



1С-Рарус®

ВНЕДРЕНЧЕСКИЙ ЦЕНТР

1С-Рарус

*1С-Рарус: Управление медицинской
организацией*

**Инструкция по установке
с целью экспертной проверки**

2020

Оглавление

Комплект поставки	
Требования к системе	
Установка	
Защита Типового решения	
Основы системы защиты Типового решения	
Установка системы защиты	
Первый запуск Типового решения	
Управление сервером защиты	
Web-сервер состояния сервера защиты	
Удаление системы защиты	
Ключи защиты	
Ввод начальных данных	
Обновления	



Начало работы



В этой главе содержатся сведения о том, как установить Типовое решение «1С-Рарус: Управление медицинской организацией» на Ваш компьютер.

Для выполнения установки Вам необходимо уметь устанавливать программы в операционной системе Windows 1, а также работать с панелью управления этой системы. Для установки сетевой версии Типового решения требуется понимание общих принципов работы локальных вычислительных сетей и навыки работы с сетевым протоколом TCP/IP.

Комплект поставки

В комплект поставки Типового решения «1С-Рарус: Управление медицинской организацией» включены:

- ☞ Дистрибутивный CD-диск;
- ☞ Руководство пользователя;
- ☞ Аппаратный ключ защиты;
- ☞ Регистрационная анкета.

Дистрибутив содержит шаблоны чистой и демонстрационной информационных баз и программу установки системы защиты Типового решения.

Типовое решение «1С-Рарус: Управление медицинской организацией» защищено от несанкционированного копирования при помощи ключа аппаратной защиты. Типовое решение не является полностью конфигурируемым, так как содержит недоступные для редактирования фрагменты исходного кода.

Требования к системе

Типовое решение «1С-Рарус: Управление медицинской организацией» можно установить при наличии установленной программы 1С:Предприятие 8. Рекомендуется использовать свежий релиз программы 1С:Предприятие 8.

Таблица 1. **Рекомендуемые требования к системе**

<i>Требование</i>	<i>Параметры системы</i>
Вариант системы «1С:Предприятие»	Локальный, сетевой, клиент-серверный
Свободного дискового пространства	от 5 Гбайт
Разрешение экранной системы	не менее 1024 x 768
Рекомендуемый размер экранных шрифтов	В поле Размер шрифта (Пуск → Настройка → Панель управления → Экран → Настройка, кнопка Дополнительно) выберите значение списка Мелкий шрифт
Объем оперативной памяти	не менее 512 Мбайт
Процессор	Pentium Celeron 2000 МГц и выше
Операционная система	Windows

Необходим свободный порт USB для установки аппаратного ключа защиты.

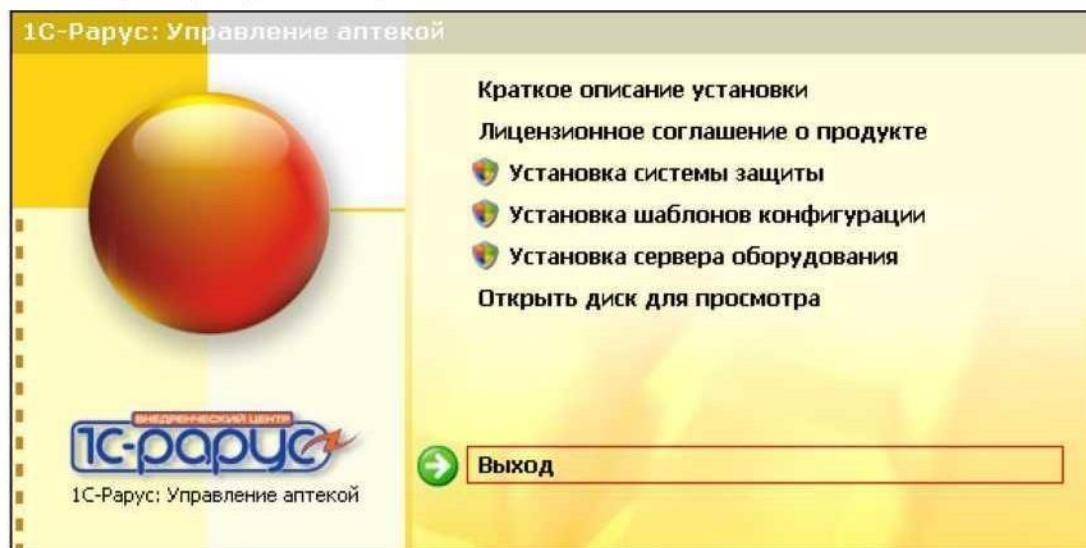
Установка

Установка Типового решения «1С-Рарус: Управление медицинской организацией» выполняется при помощи специальной программы установки, которая находится на компьютерном компакт-диске. Перед тем, как приступить к установке, следует убедиться, что жесткий диск не содержит ошибок и имеется достаточно свободного места для выполнения установки.

Вставьте компакт-диск в привод. В случае, если на вашем компьютере включен режим Автозапуска, программа установки запустится автоматически. Если этого не произойдет, для запуска программы установки выберите Пуск → Выполнить. В выданном на экран запросе укажите имя программы установки, которая находится в корневой папке CD-диска, например «d:\autorun.exe» и нажмите кнопку ОК;

Установка

На экран будет выдано окно программы установки Типового решения: 1С-Рарус: Программа установки.



В этом окне содержатся следующие пункты меню:

- ☞ Установка системы защиты. Устанавливается система защиты (см. следующий раздел).
- ☞ Установка шаблонов конфигурации. Устанавливаются файлы, используемые для создания новых баз данных Типового решения.
- ☞ Установка сервера оборудования. Устанавливается служба совместного доступа к оборудованию.
- ☞ Открыть диск для просмотра. Открывает программу проводника, но не производит установку.
- ☞ Выход. Завершает работу программы установки.

После установки шаблонов конфигурации Типового решения можно стандартным способом создать из шаблона новую информационную базу: демонстрационную или рабочую.



