2.4 Защита Типового решения

В этом разделе приводится информация о защите Типового решения.

2.4.1 *Что такое система защиты*

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

Компонента защиты, которая является неотъемлемой частью типового решения, содержит алгоритмы и данные, которые недоступны без установления связи с ключом защиты.

2.4.2 *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.

Вид лицензии поставки программного продукта задается в прошивке ключа защиты.

Типовое решение может работать либо в локальном, либо в сетевом варианте.

- Типовое решение может напрямую работать с ключом защиты, не используя компьютерную сеть. Это – локальный вариант работы. В локальном варианте работы решение устанавливается и работает только на одном компьютере.
- В сетевом варианте несколько пользователей решения работают в общей сети по протоколу TCP/IP. При этом используется единый общий сервер защиты – один из компьютеров сети, на котором устанавливается система защиты и к которому подключается ключ защиты. Все остальные компьютеры сети подключаются к этому серверу защиты. Типовое решение работает при помощи специальной программы – Сервера защиты и управления оборудованием. Сервер

позволяет работать с Типовым решением на любых компьютерах этой сети (в рамках лицензионных ограничений аппаратного ключа).

Сервер защиты и управления оборудованием и лицензионный ключ должны быть установлены на одном и том же компьютере.

- Также решение может работать на терминальном сервере. Случай работы на терминальном сервере аналогичен сетевому варианту работы. В этом случае система защиты устанавливается на терминальный сервер.

Драйвер аппаратного ключа защиты и сервер защиты Типового решения могут работать в одной из следующих систем :

- Windows 7 (32 или 64 bit);
- Windows Server 2008 (32 или 64 bit);
- Windows Vista (32 или 64 bit);
- Windows 2000 (32 или 64 bit);
- Windows XP (32 или 64 bit);
- Windows Server 2003 (32 или 64 bit).

2.4.3 *Установка системы защиты*

Установка Типового решения 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 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.

Для локального варианта работы система защиты устанавливается в каталог %CommonAppDATA%\Protect\LocalProtect.

В сетевом варианте работы система защиты устанавливается только на один компьютер сети – сервер защиты. Для сетевого варианта работы 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 и Windows 7 это обычно каталог C:\ProgramData.

Если при сетевом варианте работы 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.

Перед тем как устанавливать систему защиты, следует убедиться, что к USB-портам компьютера не подключены аппаратные ключи защиты.

Если аппаратный ключ подключен к USB-порту, то в ходе установки программа предложит отключить его.

При подключении ключа защиты к USB-порту компьютера, если система защиты еще не установлена, некоторые операционные системы могут предложить начать ее установку. В этом случае следует нажать кнопку Отмена.*

Система защиты устанавливается на компьютере при помощи мастера, предлагающего поочередно выполнить определенные действия.

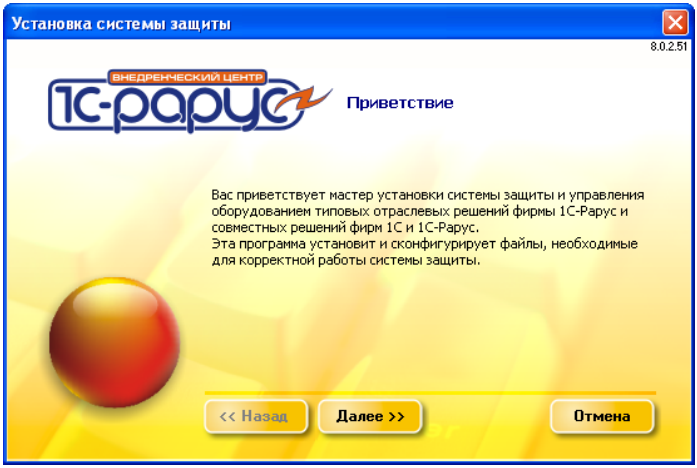
Для установки системы защиты выполните следующую последовательность действий.

1. Запустите программу Autorun.exe, которая находится в корне установочного диска.

   На открывшемся экране выберите пункт Установка системы защиты.

2. Откроется первый экран мастера установки системы защиты.

* Такое начало установки также вполне возможно. Однако далее в целях единообразия мы рассмотрим другой метод установки системы защиты, пригодный для всех операционных систем Windows.



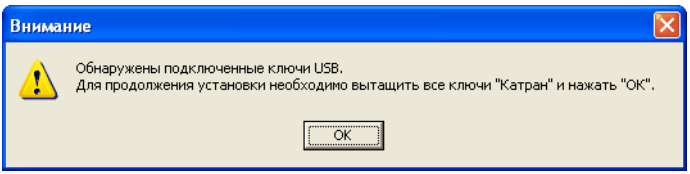
Смена экранов мастера управляется стандартными кнопками, рассмотренными в табл. **2-2**.

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

Кнопка	*Действие*
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).

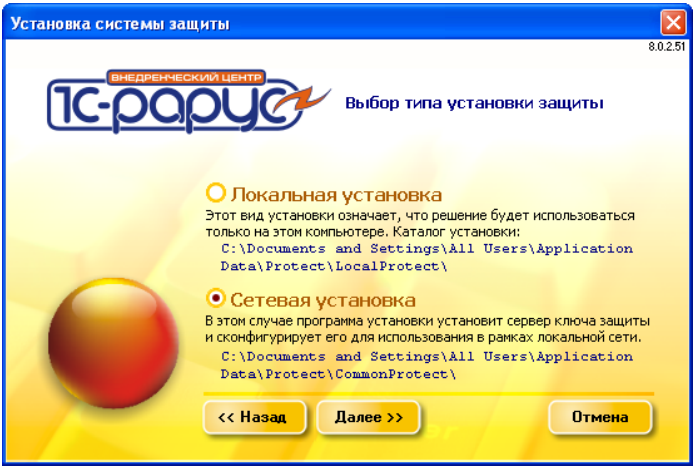
Чтобы начать установку системы защиты, нажмите кнопку Далее.

Программа произведет проверку, не подключены ли к компьютеру ключи аппаратной защиты. В том случае, если такие ключи будут обнаружены, программа выведет окно с просьбой их отключить.



Следует извлечь ключи из USB-портов компьютера (либо из портов USB-хаба, подключенного к USB-порту компьютера), после чего нажать OK.

