуемый ключ, нажав на его номер в колонке «Серийный номер». При этом откроется форма с описанием параметров ключа.

Далее следует выбрать пункт «Активировать лицензии». При этом откроется панель «Активация пакета лицензий». Следует ввести регистрационный номер и пароль для активируемого пакета и информацию о пользователе. Для завершения активации следует нажать на кнопку «Активировать».

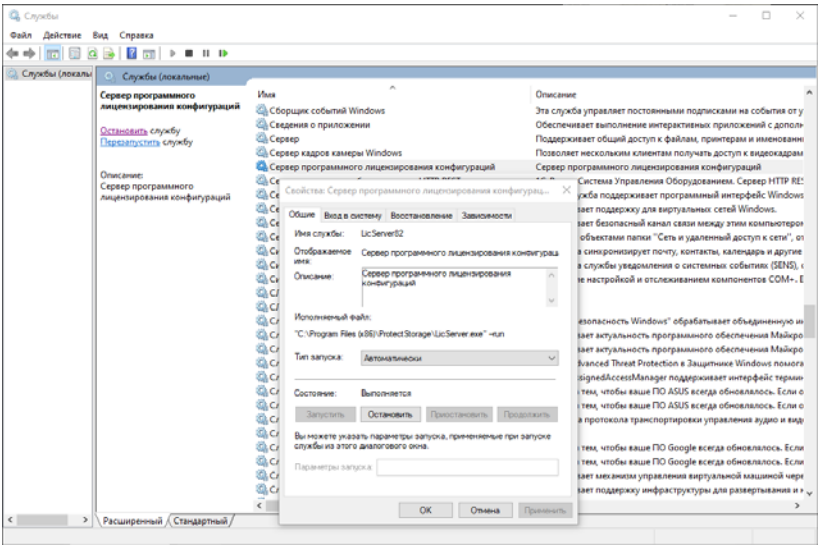


1.7. СЕРВЕР ЛИЦЕНЗИРОВАНИЯ

Сервер лицензирования предназначен для выдачи разрешений на работу программных продуктов. Список программных продуктов, на работу с которыми могут выдаваться разрешения, определяется списком подключенных к серверу лицензирования ключей защиты. Каждый экземпляр программы в обязательном порядке подключается к серверу лицензирования.

1.7.1. Windows версия

Сервер лицензирования представляет собой службу Windows. Имя службы: **LicServer82**, ее описание: «Сервер программного лицензирования конфигураций».



Система устанавливается в каталог:

%ProgramFiles%\ProtectStorage.

Свои настройки программа хранит в ini-файле, который расположен там же. Вот его типовое содержание:

port=15200

WebPort=15201

Local=1

user=Cei=Txnv7RSta=HPxTVFhjhiKqnQ6HCxmq2kbH1du4YyVLa46fx+13xxIEw

password=Cei=Txnv7RSta=HPxTVFhjhiKqnQ6HCxmq2kbH1du4YyVLa46fx+13xxIEw

Строки файла имеют следующее значение:

- «port» – номер TCP/IP-порта, к которому ожидает подключения клиента сервер лицензирования. Параметр может быть настроен через веб интерфейс сервера лицензирования.
- «WebPort» – номер TCP-IP порта, на котором доступен web-интерфейс сервера лицензирования. Настраивается вручную.
- «Local» – режим доступности сервера лицензирования. Если указано значение 0, то сервер лицензирования доступен в сети по всем сетевым интерфейсам компьютера. Если же указано значение 1, то сервер доступен только по локальному адресу Localhost (127.0.0.1), и подключение к нему возможно только с этого компьютера в режиме *Local. Параметр может быть настроен через web-интерфейс сервера лицензирования.
- «user» – зашифрованное имя пользователя web-интерфейса.
- «password» – зашифрованный пароль.

Два последних параметра настраиваются только через web-интерфейс. Если пользователь не был назначен в web-интерфейсе, то эти два параметра отсутствуют в файле настройки.