Добавление новой информационной базы в список баз описано в документации фирмы «1С»: книга «РУКОВОДСТВО ПО УСТАНОВКЕ И ЗАПУСКУ», глава 3, «Запуск системы 1С:Предприятие 8.0», раздел «Ведение списка информационных баз».

Защита Типового решения

В этом разделе приводится информация о защите Типового решения «ТС-Рарус: Управление медицинской организацией».

Основы системы защиты Типового решения

Для защиты используются аппаратные ключи компании «Катран». Ключи выполнены в форм-факторе и по технологии USB. На каждом ключе имеется наклейка, которая содержит следующую информацию:

- ☞ название Типового решения, для которого ключ предназначен;
- ☞ уникальный номер (s/n) ключа защиты и его штрих-код.

Драйвер аппаратного ключа защиты и сервер защиты Типового решения могут работать в одной из следующих систем (локальная сеть должна поддерживать протокол TCP/IP):

- ☞ Windows Server 2008 (32 bit);
- ☞ Windows Vista (32 bit);
- ☞ Windows 2000;
- ☞ Windows XP (32 или 64 bit)*;
- ☞ Windows Server 2003 (32 или 64 bit)*.



Установка системы защиты должна производиться пользователем, обладающим администраторскими правами в операционной системе.

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

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



Система защиты не может работать в системах Windows Vista (64 bit) и Windows Server 2008 (64 bit), так как для данных систем не существует сертифицированного фирмой Microsoft драйвера для ключей защиты компании «Катран».

Типовое решение может напрямую работать с ключом защиты, не используя компьютерную сеть. Это — локальный вариант установки.

* Для 64-битных систем есть соответствующий драйвер. Сервер и компоненты защиты реализованы на 32-битное приложение.

Защита Типового решения

Кроме того, Типовое решение может работать при помощи специальной программы — Сервера защиты и управления оборудованием. В этом случае ключ можно установить на любом компьютере Вашей локальной компьютерной сети. Сервер позволяет работать с Типовым решением на любых компьютерах этой сети (в рамках лицензионных ограничений аппаратного ключа).

Система защиты устанавливается в каталог %CommonAppDATA%\Protect\CommonProtect на сервере (так называемый общий каталог).

Здесь %CommonAppDATA% — это переменная окружения, указывающая каталог, содержащий данные приложений, общие для всех пользователей. Этот каталог различается в различных версиях операционной системы Windows. Например, в Windows XP и Windows Server 2003 это обычно каталог C:\Documents and Settings\All Users\Application Data. В Windows Vista это обычно каталог C:\ProgramData.



Если на данной системе уже установлены Типовые решения, система защиты которых использует другой общий каталог, то система защиты данного Типового решения также будет использовать прежний общий каталог.

Связь и синхронизация файлов на сервере и в локальных каталогах на компьютерах пользователей Типового решения осуществляются по протоколу TCP. Для этого в сервер защиты добавлен сервер синхронизации. Он позволяет клиенту запросить любой файл из общего каталога по протоколу TCP. По умолчанию сервер синхронизации устанавливается на порт 11999. Для настройки этого сервера в конфигурационном файле Config.xml в секцию Система добавлен атрибут СерверСинхронизации. Его значением является строка, содержащая имя сервера и номер порта сервера синхронизации, например, «MyServer:11999».

Система защиты устанавливается на компьютере при помощи мастера, предлагающего поочередно выполнить определенные действия. Смена экранов мастера управляется кнопками, рассмотренными в табл. 2.

Таблица 2. **Мастер системы защиты, кнопки**

<i>Кнопка</i>	<i>Действие</i>
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).

Установка производится путем копирования определенных файлов в общий каталог.

На каждом компьютере сети при первом запуске Типового решения автоматически создается локальный каталог. Локальный каталог размещается в следующем месте:

`%CommonAppDATA%\Protect\LocalProtect.`

(Здесь, как и в случае общего каталога, `%CommonAppDATA%` — это переменная окружения, указывающая каталог, содержащий данные приложений, общие для всех пользователей.)



Если на данной системе уже установлены Типовые решения, система защиты которых использует другой локальный каталог, то система защиты данного Типового решения также будет использовать прежний локальный каталог.

При каждом запуске Типового решения в локальный каталог автоматически копируются измененные и обновленные файлы из общего каталога. После этого Типовое решение работает только с файлами из локального каталога.

Установка системы защиты

Типовое решение может использоваться в однопользовательском или в сетевом режиме.

Для установки системы защиты выполните следующую последовательность действий:

1. Запустите программу `Setup.exe`, которая находится в папке `Protect` установочного диска. Появляется первый экран мастера установки системы защиты.

Защита Типового решения



Чтобы начать установку системы защиты, нажмите кнопку **Далее**.

Следующий экран программы установки появляется только в том случае, если на компьютере не установлен драйвер аппаратного ключа защиты или если в состав дистрибутива данного Типового решения включена более новая версия этого драйвера, чем установленная на компьютере. На этом экране пользователю предлагается выполнить стандартные действия, связанные с инсталляцией драйвера аппаратного ключа защиты.



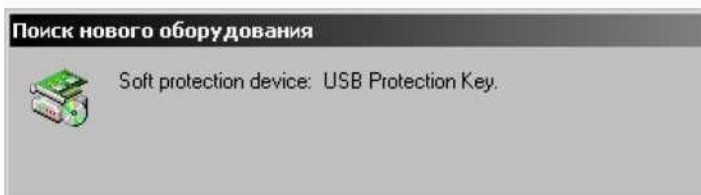
Если на компьютере ранее был установлен драйвер защиты и требуется переустановить его (например, появилась новая версия), то установите флажок **Переустановить драйвер**.



