Цифровая фотограмметрическая система

PHOTOMOD

Версия 8.1

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Ключ защиты Guardant (Windows x64)

РАКУРС

Оглавление

1. Ключ защиты Guardant

1.1. Локальный ключ защиты

В комплект поставки системы входит *уникальный ключ* аппаратной защиты *Guardant*, который предназначен для защиты системы и данных от копирования, нелегального использования и несанкционированного распространения.

Драйверы ключа аппаратной защиты устанавливаются автоматически в процессе установки программ семейства *PHOTOMOD*.

Так же при установке *PHOTOMOD* в папку системы автоматически копируется файл `PhConsts50.dll`, который необходим для корректной работы системы и является файлом ключа аппаратной защиты *Guardant*.

Если ключ аппаратной защиты *Guardant*, его драйверы и/или файл `PhConsts50.dll` не найдены ни локально, ни по сети, то выдается сообщение об ошибке системы защиты:

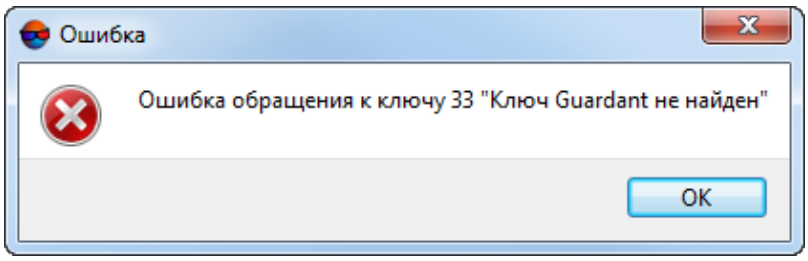


Рис. 1. Информационное сообщение

При возникновении проблем с файлом `PhConsts50.dll` скопируйте его вручную с установочного диска или обратитесь в службу технической поддержки компании «Ракурс» для получения файла лицензии. После получения файла лицензии скопируйте его в папку программных файлов системы (например, по умолчанию *C:\Program Files\PHOTOMOD_8_x64* для ЦФС *PHOTOMOD*).

Файл `PhConsts50.dll` *не* используется программами *PHOTOMOD UAS* и *PHOTOMOD AutoUAS*.

При возникновении проблем с установкой драйверов электронного ключа защиты установите драйверы вручную.

Для подключения ключа аппаратной защиты рекомендуется использовать USB-разъемы, расположенные в задней панели системного блока персонального компьютера.

В отличие фронтальных разъемов, расположенных на передней части системного блока (удобных с точки зрения доступа), разъемы на задней панели, как правило, напрямую подсоединены к материнской плате, что обеспечивает стабильное электропитание USB-устройств и максимальную скорость передачи данных.

1.1.1. Установка драйверов ключа защиты в ручном режиме

При возникновении проблем с установкой драйверов электронного ключа защиты установите драйверы вручную. Драйверы электронного ключа защиты можно скачать с официального сайта компании *Guardant*.

Пользователям ОС *Windows 10* и *Windows 11* перед началом установки драйверов ключа защиты *Guardant* необходимо убедиться, что не была активирована функция аппаратной защиты «стека» (Kernel-mode Hardware-enforced Stack Protection).

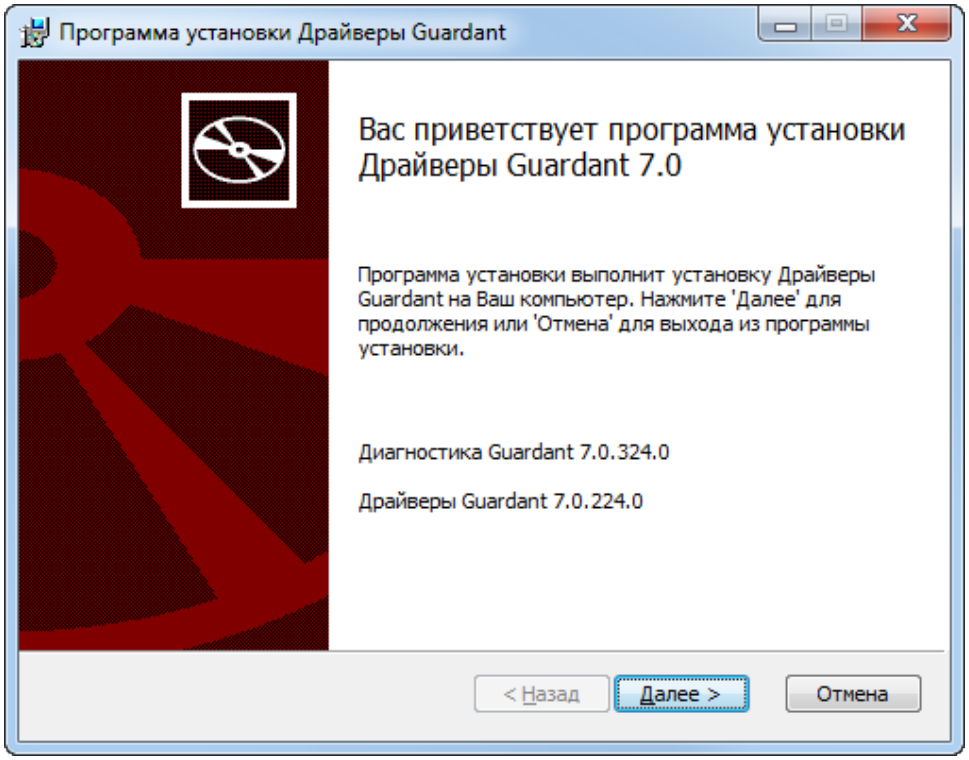
Аппаратная защита «стека» работает с процессорами *Intel* у которых есть функция Control-Flow Enforcement Technology (CET), а также с процессорами *AMD*, имеющими функцию Shadow Stack.