Внимание!

Если Вы забыли пользователя или пароль, то просто удалите строчки с «user» и «password» из конфигурационного файла и перезапустите службу сервера лицензирования.

Установка сервера лицензирования доступна как из самой программы, так и из отдельной программы установки (**Protect \ Setup.exe**). Вместе с установкой службы сервера

лицензирования программа установит драйвера аппаратного ключа.

Список портов, которые использует сервер лицензирования:

- 15200 TCP – сервер лицензирования. Его значение может быть изменено через конфигурационный файл;
- 15200 UDP – система автоконфигурирования и поиска серверов в сети. Значение изменить нельзя;
- 15201 TCP – web-интерфейс сервера лицензирования. Его значение может быть изменено через конфигурационный файл.

1.7.2. Linux версия

Сервер лицензирования представляет собой демон (службу) Linux с именем LicServer. Установка доступна из скрипта protect/licserver.sh или из открытого интернет ресурса https://rarus.ru/downloads/2553/. При скачивании через интернет, используется актуальная deb или rpm версия пакета, в зависимости от рабочей ОС.

Установка из скрипта:

1. Перейдите в каталог /protect дистрибутива решения.
2. Выполните команду sudo ./licserver.sh

Установка из внешнего ресурса:

1. Загрузите нужную версию пакета по ссылке https://rarus.ru/downloads/2553/.
2. Перейдите в каталог, в который загружен пакет.
3. Установите пакет, выполнив одну из команд:
   - sudo apt install ./licserver_№версии_amd64.deb
   - sudo yum install ./LicServer-№версии-1.x86_64.rpm

4. Проверьте правильность установки командой:
   - systemctl status LicServer
5. Должна быть информации типа:

   LicServer.service - Licensing system service

   Loaded: loaded (/lib/systemd/system/LicServer.service; enabled; vendor preset: enabled)

   Active: active (running) since Thu 2022-09-01 13:42:35 +05; 1min 43s ago
6. Если получено состояние Active: inactive (dead), то выполните следующие команды:
   - sudo systemctl enable LicServer
   - sudo systemctl start LicServer

При установке демона в системе добавляется пользователь licserver с домашней папкой /home/licsever. Демон LicServer запускается от имени пользователя licserver.

Параметры запуска сервера хранятся в ini-файле /home/licserver/.config/LicServer/LicServer.ini и аналогичны параметрам Windows версии сервера.

1.8. WEB-СЕРВЕР ЛИЦЕНЗИРОВАНИЯ

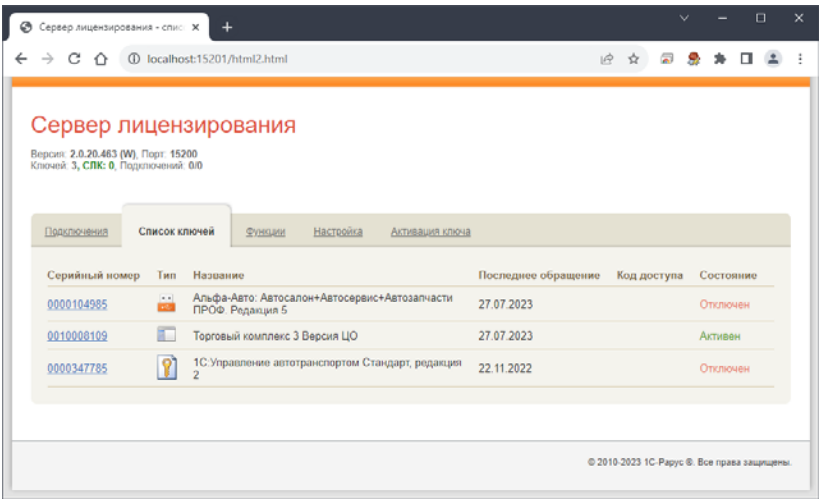
Для более детального контроля ключей и лицензий на сервере лицензирования предусмотрен web-сервер, который отображает текущее состояние сервера лицензирования. Этот web-сервер автоматически открывается после установки сервера лицензирования в браузере, установленном на компьютере пользователя по умолчанию.