3. На следующем экране мастера установки следует выбрать позицию переключателя локальной или сетевой установки.



В локальном варианте работы решение устанавливается и работает только на одном компьютере.

В сетевом варианте несколько пользователей решения работают в общей сети. При этом используется единый общий сервер защиты – один из компьютеров сети, на котором устанавливается система защиты и к которому подключается ключ защиты. Все остальные компьютеры сети подключаются к этому серверу защиты.

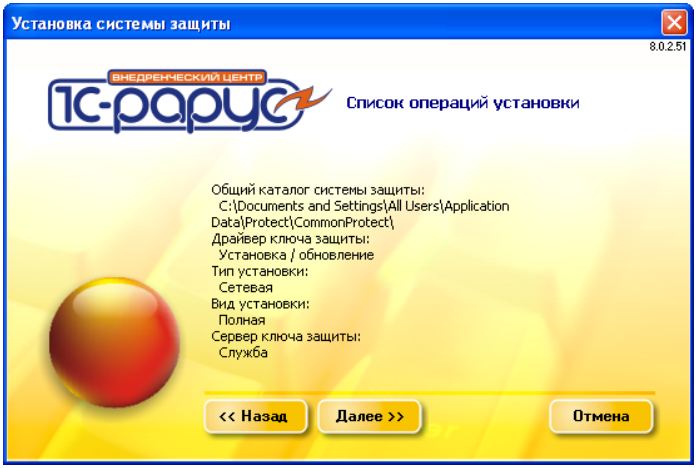
В сетевом варианте работы система защиты устанавливается только на сервер защиты. Для нее следует выбрать вариант Сетевая установка.

В случае работы на терминальном сервере также следует выбирать вариант Сетевая установка. Система защиты устанавливается на терминальный сервер.

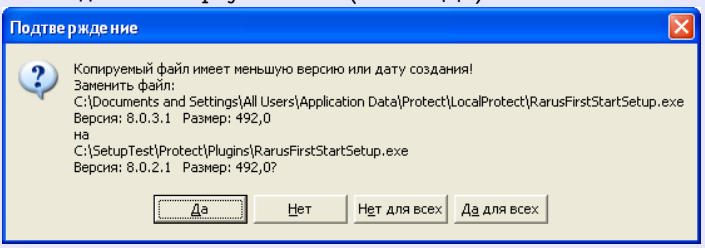
Выбрав нужный тип установки, нажмите кнопку Далее.

4. 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.



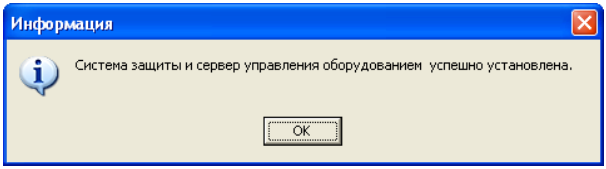
При переустановке может оказаться, что версия ранее установленного файла системы защиты выше, чем версия устанавливаемого файла. В этом случае можно подтвердить необходимость переустановки (кнопка Да) или отменить



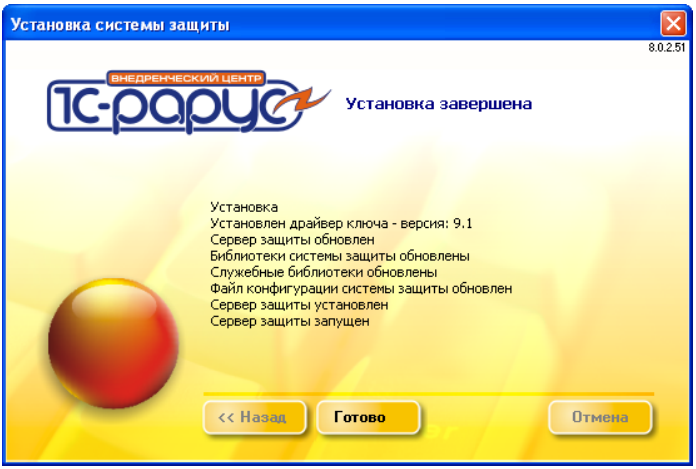
переустановку файла (кнопка Нет).

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 OK открывается заключительный экран мастера. На этом экране показываются результаты установки.



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

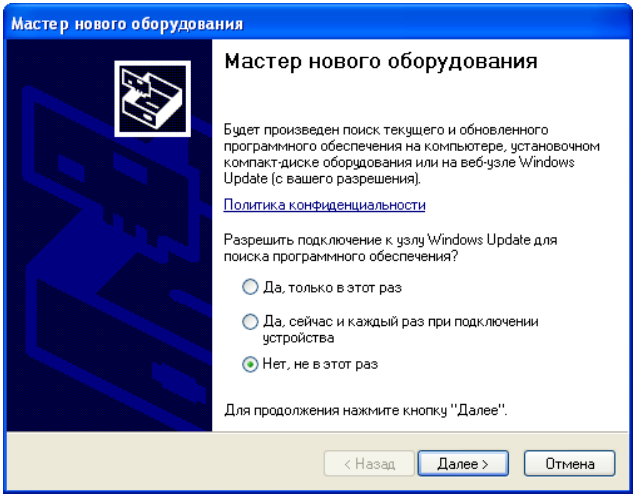
После установки системы защиты в панели управления компьютером появляется значок, соответствующий программе управления ключами защиты: Ключи защиты. Эта программа позволяет отобразить список всех лицензионных ключей, установленных на данном компьютере. Подробнее об этой программе *см.* раздел 2.4.7, «Ключи защиты» на стр. 49.

Подключение ключа защиты

После того как система защиты установлена, следует подключить ключ защиты к USB-порту компьютера.

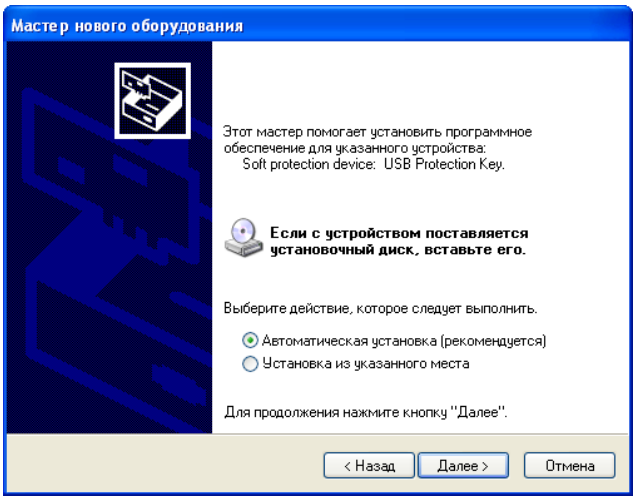
Если на компьютере установлена операционная система Windows Server 2008, Windows Vista либо Windows 7, то установка ключа защиты будет осуществлена автоматически.