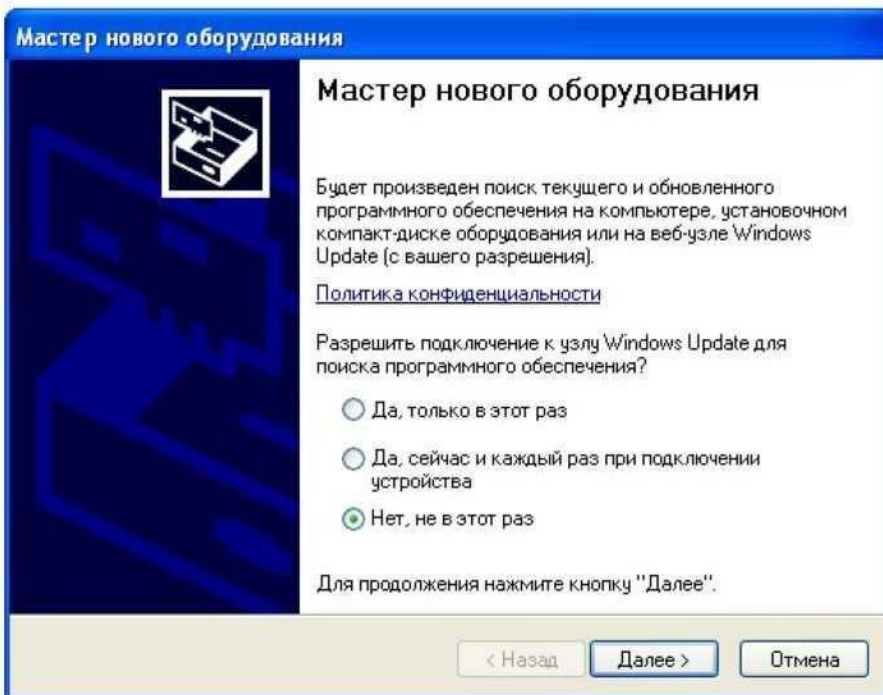
Если на компьютере установлен драйвер, версия которого совпадает с версией входящего в состав нового дистрибутива драйвера или является более новой, то программа установки пропустит этот экран и сразу перейдет к следующему.

Кнопка **Далее** недоступна, если драйвер не установлен.

2. Установите аппаратный ключ защиты в любой свободный USB-порт компьютера*.



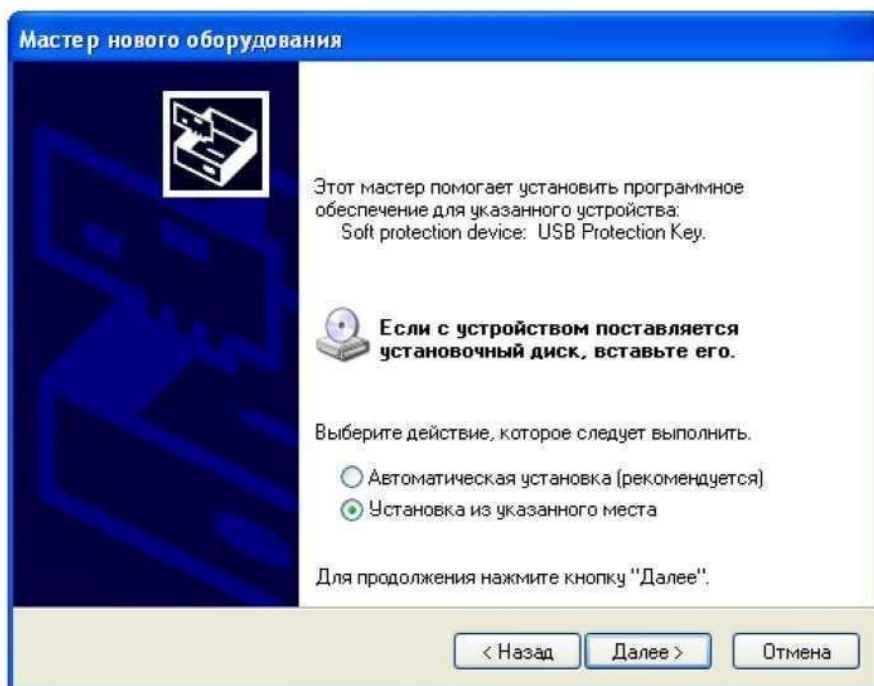
Система Windows определяет, что установлено новое устройство, после чего вызывает стандартный мастер установки нового оборудования.



Слева показан первый экран мастера обнаружения нового оборудования для системы Windows XP. В других системах внешний вид экранов мастера может незначительно отличаться.

* Ключ защиты может также быть установлен в один из портов USB-хаба, подключенного к USB-порту компьютера.

Защита Типового решения

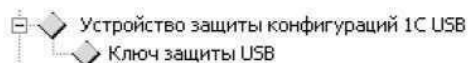


Следуя подсказкам мастера, выберите установку драйвера ключа защиты из указанной папки. Для 32-битных операционных систем драйвер находится на установочном диске Типового решения в папке Protect\Drivers.



Для 64-битных операционных систем драйвер находится в папке Protect\Drivers\la64.

Для проверки корректности установки драйвера выберите Пуск → Панель управления → Система → Оборудование, кнопка Диспетчер устройств.



Если драйвер установлен, то в окне Диспетчер устройств появляется строка Устройство защиты

конфигураций 1С USB и строки, соответствующие установленным ключам.

3. После завершения работы мастера установки нового оборудования вернитесь к мастеру установки системы защиты и нажмите

кнопку Далее. Вы перейдете на следующий экран, на котором следует выбрать позицию переключателя локальной или сетевой установки.



Выбрав нужный тип установки, нажмите кнопку Далее.

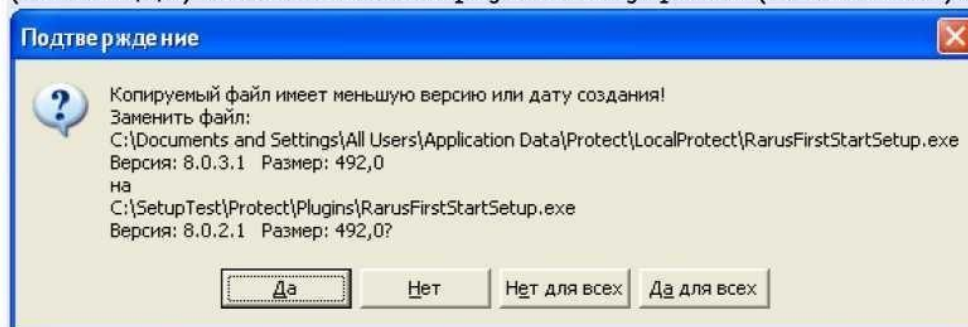
- Следующий экран мастера информационный: в нем приводится информация о принятых Вами ранее решениях по установке системы защиты. При нажатии кнопки Далее мастер начинает установку (или переустановку) системы защиты.