Web-сервер устанавливается на порт 15201. Этот параметр может быть изменен на закладке «Настройка».

Важно!

Для Windows. Сначала следует произвести установку сервера лицензирования и драйверов ключа защиты. Потом, если ключ защиты аппаратный, необходимо подключить USB-ключ защиты. После этого ключ защиты определяется системой Windows, и далее информация о нем отображается в web-отчете сервера (см. ниже).

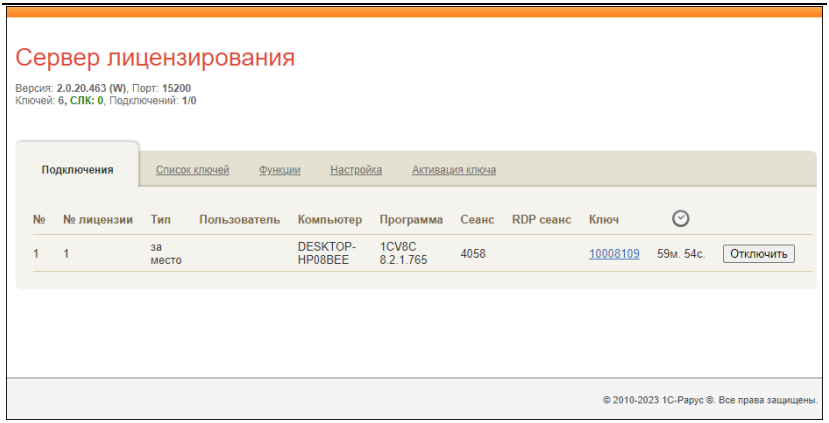
Для получения информации о сервере лицензирования, ключах и лицензиях нужно открыть в браузере адрес http://<IP адрес или имя сервера лицензирования>:15201, как показано на рисунке.



На web-сервере расположены следующие закладки.

1.8.1. Подключения

На данной закладке отображается список всех подключений к серверу лицензирования.



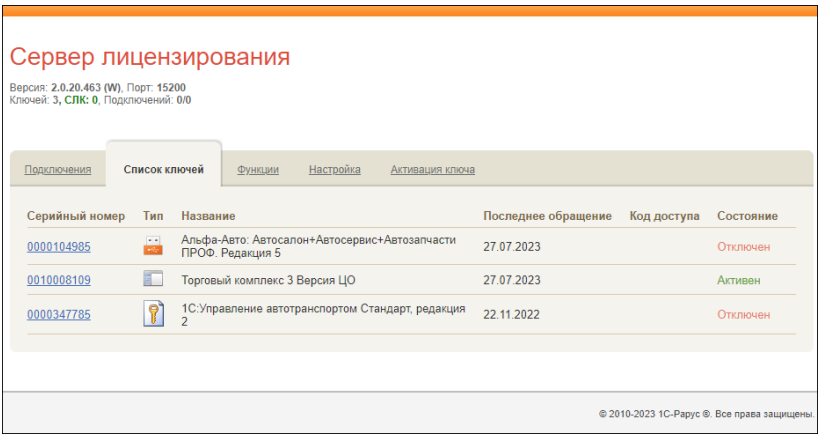
Подключение создается при старте решения на клиенте. Каждое подключение имеет номер лицензии, которую оно использует. В случае лицензирования за место, несколько подключений с одного рабочего места будут использовать одну и ту же лицензию. Во всех остальных случаях каждому подключению будет соответствовать уникальный номер выданной лицензии. Для каждой лицензии указываются:

- «Тип» – тип счетчика лицензий. Эти счетчики по-разному обрабатываются на сервере лицензирования.
- «Пользователь» – системное имя пользователя, подключившегося с данной лицензией;
- «Компьютер» – строка, идентифицирующая компьютер, с которого пришел запрос;
- «Программа» – программа, использующая данную лицензию;
- «Сеанс» – номер сеанса 1С;
- «RDP сеанс» – номер терминальной сессии (в случае работы через сервер терминалов);
- «Ключ» – ссылка на ключ, от которого получена лицензия;

- Отключить – нажатие этой кнопки освобождает лицензию на сервере. Кнопка может использоваться, например, если недостаточно лицензий для работы пользователей, и надо освободить часть использующихся лицензий (обычно поставка программного продукта имеет ограничение по числу лицензий, т. е. пользователей, одновременно работающих с программным продуктом).

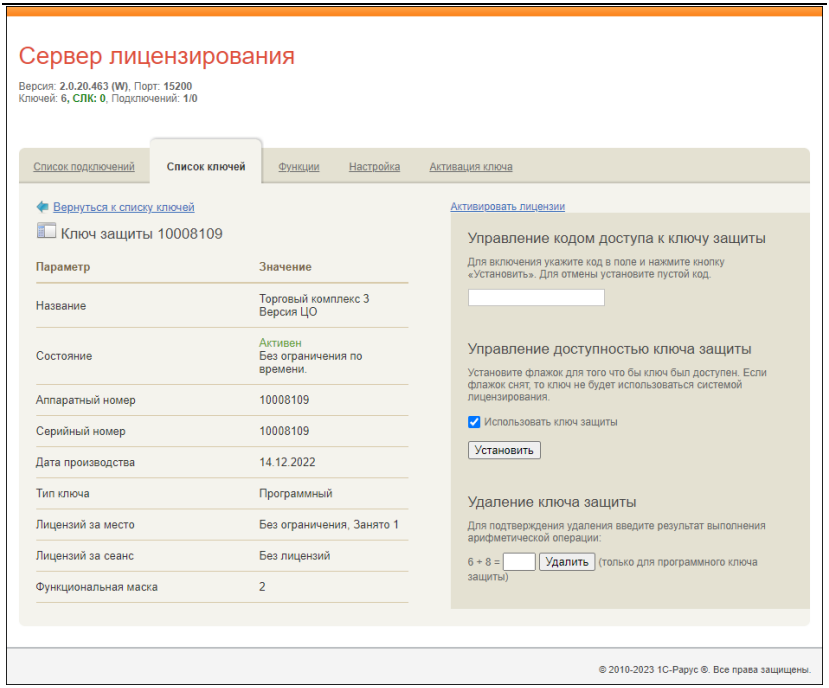
1.8.2. Список ключей

На этой закладке отображается список подключенных к серверу ключей защиты.



Для каждого ключа указывается его тип: аппаратный, программный или СЛК.

Щелчок по серийному номеру ключа открывает окно параметров данного ключа.



В этом окне может быть задан код доступа для данного ключа защиты. Этот код позволяет однозначно указать, кто сможет работать с данным ключом. Доступ к ключу будет только у того, у кого в параметрах подключения сервера задан в точности такой же код доступа (см. раздел «Настройка адреса сервера лицензирования» на стр. 11).

Это может быть удобно, например, если один сервер обслуживает сети нескольких фирм. Для ключей каждой из фирм могут быть заданы свои «пароли» – коды доступа. Таким образом, клиенты из каждой фирмы смогут обращаться только к ключу своей фирмы.