В том случае, если на компьютере установлена операционная система Windows Server 2003, Windows 2000 либо Windows XP, будет вызван стандартный мастер установки нового оборудования.



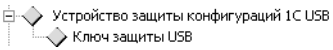
Слева показан первый экран мастера обнаружения нового оборудования для системы Windows XP. В других системах внешний вид экранов мастера может незначительно отличаться.

На этом экране следует выбрать вариант Нет, не в этот раз и нажать кнопку Далее.



На следующем экране выберите автоматическую установку и нажмите кнопку Далее.

Для проверки корректности подключения ключа защиты выберите Пуск –> Панель управления –> Система –> Оборудование, кнопка Диспетчер устройств.



Если ключ защиты успешно добавлен, то в окне Диспетчер устройств появляется строка Устройство

защиты конфигураций 1С USB и строки, соответствующие установленным ключам.

2.4.4 *Установка и удаление драйвера ключа защиты*

Установка драйвера ключа защиты происходит автоматически вместе с установкой системы защиты (*см.* раздел 2.4.3, «Установка системы защиты» на стр. 33).

Если по какой-либо причине необходимо установить вручную, переустановить или удалить этот драйвер, для этого следует использовать утилиту **UPKeyInst.exe**.

Данная утилита предназначена для работы с драйвером в операционных системах Windows 2000, Windows XP и более поздних.

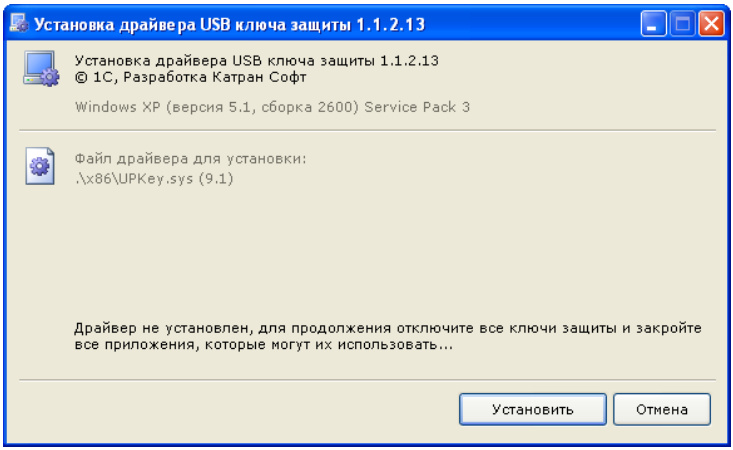
Она находится на установочном диске решения в папке Protect\Drivers.

Для успешной установки драйвера необходимо, чтобы программа была запущена от имени пользователя, обладающего правами администратора.

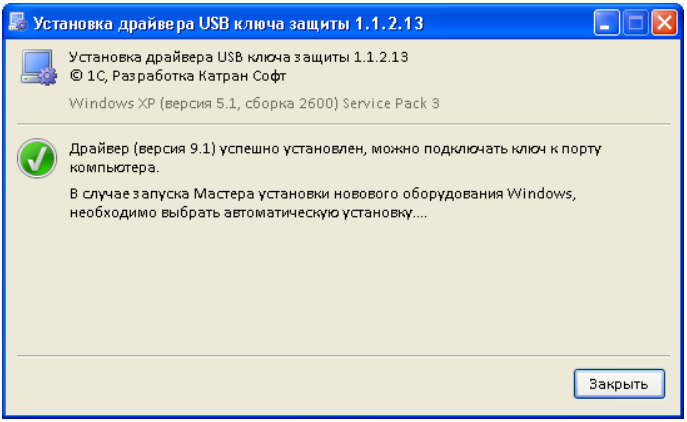
Для установки, переустановки или удаления драйвера при помощи данной утилиты сначала необходимо отсоединить все USB-ключи и завершить все использующие их приложения.

Установка драйвера

Для установки драйвера ключа защиты следует запустить утилиту **UPKeyInst.exe** и нажать кнопку Установить.



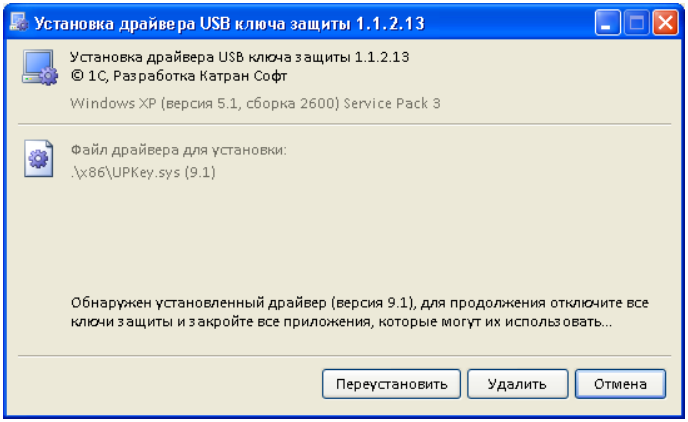
При завершении установки появляется сообщение об этом.



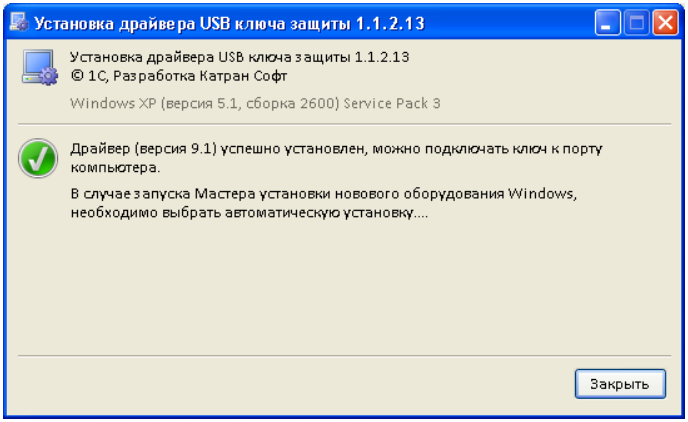
После этого следует подключить ключ. В том случае, если запустится Мастер установки нового оборудования Windows, следует выбрать пункт Автоматическая установка
(*см.* раздел «Подключение ключа защиты» на стр. 38).