Следует учесть, что данная технология доступна только для пользователей *Pro* и *Enterprise* редакций *Windows*.

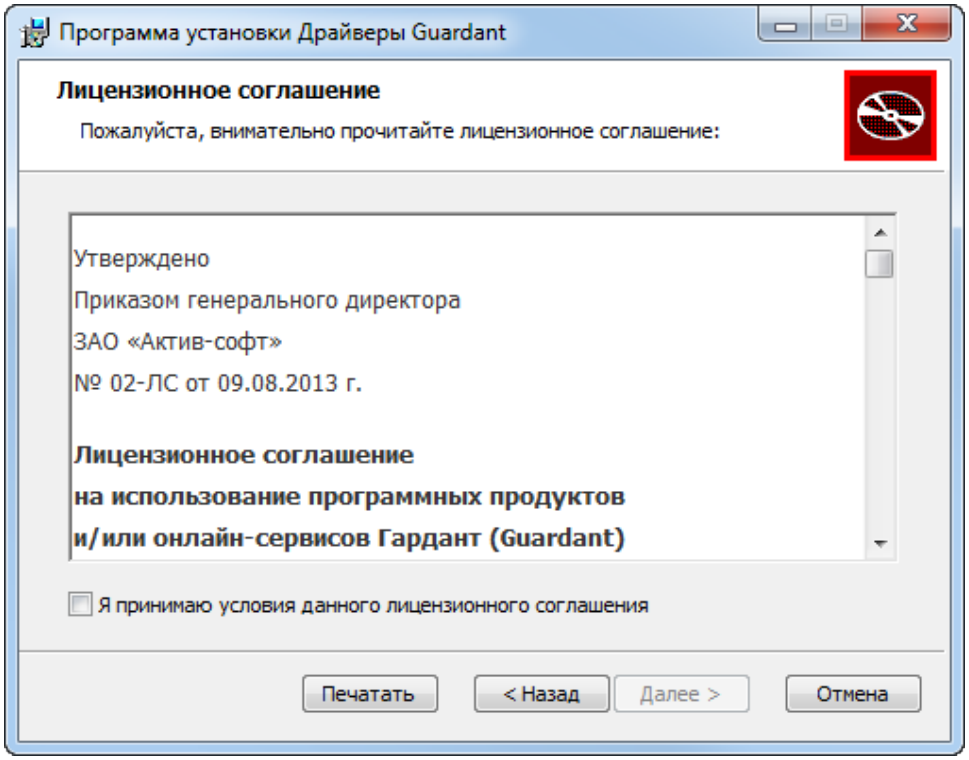
Пользователям ОС *Windows 7* и *Windows Server 2008 Release 2* (так же известна под названиями *Windows Server 2008 R2* или *Windows Server 7*) перед установкой драйверов ключа защиты *Guardant* требуется установить обновление операционной системы *KB4474419*.

Установите драйверы ключа защиты, для используемой Вами версии ОС *Windows*, с использованием настроек по умолчанию. Например, `GrdDrivers-x64.msi` (драйверы Guardant, MSI, x64) — драйверы для 64-разрядных редакций ОС *Windows*, начиная с *Windows XP*:

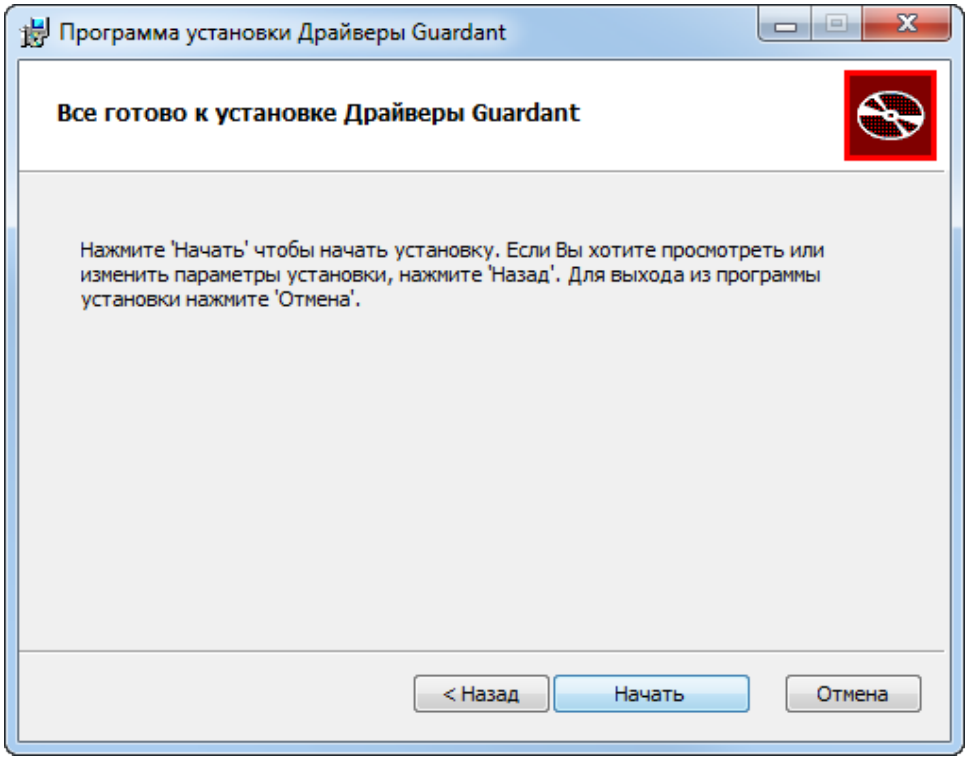
1. Прочтите приветствие и предупреждение. Нажмите на кнопку **Далее**:



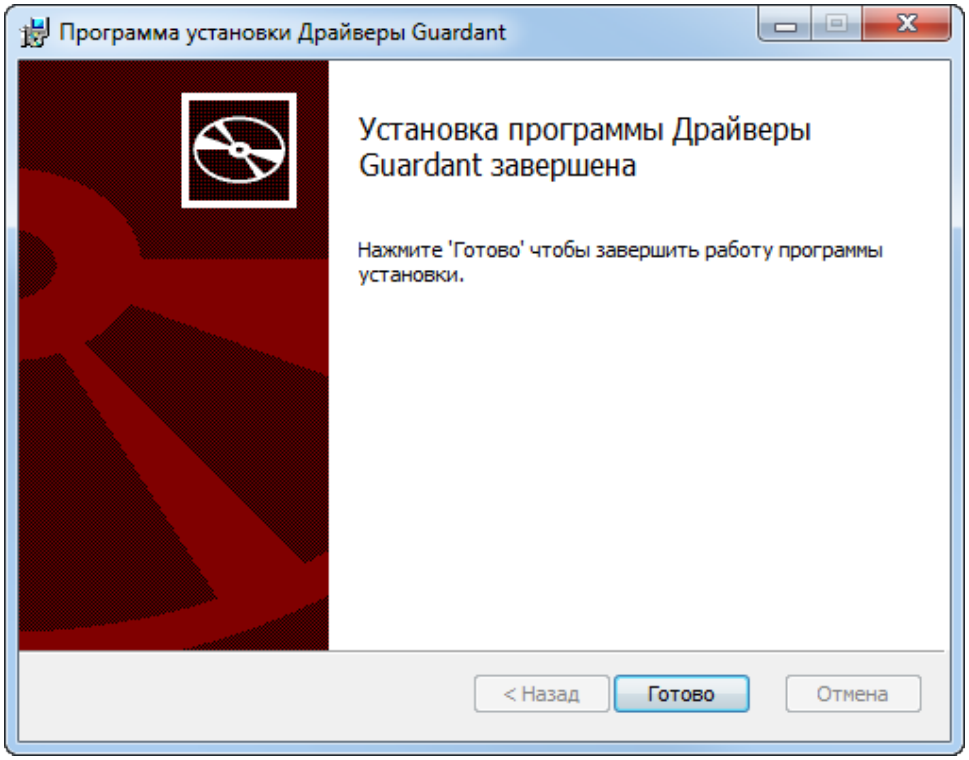
2. Прочтите лицензионное соглашение. Установите флажок **Я принимаю условия данного лицензионного соглашения** и нажмите на кнопку **Далее**:



3. Нажмите на кнопку **Начать**:



4. Дождитесь завершения операции:



5. Нажмите на кнопку **Установить**.

1.2. Сетевой ключ защиты

Сетевая версия ключа *Guardant* предназначена для защиты системы при помощи сетевых (плавающих) лицензий.

Плавающие лицензии представляют собой подход к лицензированию программного обеспечения, при котором ограниченное количество лицензий (рабочих мест) распределяется между количеством пользователей, большим чем число доступных лицензий.

Когда пользователь запрашивает лицензию у сервера лицензий, сервер разрешает запуск приложения при наличии свободной лицензии. При завершении работы приложения занятая им лицензия освобождается и может быть затребована другим пользователем.

Сервер лицензий может распределять лицензии внутри локальной сети (LAN), интранете, частной виртуальной сети (VPN) или же в интернете. *Плавающие лицензии* известны так же как *конкурирующие лицензии* или *сетевые лицензии* и часто используются корпоративными пользователями приложений.

Для работы с сетевой версией системы драйверы электронного ключа защиты должны быть установлены на каждую отдельную рабочую станцию. Сетевой ключ аппаратной защиты *Guardant* должен быть вставлен в USB-порт одной из рабочих станций, доступной для всех узлов сети.

Рекомендуется устанавливать ключ защиты на рабочую станцию, которая не используется для обработки проектов, записи CD/DVD и т. д.