Защита Типового решения

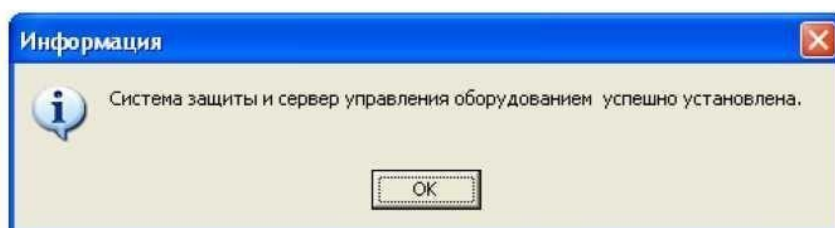


При переустановке может оказаться, что версия ранее установленного файла системы защиты выше, чем версия устанавливаемого файла. В этом случае можно подтвердить необходимость переустановки (кнопка Да) или отменить переустановку файла (кнопка Нет).



Поскольку система защиты состоит из нескольких файлов, такое окно может возникать при перезаписи каждого из них. При нажатии кнопки Да для всех при дальнейшей установке файлы будут перезаписаны автоматически. При нажатии кнопки Нет для всех ни один из существующих на компьютере файлов системы защиты перезаписан не будет.

5. При завершении установки появляется сообщение об этом.



После нажатия кнопки ОК выводится заключительный экран мастера установки.

Заключительный экран мастера показывает результаты установки.



После нажатия кнопки Готово процесс установки сервера защиты и управления оборудованием полностью завершается.

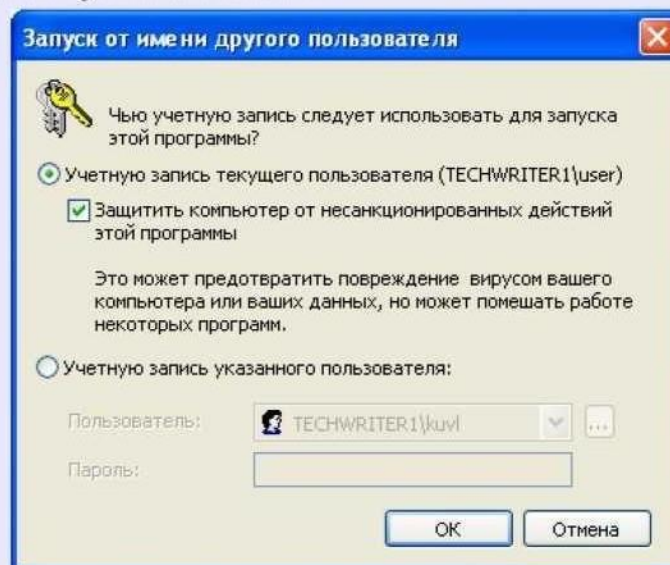
Первый запуск Типового решения

Первый запуск Типового решения «1С-Рарус: Управление медицинской организацией», так же как и установка системы защиты (см. главу 3.4.2, «Установка системы защиты» на стр. 130), должен производиться пользователем, обладающим администраторскими правами в операционной системе. Это необходимо для регистрации Типового решения в системе.

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



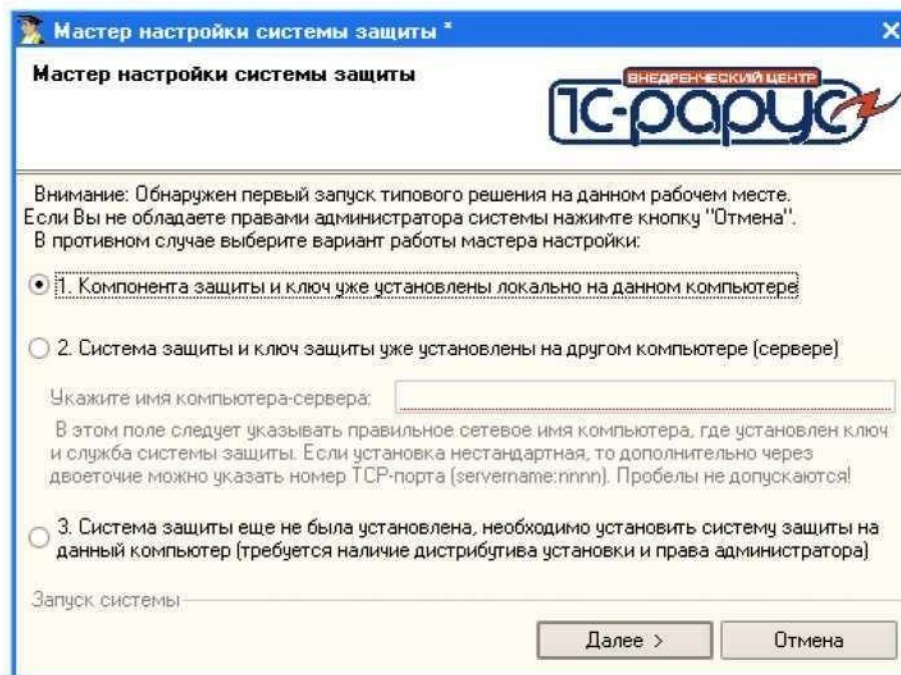
Если пользователь не обладает правами администратора, то первый запуск Типового решения невозможен. В этом случае система предложит указать новую учетную запись пользователя, у которой есть права администратора. Типовое решение будет запущено от имени этой новой учетной записи.



Для последующих запусков Типового решения наличие у пользователя прав администратора необязательно.

Защита Типового решения

При первом запуске Типового решения появляется экран настройки системы защиты.



На этом экране необходимо выбрать, какой тип установки системы защиты был использован (в том случае, если система защиты уже установлена): серверный или локальный (см. раздел «Установка системы защиты»).

