ГАЗИНФОРМ СЕРВИС

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4»

Руководство администратора безопасности
Часть 2. Развертывание и аудит

Санкт-Петербург, 2024

Аннотация

В документе содержатся сведения о подсистемах развертывания и сбора событий средства защиты информации от несанкционированного доступа «Блокхост-Сеть 4»:

– назначение подсистем и их основные функциональные возможности;
– описание интерфейса подсистем и основные принципы работы с ним.

Содержание

Введение

Подсистема развертывания предназначена для установки программного обеспечения, в том числе клиентской части СЗИ от НСД «Блокхост-Сеть 4» (далее по тексту – клиент Блокхост-Сеть) на рабочие станции.

Подсистема сбора событий аудита предназначена для сбора, просмотра и фильтрации событий аудита клиентских рабочих станций, формирования сводных отчетов с информацией о состоянии клиентов, подключенных к серверам иерархии.

Знаки, расположенные на полях руководства, указывают на примечания.

Степени важности примечаний:

Важная информация

Указания, требующие особого внимания.

Дополнительная информация

Указания, позволяющие упростить работу с подсистемой.

1 Назначение подсистем

Подсистема развертывания позволяет управлять процессом установки программного обеспечения (в частности, клиента Блокхост-Сеть) на рабочие станции в сети и осуществлять мониторинг рабочих станций. Подсистема развертывания автоматически устанавливается в процессе установки серверной части СЗИ от НСД «Блокхост-Сеть 4».

Процесс установки серверной части СЗИ подробно описан в документах «СЗИ от НСД «Блокхост-Сеть 4». Руководство по инсталляции в ОС Linux» и «СЗИ от НСД «Блокхост-Сеть 4». Руководство по инсталляции в ОС Windows».

Подсистема сбора событий аудита предназначена для сбора событий аудита с клиентских рабочих станций, формирования сводных отчетов с информацией о состоянии клиентов, подключенных к серверам иерархии, просмотра и фильтрации событий аудита, собранных с клиентских компьютеров на сервер, а также напрямую из журнала клиентского компьютера.

2 Подсистема развертывания

Основная работа с подсистемой развертывания осуществляется во вкладках ***Агенты***, ***Пакеты установки*** и ***Задачи***, доступных по кнопке .

Подсистема развертывания предназначается для управления процессом установки или удаления программного обеспечения, в том числе клиентов Блокхост-Сеть на рабочие станции (рисунок 2.1).

Вкладка ***Агенты*** предназначена для управления списком рабочих станций, на которых установлены агенты развертывания.

Вкладка ***Пакеты установки*** предназначена для управления созданными пакетами для инсталляции ПО.

Вкладка ***Задачи*** предназначена для управления задачами по установке инсталляционных пакетов на клиентские рабочие станции.

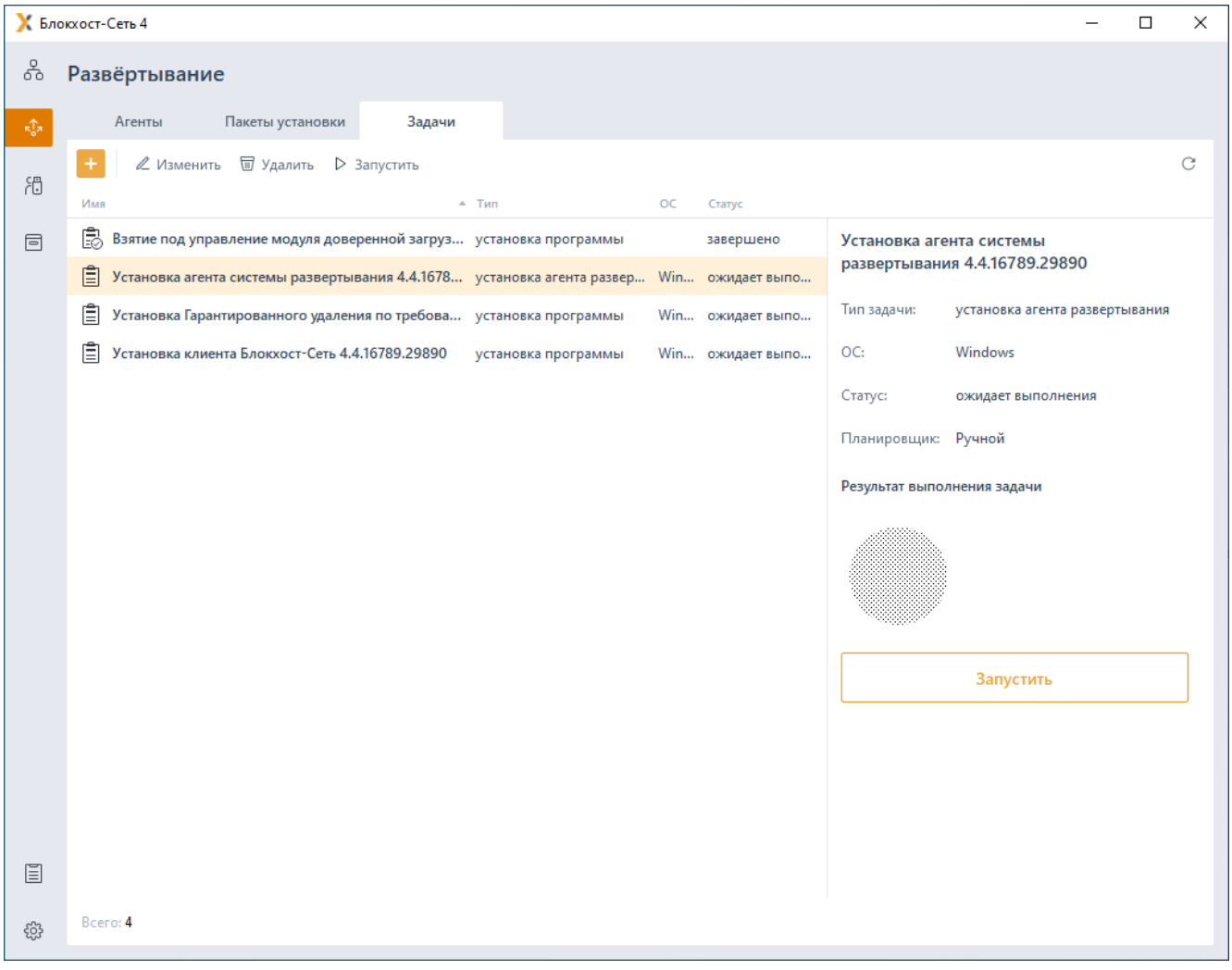


Рисунок 2.1 – Раздел «Развертывание»

При установке серверной части СЗИ во вкладке ***Задачи*** автоматически создаются

задачи (рисунок 2.1):

– взятие под управление средства доверенной загрузки «SafeNode System Loader»;

– на установку агента развертывания на клиентские рабочие станции;

– на установку клиента Блокхост-Сеть на клиентские рабочие станции;

– на установку гарантированного удаления по требованию на клиентские рабочие станции.

Необходимо учитывать, что предустановленные задачи создаются для той же ОС, под управлением которой находится сервер СЗИ, и выполнение предустановленных задач возможно только для клиентских рабочих станций, находящихся под управлением ОС, аналогичной ОС сервера.

Если необходимо выполнить установку агента развертывания, клиента Блокхост-Сеть или подсистему гарантированного удаления на клиентских рабочих станциях под управлением ОС, отличной от ОС сервера, требуется сформировать пакет установки под определенный инсталлятор и создать задачу на его установку на клиентских рабочих станциях.

Для настройки взаимодействия между сервером СЗИ и клиентскими рабочими станциями для управления и установки ПО с помощью консоли администрирования необходимо последовательно выполнить задачи на установку агента развертывания на требуемых клиентских рабочих станциях (подробное описание приведено в разделе ***«Установка агента подсистемы развертывания»***), и на установку клиента Блокхост-Сеть (подробное описание приведено в разделе ***«Установка клиента Блокхост-Сеть»***).

3 Установка агента подсистемы развертывания

Агент развертывания позволяет осуществлять взаимодействие между сервером СЗИ и клиентскими рабочими станциями для управления и установки ПО с помощью консоли администрирования.

Агент развертывания может быть установлен различными способами:

– с использованием функциональных возможностей подсистемы развертывания;

– локально вручную на клиентской рабочей станции (подробно установка агента подсистемы развертывания локально на рабочей станции описана в документах «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство по инсталляции в ОС Windows» и «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство по инсталляции в ОС Linux»);

– с использованием сторонних систем развертывания.

3.1 Установка агента развертывания с помощью подсистемы развертывания

3.1.1 Установка агента через предустановленную задачу

Для установки агента развертывания на рабочие станции перейдите во вкладку ***Задачи*** и внесите корректировки в параметры автоматически созданной задачи ***Установка агента системы развертывания <номер версии>***, открыв задачу на редактирование по кнопке Изменить в меню или с помощью контекстного меню (рисунок 3.1).

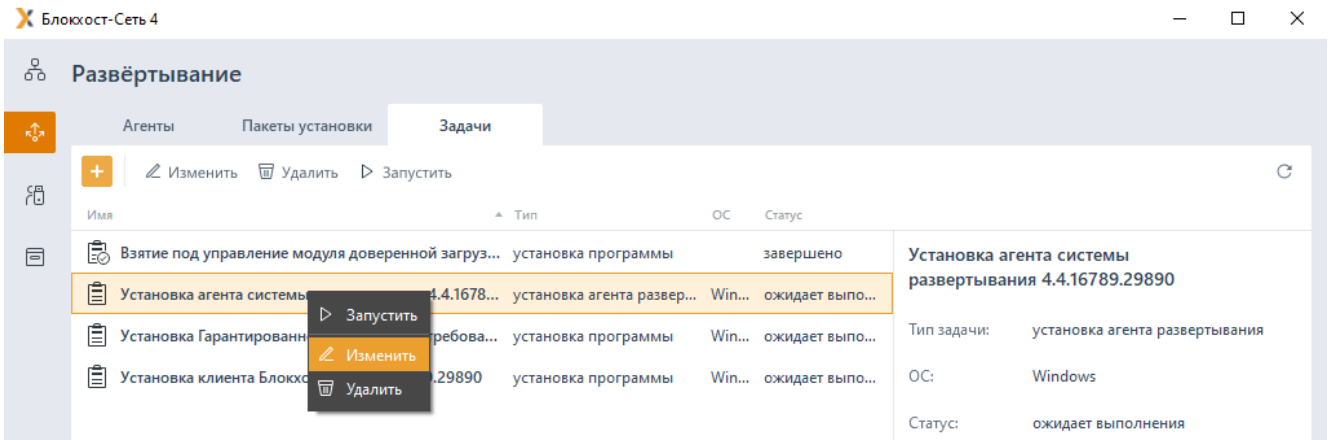


Рисунок 3.1 – Изменение автоматически созданной задачи на установку агента

3.1.1.1 Формирование списка рабочих станций для установки агента

В появившемся окне (рисунок 3.2) перейдите во вкладку ***Компьютеры*** (рисунок 3.3) и сформируйте список рабочих станций, на которые будет устанавливаться агент развертывания.

При добавлении клиентских рабочих станций в список задачи на установку необходимо учитывать, что для выбора будут доступны только клиентские рабочие станции под управлением ОС, аналогичной той ОС, для которой была создана задача.

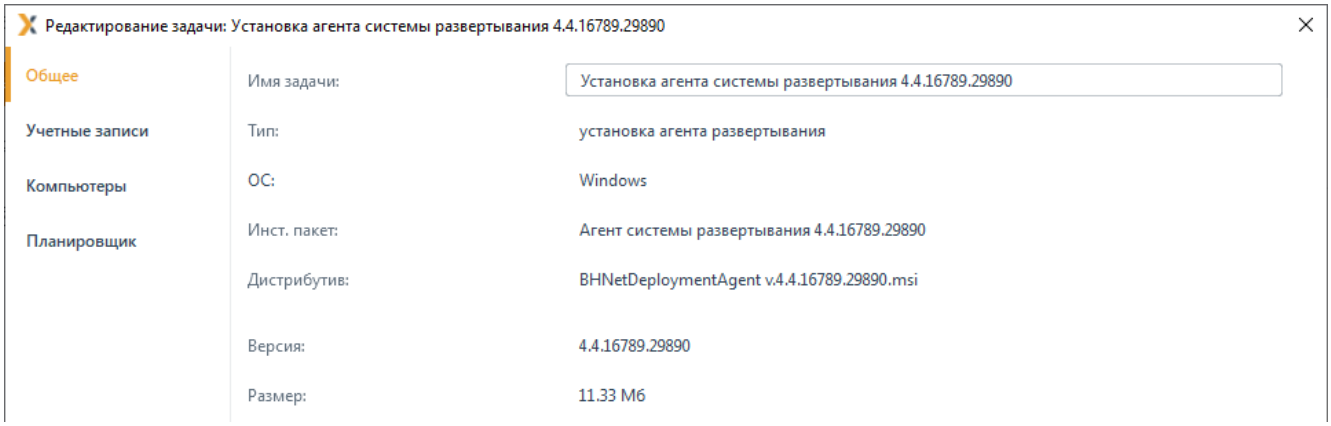


Рисунок 3.2 – Редактирование задачи на установку агента развертывания

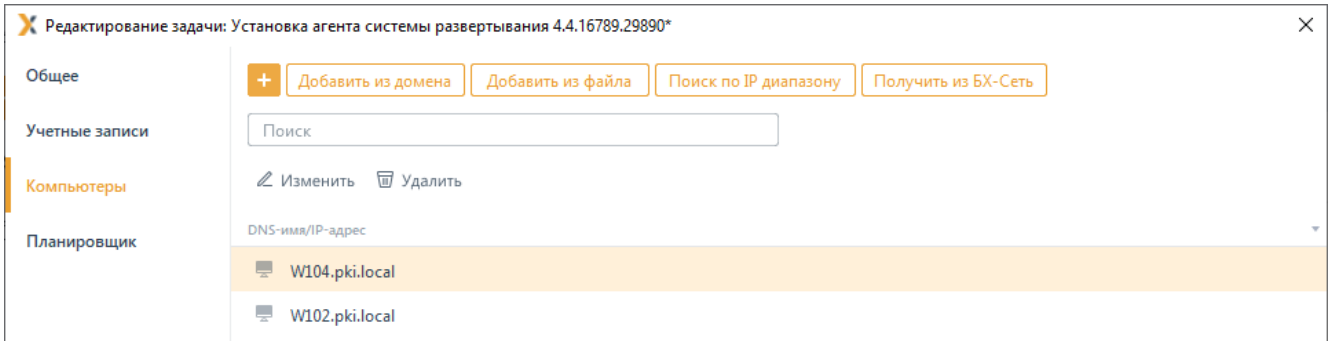


Рисунок 3.3 – Добавление рабочих станций в список установки агента развертывания

Добавление рабочих станций в список возможно несколькими способами:

1) По кнопке + – в открывшееся поле ввода ввести имя или IP-адрес рабочей станции и нажать клавишу <**Enter**> (рисунок 3.4 а).

2) По кнопке ***Добавить из домена*** – в открывшемся окне (рисунок 3.4 б) выбрать нужный домен или, при отсутствии необходимого домена в списке, добавить его по кнопке ⊕ Добавить домен, перейти в необходимый *Organization Unit* для выбора рабочих станций, на которые будет устанавливаться агент развертывания, и нажать кнопку ***Добавить***.

Домены подразделяются на:

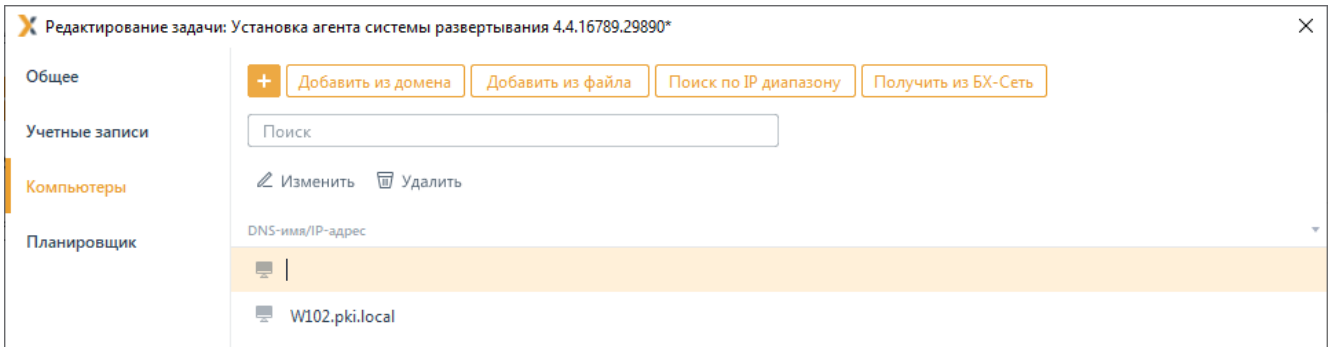
– *системные* домены, которые добавляются в список доменов автоматически. Подключение к системному домену (при раскрытии дерева или по двойному щелчку) происходит из-под текущей учетной записи или, в случае неудачи, запрашивается логин/пароль для подключения. Системный домен невозможно удалить из списка;

– *пользовательские* домены, которые добавляются по кнопке Добавить домен. При подключении к пользовательскому домену (при раскрытии дерева или по двойному щелчку) всегда запрашивается логин/пароль для подключения (попытка подключения из-под текущей учетной записи не выполняется). Пользовательский домен возможно удалить из списка.

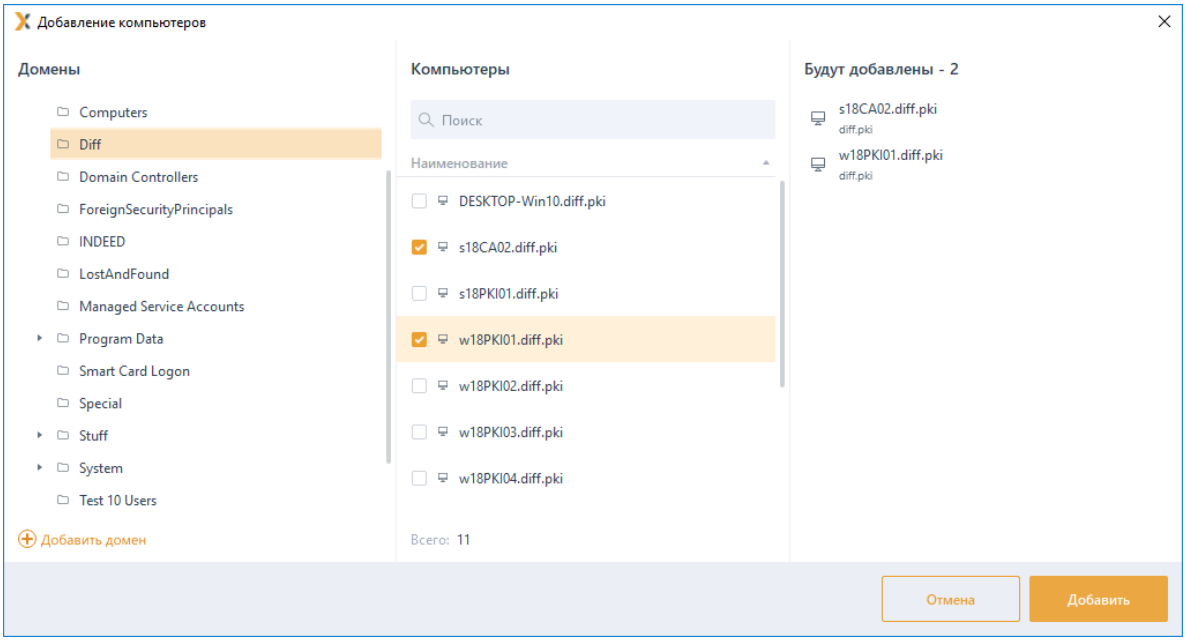
Администратор имеет возможность выполнить подключение/переподключение к домену под нужной ему учетной записью (ввести логин/пароль).

3) По кнопке ***Поиск по IP диапазону*** – в открывшемся окне (рисунок 3.4 в) для поиска IP-адресов в заданном диапазоне ввести начальный и конечный IP-адреса в соответствующие поля и нажать кнопку ***Найти***, после чего выбрать из списка рабочие станции, на которые будет устанавливаться агент развертывания, и нажать кнопку ***Добавить***.

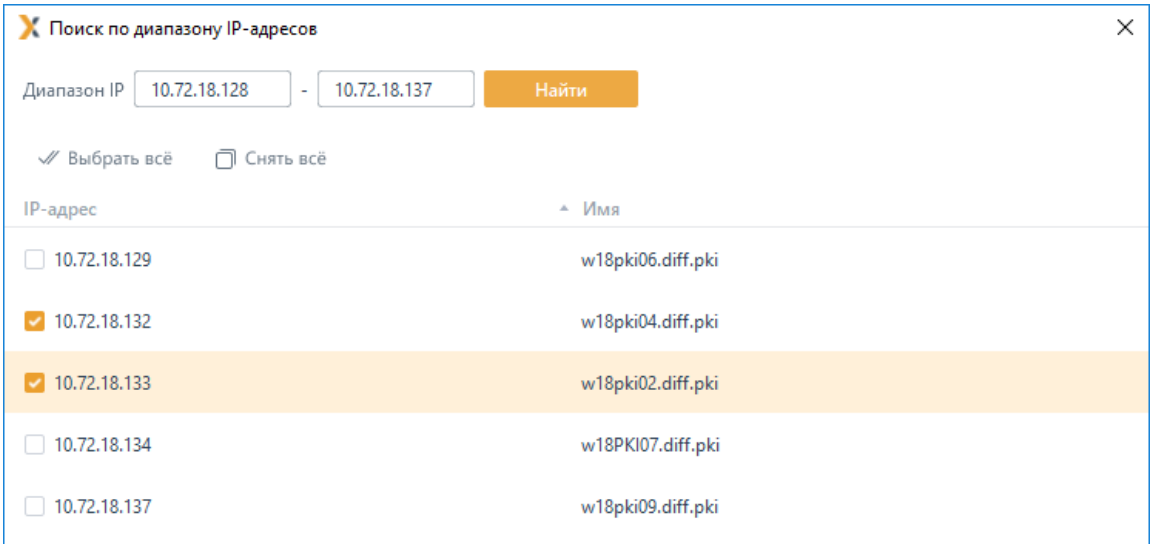
4) По кнопке ***Получить из БХ-Сеть*** – будет сформирован список клиентов Блокхост-Сеть, зарегистрированных на сервере СЗИ (рисунок 3.4 г).