Если на рабочей станции, на которую установлен ключ защиты, недостаточен объем памяти либо выполняются ресурсоемкие задачи, может возникнуть сбой в системе защиты или потеря данных.

При использовании нескольких ключей защиты в локальной сети процесс запуска модулей системы на отдельном компьютере может замедляться. Также существует вероятность отсутствия доступа к ключу защиты. В таких случаях рекомендуется изменить настройки защиты сетевого ключа.

Данная ситуация может возникнуть при использовании в одной локальной сети нескольких различных поставок *PHOTOMOD*.

Чтобы настроить доступ к нужному ключу защиты или ускорить процессы запуска модулей системы, выполните следующие действия:

Для настройки доступа к ключу защиты необходимо обладать правами администратора.

Описанную ниже последовательность действий необходимо выполнить на каждом *узле сети*, использование которого предполагается в обработке данных.

1. Создайте файл `PhConsts50.dll.host`. В любом текстовом редакторе запишите в него сетевое имя компьютера, в USB-разъеме которого находится нужный ключ защиты (например — `activator`);

2. Разместите файл `PhConsts50.dll.host` в программной папке системы (по умолчанию *C:\Program Files\PHOTOMOD_8_x64* для ЦФС *PHOTOMOD*).

   Операция с файлом `PhConsts50.dll.host` может быть выполнена для всех продуктов компании «Ракурс», включая *PHOTOMOD UAS* и *PHOTOMOD AutoUAS*.

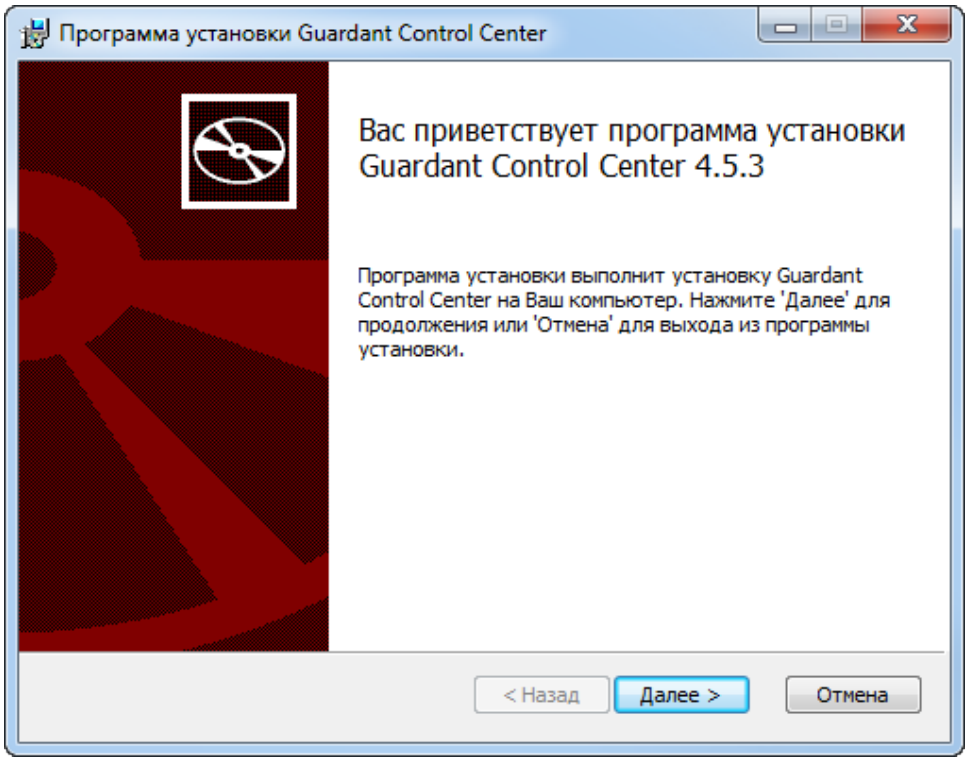
1.2.1. Программа Guardant control center

Программа *Guardant control center* является инструментом контроля подключений рабочих станций к ключам с лицензией.