Возможны следующие варианты выбора:

1. Компонента защиты и ключ уже установлены локально на данном компьютере.

В этом случае после нажатия кнопки **Далее** система проверит правильность установленного ключа защиты и, если проверка прошла успешно, загрузит Типовое решение.

2. Система защиты и ключ уже установлены на другом компьютере (сервере).

В этом случае система требует введения сетевого имени сервера*.

После нажатия кнопки **Далее** система проверит подключение к серверу защиты и управления оборудованием и, в случае корректного подключения, загрузит Типовое решение.


* Если установка нестандартная, то дополнительно через двоеточие (без пробелов) можно указать номер TCP-порта (например, MyServer:14144).

3. Система защиты еще не была установлена.

При выборе этого варианта после нажатия кнопки Далее начинается установка системы защиты (см. раздел «Установка системы защиты»).

Управление сервером защиты

Программа сервера — файл KeyServer.exe — располагается в общем каталоге.

Если сервер защиты работает и операционная система, установленная на компьютере, не является Windows Vista, то в правом нижнем углу экрана будет отображен значок . Если этот значок отображается не цветным, а монохромным, это обозначает, что при запуске сервера защиты произошла ошибка и сервер защиты в данный момент не работает. Уточнить причину ошибки можно с помощью web-отчета, подробнее о котором см. раздел «Web-сервер состояния сервера защиты».



Если на компьютере установлена операционная система Windows Vista, то значок сервера защиты не выводится. В этом случае узнать о состоянии сервера защиты можно при помощи web-отчета.

Если сервер установлен в качестве службы, то управление сервером производится посредством программы управления службами (Пуск → Панель управления → Администрирование → Службы). Имя службы — «RKeyServer». Выводимое имя — «Сервер защиты».

Web-сервер состояния сервера защиты

Для более детального контроля ключей и лицензий в сервере защиты предусмотрен web-сервер, который позволяет получить описание текущего состояния сервера защиты. Сервер состояния устанавливается на порт 11998. Этот параметр не настраивается.

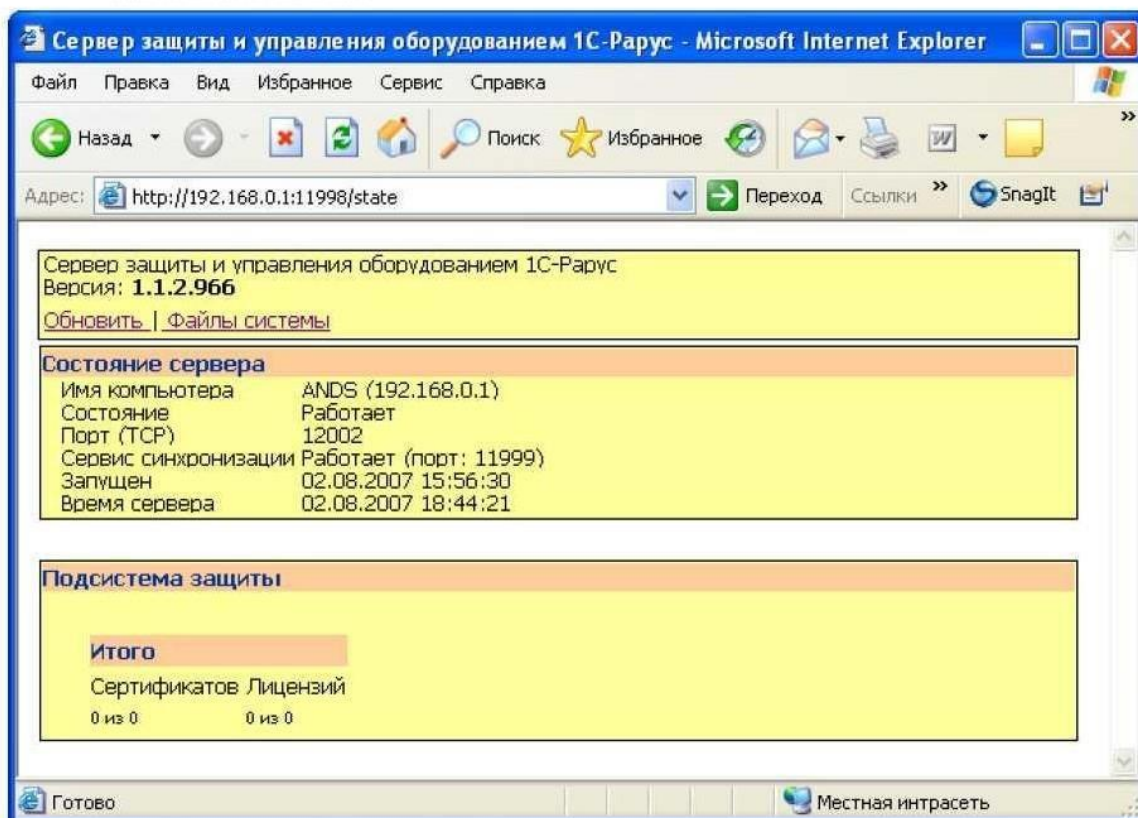


Информация о ключах доступна только после того, как Типовое решение обратится к ключу.

Для получения статистики нужно обратиться при помощи программы Internet Explorer (или другого обозревателя web-страниц) на адрес