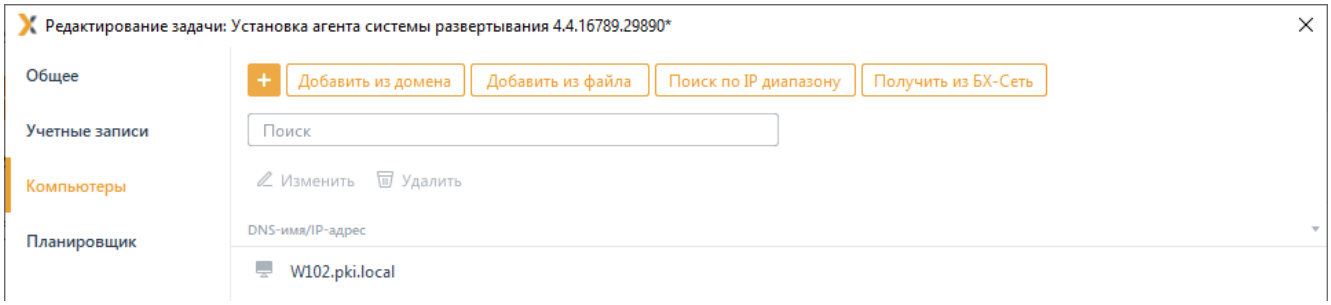
а)



б)



в)



г)

Рисунок 3.4 – Способы получения списка рабочих станция для установки агента

3.1.1.2 Формирование списка учетных записей пользователей

После добавления рабочих станций в список перейдите во вкладку ***Учетные записи*** (рисунок 3.5) и по кнопке + добавьте учетные записи пользователей (локальные или доменные), обладающие административными правами на рабочих станциях, на которые будет устанавливаться агент развертывания.

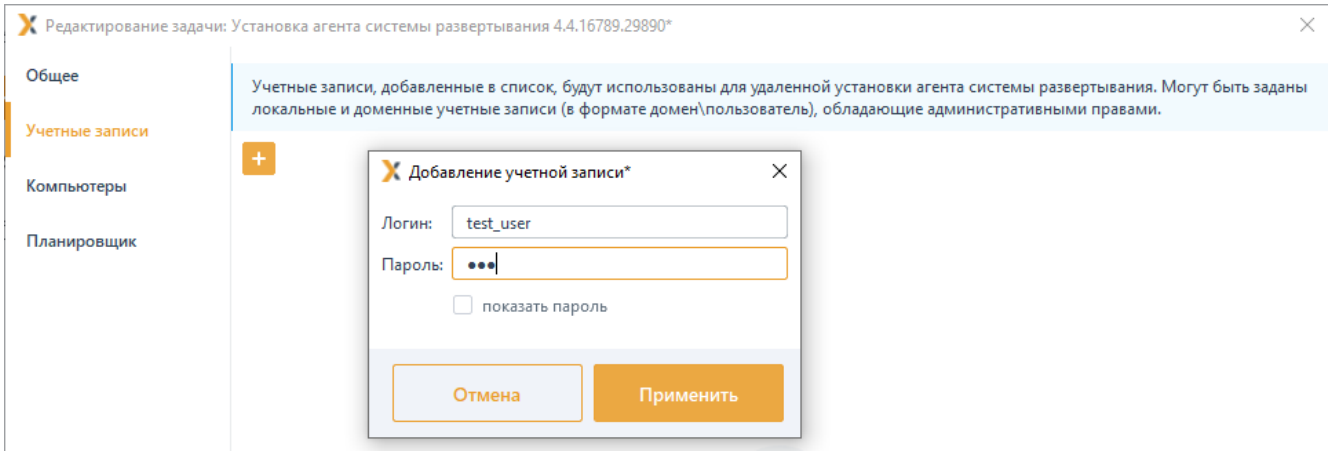


Рисунок 3.5 – Добавление административных учетных записей для установки агента

Если в списке рабочих станции при установке агента развертывания имеется рабочая станция с локальной учетной записью с административными правами (вне домена), может возникнуть ошибка вида:

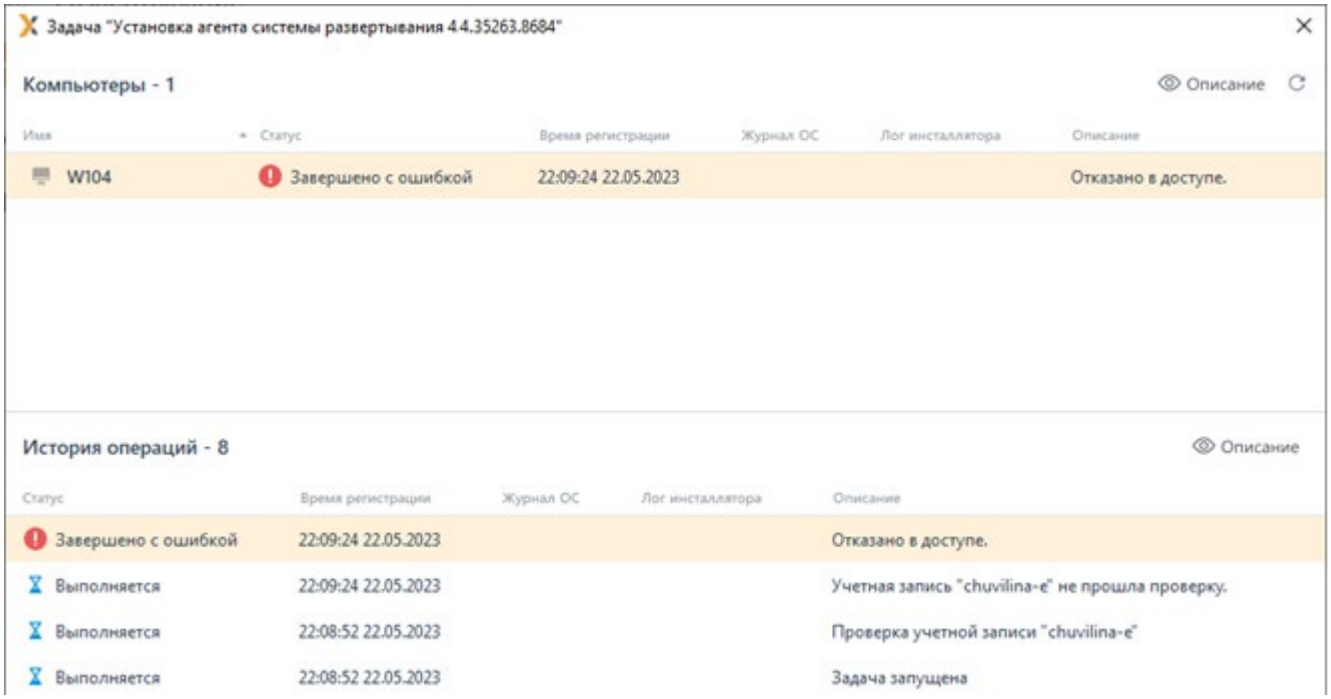


Рисунок 3.6 – Установка агента развертывания завершена с ошибкой

Для корректной установки агента развертывания необходимо предоставить локальной учетной записи доступ к доменной папке *admin$*, которую использует СЗИ при установке

агента развертывания:

– в редакторе реестра перейдите по пути ***HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System;***

– создайте новый параметр ***DWORD (32-bit)*** с именем ***LocalAccountTokenFilterPolicy*** и присвойте ему значение 1;

– выполните перезагрузку рабочей станции.

3.1.1.3 Указание параметров планировщика задачи по установке агента

Перейдите на вкладку ***Планировщик*** (рисунок 3.7) и укажите параметры планировщика для выполнения задачи установки агента развертывания на рабочих станциях.

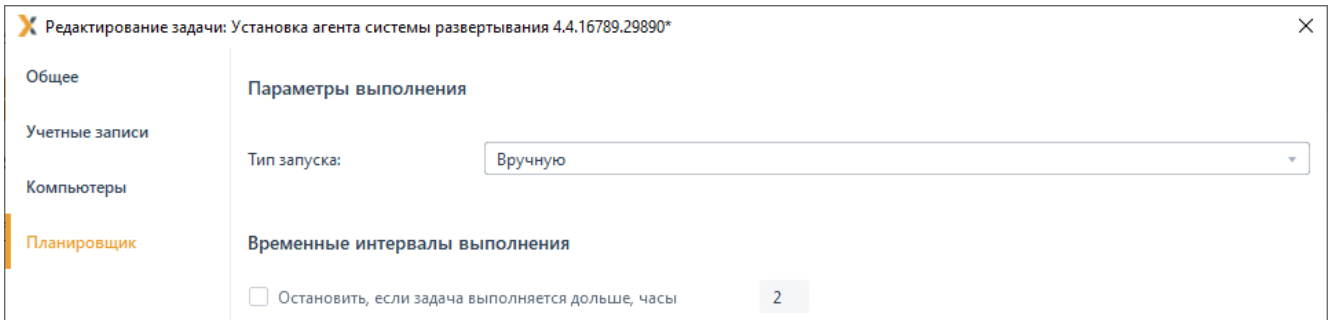


Рисунок 3.7 – Вкладка ***Планировщик*** окна редактирования параметров задачи

Возможны следующие типы запуска задачи по установке агента развертывания на рабочих станциях:

– ***Вручную*** (рисунок 3.7) – задача запускается после сохранения изменений вручную во вкладке ***Задачи*** по кнопке ▷ Запустить (рисунок 3.1);

– ***Сразу после создания/редактирования задачи*** (рисунок 3.8 а) – задача запустится, как только будет закрыто окно ее редактирования;

– ***Однократно в заданное время*** (рисунок 3.8 б) – в соответствующих полях указывается дата и время запуска задачи;

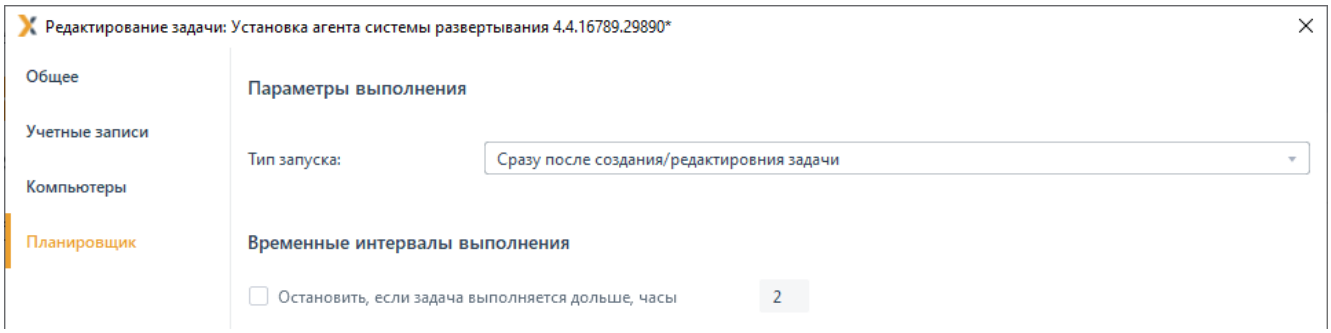
– ***По расписанию*** (рисунок 3.8 в) – указывается дата и время первого запуска задачи и интервал повторного запуска задачи:

- *дату запуска задачи* можно ввести вручную или выбрать из календаря, раскрывающегося при нажатии на кнопку раскрытия списка;
- *время первого запуска* задачи также можно указать, введя его значение вручную или установив курсор на необходимый параметр (часы, минуты, секунды) откорректировать его значение с помощью кнопок прокрутки;
- *интервал запуска* задачи может быть выбран в днях или часах:

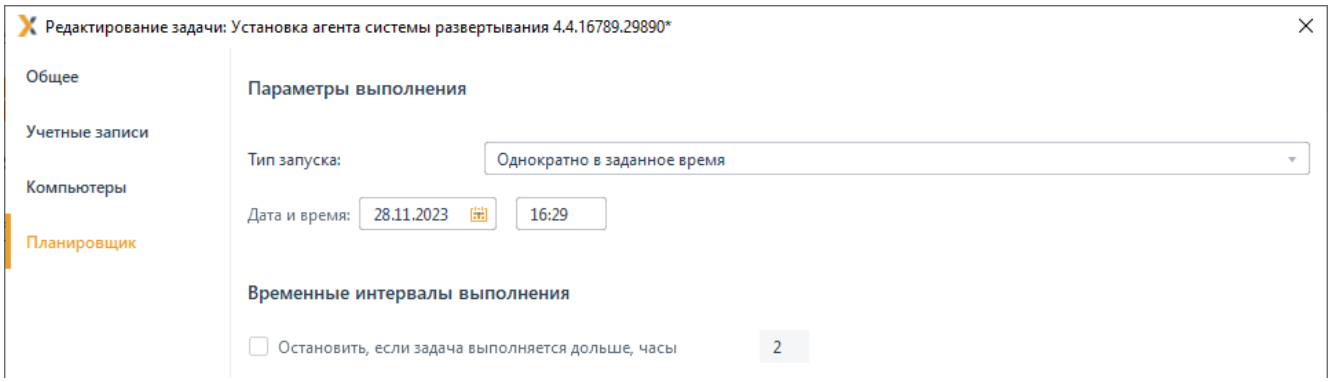
- запуск задачи в ***днях***, минимальное количество дней – 1 день, максимальное количество дней – 99;
- запуск задачи в ***часах***, минимальное количество часов – 1 час, максимальное количество часов – 23 часа;

- для рабочих станций задачи, имеющих статус «ожидает выполнения», повторный запуск задачи выполняется всегда;
- опционально, повторный запуск задачи может выполняться также для следующих рабочих станций:
  - ***Недоступных*** – задача будет повторно запущена на рабочих станциях, которые были недоступны при ее предыдущем запуске;
  - ***С ошибками*** – задача будет повторно запущена на рабочих станциях, на которых ее предыдущее выполнение завершилось ошибкой;

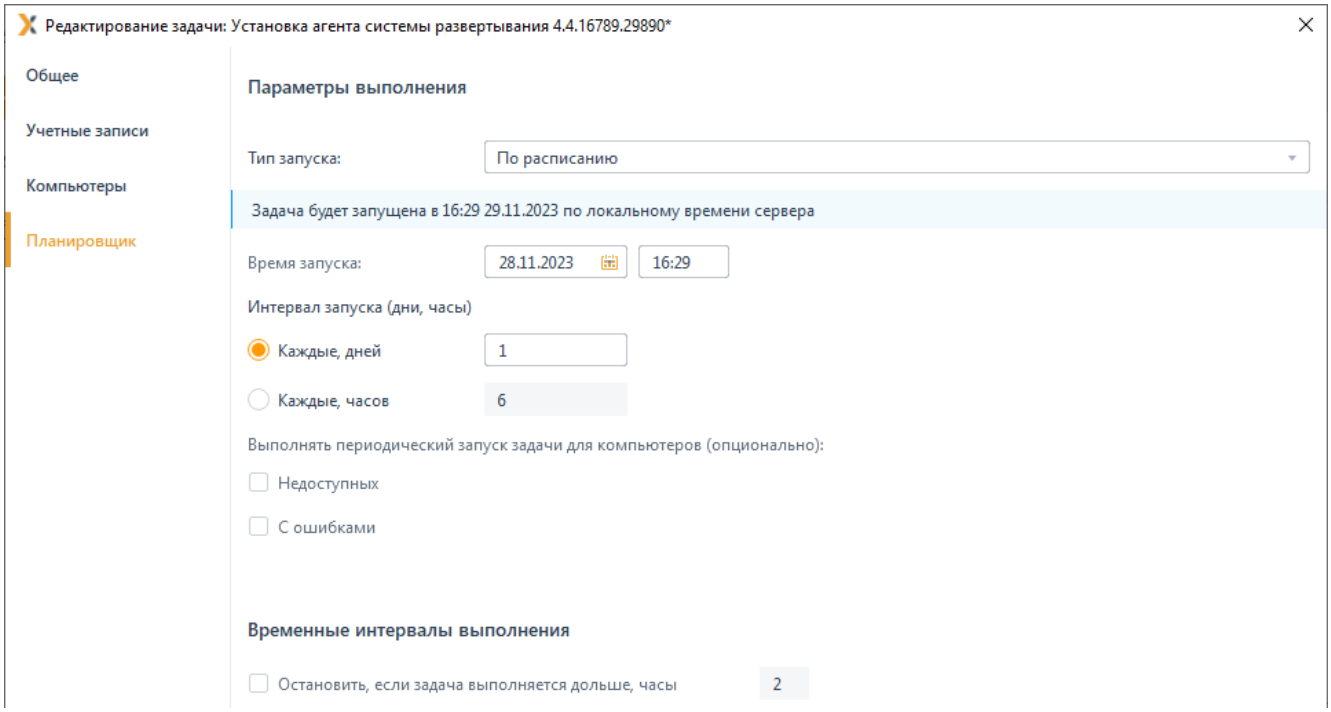
– ***После завершения другой задачи*** (рисунок 3.8 г) – задача будет запущена после того, как завершится предыдущая задача. Для выбора задачи, после которой будет запущена текущая, необходимо нажать в поле ***Связанная задача*** кнопку ***Выбрать,*** в открывшемся окне (рисунок 3.9) выделить необходимую задачу и нажать кнопку ***Выбрать***.



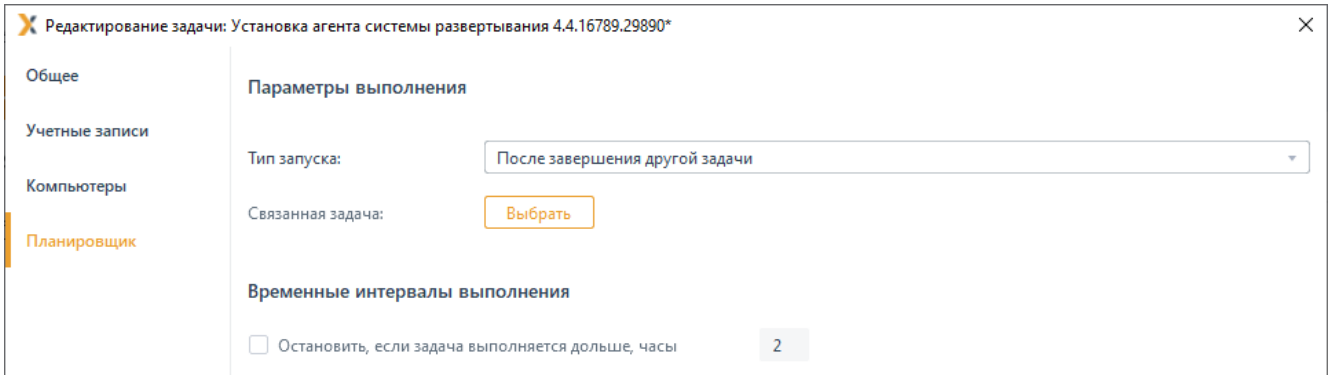
а)



б)



в)



г)

Рисунок 3.8 – Параметры типа запуска задачи

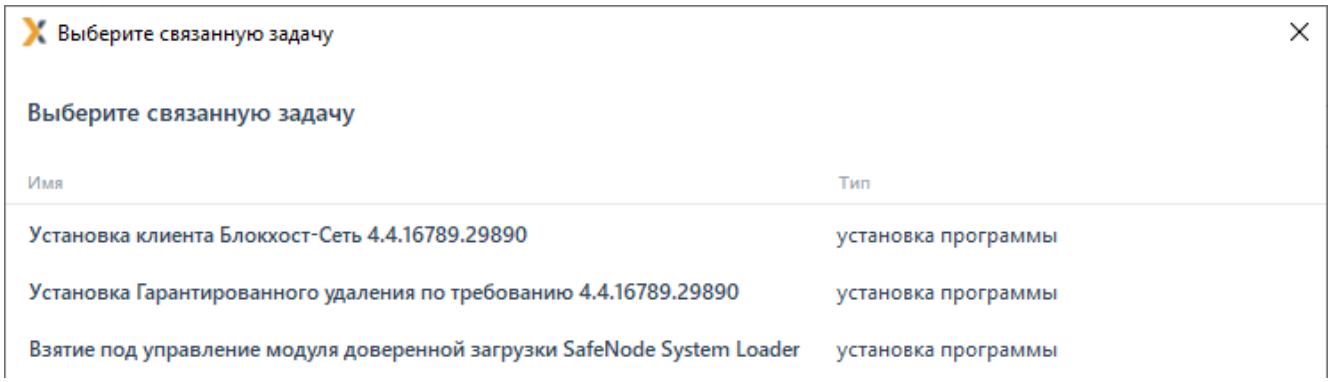


Рисунок 3.9 – Окно выбора связанной задачи

Также во вкладке ***Планировщик*** можно указать параметры прекращения выполнения

«зависшей» задачи (если задача выполняется длительное время). Для этого отметьте параметр ***Остановить, если задача выполняется дольше (часы)*** (рисунок 3.8) и введите в открывшееся поле ввода необходимое значение в часах.

3.1.1.4 Сохранение изменений, внесенных в задачу по установке агента

Для сохранения внесенных в задачу по установке агента развертывания изменений, нажмите кнопку ***OK*** (рисунок 3.10).

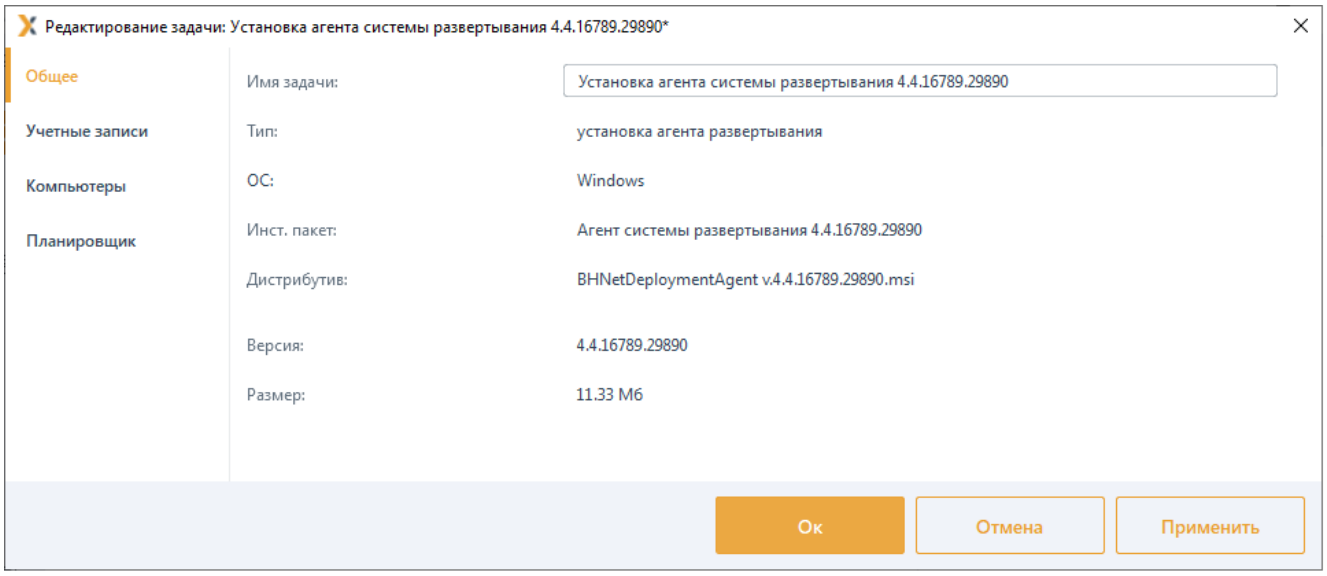


Рисунок 3.10 – Сохранение изменений в задаче

Нажатие на кнопку ***Отмена*** позволит выйти из окна редактирования параметров задачи без внесения изменений.