Переустановка драйвера

Для переустановки драйвера ключа защиты следует запустить утилиту **UPKeyInst.exe** и нажать кнопку Переустановить.



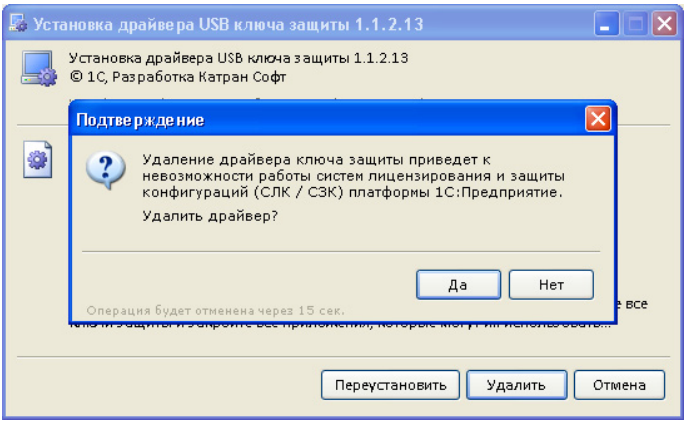
При завершении установки появляется сообщение об этом.



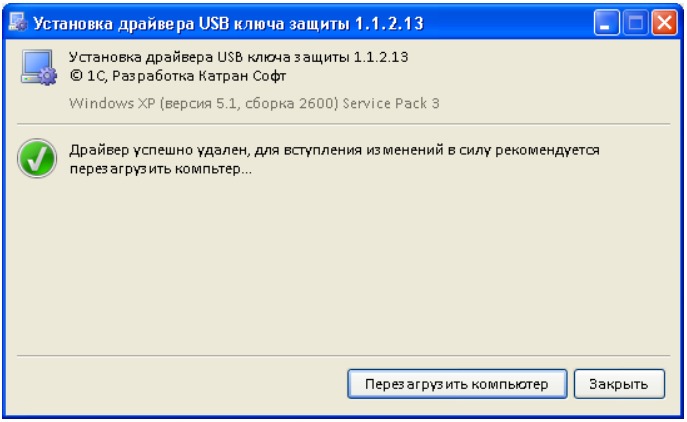
После этого следует подключить ключ. В том случае, если запустится Мастер установки нового оборудования Windows, следует выбрать пункт Автоматическая установка
(*см.* раздел «Подключение ключа защиты» на стр. 38).

Удаление драйвера

Для удаления драйвера ключа защиты следует запустить утилиту **UPKeyInst.exe** и нажать кнопку Удалить. Программа попросит подтвердить удаление.



При завершении установки появляется сообщение об этом.

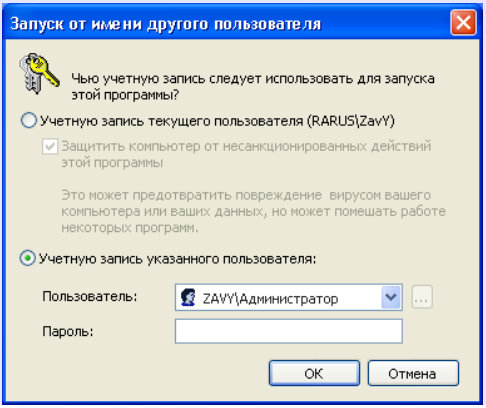


2.4.5 *Первый запуск Типового решения*

Первый запуск Типового решения, так же как и установка системы защиты (*см.* главу 2.4.3, «Установка системы защиты» на стр. 33), должен производиться пользователем, обладающим администраторскими правами в операционной системе. Это необходимо для регистрации Типового решения в системе.

Если первый запуск происходит в операционной системе Windows Vista или Windows 7 (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.

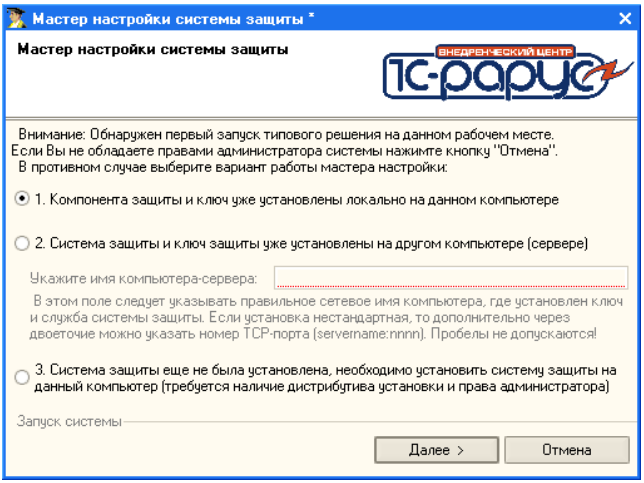
При обновлении Типового решения на новую версию также может потребоваться наличие у пользователя прав администратора.

Дальнейшие действия при первом запуске решения различаются для локального и сетевого вариантов работы.

Локальный вариант работы

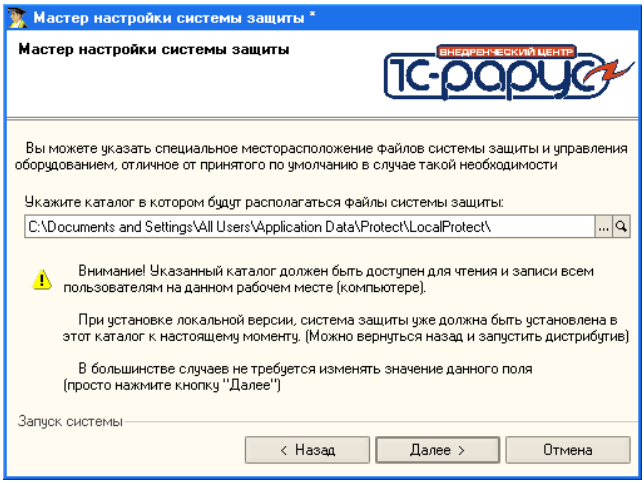
В локальном варианте работы решение устанавливается и работает на одном компьютере. Ключ защиты подключается к этому же компьютеру.