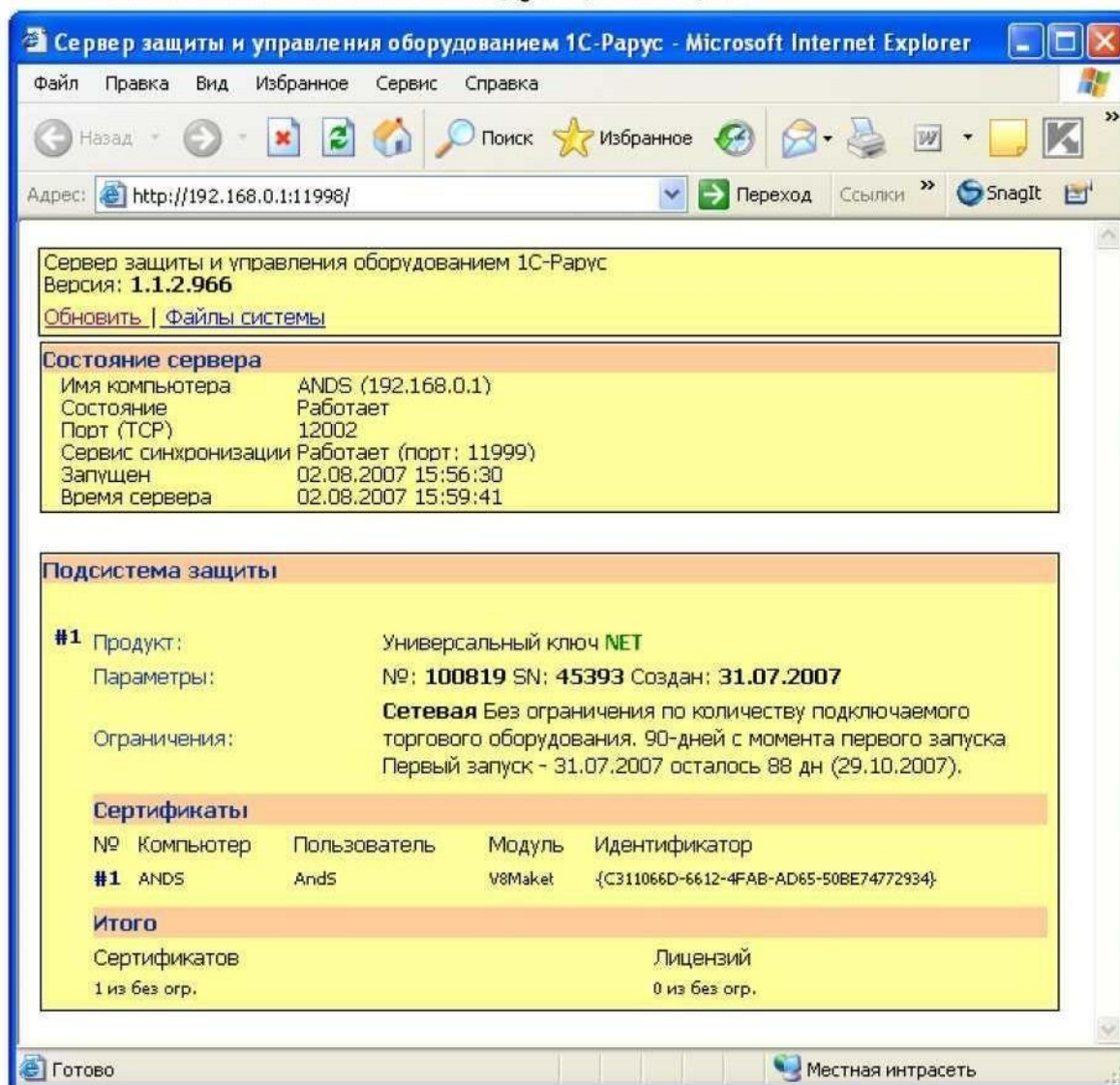
Защита Типового решения

<http://<IP адрес или имя компьютера, на котором запущен сервер защиты>:11998>.



При вводе этого адреса отображается чистый бланк отчета. Для заполнения этого бланка требуется кликнуть по гиперссылке Обновить.

Web-отчет состоит из следующих секций:



☞ Заголовок. Содержит параметр Версия, в котором отображается версия запущенного сервера защиты.

☞ Состояние сервера. Параметры этой секции рассмотрены в табл. 3.

Таблица 3. **Параметры состояния сервера защиты**

Графа	Содержимое
Имя компьютера	Сетевое имя (IP-адрес) компьютера, на котором запущен сервер защиты.
Состояние	Состояние сервера защиты.
Порт (TCP)	Порт сервера защиты.
Сервис синхронизации	Состояние сервиса синхронизации файлов системы защиты. Если сервис работает, в скобках указывается порт, на котором сервис установлен.
Запущен	Дата и время старта сервера защиты.

Защита Типового решения

Таблица 3. **Параметры состояния сервера защиты** (продолжение)

<i>Графа</i>	<i>Содержимое</i>
Время сервера	Текущие дата и время сервера защиты.

☞ Подсистема защиты. Параметры этой секции рассмотрены в табл. 4.

Таблица 4. **Параметры подсистемы защиты**

<i>Графа</i>	<i>Содержимое</i>
Продукт	Наименование ключа защиты Типового решения.
Параметры	Серийный и аппаратный номера и дата прошивки ключа защиты.
Ограничения	Список лицензионных ограничений использования Типового решения: по количеству пользователей, по количеству подключаемого оборудования, по конечной дате работы ключа защиты.

Секция Подсистема защиты состоит из разделов и подразделов:

☞ Сертификаты. Параметры этого раздела рассмотрены в табл. 5.

Таблица 5. **Сертификаты**

<i>Графа</i>	<i>Содержимое</i>
Компьютер	Имя компьютера, на котором запущено Типовое решение.
Пользователь	Пользователь Windows, от имени которого запущено Типовое решение.
Модуль	Имя компоненты Типового решения.
Идентификатор	Уникальный идентификатор сертификата сессии Типового решения (GUID).

☞ Лицензии на оборудование. Параметры этого подраздела рассмотрены в табл. 6.

Таблица 6. **Лицензии на оборудование**

<i>Графа</i>	<i>Содержимое</i>
Идентификатор	Уникальный идентификатор лицензии сессии подключения оборудования (GUID).
Оборудование	Имя экземпляра оборудования, на который выписана лицензия.