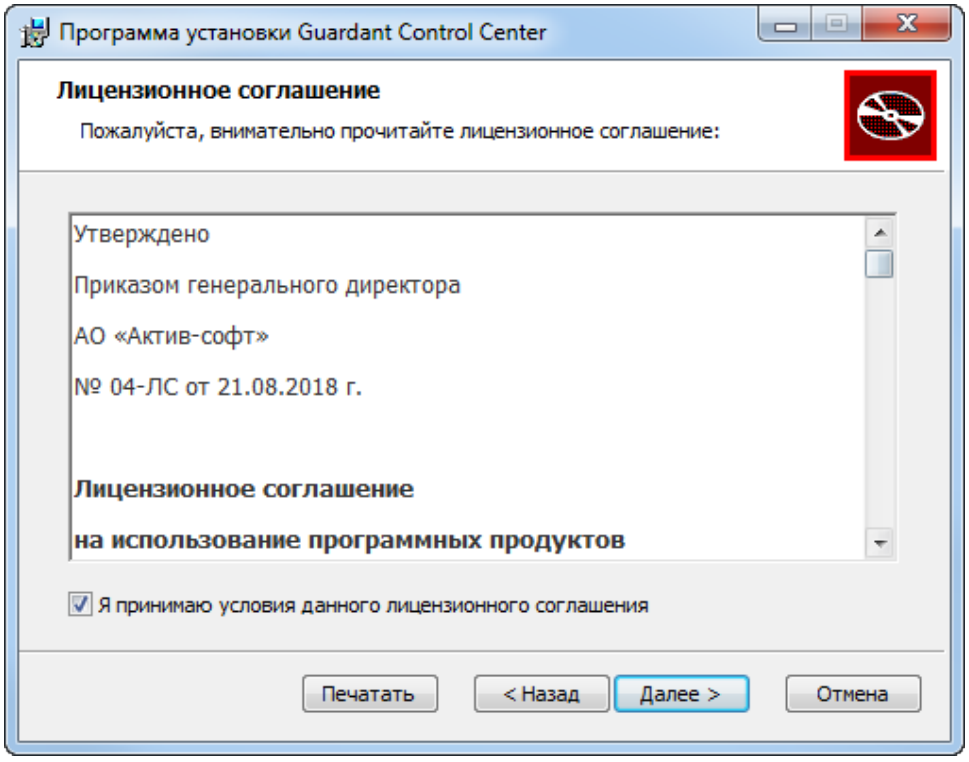
Для того чтобы воспользоваться им, этого откройте каталог *\redists* в папке программных файлов продукта компании «Ракурс» (например, по умолчанию *C:\Program Files\PHOTOMOD_8_x64\redists* для ЦФС *PHOTOMOD*).

Запустите файл `grdcontrol-N.N.N.msi`, где **N.N.N** — номер версии. Установите программу с использованием настроек по умолчанию:

1. Прочтите приветствие и предупреждение. Нажмите на кнопку **Далее**:

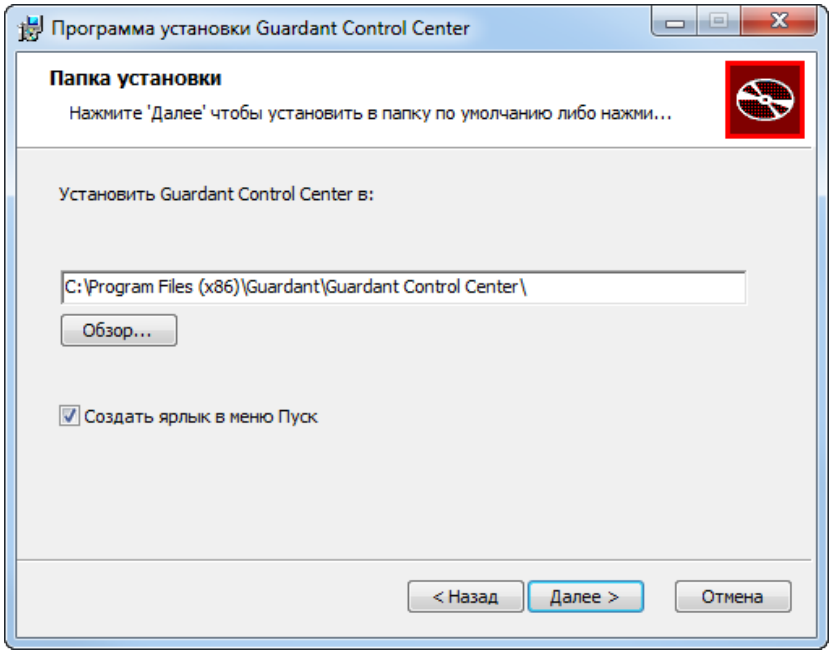


2. Прочтите лицензионное соглашение. Установите флажок **Я принимаю условия данного лицензионного соглашения** и нажмите на кнопку **Далее**:



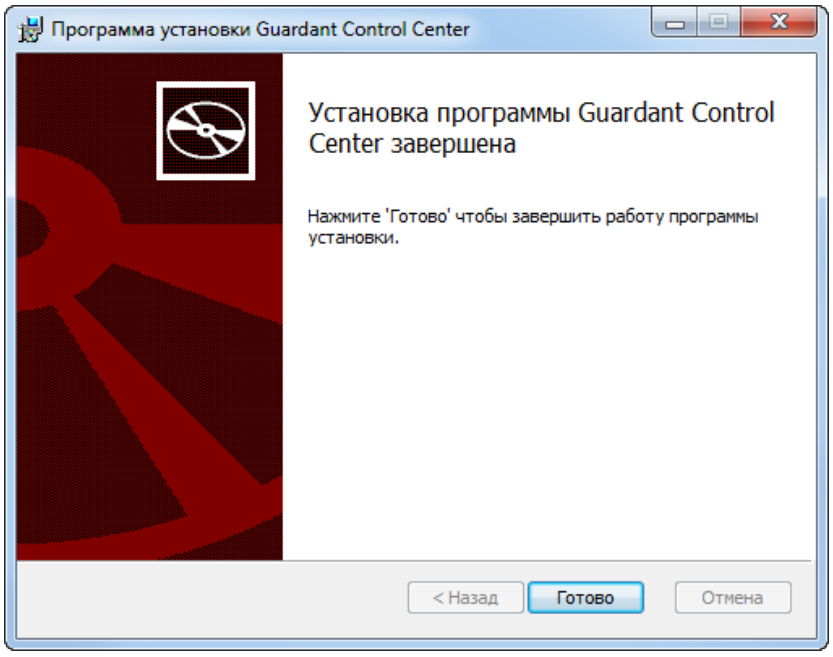
3. Выберите папку для размещения программных файлов. Нажмите на кнопку **Далее**.