3.1.1.5 Запуск задачи по установке агента

В зависимости от установленных параметров планировщика запуск задачи будет осуществлен автоматически или вручную (подробнее в пункте ***«Запуск задачи»***).

Для отслеживания состояния задачи в ходе ее выполнения на рабочей станции, перейдите по ссылке ***Все результаты*** (рисунок 6.2).

По кнопке Описание в верхней части окна (рисунок 6.3) возможен просмотр статуса выполнения задачи.

В результате выполнения задачи по установке агента на всех указанных в списке рабочих станциях будет установлен агент развертывания.

3.1.2 Установка агента с помощью пакетов установки

Установка агента развертывания на клиентские рабочие станции под управлением ОС, отличной от ОС сервера, осуществляется с помощью пакетов установки.

Перед установкой агента развертывания на клиентские рабочие станции необходимо

сформировать пакет установки агента требующейся ОС клиента с помощью подсистемы развертывания.

Для формирования пакета установки перейдите во вкладку ***Пакеты установки*** по кнопке (рисунок 3.11).

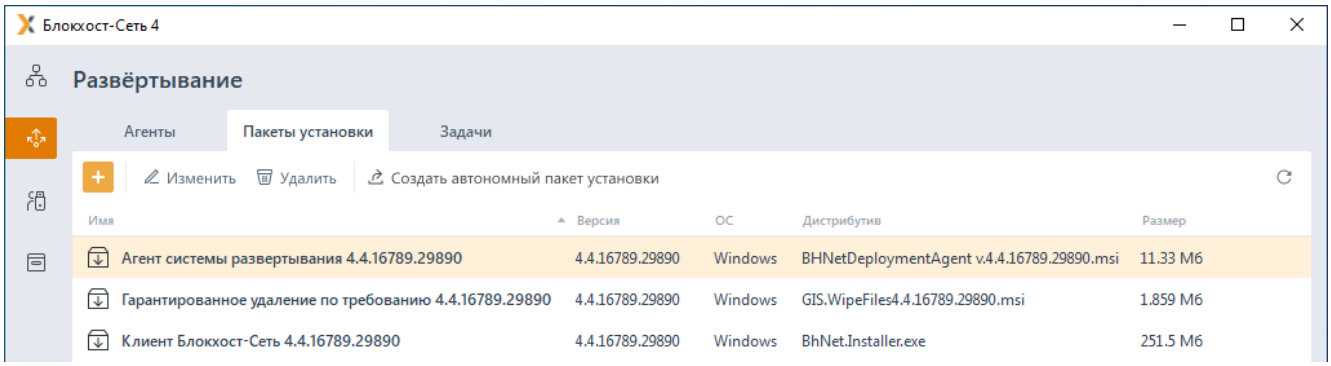


Рисунок 3.11 – Вкладка ***Пакеты установки***

По кнопке запустите создание пакета установки с помощью мастера создания пакетов установки (рисунок 3.12).

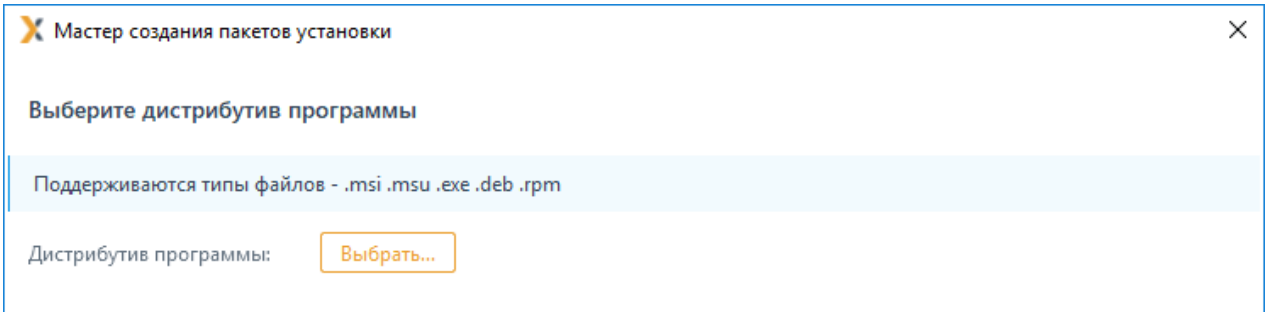


Рисунок 3.12 – Мастер создания пакетов установки

По кнопке ***Выбрать*** выберите из списка дистрибутив, содержащий установку агента в зависимости от используемой ОС (ниже приведен пример установки агента для ОС Astra Linux «Смоленск» версия 1.7) (рисунок 3.13).

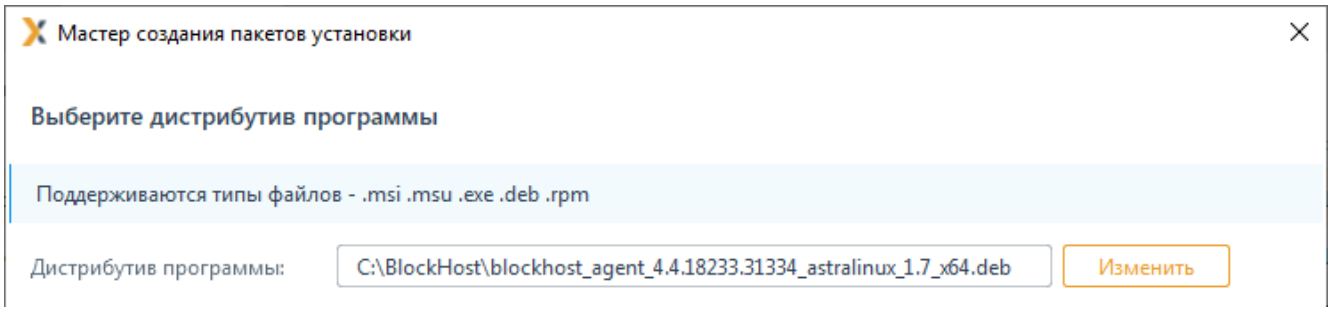


Рисунок 3.13 – Выбор пакета установки

Задайте имя создаваемого пакета (рисунок 3.14).

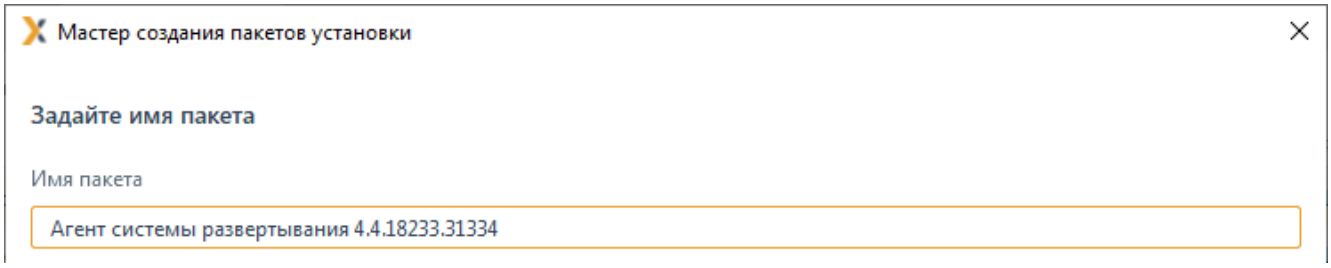


Рисунок 3.14 – Ввод имени пакета установки

По окончанию создания пакета установки, в списке появится новый пакет с заданным именем (рисунок 3.15).

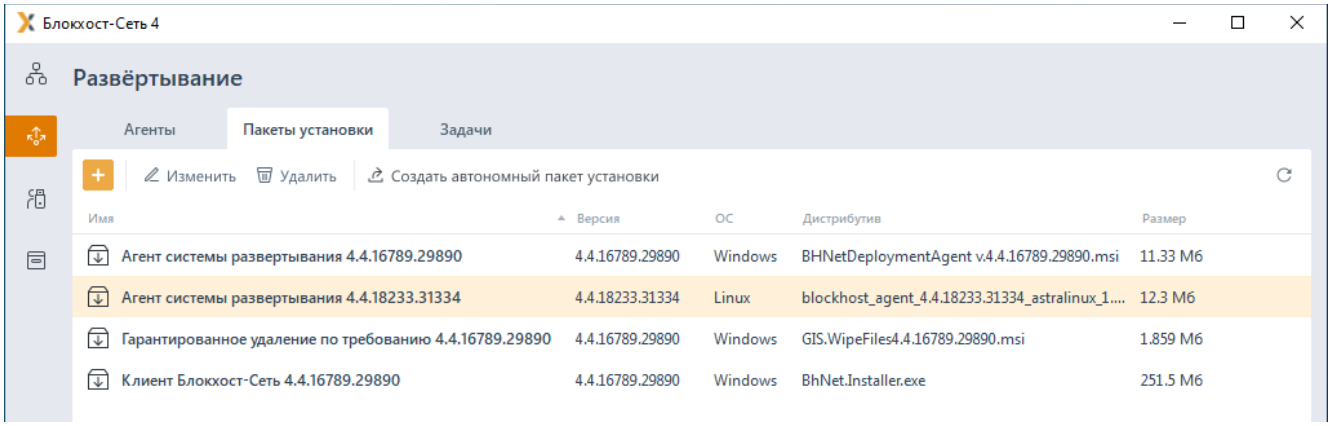


Рисунок 3.15 – Отображение созданного пакета установки в списке

Для создания задачи на установку агента развертывания на рабочие станции с помощью созданного пакета перейдите во вкладку ***Задачи***, раскройте меню создания задач по кнопке + и выберите пункт ***Установка агента развертывания*** (рисунок 3.16).

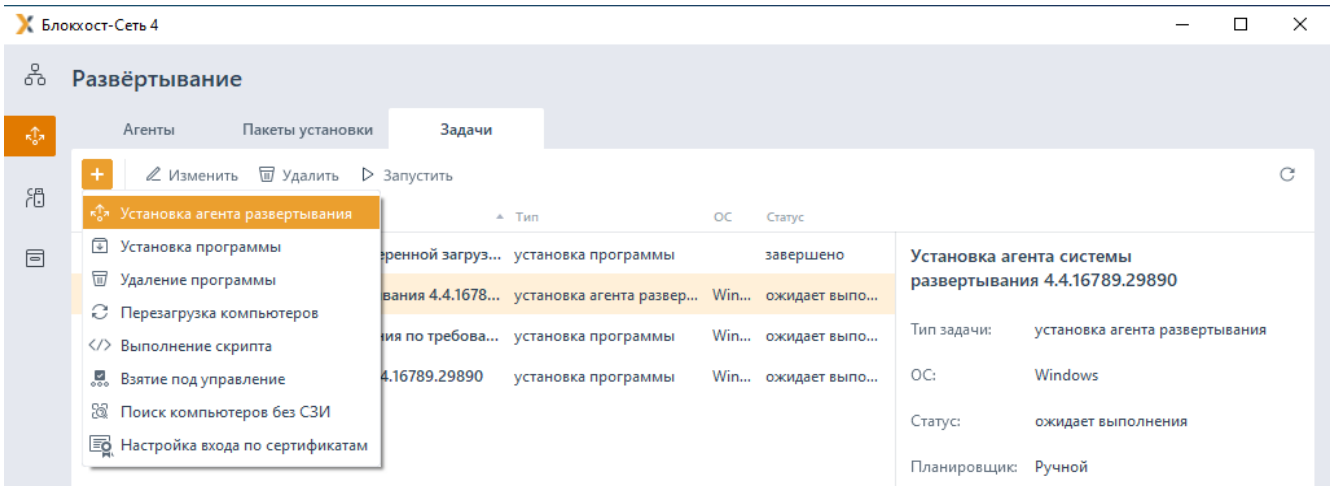


Рисунок 3.16 – Создание задачи на установку агента

В открывшемся окне создания задачи на установку агента развертывания (рисунок 3.17) выберите пакет установки ***blockhost_agent_<номер версии>_astralinux_1.7_x64*** и нажмите кнопку ***Далее***.

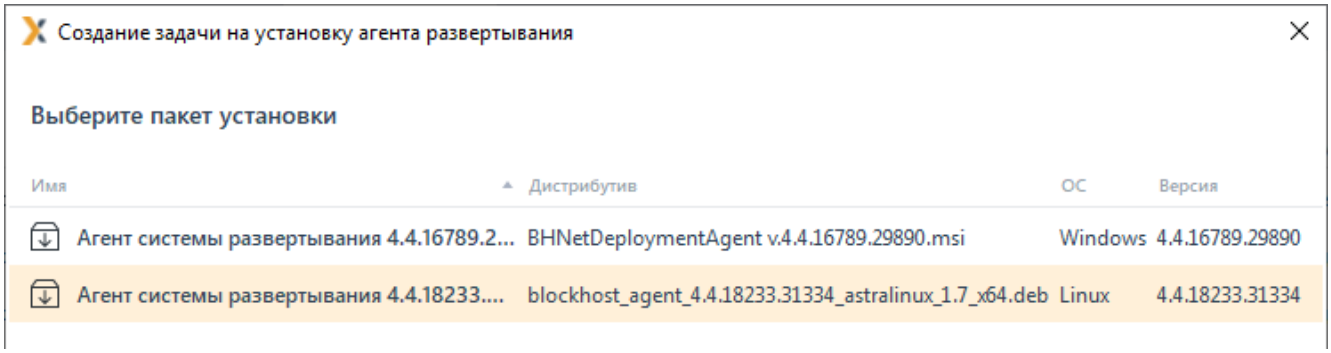


Рисунок 3.17 – Выбор пакета установки

В следующем окне (рисунок 3.18) сформируйте список рабочих станций на которые будет устанавливаться агент развертывания.

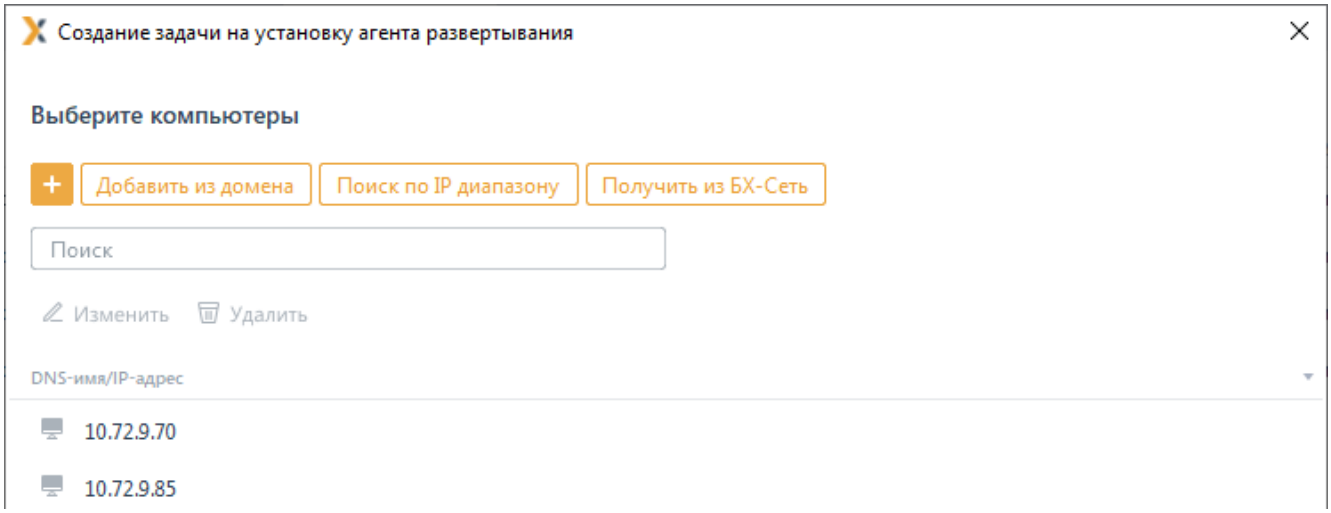


Рисунок 3.18 – Выбор рабочих станций для установки агента

Способы добавления рабочих станций в список описаны в пункте ***«Формирование списка рабочих станций для установки агента»***.

В следующем окне по кнопке  добавьте учетные записи пользователей, обладающие административными правами на рабочих станциях, на которые будет устанавливаться агент развертывания:

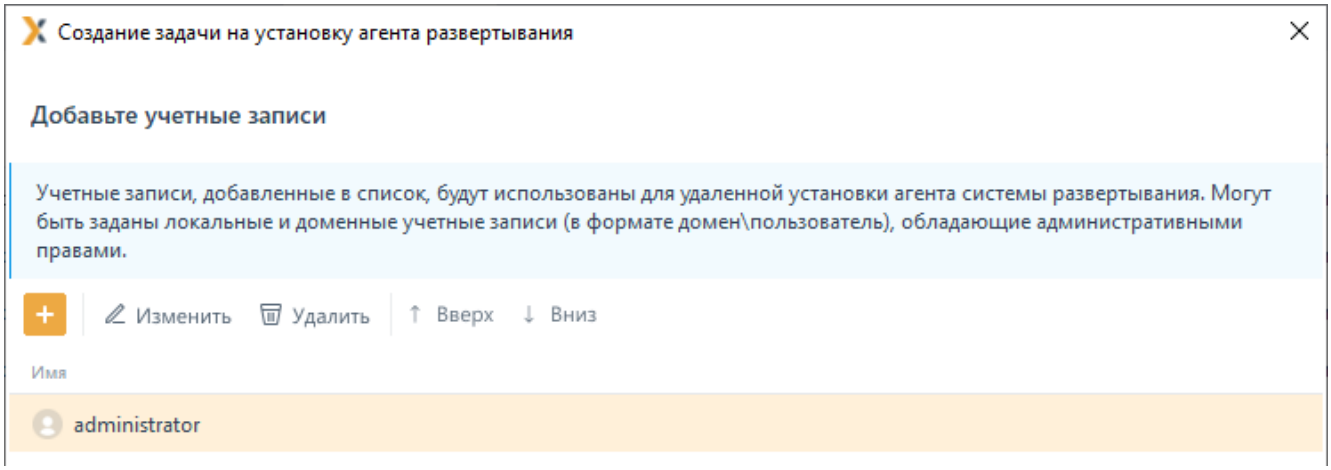


Рисунок 3.19 – Добавление административных учетных записей для установки агента

В следующем окне (рисунок 3.20) укажите параметры планировщика для выполнения задачи установки агента развертывания на рабочих станциях.

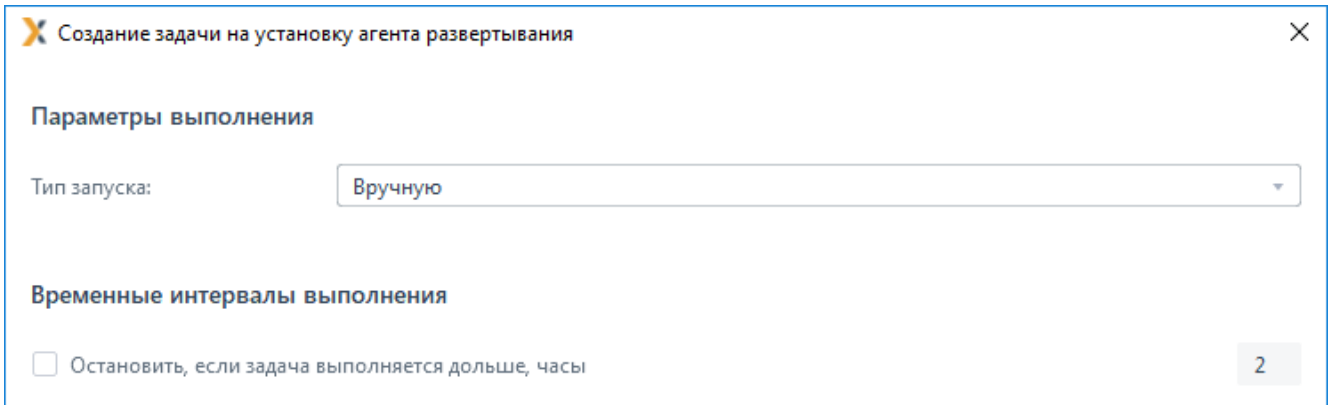


Рисунок 3.20 – Задание параметров выполнения задачи

Возможные типы запуска задачи приведены в описании установки агента развертывания в пункте ***«Указание параметров планировщика задачи по установке агента»***.

В следующем окне введите имя создаваемой задачи и сохраните задачу по кнопке ***Создать*** (рисунок 3.21).

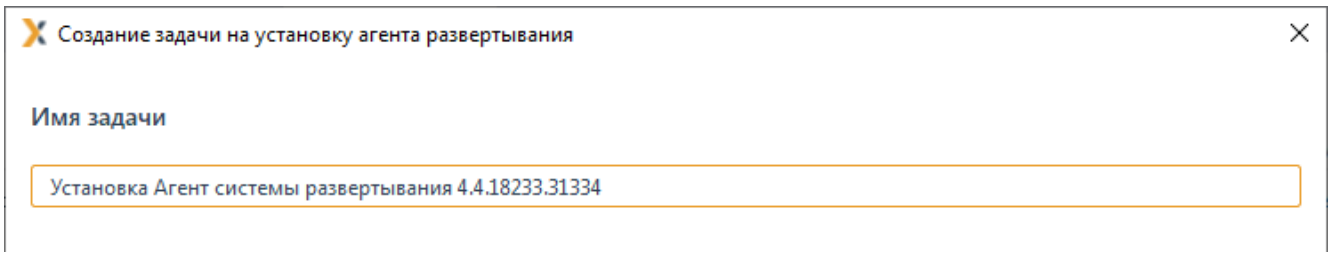


Рисунок 3.21 – Сохранение задачи

В зависимости от установленных параметров планировщика запуск задачи будет осуществлен автоматически или вручную (подробнее в пункте ***«Запуск задачи»***).

Для отслеживания состояния задачи в ходе ее выполнения на рабочей станции,

перейдите по ссылке ***Все результаты*** (рисунок 6.2).

По кнопке Описание в верхней части окна (рисунок 6.3) возможен просмотр статуса выполнения задачи.

В результате выполнения задачи по установке агента на всех указанных в списке рабочих станциях будет установлен агент развертывания.

3.2 Особенности установки агента развертывания на ОС Linux

Централизованная установка агента развертывания и клиента Блокхост-Сеть с помощью подсистемы развертывания СЗИ от НСД «Блокхост-Сеть 4» доступна для ОС Astra Linux «Смоленск» 1.7, Альт 8 СП, РЕД ОС 7.3 Муром.