Таблица 6. **Лицензии на оборудование** (продолжение)

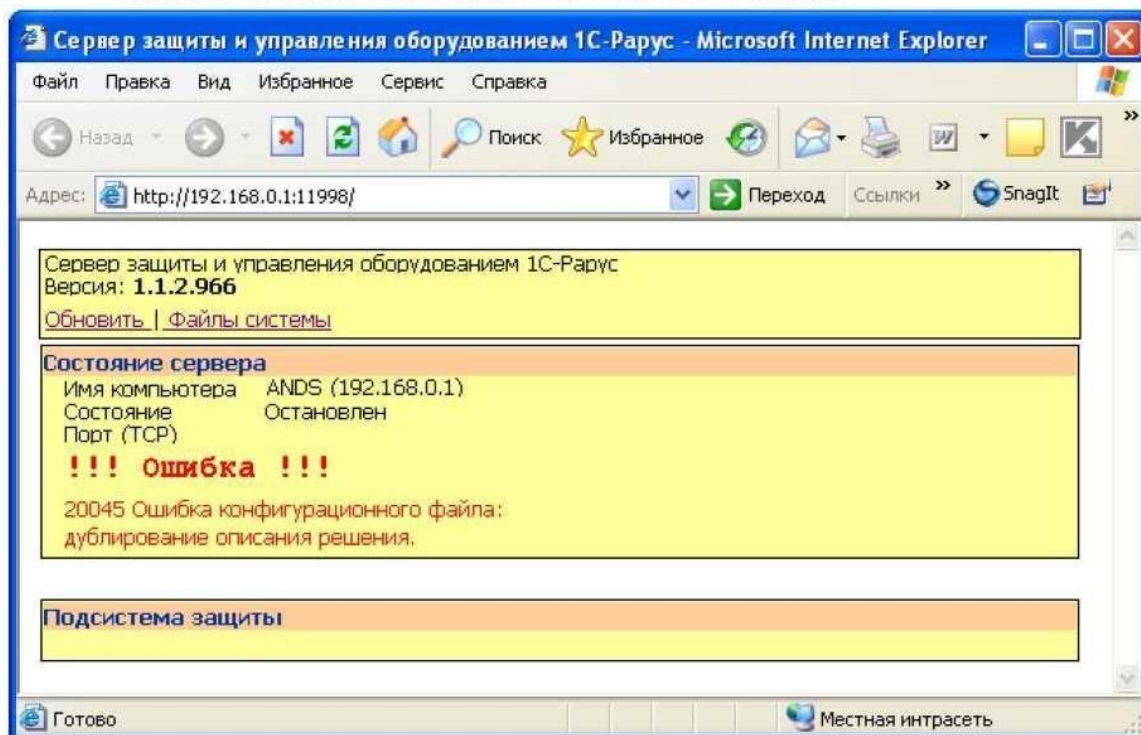
<i>Графа</i>	<i>Содержимое</i>
Лицензий	Требуемое количество лицензий для данного экземпляра оборудования.

Итого. Параметры этого раздела рассмотрены в табл. 7.

Таблица 7. **Итоговая таблица системы защиты**

<i>Графа</i>	<i>Содержимое</i>
Сертифика- тов	Реально выданное количество сертификатов.
Лицензий	Реально выписанное количество лицензий.

Кроме того, web-отчет предоставляет сведения об ошибках, возникающих при запуске и при работе системы защиты. При этом в секцию Состояние сервера выводится слово Ошибка, а также код, наименование и описание возникшей ошибки.



Удаление системы защиты

Для удаления системы защиты выберите Пуск → Настройка → Панель управления → Установка и удаление программ → 1С-

Защита Типового решения

Рарус: Система защиты и управления оборудованием —> Заменить/Удалить.

На экране появляется сообщение, говорящее, что систему защиты можно удалить. Для удаления системы нажмите кнопку Далее.

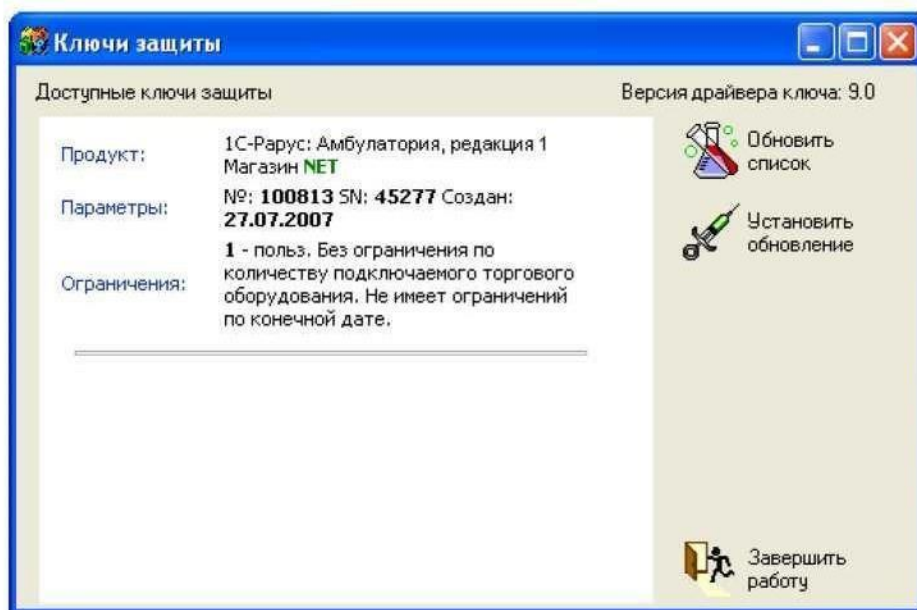


Ключи защиты



Ключи
защиты

После установки системы защиты в панели управления компьютером (Пуск —> Настройка —> Панель управления) появляется значок, соответствующий программе управления ключами защиты: Ключи защиты. Эта программа позволяет проверить правильность установки ключей на текущем компьютере. Кроме того, она дает возможность установки обновлений (например, при покупке дополнительных лицензий на работу Типовых решений).



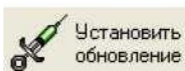
При двойном щелчке по значку Ключи защиты появляется диалоговое окно Ключи защиты.

Слева в этом окне перечислены ключи, установленные на текущем компьютере, вместе с их параметрами.

Кнопки, которые управляют работой программы, рассмотрены в табл. 8.

Таблица 8. **Ключи защиты 1С-Рарус, кнопки**

Кнопка	Действие
Обновить список	Заново формирует список (после удаления или вставки ключа).
Установить обновление	Вызывает программу установки обновления, описанную ниже.
Завершить работу	Закрывает диалоговое окно.