При первом запуске Типового решения появляется экран настройки системы защиты.



На этом экране необходимо выбрать первый вариант: Компонента защиты и ключ уже установлены локально на данном компьютере. Выбрав этот вариант, нажимаем кнопку Далее.

После нажатия кнопки Далее мастер предложит указать локальный каталог – каталог, в котором будут располагаться файлы системы защиты.



По умолчанию локальный каталог размещается в следующем месте: %CommonAppDATA%\Protect\LocalProtect.

Локальный каталог должен быть доступен для записи и чтения для всех пользователей данного компьютера.

После нажатия кнопки Далее система проверит правильность установленного ключа защиты и, если проверка прошла успешно, загрузит Типовое решение.

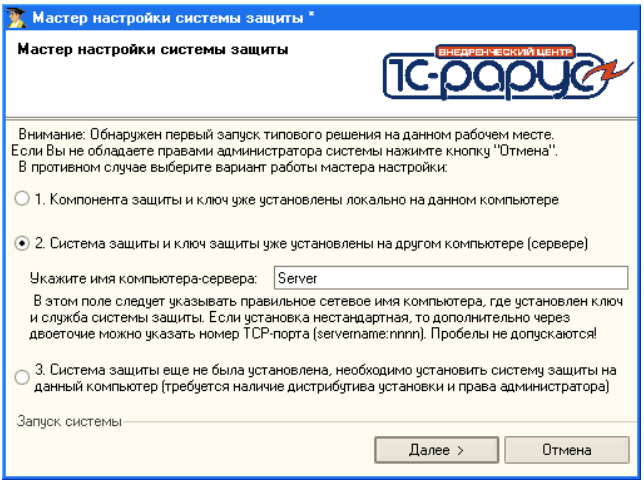
Сетевой вариант работы

В сетевом варианте несколько пользователей решения работают в общей сети. При этом используется единый общий сервер защиты – один из компьютеров сети, на котором устанавливается система защиты и к которому подключается ключ защиты. Все остальные компьютеры сети подключаются к этому серверу защиты. Сервер защиты работает по протоколу TCP/IP и устанавливается по умолчанию на порт 11999.

Следует убедиться, что порт сервера защиты не блокируется файрволом.

На каждом компьютере сети при первом запуске Типового решения автоматически создается локальный каталог, аналогично локальному варианту установки. 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.

При первом запуске Типового решения появляется экран настройки системы защиты.



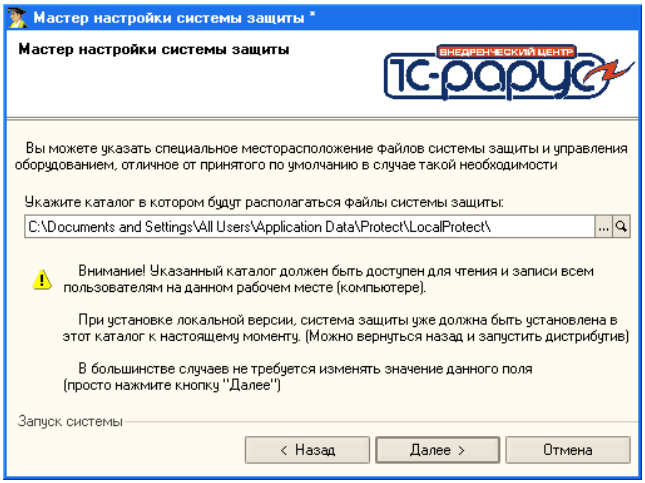
На этом экране необходимо выбрать второй вариант: Система защиты и ключ уже установлены на другом компьютере (сервере).

Этот вариант следует выбирать при работе в сетевом режиме независимо от того, на каком именно компьютере осуществляется данный запуск решения: на том, к которому подключен ключ защиты, или на одном из остальных компьютеров сети.

Система требует введения сетевого имени компьютера-сервера, к которому подключен ключ защиты*. Введя это имя, следует нажать кнопку Далее.

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

После нажатия кнопки Далее мастер предложит указать локальный каталог, в котором будут располагаться файлы системы защиты.



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

2.4.6 *Управление сервером защиты*

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

Если на компьютере установлена операционная система Windows XP или Windows Server 2003 и сервер защиты работает, 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 2.4.9, «Web-сервер состояния сервера защиты» на стр. 52.

Если на компьютере установлена операционная система Windows 2000, Windows Server 2008, Windows Vista или Windows 7, 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».

2.4.7 *Ключи защиты*

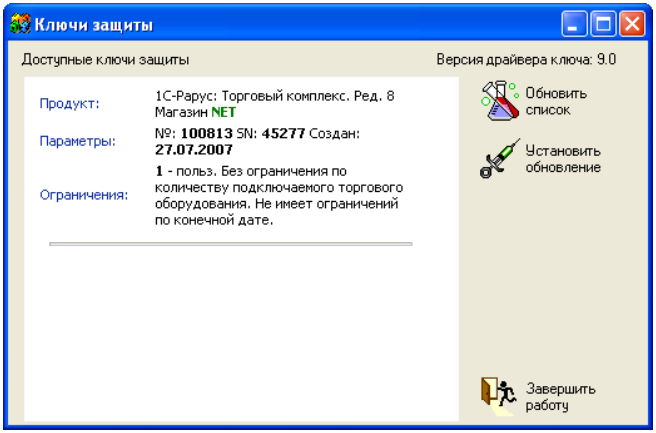
После установки системы защиты в панели управления появляется значок, соответствующий программе управления ключами защиты: Ключи защиты.

Для 32-битных операционных систем данный значок размещается непосредственно в панели управления, а для 64-битных – в группе View x86 Control Panel Icons.

Программа управления ключами защиты позволяет проверить правильность установки ключей на текущем компьютере. Кроме того, она дает возможность установки обновлений (например, при покупке дополнительных лицензий на работу Типовых решений).