На некоторых ОС Linux может быть установлен запрет на подключение по имени пользователя и паролю в рамках безопасности. В этом случае установка агента развертывания на рабочие станции под управлением ОС Linux возможна с использованием для подключения по протоколу SSH сгенерированных администратором ключей.

Перед установкой агента развертывания на ОС Linux через подсистему развертывания необходимо убедиться, что:

– на клиентской рабочей станции включен протокол SSH:

Переустановка SSH:

```
sudo apt-get remove --purge openssh-server
sudo apt-get update
sudo apt-get install openssh-server
```

Команды для проверки работы протокола SSH:

```
systemctl -l --type service --all|grep ssh
sudo systemctl status sshd
```

Перед установкой агента развертывания на ОС Альт 8 СП также необходимо отредактировать файл /etc/sudoers:

```
su –
pluma /etc/sudoers
```

В открывшемся редакторе в строке ***# WHEEL_USERS ALL=(ALL) ALL*** необходимо убирать символ «**#**» и сохранить файл.

Для установки агента развертывания на рабочие станции под управлением ОС Linux с использованием подключения по протоколу SSH необходимо выполнить последовательно шаги, описанные в пункте ***Установка агента с помощью пакетов установки***.

После добавления учетных записей пользователей, обладающих административными правами на рабочих станциях, на которые будет устанавливаться агент развертывания (рисунок 3.19), появится окно (рисунок 3.22), в котором необходимо установить флаг ***Использовать ключ при подключении по SSH***.

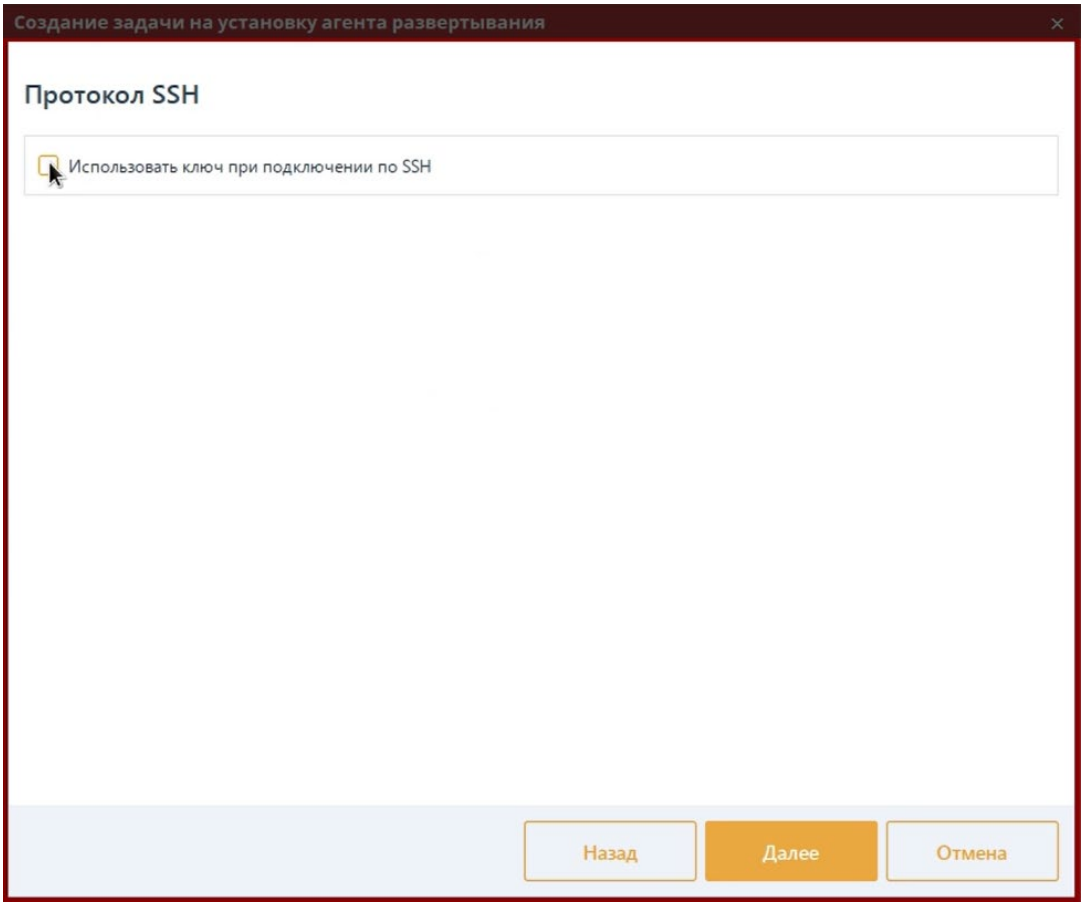


Рисунок 3.22 – Подключение по протоколу SSH

При подключении к рабочей станции по протоколу SSH с использованием ключа запуск задачи на установку агента развёртывания доступен только вручную.

При запуске созданной задачи на установку агента развертывания по протоколу SSH с использованием ключа, появится окно выбора приватного ключа (рисунок 3.23).

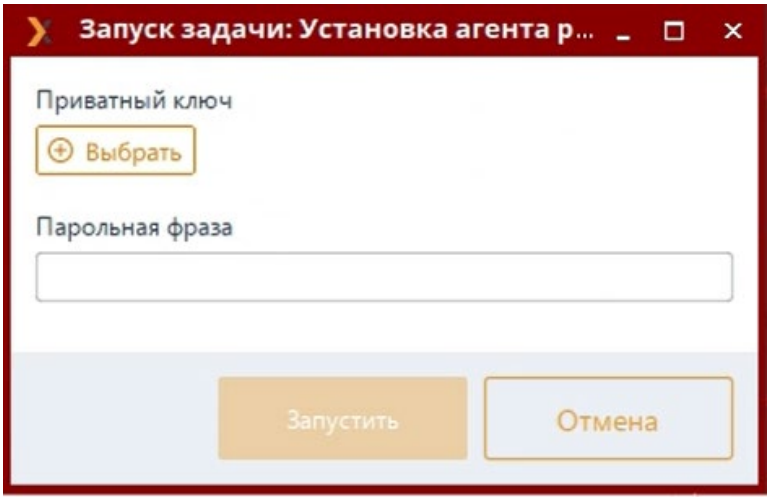


Рисунок 3.23 – Запуск задачи на установку агента с подключением по протоколу SSH

По кнопке Выбрать необходимо указать путь к директории, в которой находится приватный ключ (рисунок 3.24) и ввести парольную фразу (рисунок 3.25).

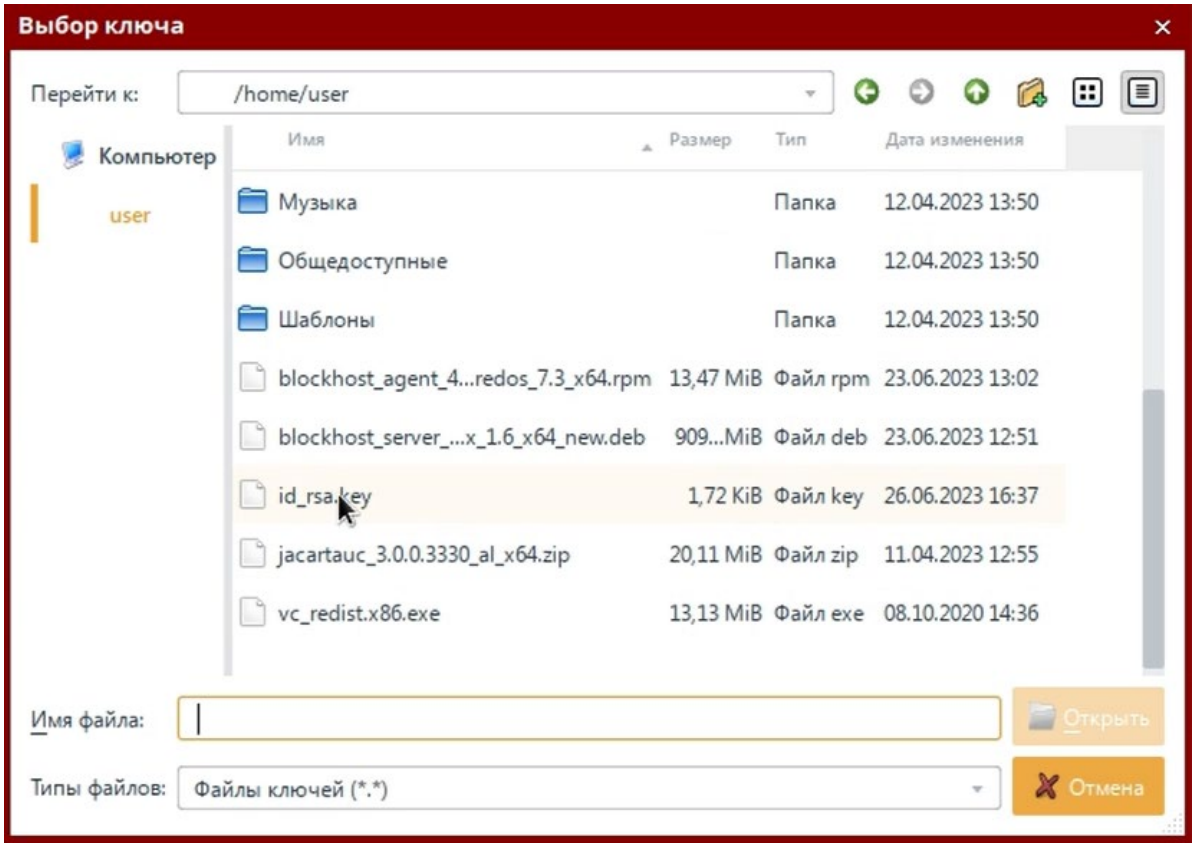


Рисунок 3.24 – Выбор приватного ключа

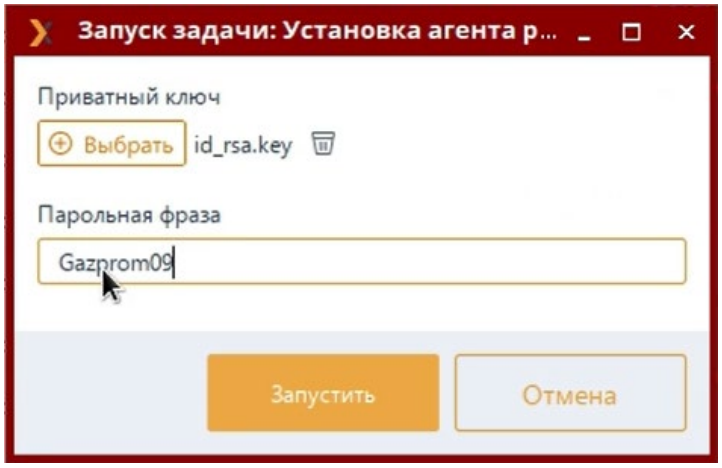


Рисунок 3.25 – Ввод парольной фразы

Парольная фраза может быть не установлена на ключе.

Путь к директории приватного ключа и парольную фразу необходимо вводить при каждом запуске задачи на установку агента развертывания по протоколу SSH с использованием ключа, т.к. эти данные не хранятся в БД сервера Блокхост.

3.3 Локальная установка агента

Агент развертывания не имеет графического интерфейса и устанавливается в качестве службы *GIS.Client.DeploymentSystem*.

Для локальной установки агента развертывания на рабочие станции скопируйте с сервера СЗИ на рабочую станцию (или съемный носитель) инсталляционный пакет агента и запустите его на выполнение (по умолчанию инсталляционный пакет агента расположен в каталоге *C:\BlockHost\DeploymentSystem\default\Агент Системы развертывания)*.

Подробно локальная установка агента подсистемы развертывания описана в документах «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство по инсталляции в ОС Windows» и «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство по инсталляции в ОС Linux».

3.4 Установка агента с помощью сторонних систем развертывания

Установка агента развертывания с использованием сторонних систем развертывания осуществляется с помощью дистрибутива *BHNetDeploymentAgent <номер_версии>.msi.* Установка дистрибутива выполняется на контроллере домена в настройках групповых политик в соответствии с документацией на используемое средство.

3.5 Удаление агента развертывания

Удаление агента подсистемы развертывания доступно только локально на клиентской рабочей станции.

Подробно локальное удаление агента подсистемы развертывания описано в документах «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство по инсталляции в ОС Windows» и «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство по инсталляции в ОС Linux».

4 Установка клиента Блокхост-Сеть

Клиент Блокхост-Сеть может быть установлен различными способами:

– с использованием функциональных возможностей подсистемы развертывания;

– локально вручную на клиентской рабочей станции (подробно установка клиента локально на рабочей станции описана в документах «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство по инсталляции в ОС Windows» и «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство по инсталляции в ОС Linux»);

– с использованием сторонних систем развертывания.

4.1 Установка клиента Блокхост-Сеть с помощью подсистемы развертывания

4.1.1 Установка клиента Блокхост-Сеть через предустановленную задачу

Для установки клиента Блокхост-Сеть на рабочие станции перейдите во вкладку ***Задачи*** и внесите корректировки в параметры автоматически созданной задачи ***Установка клиента Блокхост-Сеть <номер версии>***, открыв задачу на редактирование по кнопке Изменить в меню или с помощью контекстного меню (рисунок 4.1).

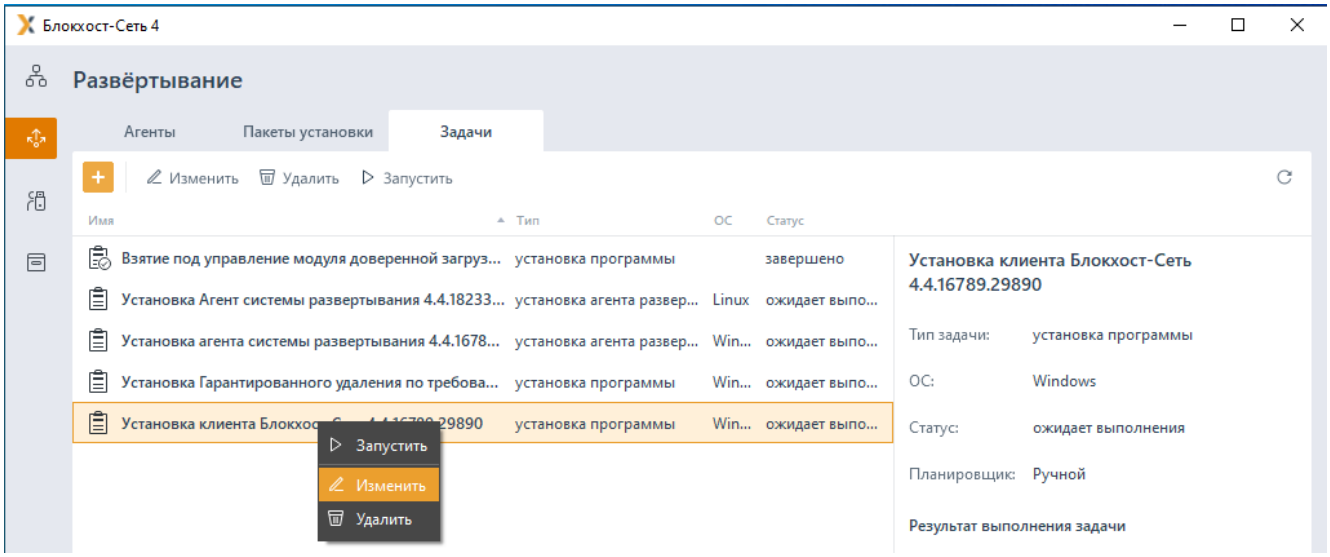


Рисунок 4.1 – Установка клиента Блокхост-Сеть

4.1.1.1 Выбор устанавливаемых модулей

В появившемся окне (рисунок 4.2) перейдите во вкладку ***Модули*** (рисунок 4.3) и сформируйте список модулей, которые будут доступны на рабочих станциях с установленным клиентом Блокхост-Сеть.

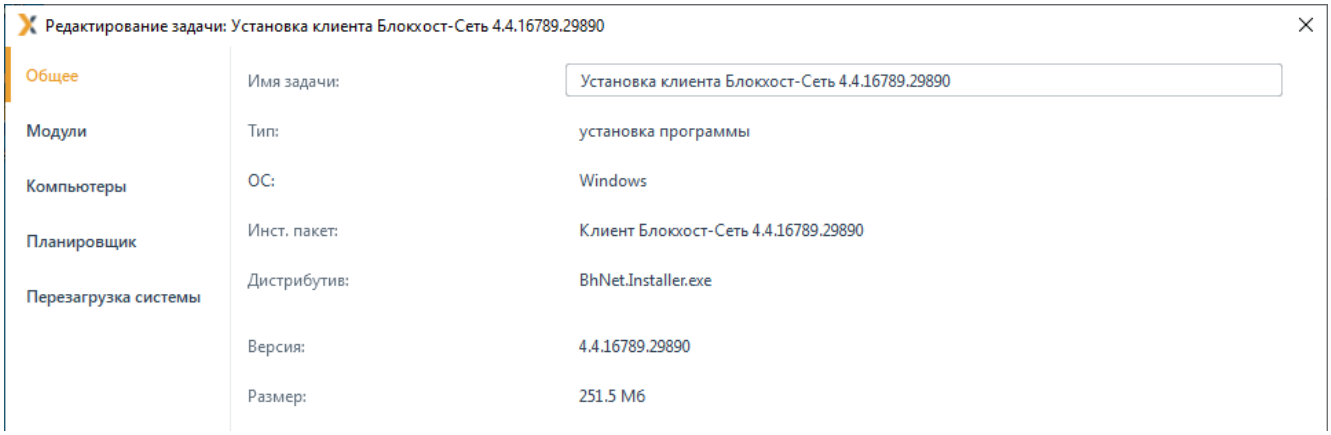


Рисунок 4.2 – Редактирование задачи на установку клиента Блокхост-Сеть

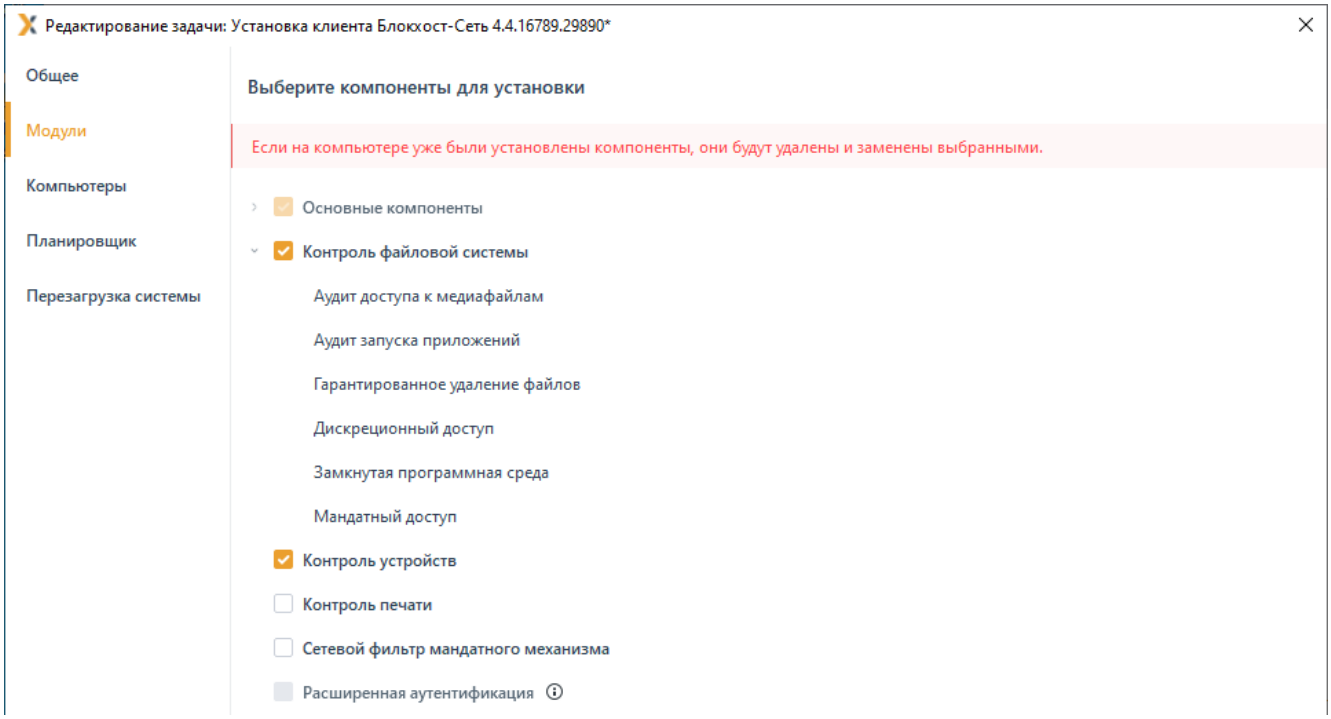


Рисунок 4.3 – Выбор модулей для установки на рабочие станции

К добавлению/изменению доступны только дополнительные модули. Обязательные модули, содержащие стандартный набор основных компонент СЗИ, устанавливаются на клиентские рабочие станции по умолчанию, отключить установку основных компонент невозможно.

К дополнительно устанавливаемым относятся следующие компоненты:

– ***Контроль файловой системы*** – включающий в себя:

- *Аудит доступа к медиафайлам* – регистрация событий аудита при попытках доступа к определённым типам файлов: аудиофайлам, видеофайлам и изображениям;
- *Аудит запуска приложений* – регистрация событий аудита запуска и

прекращения работы исполняемых файлов;

- *Гарантированное удаление файлов* – настройка гарантированного удаления объектов файловой системы с системных и не системных дисков без возможности их дальнейшего восстановления;
- *Дискреционный доступ* – настройка доступа пользователей к объектам файловой системы: логическим дискам, каталогам и файлам;
- *Замкнутая программная среда* – формирование списка разрешенных для запуска процессов, доступных для выбранного пользователя на клиентской рабочей станции;
- *Мандатный доступ* – настройка доступа пользователя к файловым ресурсам станции с помощью присвоения пользователям и ресурсам определенных меток.

– ***Контроль устройств*** - разграничение доступа пользователей к отчуждаемым носителям информации и подключаемым устройствам ввода-вывода;

– ***Контроль печати*** – управление расширенными возможностями контроля печати на клиентской рабочей станции: разграничение прав печати, простановка специального колонтитула для указанных приложений, расширенный аудит печати;

– ***Сетевой фильтр мандатного механизма*** – компонент, необходимый для работы мандатного разграничения доступа;

– ***Расширенная аутентификация*** – расширенные настройки механизма аутентификации, позволяющие проводить двухфакторную аутентификацию по сети и разграничивать доступ на уровне создания сессии пользователя[1].

4.1.1.2 Формирование списка рабочих станций для установки клиента

После выбора устанавливаемых модулей перейдите во вкладку ***Компьютеры*** (рисунок 4.4) и по кнопке  сформируйте список рабочих станций, на которые будет устанавливаться клиент Блокхост-Сеть.