Настоятельно не рекомендуется использовать для установки папку, в названии которой содержатся символы, отличные от латинских. По умолчанию для установки программны создается папка *C:\Program Files (x86)\Guardant\Guardant Control Center*.



4. Нажмите на кнопку **Начать**.

5. Дождитесь завершения процесса установки. Нажмите на кнопку **Готово**.



После завершения установки программы, на рабочем столе *Windows* появляется ярлык **Guardant control center**.

На компьютере с установленной программой *Guardant control center*, с ключом *Guardant* установленным в USB-разъем и установленными драйверами ключа защиты, данный ярлык открывает окно сервиса **Guardant control center**, в браузере, используемом по умолчанию (адрес в адресной строке: `http://localhost:3189/#/dongles/list`):

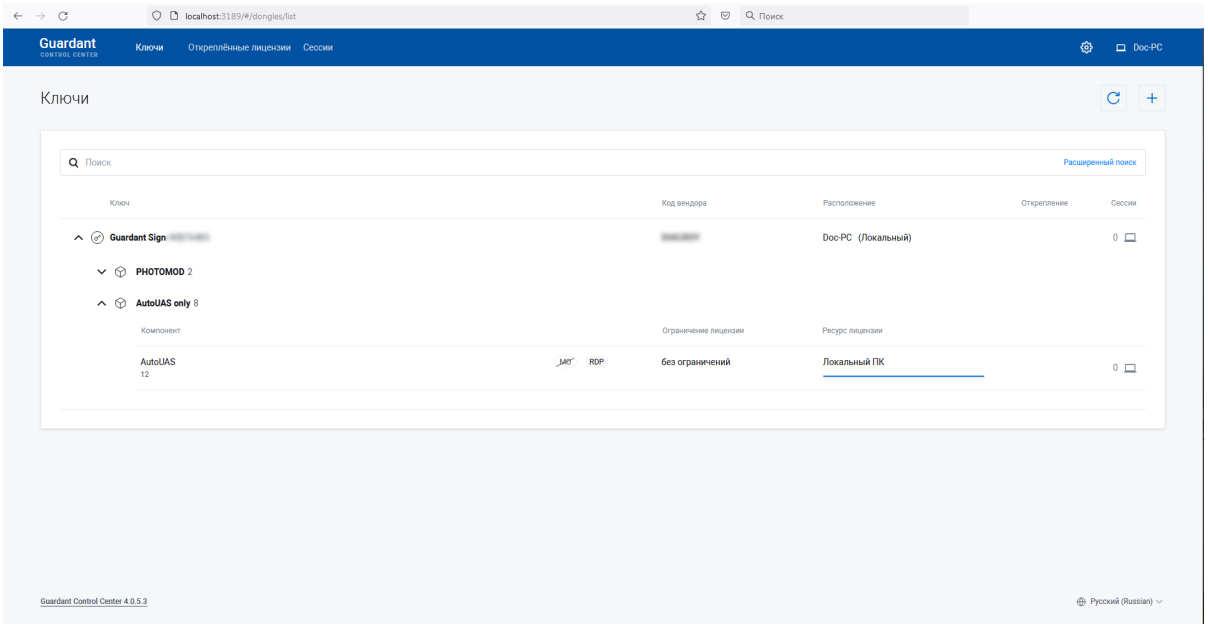


Рис. 2. Guardant control center (ключи, установленные на текущей рабочей станции)

В данном окне отображаются ключи, установленные в USB-разъем текущей рабочей станции. Для перехода к просмотру информации о сетевом ключе, используйте сетевое имя компьютера в USB-разъеме которого находится нужный ключ защиты (например, если имя такого компьютера — `activator`, то в адресной строке браузера нужно ввести `http://activator:3189/#/dongles/list`):