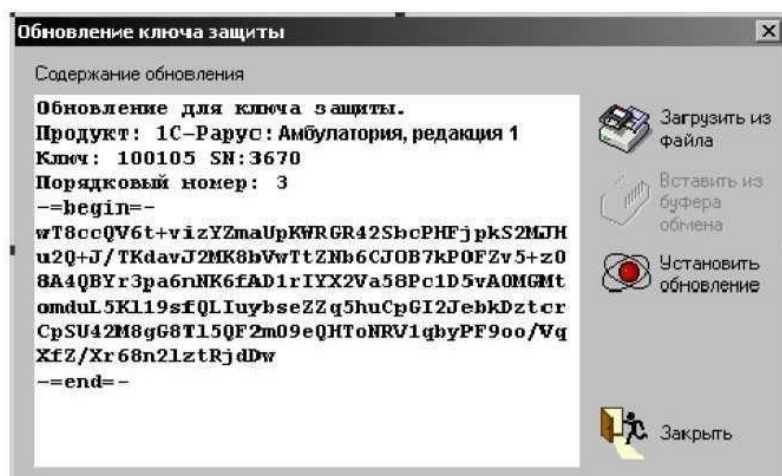
При нажатии кнопки **Установить обновление** появляется диалоговое окно **Обновление ключа защиты**.



Обновление можно использовать только для того ключа, для которого оно выписано. Каждое обновление можно установить только один раз, после чего можно будет устанавливать только обновление с большим порядковым номером. Пакет обновления устанавливается, как правило, для увеличения количества лицензий, прошитых в ключ.

В случае, если обновление не устанавливается, следует обратиться в службу технической поддержки.

Защита Типового решения



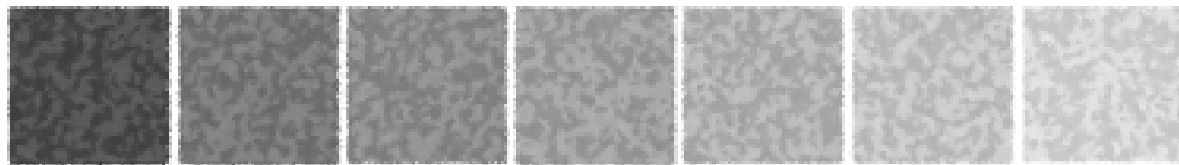
В левой части диалогового окна Обновление ключа защиты располагается информация об обновлении (эта информация начинается с заголовка, описывающего Типовое решение, ключ защиты для которого обновляется, и сам ключ защиты).

Кнопки, которые управляют работой программы, рассмотрены в табл. 9.

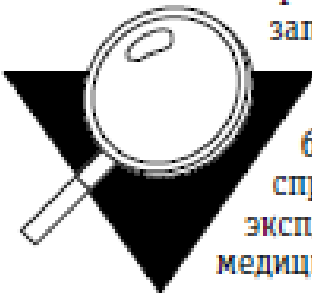
Таблица -9. **Обновление ключа защиты, кнопки**

Кнопка	Действие
Загрузить из файла	Позволяет загрузить обновление из файла. (Обычно файл обновления имеет название Update.kUpd.) Содержимое выбранного файла показывается слева.
Вставить из буфера обмена	Если текст файла обновления целиком забран в буфер обмена, то содержимое этого файла копируется в диалоговое окно.
Установить обновление	Устанавливает обновление, которое показывается в диалоговом окне. Обновление устанавливается несколько секунд, после чего появляется сообщение о результате выполнения программы.
Закреть	Закрывает диалоговое окно.

После обновления ключа защиты рекомендуется перезагрузить Сервер защиты и управления оборудованием (в случае сетевой установки системы защиты) или перезагрузить компьютер.



Ввод начальных данных



Прежде чем начать эксплуатацию Типового решения «1С-Рарус: Управление медицинской организацией», необходимо заполнить вашу рабочую базу данных информацией, которая определяет режимы дальнейшей работы. Порядок работы с Типовым решением аналогичен порядку работы с любой базой данных системы 1С:Предприятие 8. Так, многие справочники можно заполнять непосредственно в ходе эксплуатации Типового решения «1С-Рарус: Управление медицинской организацией».

Большинство значений констант автоматически заполняются при первом запуске Типового решения с пустой базой данных. Однако следует изменить значения констант так, чтобы они отвечали особенностям учета в вашей компании. Диалоговое окно констант автоматически открывается при первом запуске Типового решения.

Далее следует заполнить справочники следующих подсистем.

- ☞ см. «Структура компании» ;
- ☞ см. «Номенклатурные»
- ☞ см. «Статьи и свойства»
- ☞ см. «Классификаторы».

Наконец, следует ввести документы начальных остатков.

1. «Ввод остатков товаров»
Рекомендуется вводить суммарный остаток товаров на главный склад, а затем переместить необходимые товары на розничные и ордерные склады. Раздельно вводятся остатки товаров компании, принятые на комиссию и переданные на комиссию.
2. «Закрытие накопительных сумм»
Цены на товары задаются раздельно в разрезе типов цен.
3. «Приходный кассовый ордер»
«Банковская выписка»
Введите остатки денежных средств раздельно по кассам и банковским счетам компании. В качестве контрагента следует выбрать служебный элемент: «Ввод начальных остатков». Для каждой организации с этим

контрагентом должен быть заключен свой договор (в валюте остатков денежных средств). Возникшую задолженность погасите документом «Ввод остатков взаиморасчетов» (см. «Ввод остатков взаиморасчетов»).

4. см. «Ввод остатков взаиморасчетов»
Введите текущие значения долгов компании и контрагентов в разрезе договоров.

Обновления

Зарегистрированным пользователям могут предоставляться соответствующие обновления Типового решения «1С-Parus: Управление медицинской организацией», а также обновления базовой платформы «1С:Предприятие 8».



Зарегистрированным считается пользователь, приславший оригинал возвратной части анкеты по указанному на ней адресу.

Обновления предоставляются пользователю на твердых носителях или в электронном виде. Последовательность действий при обновлении описана в документации на программу «1С:Предприятие 8».