[1] Установка модуля расширенной аутентификации через выбор компонентов не поддерживается. Модуль устанавливается с помощью отдельного инсталлятора «BlockHost.Net 4 extended auth.msi», входящего в комплект поставки.

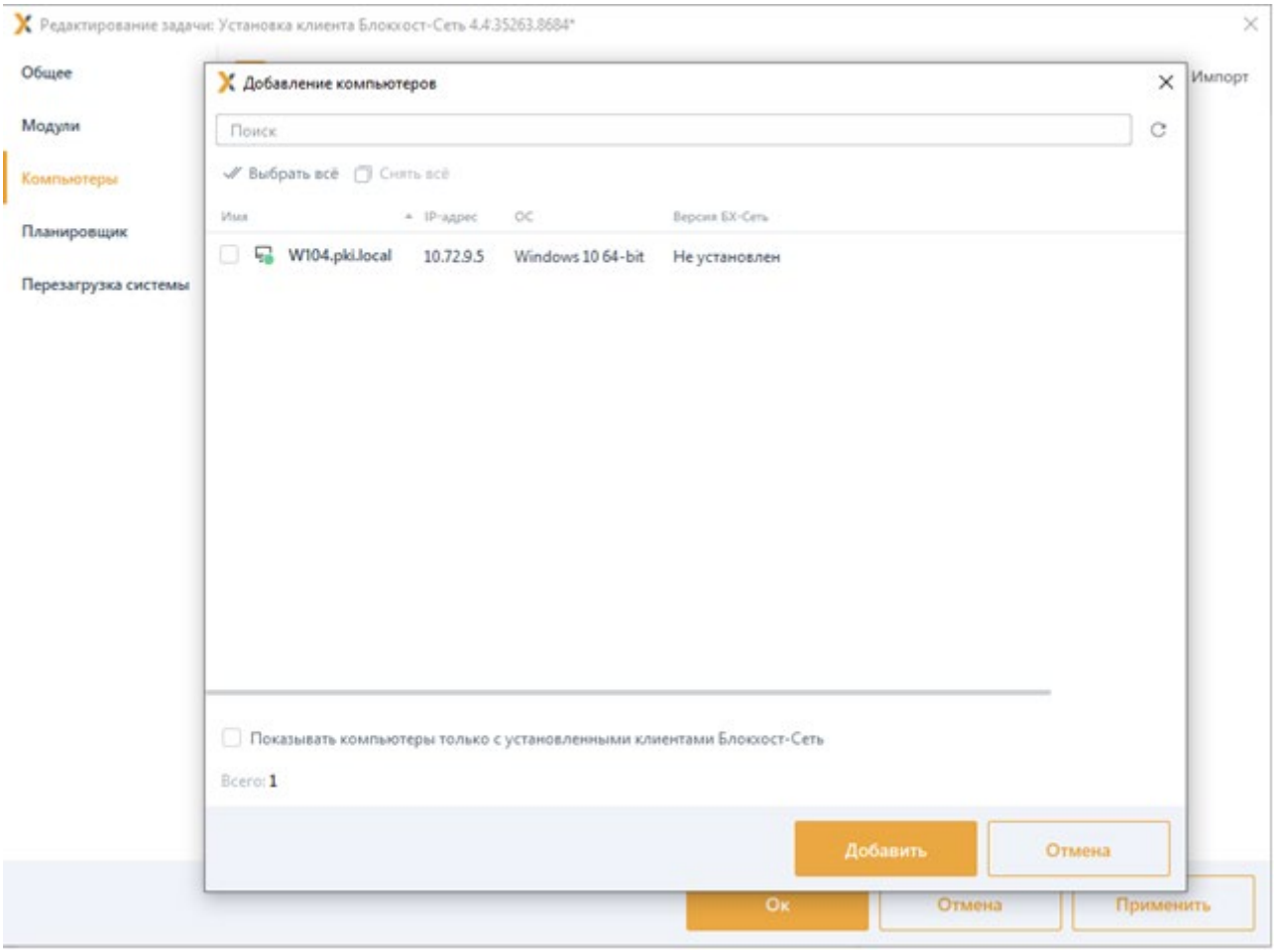


Рисунок 4.4 – Добавление рабочих станций в список установки клиента

Список рабочих станций, доступных для установки клиента Блокхост-Сеть формируется из рабочих станций, на которых уже установлен агент развертывания.

При необходимости фильтрации списка рабочих станций до компьютеров, на которых уже установлен клиент Блокхост-Сеть, установите параметр ***Показывать компьютеры только с установленными клиентами Блокхост-Сеть***.

4.1.1.3 Импорт/экспорт рабочих станций

При формировании списка рабочих станций, возможен экспорт/импорт списка рабочих станций из задачи/в задачу (рисунок 4.5).

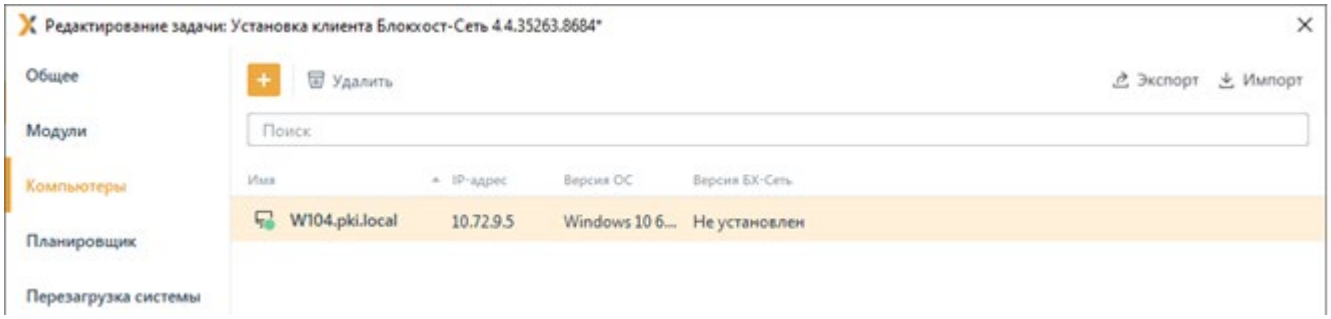


Рисунок 4.5 – Экспорт/импорт рабочих станций

Для экспортирования списка рабочих станций, нажмите кнопку ***Экспорт***, при этом весь список рабочих станций, добавленных в задачу, выгрузится в заданный файл по указанному в появившемся окне местоположению (рисунок 4.6).

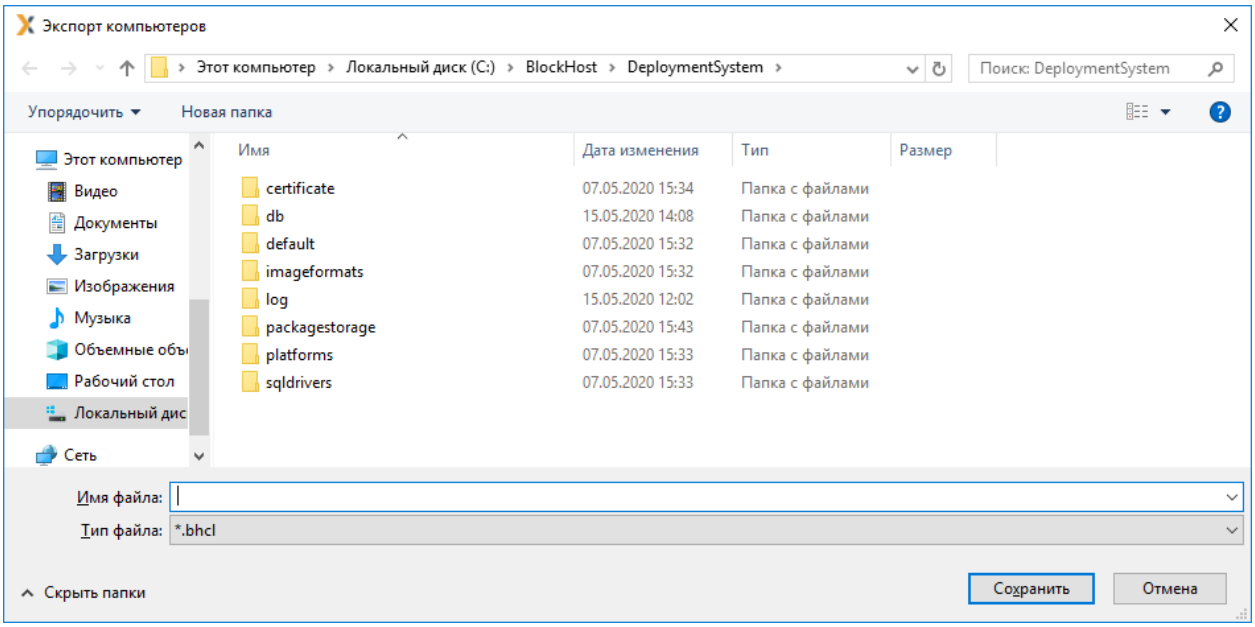


Рисунок 4.6 – Выбор директории для экспорта рабочих станций

Для импорта списка рабочих станций в редактируемую задачу, нажмите кнопку ***Импорт*** и в появившемся окне выберите файл, содержащий список импортируемых рабочих станций (рисунок 4.7).

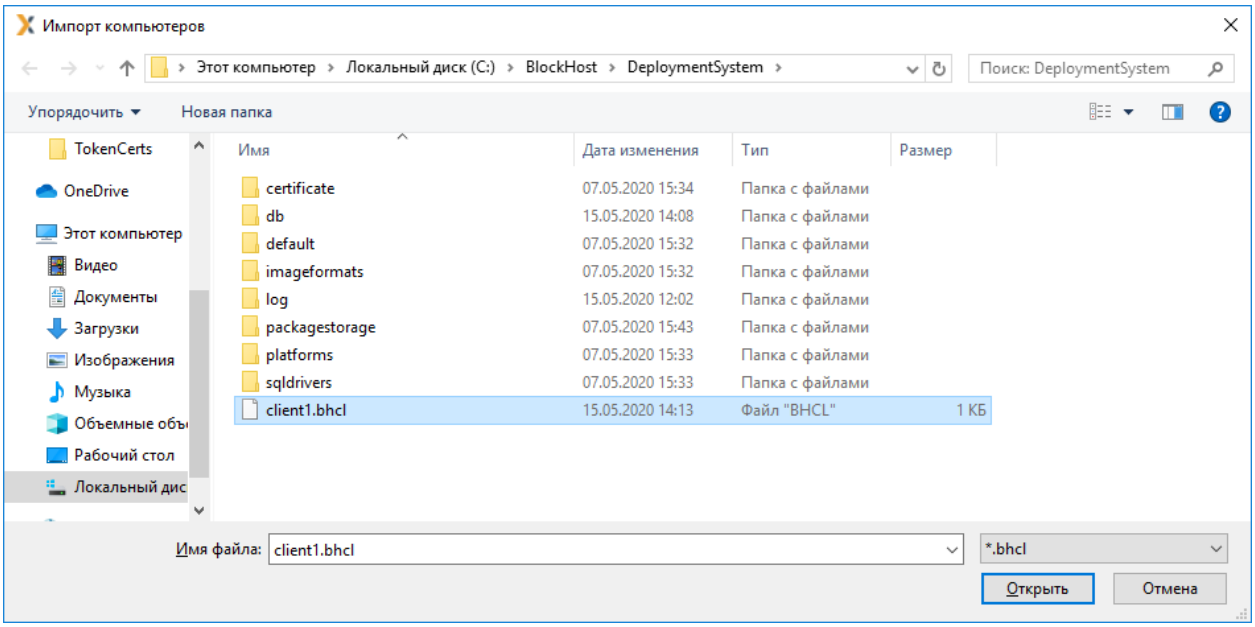


Рисунок 4.7 – Выбор файла для импорта рабочих станций

4.1.1.4 Указание параметров планировщика задачи

Перейдите на вкладку ***Планировщик*** (рисунок 4.8) и укажите параметры планировщика

для выполнения задачи установки клиента Блокхост-Сеть на рабочих станциях.

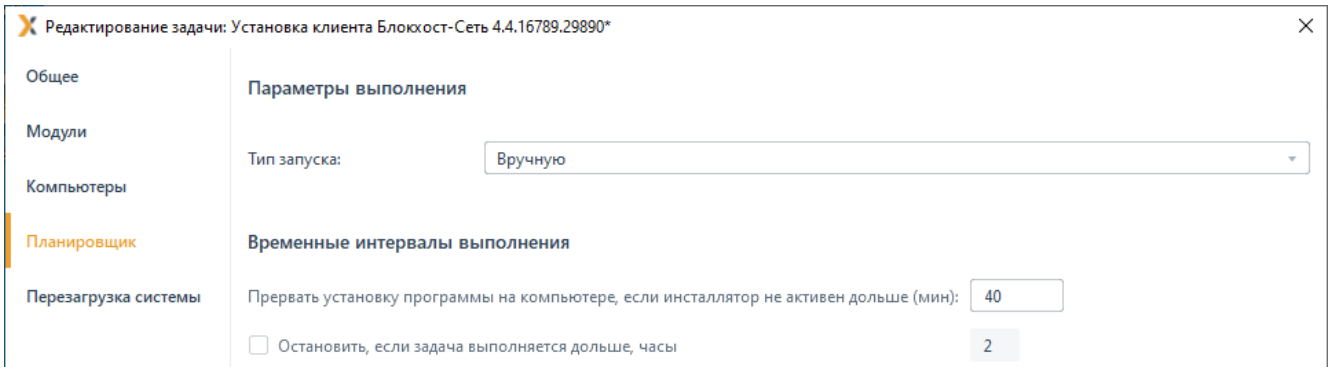


Рисунок 4.8 – Вкладка ***Планировщик*** окна редактирования параметров задачи

Возможные типы запуска задачи приведены в описании установки агента развертывания в пункте ***«Указание параметров планировщика задачи по установке агента»***.

4.1.1.5 Параметры перезагрузки рабочих станций

Перейдите на вкладку ***Перезагрузка системы*** (рисунок 4.9) и укажите параметры перезагрузки рабочих станций после установки клиента Блокхост-Сеть на рабочих станциях.

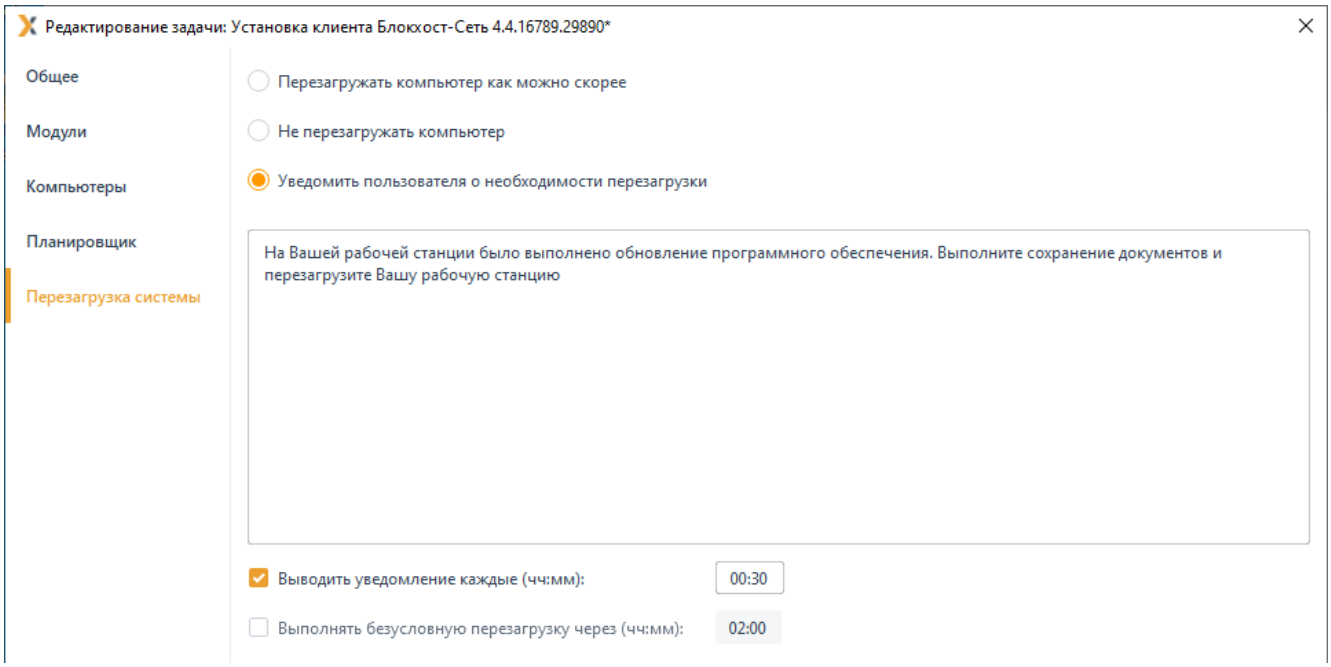


Рисунок 4.9 – Вкладка ***Перезагрузка системы*** окна редактирования параметров задачи

Доступны следующие виды перезагрузки рабочей станции:

– ***Перезагружать компьютер как можно скорее*** – рабочая станция будет перезагружена в течение 5 минут после завершения задачи. Пользователи не смогут отказаться или отложить перезагрузку.

На клиентской рабочей станции появится сообщение о необходимости перезагрузки рабочей станции (рисунок 4.10).

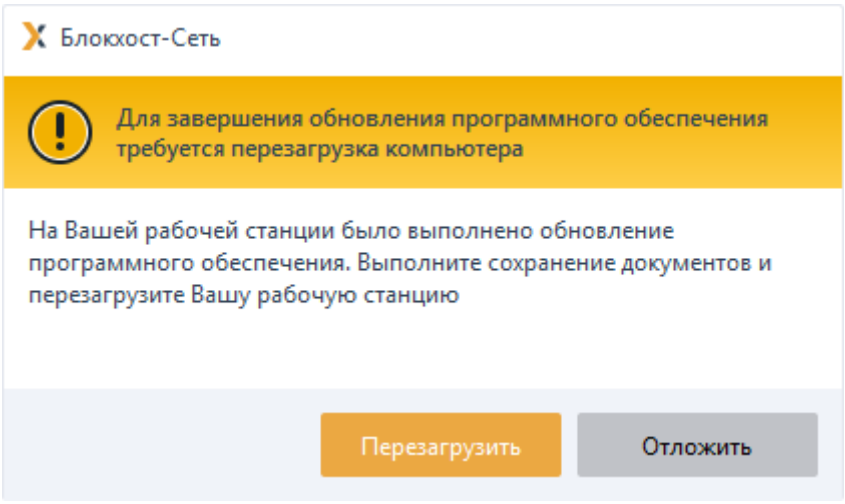


Рисунок 4.10 – Сообщение с предупреждением о перезарузке рабочей станции

– ***Не перезагружать компьютер*** – рабочая станция не будет перезагружена после завершения выполнения задачи.

– ***Уведомить пользователя о необходимости перезагрузки*** – после завершения задачи, на рабочей станции откроется окно с сообщением о необходимости перезагрузки рабочей станции (рисунок 4.10). Возможно настроить частоту вывода уведомления о перезагрузке пользователю и задать безусловную перезагрузку по истечении указанного временного интервала (по умолчанию 2 минуты).

На клиентской рабочей станции появится сообщение о необходимости перезагрузки с указанием времени, оставшимся до автоматической перезагрузки рабочей станции установленным администратором (рисунок 4.10). В окне пользователь может согласиться с перезагрузкой, нажав ***Перезагрузить сейчас***, или дождаться истечения установленного администратором временного интервала безусловной перезагрузки.

4.1.1.6 Сохранение изменений, внесенных в задачу

Для сохранения внесенных в задачу по установке клиента Блокхост-Сеть, последовательно нажмите кнопки ***Сохранить*** и ***ОК*** (рисунок 4.11).

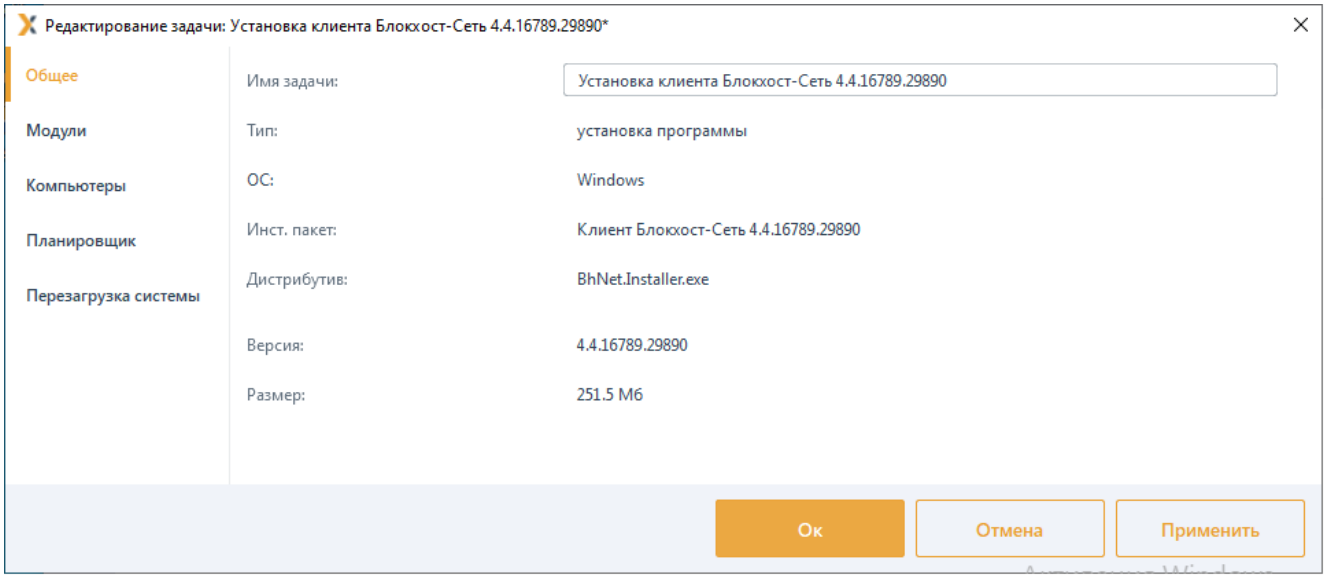


Рисунок 4.11 – Сохранение изменений в задаче

Нажатие на кнопку ***Отмена*** позволит выйти из окна редактирования параметров задачи без внесения изменений.

4.1.1.7 Запуск задачи по установке клиента

В зависимости от установленных параметров планировщика запуск задачи будет осуществлен автоматически или вручную (подробнее в пункте ***«Запуск задачи»***).

Для отслеживания состояния задачи в ходе ее выполнения на рабочей станции, перейдите по ссылке ***Все результаты*** (рисунок 6.2).

По кнопке Описание в верхней части окна (рисунок 6.3) возможен просмотр статуса выполнения задачи.