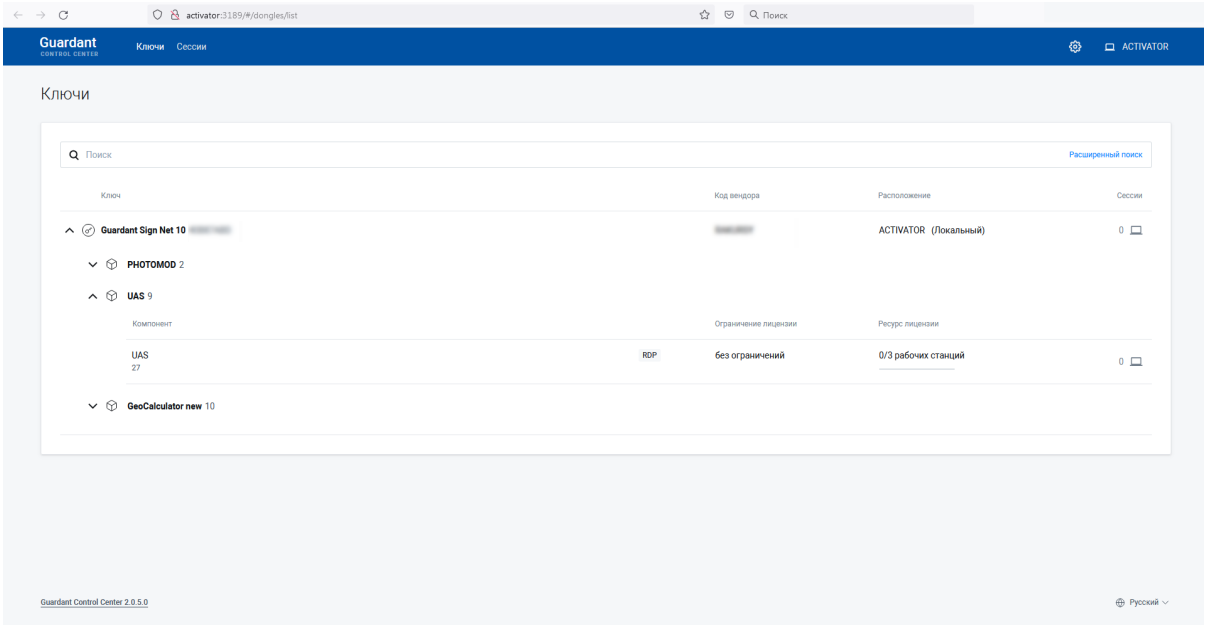


Рис. 3. Guardant control center (информация об используемом сетевом ключе)

Руководство пользователя *Guardant control center* доступно на сайте компании «Guardant».

2. Проверка информации о поставке

Для проверки соответствия ключа защиты и его файла выполните следующие действия:

1. Выберите **Информация о поставке** в контекстном меню служебного модуля *System Monitor* (значок в области уведомлений *Windows*). Запускается процесс проверки лицензий, после чего открывается окно **Информация о поставке PHOTOMOD**.