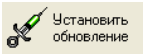
Точный путь к Панели управления зависит от версии Windows. Например, для того чтобы открыть Панель управления в Windows XP или Windows 7, следует выбрать Пуск –> Панель управления.

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. **2-3**.



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

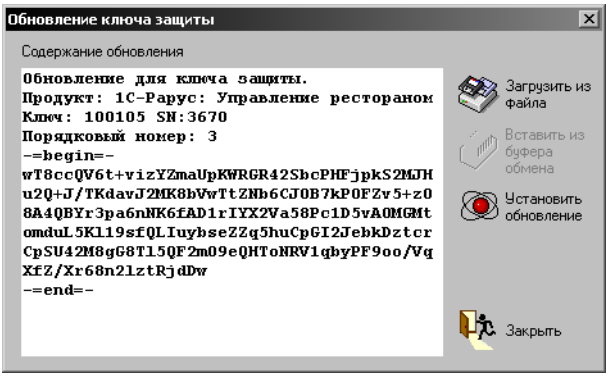
Таблица 2-3. **Ключи защиты 1С-Рарус, кнопки**

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.

Обновление можно использовать только для того ключа, для которого оно выписано. Каждое обновление можно установить только один раз, после чего можно будет установить обновление с бо́льшим 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.



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).

Как правило, для обновления ключа следует произвести следующие действия:

1. нажать кнопку Загрузить из файла, после чего выбрать файл для загрузки обновления (обычно файл обновления имеет название Update.kUpd);
2. нажать кнопку Установить обновление.

Кнопки, которые управляют работой программы, более подробно рассмотрены в табл. **2-4**.

Таблица 2-4. **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.
Закрыть	Закрывает диалоговое окно.

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

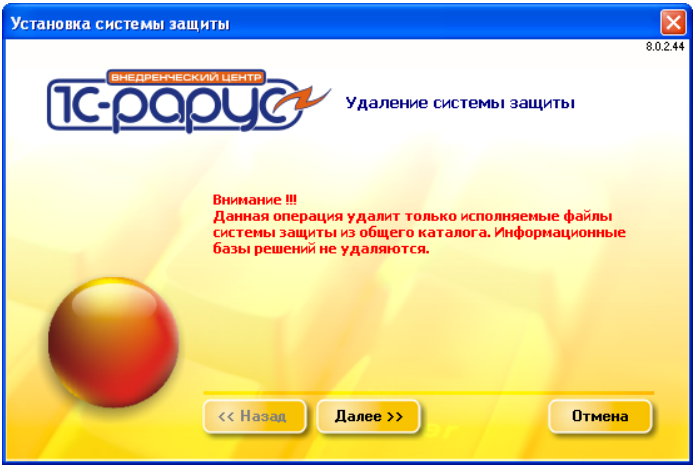
2.4.8 *Удаление системы защиты*

Для удаления системы защиты следует открыть Панель управления. Точный путь к Панели управления зависит от версии Windows. Например, для того чтобы открыть Панель управления в Windows XP или Windows 7, следует выбрать Пуск –> Панель управления.

В Панели управления следует выбрать пункт Установка и удаление программ или (для Windows Vista либо Windows 7) Программы и компоненты. Откроется список всех установленных программ.

В этом списке следует выбрать 1С-Рарус: Система защиты и сервер управления оборудованием –> Заменить/Удалить.

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

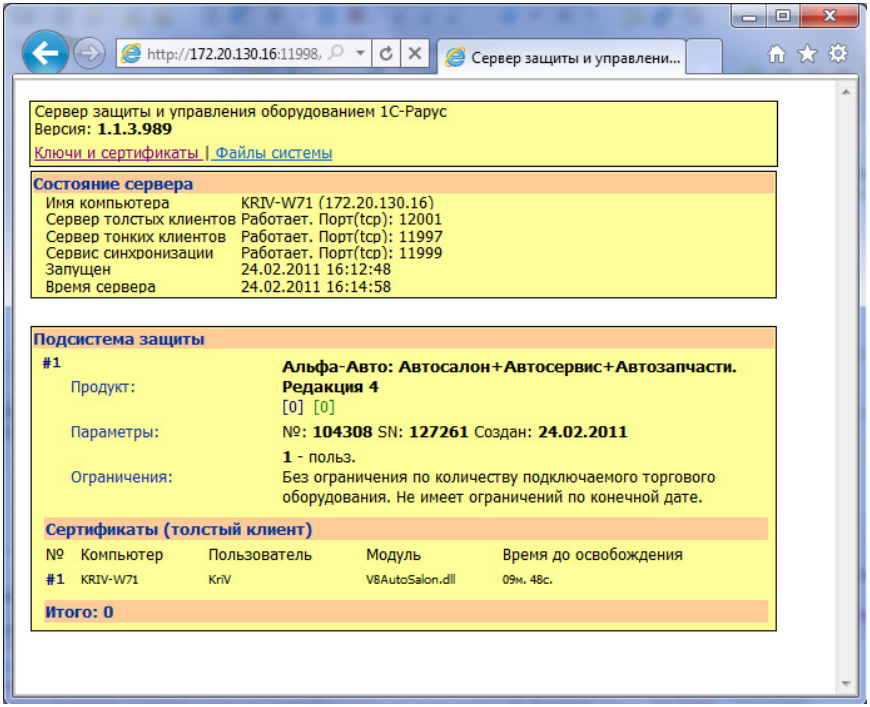


2.4.9 *Web-сервер состояния сервера защиты*

Для более детального контроля ключей и лицензий на сервере защиты предусмотрен web-сервер, который отображает текущее состояние 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 информации о сервере защиты и ключах нужно открыть в браузере адрес http://<IP адрес или имя сервера защиты>:11998, как показано на рисунке.



Web-отчет состоит из секций, рассмотренных в табл. **2-5**.