В результате выполнения задачи по установке клиента на всех указанных в списке рабочих станциях будет установлена клиентская часть СЗИ.

4.1.2 Установка клиента Блокхост-Сеть с помощью пакетов установки

Установка клиента Блокхост-Сеть на клиентские рабочие станции под управлением ОС, отличной от ОС сервера, осуществляется с помощью пакетов установки.

Перед установкой клиента Блокхост-Сеть на рабочие станции необходимо сформировать пакет установки агента требующейся ОС клиента с помощью подсистемы развертывания.

Для формирования пакета установки перейдите во вкладку ***Пакеты установки*** по кнопке (рисунок 4.12).

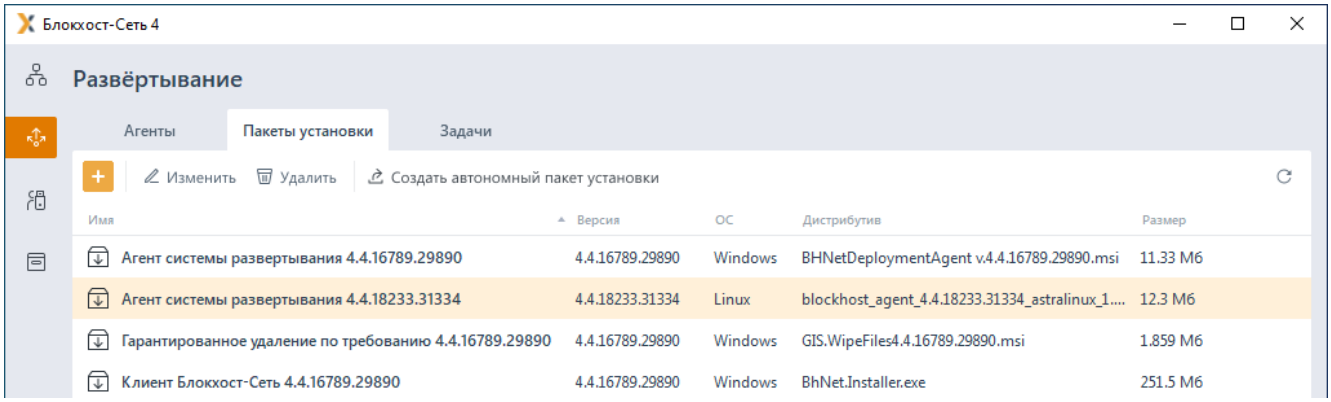


Рисунок 4.12 – Вкладка ***Пакеты установки***

По кнопке  запустите создание пакета установки с помощью мастера создания пакетов установки (рисунок 4.13).

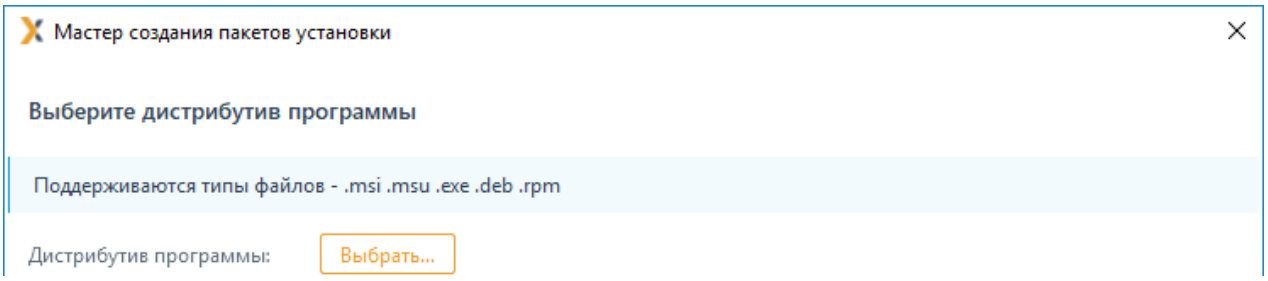


Рисунок 4.13 – Мастер создания пакетов установки

По кнопке ***Выбрать*** из списка выберите дистрибутив, содержащий установку клиента в зависимости от используемой ОС (ниже приведен пример установки клиента для ОС Astra Linux «Смоленск» 1.7) (рисунок 4.14).

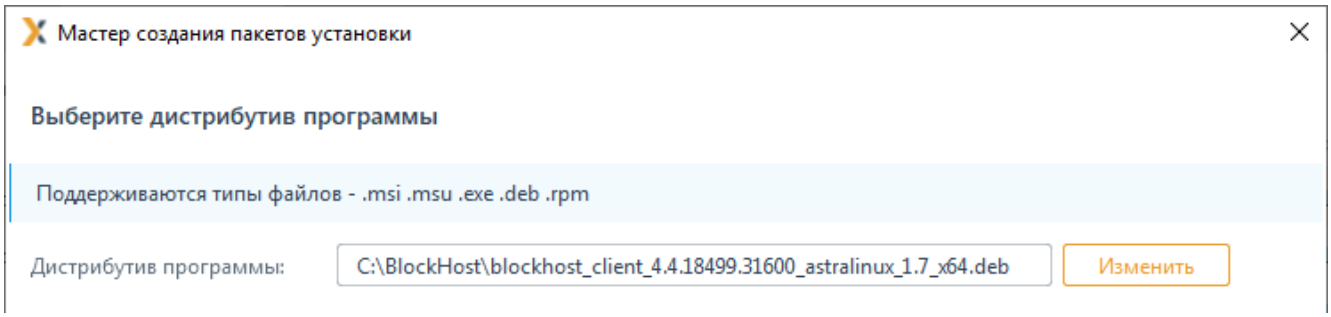


Рисунок 4.14 – Выбор пакета установки

Задайте имя создаваемого пакета (рисунок 4.15).

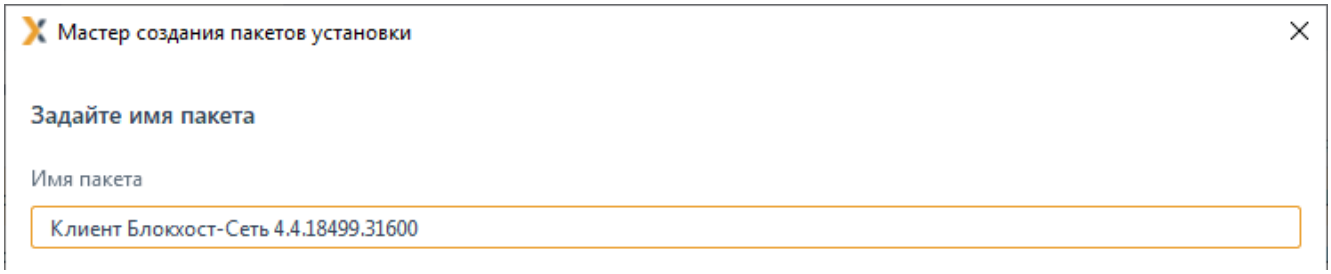


Рисунок 4.15 – Ввод имени пакета установки

По окончанию создания пакета установки, в списке появится новый пакет с заданным именем (рисунок 4.16).

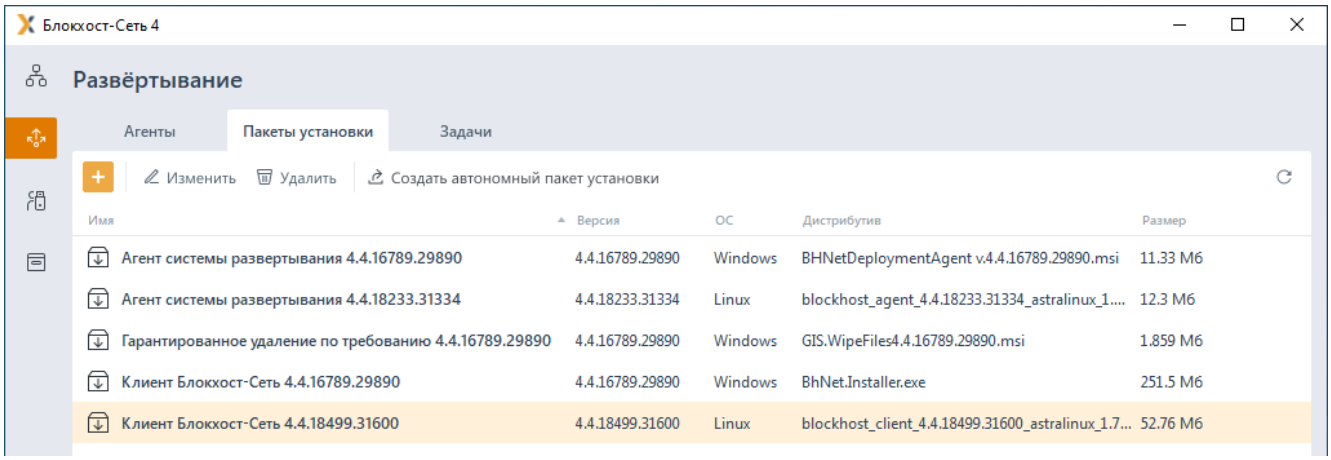


Рисунок 4.16 – Отображение созданного пакета установки в списке

Для создания задачи на установку клиента на рабочие станции с помощью созданного пакета перейдите во вкладку ***Задачи***, раскройте меню создания задач по кнопке + и выберите пункт ***Установка программы*** (рисунок 4.17).

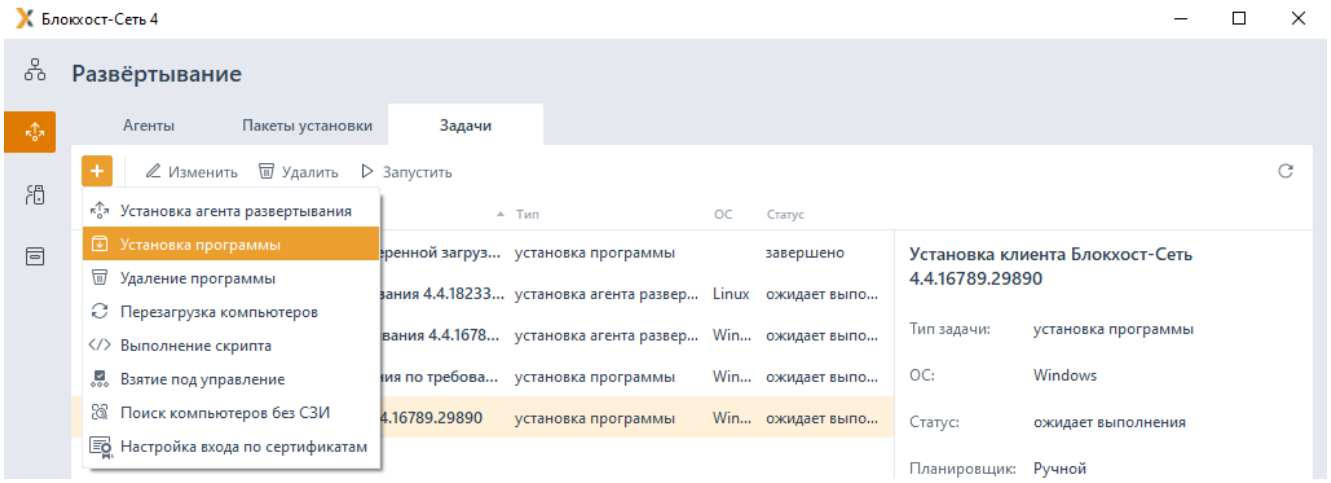


Рисунок 4.17 – Создание задачи на установку клиента Блокхост-Сеть

В открывшемся окне создания задачи на установку клиента Блокхост-Сеть (рисунок 4.18) выберите созданный на предыдущем шаге пакет установки и нажмите кнопку ***Далее***.

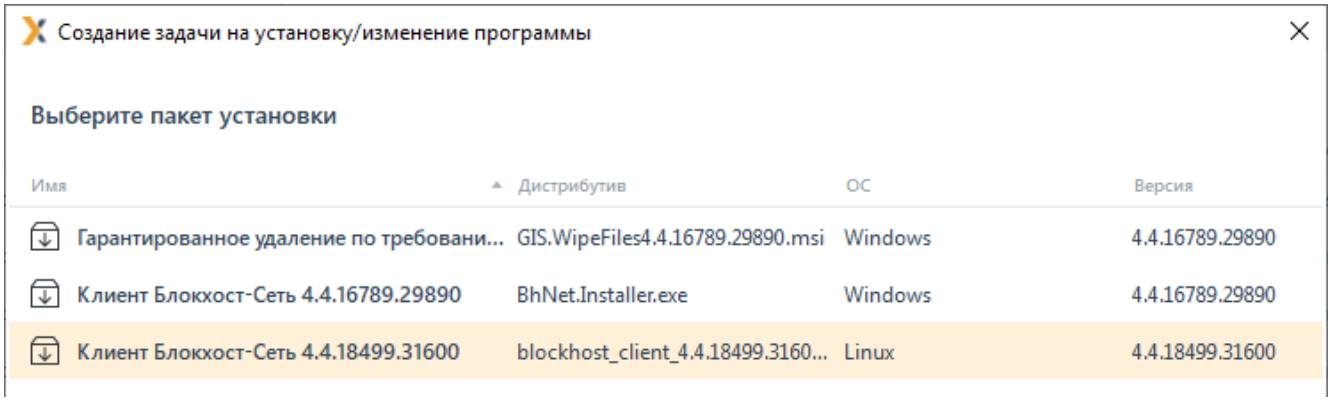


Рисунок 4.18 – Выбор пакета установки

В следующем окне (рисунок 4.19) выберите рабочие станции с установленным агентом развертывания, на которые будет устанавливаться клиент Блокхост-Сеть.

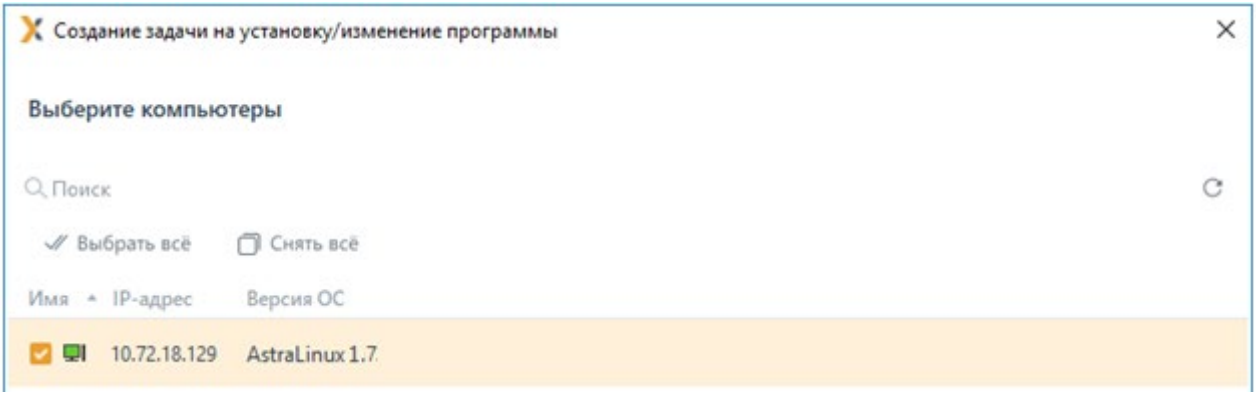


Рисунок 4.19 – Выбор рабочих станций для установки клиента

В следующем окне (рисунок 4.20) укажите параметры планировщика для выполнения задачи установки клиента Блокхост-Сеть на рабочих станциях.

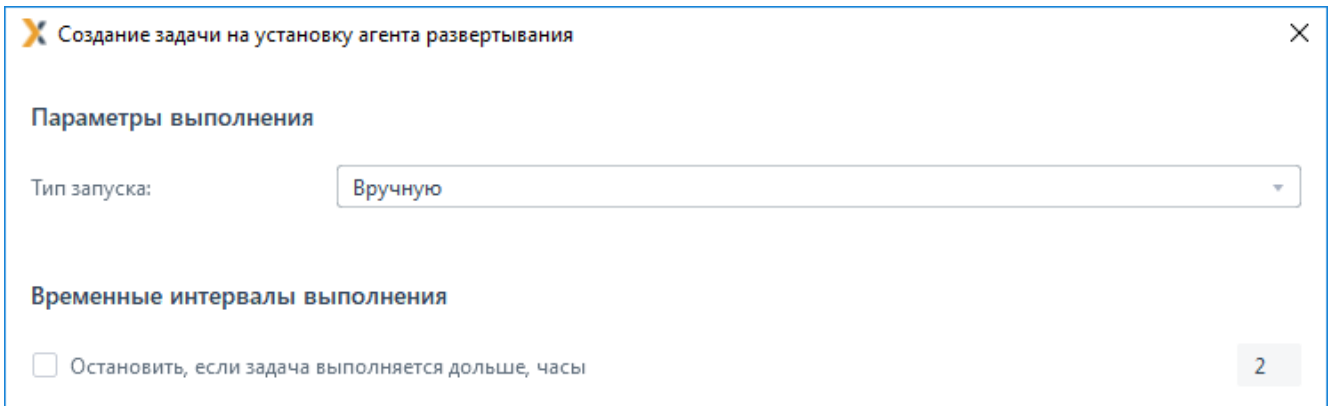


Рисунок 4.20 – Задание параметров выполнения задачи

Возможные типы запуска задачи приведены в описании установки агента развертывания в пункте ***«Указание параметров планировщика задачи по установке агента»***.

В следующем окне (рисунок 4.21) укажите параметры перезагрузки рабочих станций.

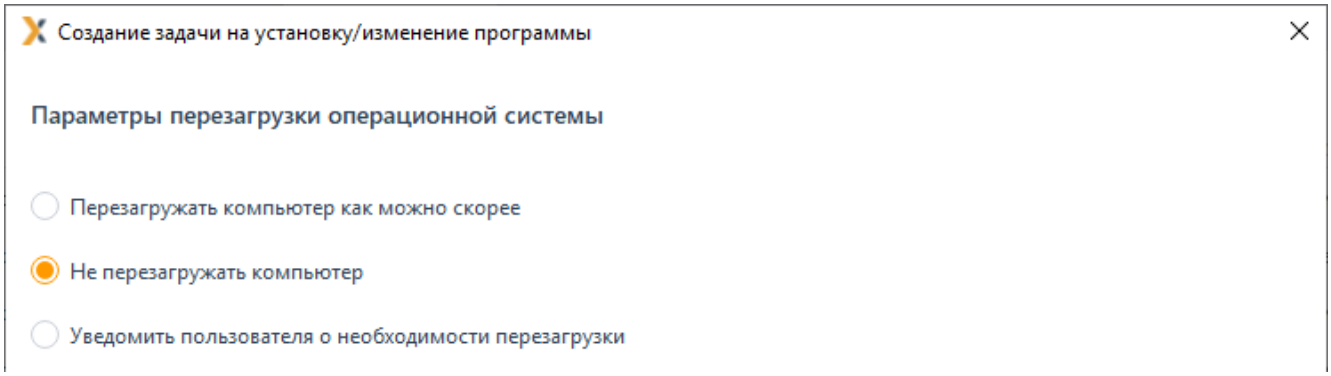


Рисунок 4.21 – Задание параметров перезагрузки рабочих станций

Возможные типы перезагрузки рабочих станций приведены в пункте ***«Параметры перезагрузки рабочих станций»***.

В следующем окне введите имя создаваемой задачи и сохраните задачу по кнопке ***Создать*** (рисунок 4.22).

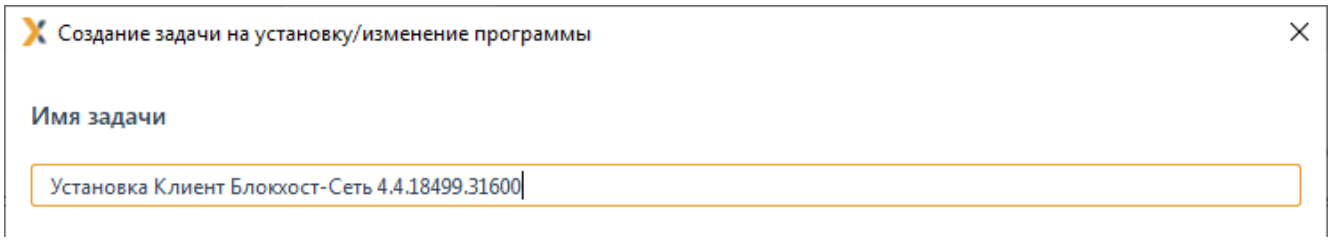


Рисунок 4.22 – Сохранение задачи

В зависимости от установленных параметров планировщика запуск задачи будет осуществлен автоматически или вручную (подробнее в пункте ***«Запуск задачи»***).

Для отслеживания состояния задачи в ходе ее выполнения на рабочей станции, перейдите по ссылке ***Все результаты*** (рисунок 6.2).

По кнопке Описание в верхней части окна (рисунок 6.3) возможен просмотр статуса выполнения задачи.

В результате выполнения задачи по установке клиента Блокхост-Сеть на всех указанных в списке рабочих станциях будет установлен клиент Блокхост-Сеть, в список пользователей которого будут добавлены все локальные пользователи рабочей станции, а также доменные пользователи, профиль которых имеется на рабочей станции.

4.2 Локальная установка клиента

Для локальной установки клиента Блокхост-Сеть на рабочие станции скопируйте с сервера СЗИ на рабочую станцию (или съемный носитель) инсталляционный пакет клиента и запустите его на выполнение.

Подробно локальная установка клиента Блокхост-Сеть описана в документах «Средство

защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство по инсталляции в ОС Windows» и «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство по инсталляции в ОС Linux».

4.3 Установка клиента с помощью сторонних систем развертывания

Для установки клиента Блокхост-Сеть с использованием групповых политик необходимо подготовить файл-установщик для развертывания с использованием сторонних систем.

Перейдите во вкладку ***Пакеты установки***, выберите из списка дистрибутив, содержащий установку клиента Блокхост-Сеть и нажмите на кнопку Создать автономный пакет установки (рисунок 4.23).