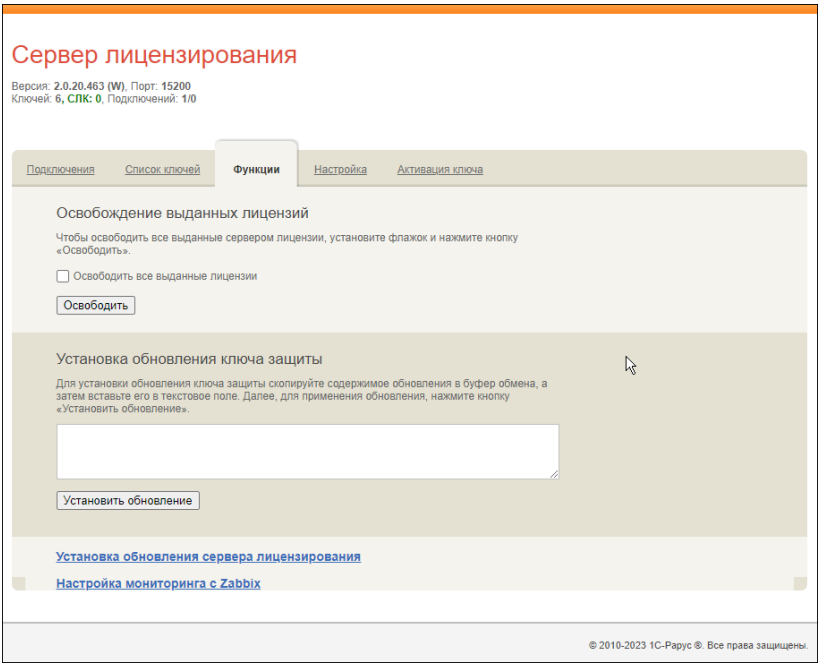
Также на данной форме расположен флажок «Использовать ключ защиты». Если этот флажок снят, то данный ключ не

будет использоваться. Таким образом можно запретить использование ключа, не отключая его от сервера.

Раздел «Удаление ключа защиты» предназначен для удаления ключей, которые перестали использоваться по разным причинам. Для защиты от случайного удаления предусмотрен ввод пользователем контрольной суммы для подтверждения выполнения операции, слагаемые которой отображаются на форме. Удаление работает только для программных ключей.

1.8.3. Функции

При помощи данной закладки можно использовать функции управления сервером лицензирования.



Установив флажок «Освободить все выданные лицензии» и нажав кнопку «Освободить», можно освободить все выданные лицензии, т. е. отключить всех пользователей от сервера.

Данная функция может быть полезна, например, если нужно отключить большое количество рабочих станций одновременно.

Внимание!

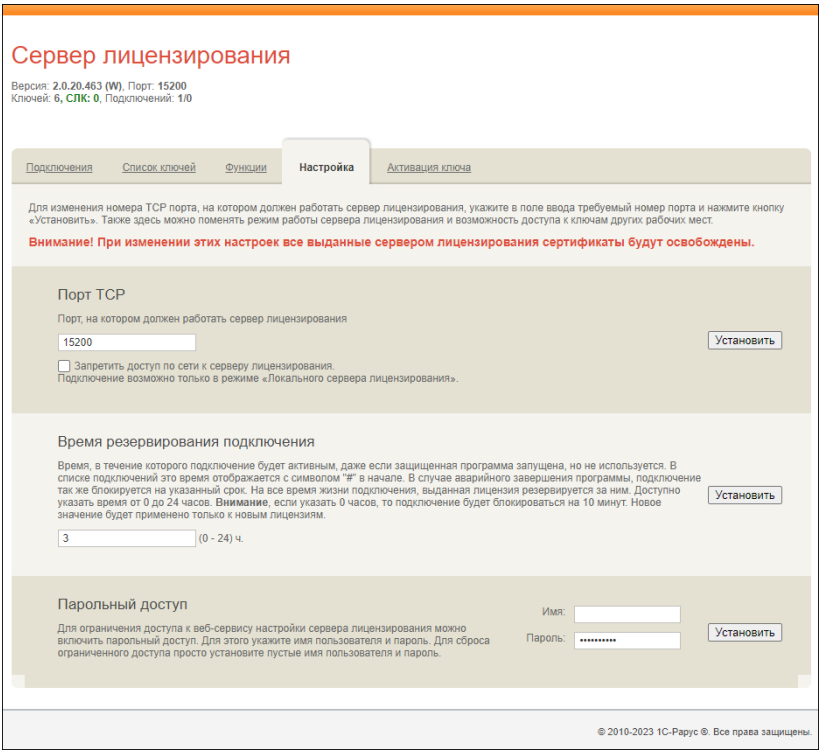
При перезапуске сервера лицензирования список подключений сохраняется.