Таблица 2-5. **Web-отчет**

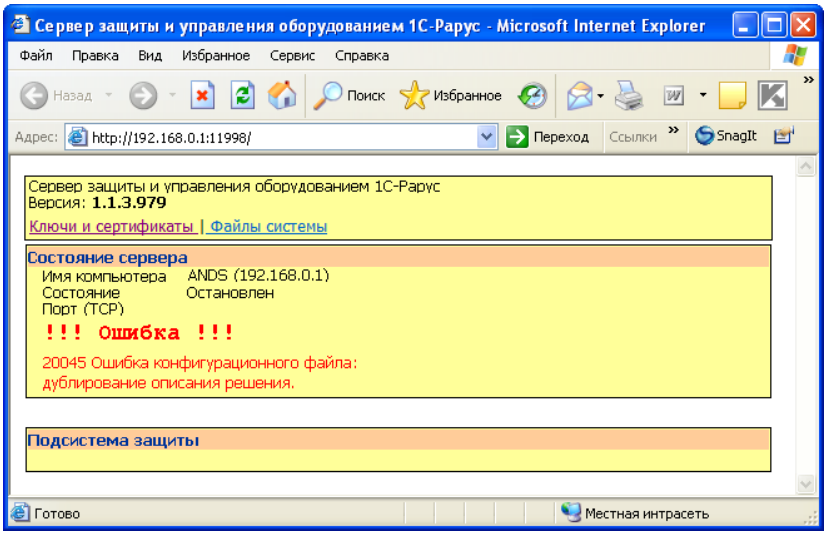
Графа	*Содержимое*
Заголовок	Содержит параметр Версия, в котором отображается версия запущенного сервера защиты.
Состояние сервера	
Имя компьютера	Сетевое имя (IP-адрес) компьютера, на котором запущен сервер защиты.
Состояние	Состояние сервера защиты.
Порт (TCP)	Порт сервера защиты.
Сервис синхронизации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

Таблица 2-5. **Web-отчет** (продолжение)

Графа	*Содержимое*
Время сервера	Текущие дата и время сервера защиты.
Подсистема защиты	
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.
Сертификаты	
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	
Идентификатор	Уникальный идентификатор лицензии сессии подключения оборудования (GUID).
Оборудование	Имя экземпляра оборудования, на который выписана лицензия.
Лицензий	Требуемое количество лицензий для данного экземпляра оборудования.
Итого	
Сертификатов	Реально выданное количество сертификатов.
Лицензий	Реально выписанное количество лицензий.

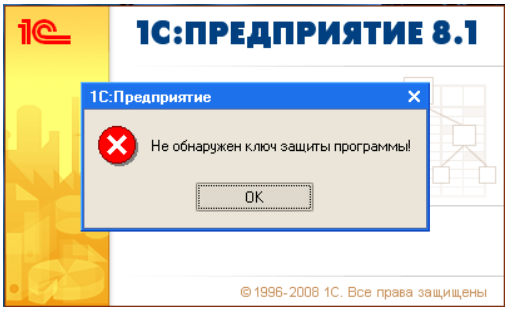
Кроме того, web-отчет предоставляет сведения об ошибках, возникающих при запуске и при работе системы защиты. При этом в секцию Состояние сервера выводится слово Ошибка, а также код,

наименование и описание возникшей ошибки, которые могут потребоваться при обращении в службу технической поддержки.



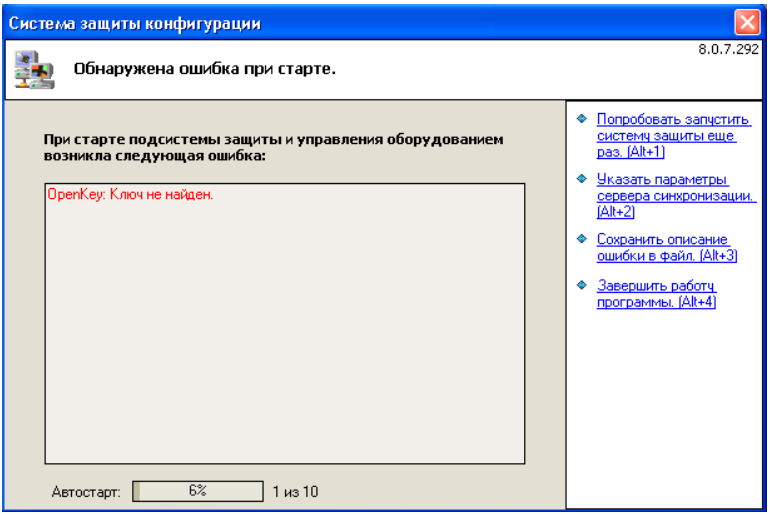
2.4.10 *Часто задаваемые вопросы*

1. При старте программы выдается сообщение:



Данное сообщение появляется в том случае, если система не может найти платформенный ключ. Для решения данной проблемы необходимо обратиться в фирму 1С.

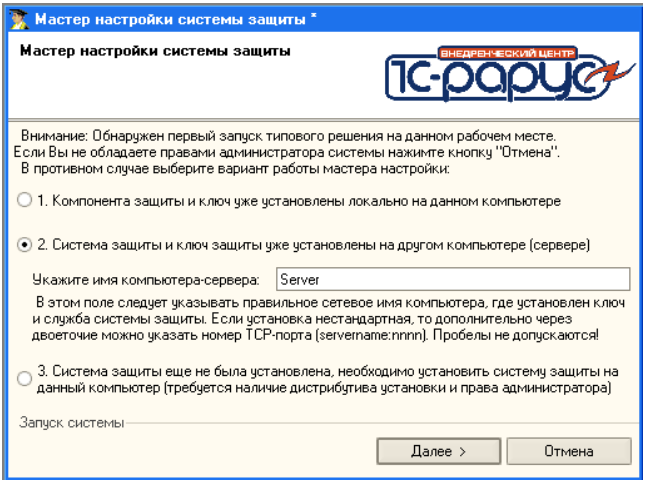
2. При старте системы защиты появляется сообщение:



Данная ошибка может появиться в следующих двух случаях.

☞ Установлена сетевая система защиты, но при первом старте защиты был выбран локальный вариант работы ключа.