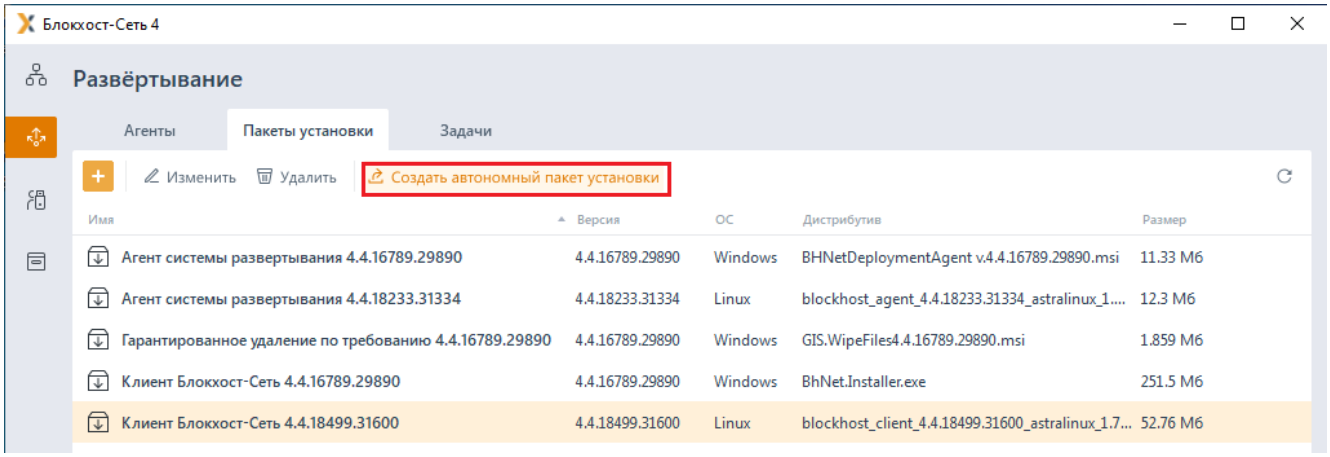


Рисунок 4.23 – Создание автономного пакета для установки сторонними средствами

В открывшемся окне (рисунок 4.24) по кнопке ***Выбрать*** укажите каталог, в который будет сохранен подготовленный пакет и нажмите кнопку ***Создать***.

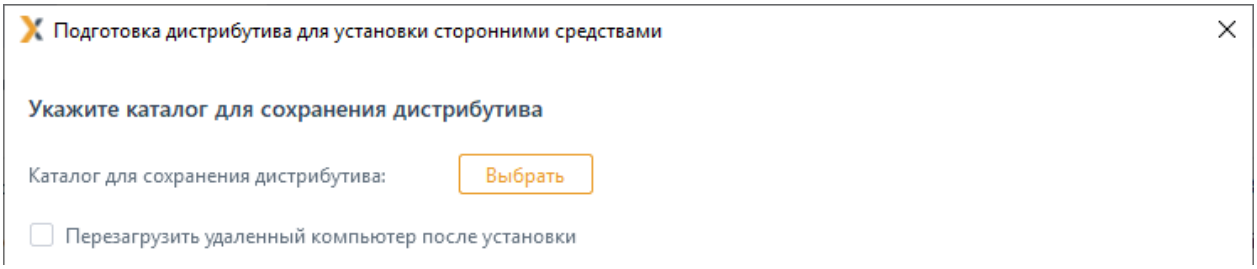


Рисунок 4.24 – Подготовка дистрибутива для установки сторонними средствами

В случае успешного завершения операции подготовки дистрибутива появится окно, содержащее директорию и наименование созданного пакета (рисунок 4.25). Для завершения подготовки инсталляционного пакета нажмите кнопку ***Завершить***.

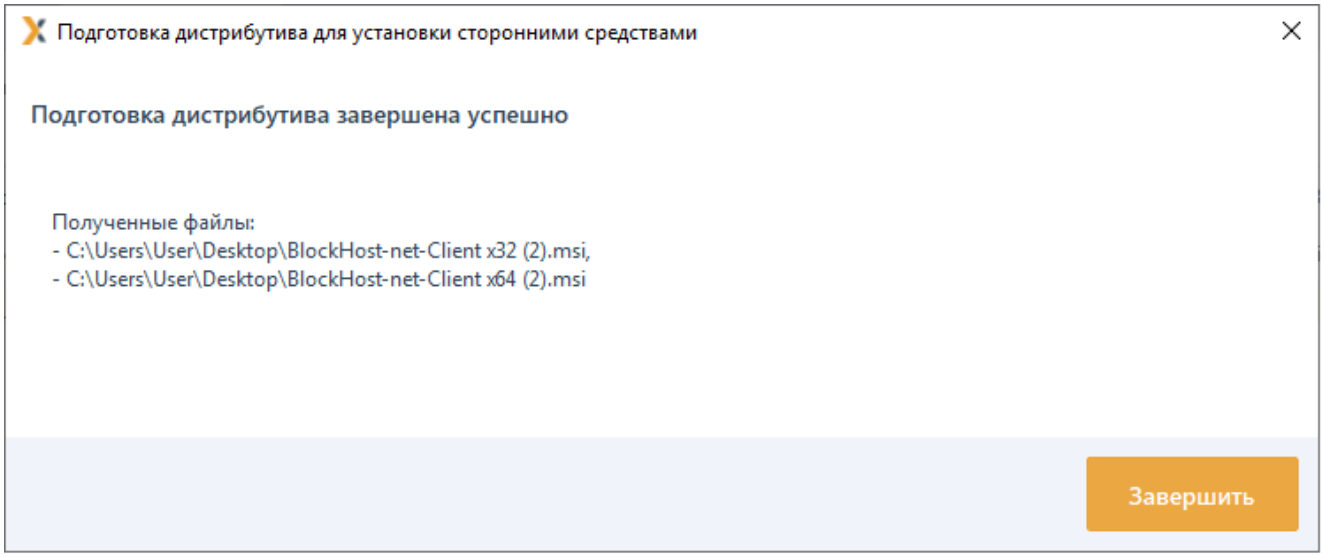


Рисунок 4.25 – Окно завершения подготовки инсталляционного пакета

Дальнейшие действия по установке подготовленного дистрибутива выполняются на контроллере домена в настройках групповых политик в соответствии с документацией на используемое средство.

4.4 Удаление клиента Блокхост-Сеть через подсистему развертывания

Для удаления клиента Блокхост-Сеть на рабочих станциях перейдите во вкладку ***Задачи***, раскройте меню задач по кнопке + и выберите пункт ***Удаление программы*** (рисунок 4.26).

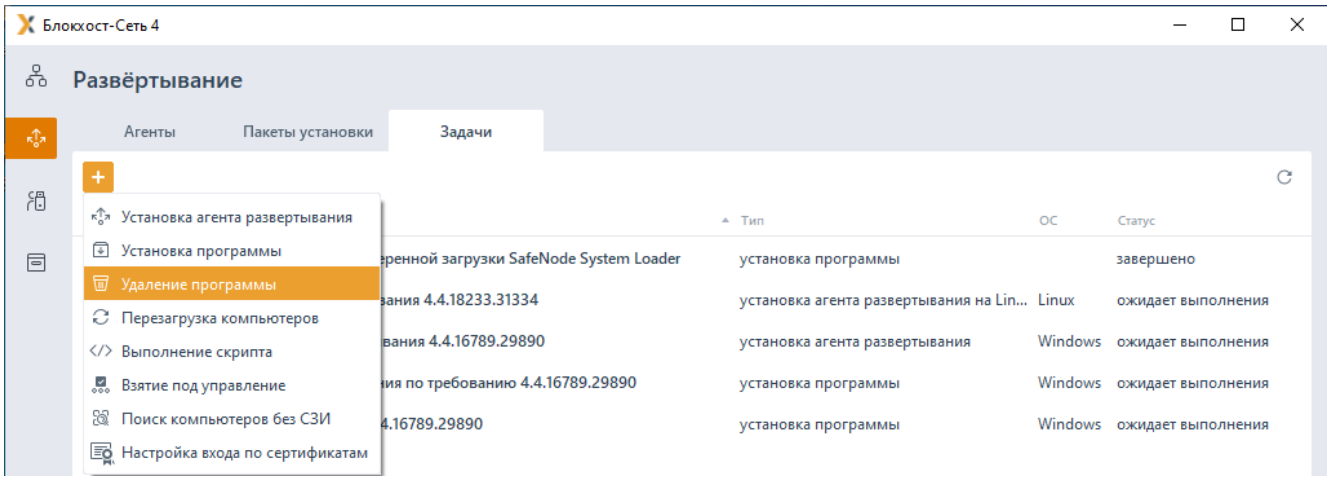


Рисунок 4.26 – Выбор задачи на удаление программы

В открывшемся окне создания задачи на удаление программы (рисунок 4.27) выберите ***Удаление Блокхост-Сеть Клиент.***

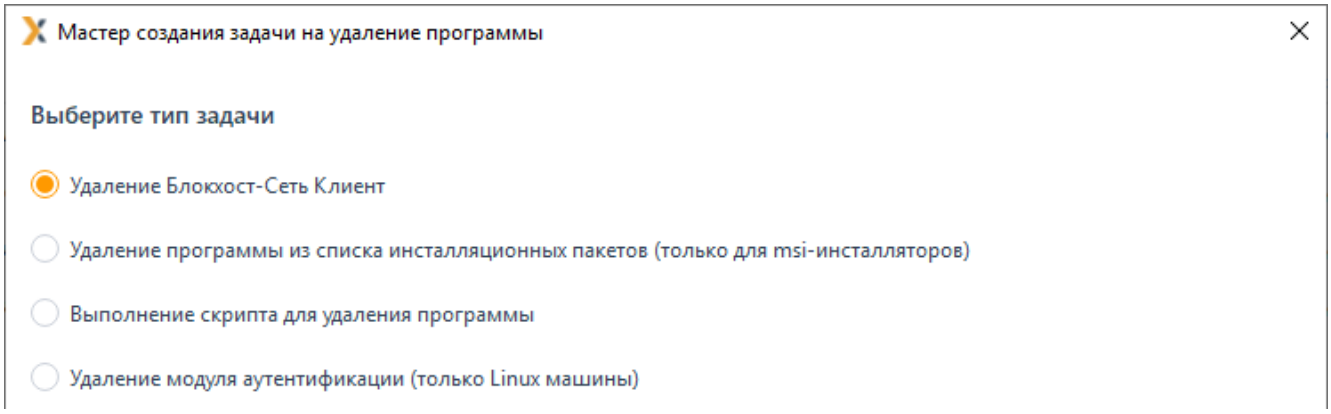


Рисунок 4.27 – Выбор задачи на удаление клиента

После нажатия на кнопку ***Далее*** появится окно выбора рабочих станций, с которых необходимо удалить клиента Блокхост-Сеть (рисунок 4.28). Выберите клиентских рабочие станции для удаления клиента и нажмите ***Далее***.

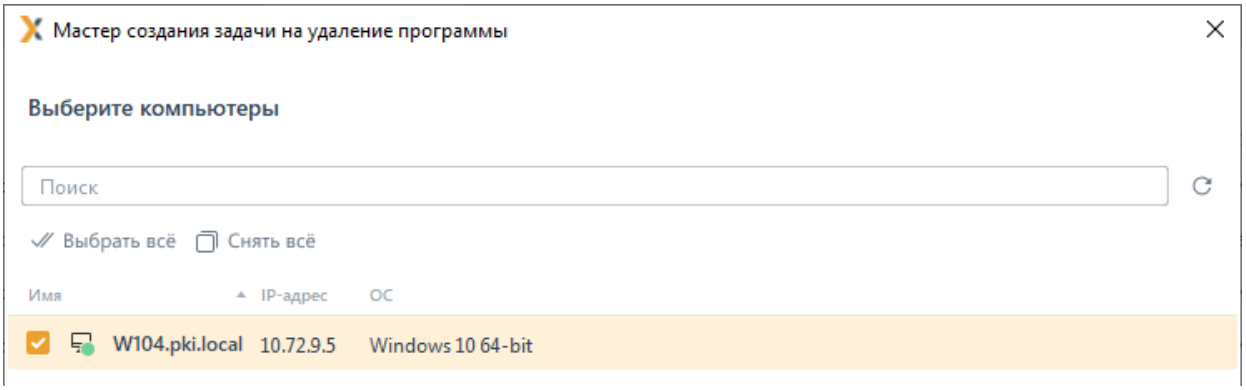


Рисунок 4.28 – Выбор рабочих станций для удаления клиента

Задайте параметры планировщика запуска задачи (подробнее в пункте ***«Указание параметров планировщика задачи по установке агента»***) и определите интервалы времени выполнения задачи.

Укажите параметры перезагрузки рабочих станций после выполнения задачи (подробнее в пункте ***«Параметры перезагрузки рабочих станций»***).

Введите имя создаваемой задачи (рисунок 4.29) и нажмите кнопку ***Создать.***

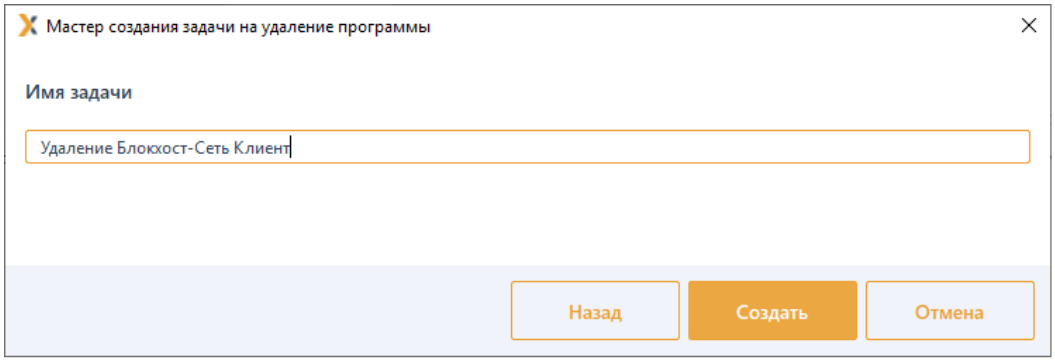


Рисунок 4.29 – Ввод наименования задачи для удаления клиента

В случае успешного завершения создания задачи появится окно с сообщением о создании задачи на удаление клиента Блокхост-Сеть.

В результате во вкладке ***Задачи*** в список задач будет добавлена новая задача, с заданными в ходе работы мастера создания задачи параметрами (рисунок 4.30).

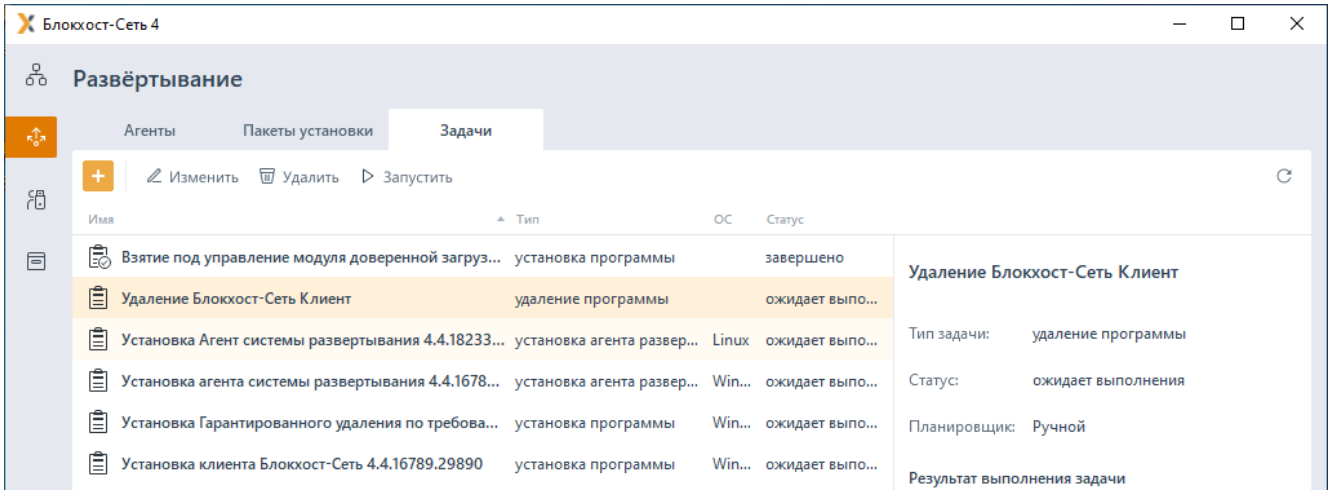


Рисунок 4.30 – Отображение в списке задачи на удаление клиента Блокхост-Сеть

Окончательное удаление компонентов клиентской части СЗИ с рабочей станции произойдет после перезагрузки рабочих станций, в зависимости от выбранных при создании задачи на удаление клиента Блокхост-Сеть параметров перезагрузки.

5 Установка модуля аутентификации клиента Блокхост-Сеть

Установка модуля аутентификации необходима только на рабочих станциях под управлением ОС Linux.

После установки клиента Блокхост-Сеть на рабочие станции под управлением ОС Linux необходимо выполнить установку модуля аутентификации.

Установка модуля аутентификации необходима в том числе для удобства при вводе аутентификационных данных пользователем, т.к. предполагает использование обновленного интерфейса, схожего с интерфейсом ОС Windows (рисунок 5.1).

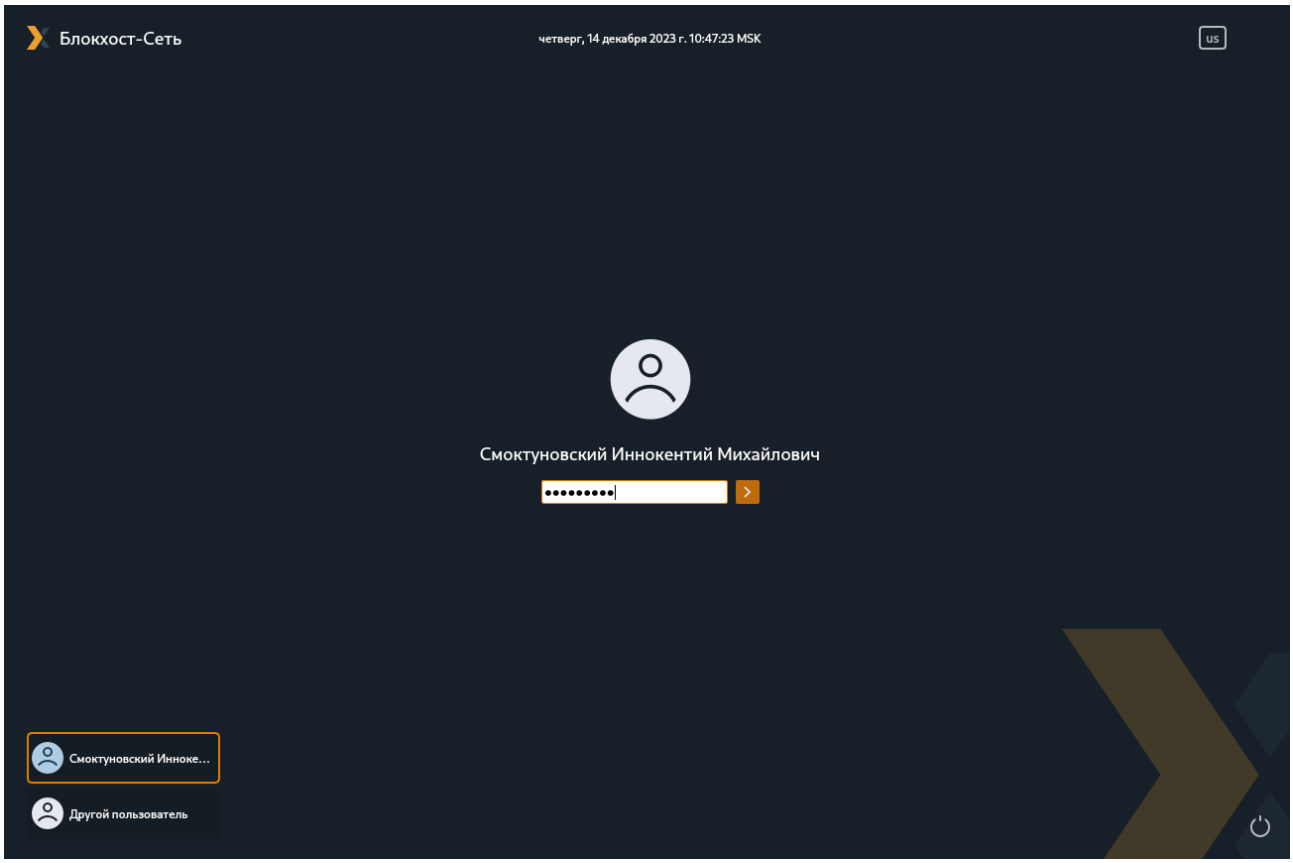


Рисунок 5.1 – Окно входа после установки модуля аутентификации

Модуль аутентификации может быть установлен различными способами:

– с использованием функциональных возможностей подсистемы развертывания;

– локально вручную на клиентской рабочей станции (подробно установка модуля аутентификации локально на рабочей станции описана в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство по инсталляции в ОС Linux»).

5.1 Установка модуля аутентификации с помощью подсистемы развертывания

5.1.1 Установка модуля аутентификации через предустановленную задачу

Для установки модуля аутентификации на рабочие станции перейдите во вкладку ***Задачи*** и внесите корректировки в параметры автоматически созданной задачи ***Установка модуля аутентификации Блокхост-Сеть <номер версии>***, открыв задачу на редактирование по кнопке Изменить в меню или с помощью контекстного меню (рисунок 5.2).

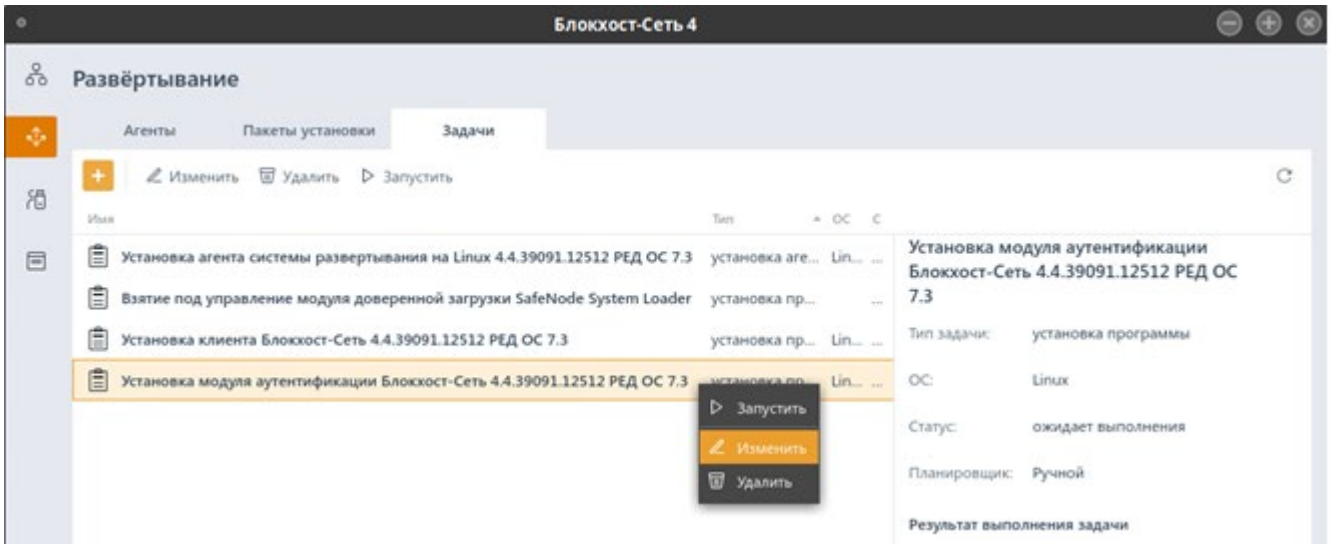


Рисунок 5.2 – Установка модуля аутентификации

5.1.1.1 Формирование списка рабочих станций для установки клиента

В появившемся окне перейдите во вкладку ***Компьютеры*** (рисунок 4.4) и по кнопке + сформируйте список рабочих станций, на которые будет устанавливаться модуль аутентификации.