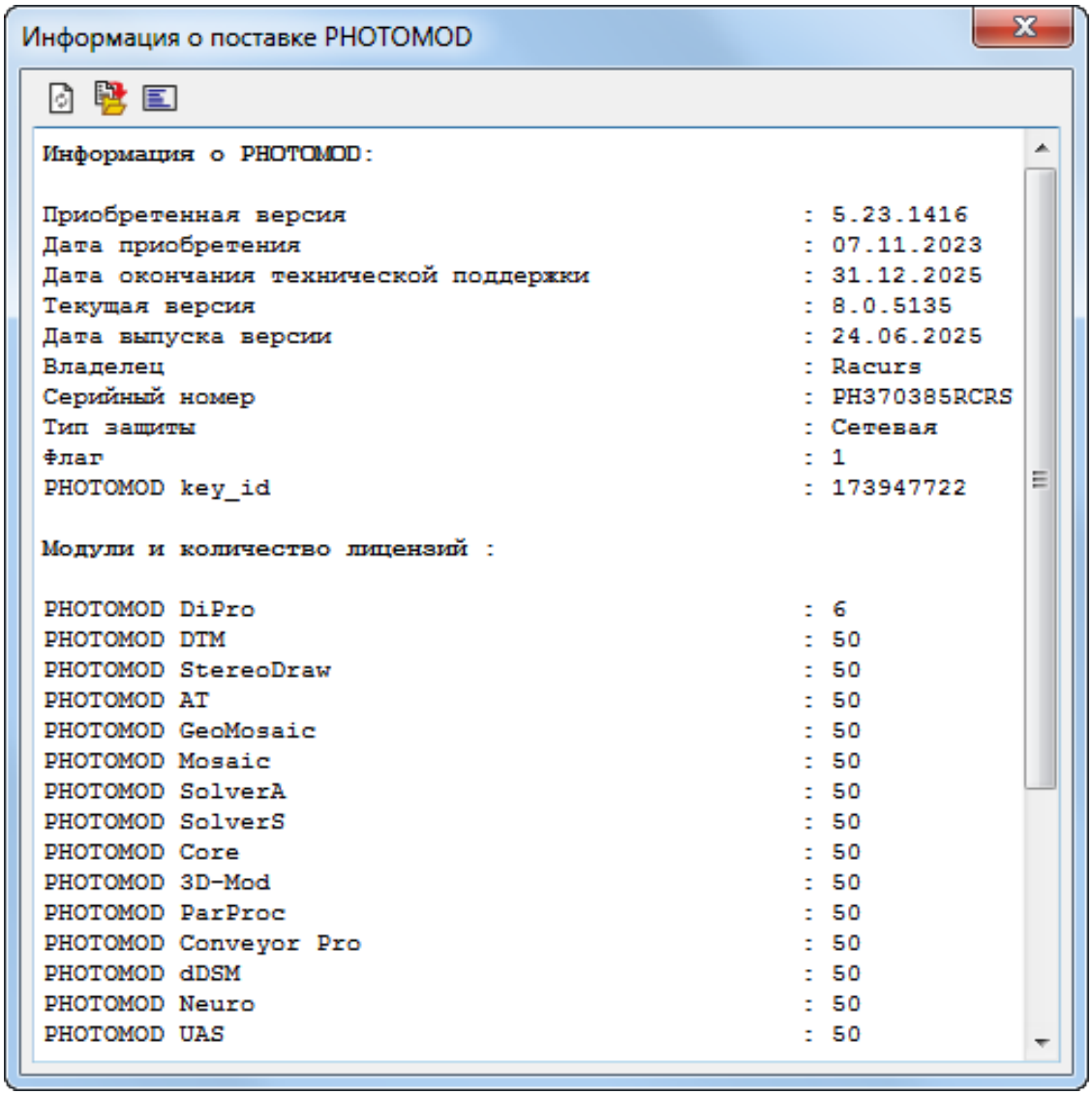


Рис. 4. Информация о поставке

2. Сравните уникальный номер ключа защиты в строке Серийный номер с номером на этикетке, которая наклеена на ключ защиты.

3. Нажмите на кнопку в панели инструментов окна. Дождитесь завершения выполнения операции.

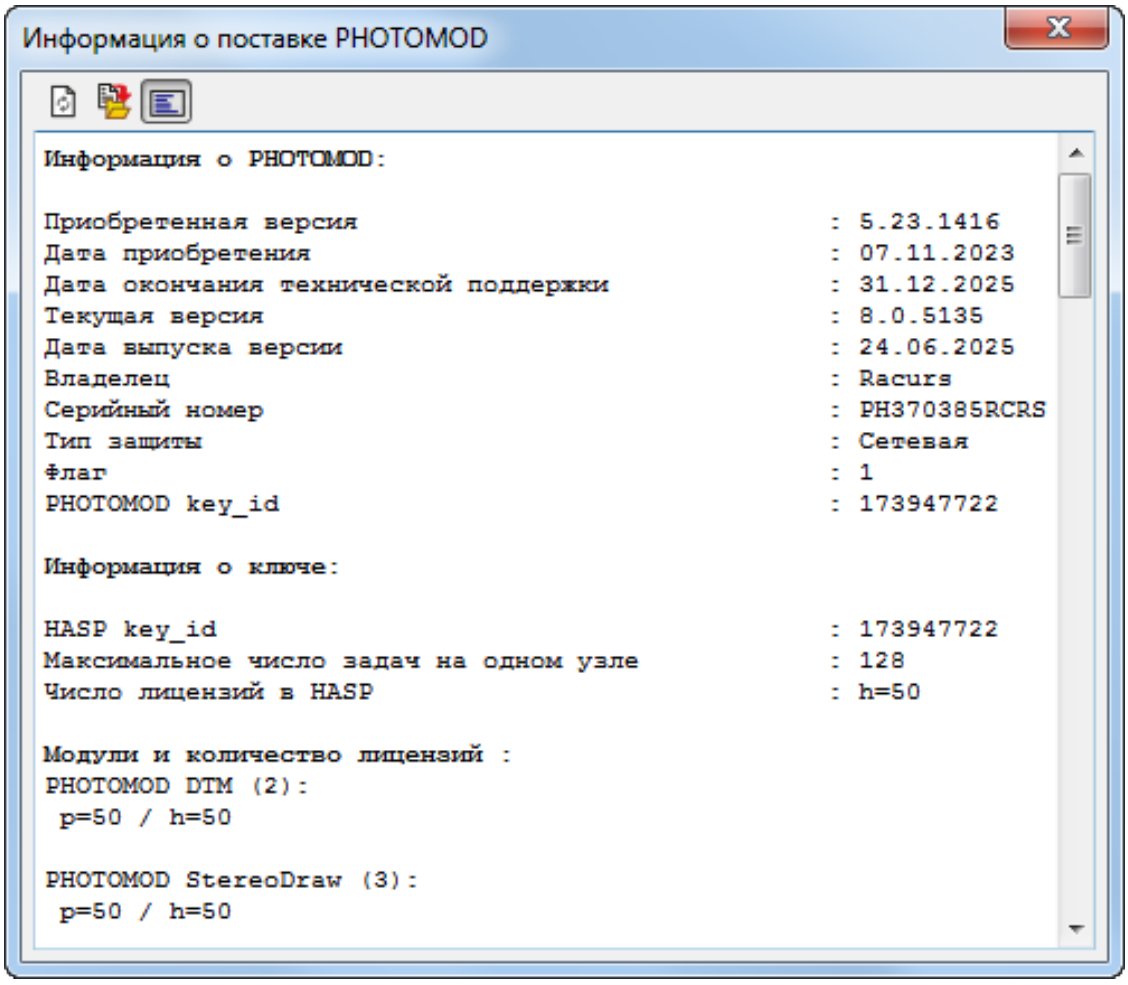


Рис. 5. Информация о поставке

Кнопка позволяет обновить содержимое окна.

Кнопка позволяет сохранить содержимое окна в файл с расширением `*.txt`.

4. Сравните количество лицензий на модули в каждой строке ниже названия модуля. Количество лицензий в ключе защиты и в файле ключа защиты должны совпадать.

h — количество лицензий в ключе защиты, *p* — количество лицензий в файле ключа защиты.

5. В случае несовпадения данных обратитесь в службу технической поддержки компании «Ракурс».