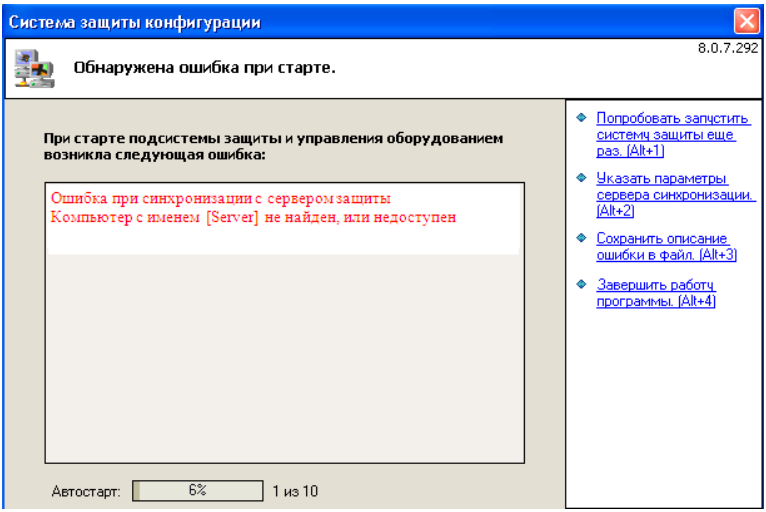
В данном случае необходимо нажать на гиперссылку Указать параметры сервера синхронизации и прописать имя компьютера сервера.



☞ Драйвер ключа защиты некорректно установился.

В данном случае необходимо переустановить драйвер. Для этого в папке установочного диска **Drivers** следует запустить **UPKeyInst.exe**. С помощью данной утилиты сначала необходимо удалить драйвер, затем установить. Работа этой утилиты описана выше: *см.* раздел 2.4.4, «Установка и удаление драйвера ключа защиты» на стр. 40.

3. При запуске программы появляется следующая ошибка.



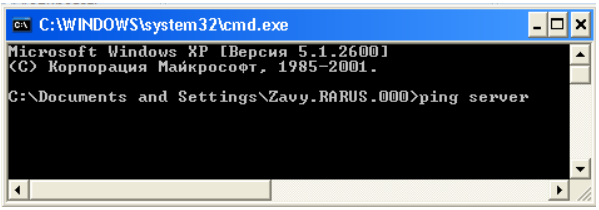
Данная ошибка может появиться в нескольких случаях.

☞ Неверно указано имя компьютера сервера.

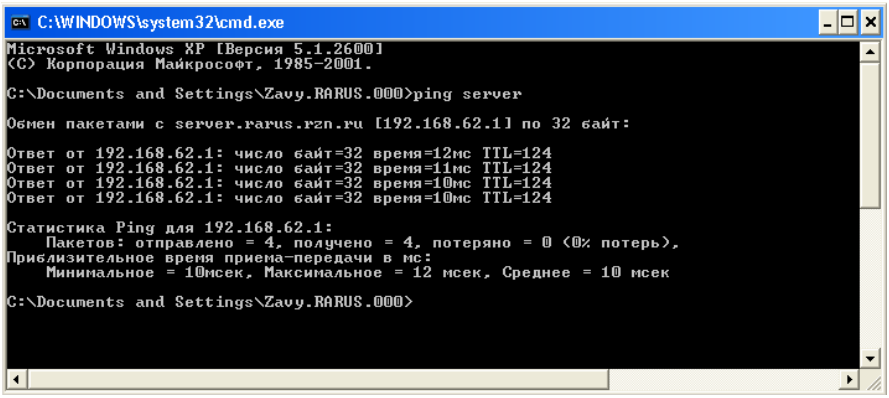
Необходимо проверить правильность написания имени сервера и при необходимости исправить это имя.

☞ Нет связи с сервером.

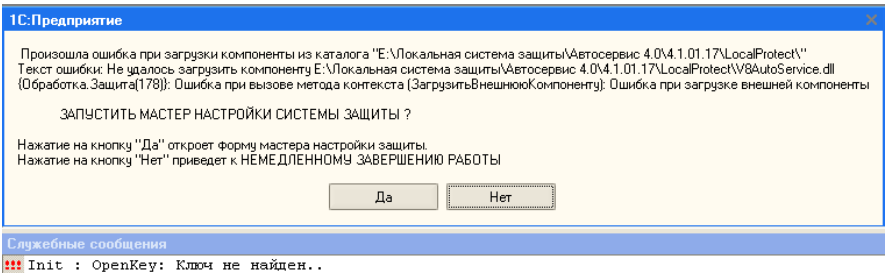
Необходимо проверить связь с сервером. Для это следует запустить Командную строку и проверить, проходит ли ping по **имени** компьютера сервера.



Ping должен выполниться успешно.



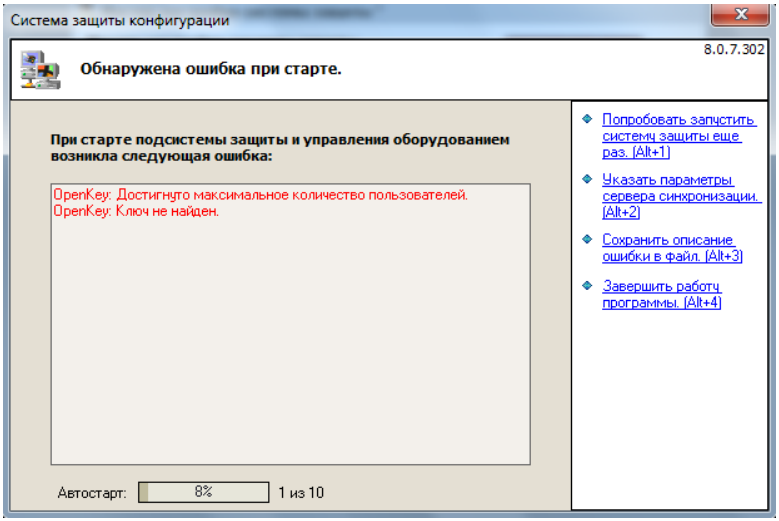
4. При старте системы защиты конфигурации появляется подобное сообщение.



В этом случае необходимо обратить особое внимание на текст в области служебных сообщений.

Обычно в служебных сообщениях содержится описание, почему произошла данная ошибка. Например, на иллюстрации в области служебных сообщений содержится сообщение «Ключ не найден».

5. При запуске программы появляется следующая ошибка.



Данная ошибка появляется, когда достигнуто максимальное количество лицензий ключа.

Для более детального контроля ключей и лицензий на сервере защиты предусмотрен web-сервер (*см.* раздел 2.4.9, «Web-сервер состояния сервера защиты» на стр. 52). Для получения статистики нужно обратиться при помощи программы Internet Explorer (или другого обозревателя web-страниц) на адрес http://<IP адрес или имя компьютера, на котором запущен сервер защиты>:11998.