Также при помощи данной закладки можно обновить аппаратный ключ из текстового файла. Для этого текст обновления копируется в буфер обмена, а оттуда – в текстовое поле на закладке, после чего следует нажать кнопку «Установить обновление». Текст обновления нужно копировать целиком. Не нужно удалять из него заголовок, так как это приведет к неработоспособности обновления.

После обновления ключа защиты рекомендуется перезапустить сервер лицензирования (в случае сетевой установки системы лицензирования).

Функции обновления сервера лицензирования и мониторинга с Zabbix не имеют прямого отношения к защите решения и вынесены в отдельный документ «Дополнительный_функционал_сервера_лицензирования».

1.8.4. Настройка



На данной закладке можно поменять номер TCP порта сервера лицензирования. Для этого следует указать новый номер порта в соответствующем поле и нажать кнопку «Установить». По умолчанию сервер подключен к сетевому порту 15200.

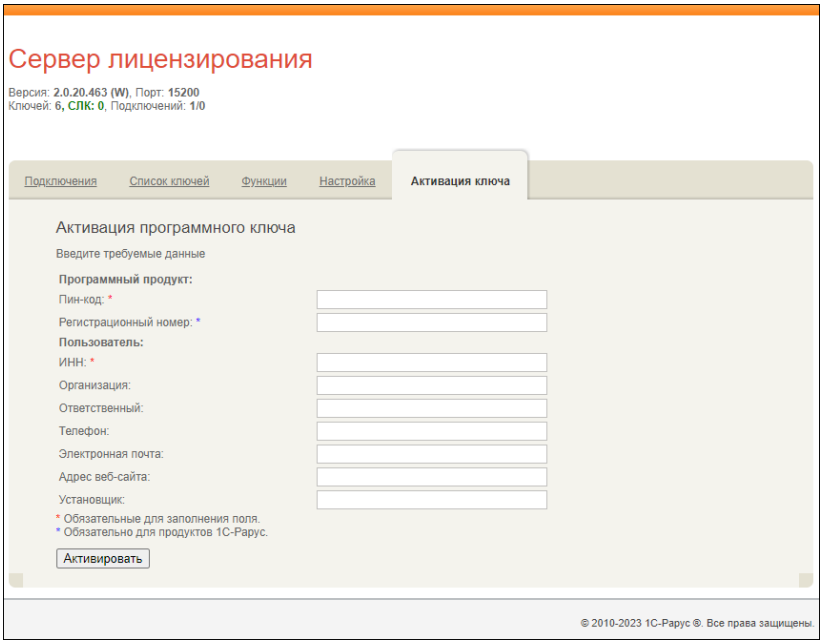
Если флажок «Запретить доступ по сети» установлен, то к данному серверу будет отсутствовать доступ по сети.

Кроме того, на данной закладке можно задать ограничение доступа к серверу лицензирования. Если указать в соответствующих полях имя пользователя и пароль и нажать

кнопку «Установить», то при попытке подключения к серверу лицензирования пользователям будет выдаваться запрос на авторизацию.

1.8.5. Активация ключа

На данной закладке возможно выполнить активацию программного ключа при наличии подключения к Интернету. Для этого потребуется ввести регистрационный номер, пин-код ключа и информацию о пользователе. Для выполнения активации следует нажать на кнопку «Активировать».



Компания «1С-Рарус»
Москва, 127434
Дмитровское шоссе, 9Б
Тел. +7 (495) 223-04-04
rarus.ru alfa@rarus.ru