Список рабочих станций, доступных для установки модуля аутентификации формируется из рабочих станций, на которых уже установлен клиент Блокхост-Сеть.

При формировании списка рабочих станций, возможен экспорт/импорт списка рабочих станций из задачи/в задачу (рисунок 4.5).

Для экспортирования списка рабочих станций, нажмите кнопку ***Экспорт***, при этом весь список рабочих станций, добавленных в задачу, выгрузится в заданный файл по указанному в появившемся окне местоположению (рисунок 4.6).

Для импорта списка рабочих станций в редактируемую задачу, нажмите кнопку ***Импорт*** и в появившемся окне выберите файл, содержащий список импортируемых рабочих станций (рисунок 4.7).

5.1.1.2 Указание параметров планировщика задачи

Перейдите на вкладку ***Планировщик*** (рисунок 4.8) и укажите параметры планировщика для выполнения задачи установки модуля аутентификации на рабочих станциях.

Возможные типы запуска задачи приведены в описании установки агента развертывания в пункте ***«Указание параметров планировщика задачи по установке агента»***.

5.1.1.3 Параметры перезагрузки рабочих станций

Перейдите на вкладку ***Перезагрузка системы*** (рисунок 4.9) и укажите параметры перезагрузки рабочих станций после установки модуля аутентификации на рабочих станциях.

Возможные параметры перезагрузки рабочих станций приведены в описании установки клиента Блокхост-Сеть в пункте ***«Параметры перезагрузки рабочих станций»***.

5.1.1.4 Сохранение изменений, внесенных в задачу

Для сохранения внесенных в задачу по установке модуля аутентификации, последовательно нажмите кнопки ***Применить*** и ***ОК*** (рисунок 5.3).

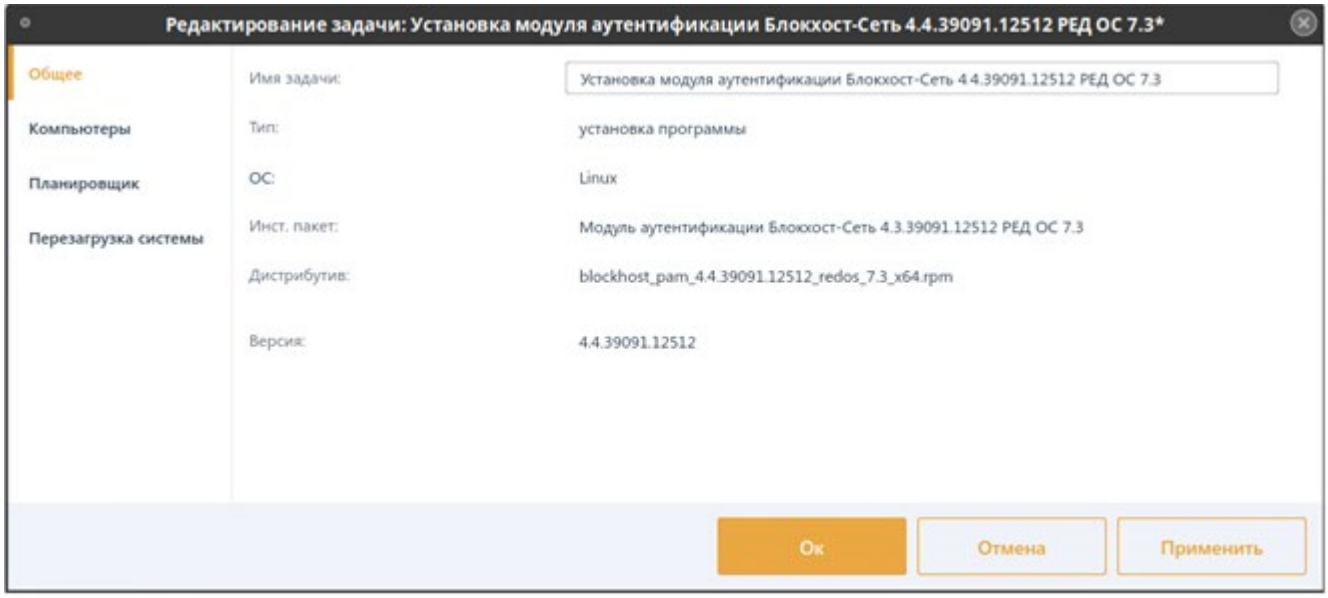


Рисунок 5.3 – Сохранение изменений в задаче

Нажатие на кнопку ***Отмена*** позволит выйти из окна редактирования параметров задачи без внесения изменений.

5.1.1.5 Запуск задачи по установке модуля аутентификации

В зависимости от установленных параметров планировщика запуск задачи будет осуществлен автоматически или вручную (подробнее в пункте ***«Запуск задачи»***).

Для отслеживания состояния задачи в ходе ее выполнения на рабочей станции, перейдите по ссылке ***Все результаты*** (рисунок 6.2).

По кнопке Описание в верхней части окна (рисунок 6.3) возможен просмотр статуса выполнения задачи.

В результате выполнения задачи по установке модуля аутентификации на всех указанных в списке рабочих станциях будет установлен модуль аутентификации.

5.1.2 Установка модуля аутентификации с помощью пакетов установки

Установка модуля аутентификации на клиентские рабочие станции под управлением ОС, отличной от ОС сервера, осуществляется с помощью пакетов установки.

Перед установкой модуля аутентификации на рабочие станции необходимо сформировать пакет установки модуля аутентификации требующейся ОС клиента с помощью подсистемы развертывания.

Для формирования пакета установки перейдите во вкладку ***Пакеты установки*** по кнопке (рисунок 4.12).

По кнопке запустите создание пакета установки с помощью мастера создания пакетов установки (рисунок 4.13).

По кнопке ***Выбрать*** из списка выберите дистрибутив, содержащий установку модуля аутентификации в зависимости от используемой ОС (ниже приведен пример установки модуля аутентификации для ОС Astra Linux «Смоленск» 1.7) (рисунок 5.4).

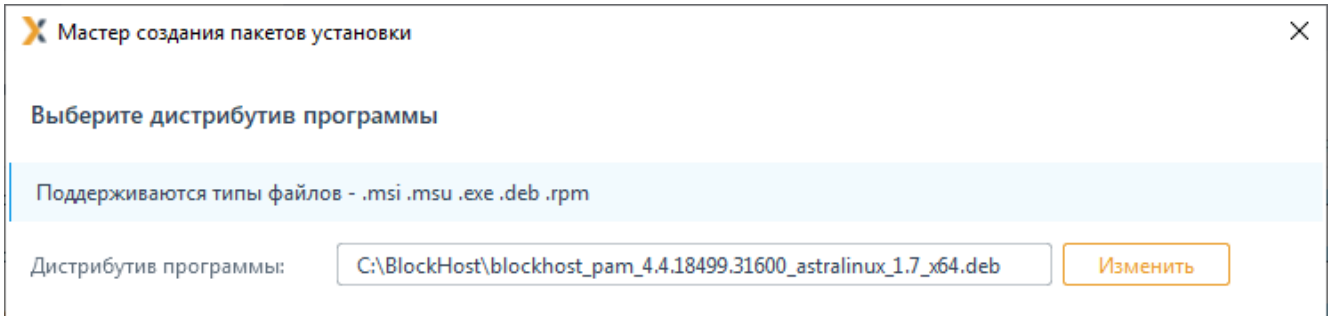


Рисунок 5.4 – Выбор пакета установки

Задайте имя создаваемого пакета (рисунок 5.5).

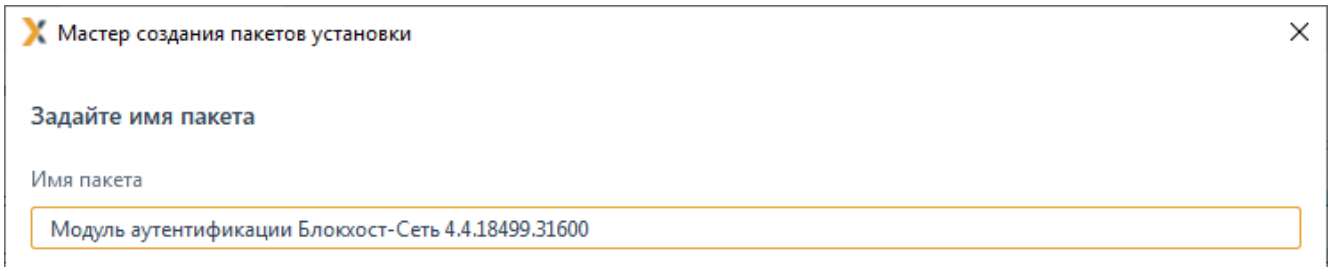


Рисунок 5.5 – Ввод имени пакета установки

По окончанию создания пакета установки, в списке появится новый пакет с заданным именем (рисунок 5.6).

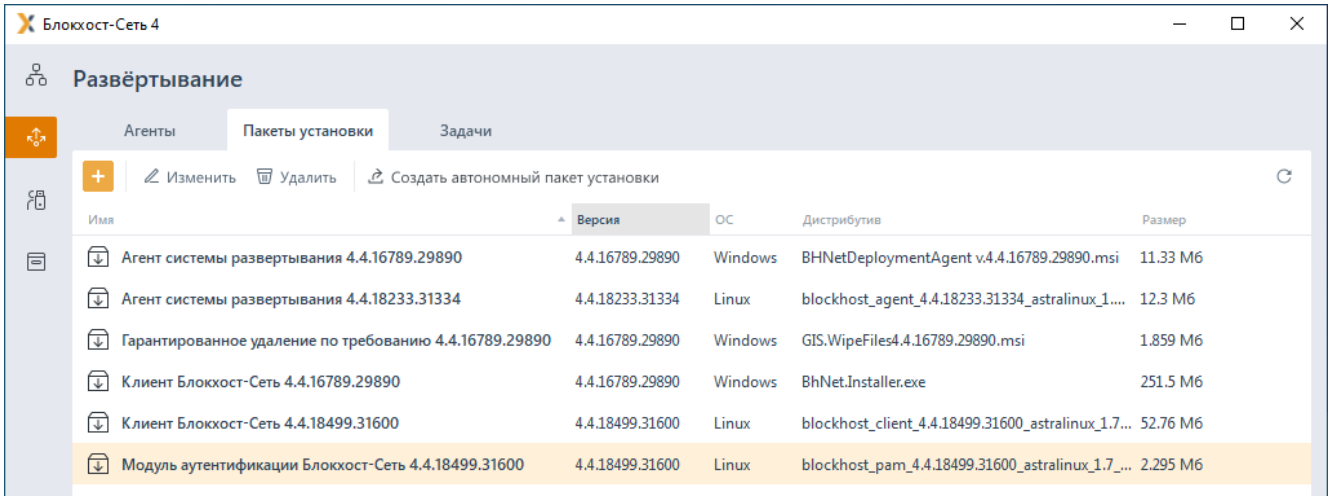


Рисунок 5.6 – Отображение созданного пакета установки в списке

Для создания задачи на установку модуля аутентификации на рабочие станции с помощью созданного пакета перейдите во вкладку ***Задачи***, раскройте меню создания задач по кнопке + и выберите пункт ***Установка программы*** (рисунок 4.17).

В открывшемся окне создания задачи на установку (рисунок 5.7) выберите созданный на предыдущем шаге пакет установки и нажмите кнопку ***Далее***.

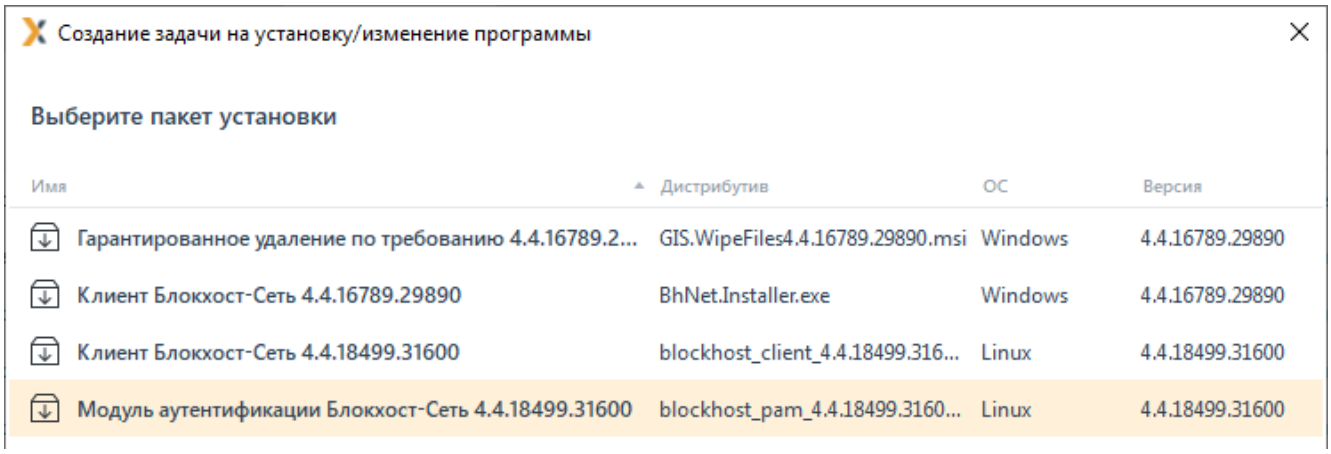


Рисунок 5.7 – Выбор пакета установки

В следующем окне (рисунок 4.19) выберите рабочие станции с установленным клиентом Блокхост-Сеть, на которые будет устанавливаться модуль аутентификации.

В следующем окне (рисунок 4.20) укажите параметры планировщика для выполнения задачи установки модуля аутентификации на рабочих станциях.

Возможные типы запуска задачи приведены в описании установки агента развертывания в пункте ***«Указание параметров планировщика задачи по установке агента»***.

В следующем окне (рисунок 4.21) укажите параметры перезагрузки рабочих станций.

Возможные типы перезагрузки рабочих станций приведены в пункте ***«Параметры перезагрузки рабочих станций»***.

В следующем окне введите имя создаваемой задачи и сохраните задачу по кнопке ***Создать*** (рисунок 5.8).

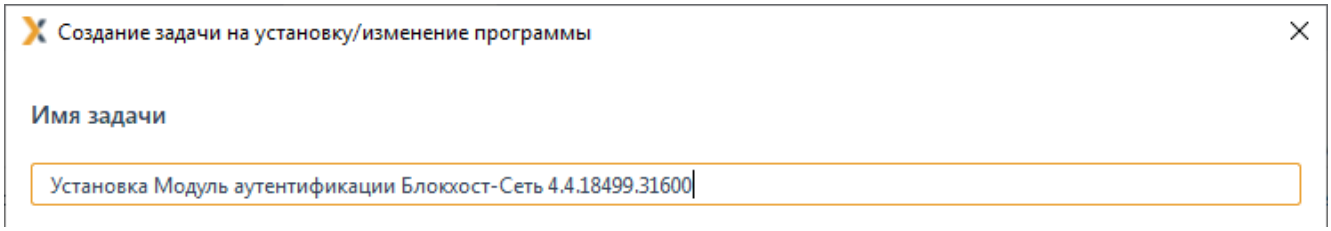


Рисунок 5.8 – Сохранение задачи

В зависимости от установленных параметров планировщика запуск задачи будет осуществлен автоматически или вручную (подробнее в пункте ***«Запуск задачи»***).

Для отслеживания состояния задачи в ходе ее выполнения на рабочей станции, перейдите по ссылке ***Все результаты*** (рисунок 6.2).

По кнопке Описание в верхней части окна (рисунок 6.3) возможен просмотр статуса выполнения задачи.

В результате выполнения задачи по установке модуля аутентификации на всех указанных в списке рабочих станциях будет установлен модуль аутентификации.

5.2 Локальная установка модуля аутентификации

Для локальной установки модуля аутентификации на рабочие станции скопируйте с сервера СЗИ на рабочую станцию (или съемный носитель) инсталляционный пакет модуля аутентификации и запустите его на выполнение.

Подробно локальная установка модуля аутентификации описана в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство по инсталляции в ОС Linux».

5.3 Удаление модуля аутентификации

Для удаления модуля аутентификации с рабочих станциях перейдите во вкладку ***Задачи***, раскройте меню задач по кнопке + и выберите пункт ***Удаление программы*** (рисунок 5.9).

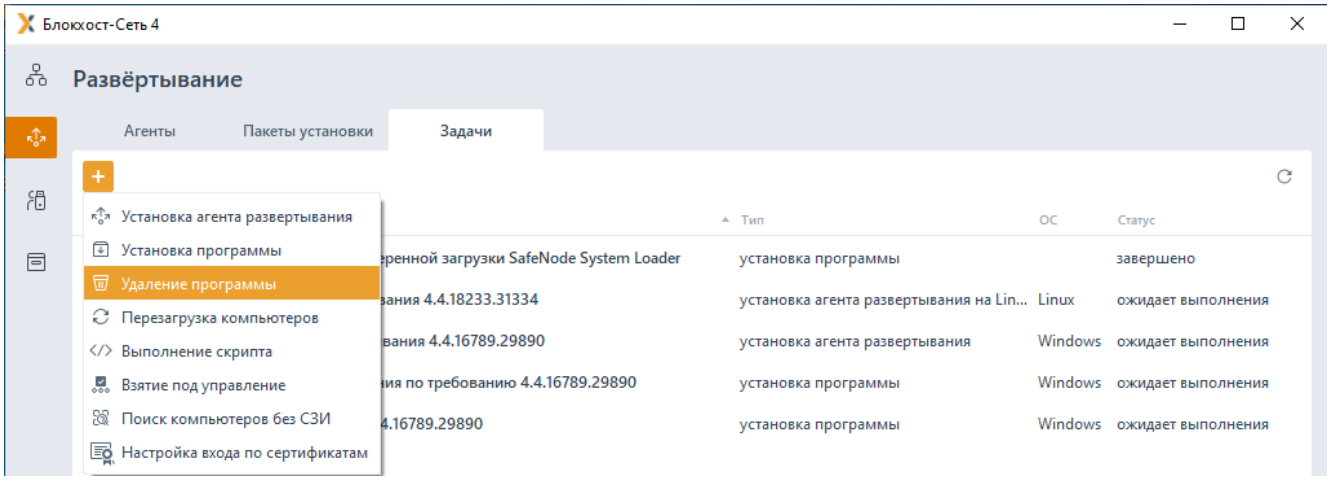


Рисунок 5.9 – Выбор задачи на удаление программы

В открывшемся окне создания задачи на удаление программы (рисунок 5.10) выберите ***Удаление модуля аутентификации (только Linux машины).***

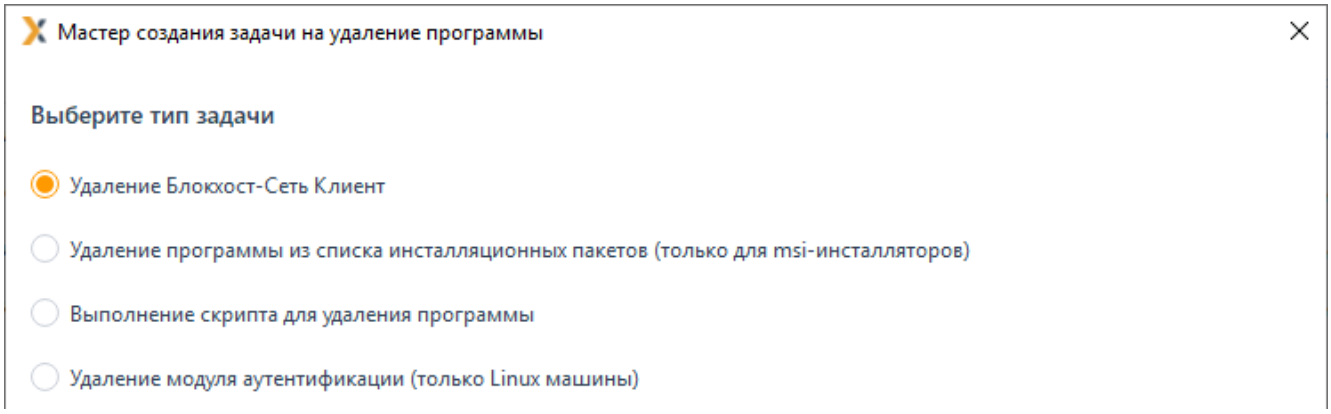


Рисунок 5.10 – Выбор задачи на удаление модуля аутентификации

После нажатия на кнопку ***Далее*** появится окно выбора рабочих станций, с которых необходимо удалить модуль аутентификации (рисунок 5.11). Выберите клиентских рабочие станции для удаления модуля аутентификации и нажмите ***Далее***.

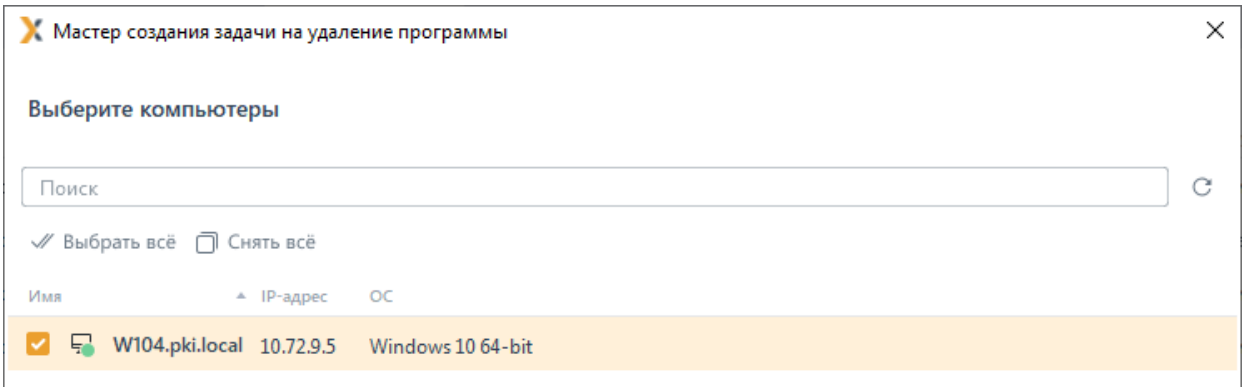


Рисунок 5.11 – Выбор рабочих станций для удаления модуля аутентификации

Задайте параметры планировщика запуска задачи (подробнее в пункте ***«Указание***

параметров планировщика задачи по установке агента») и определите интервалы времени выполнения задачи.

Укажите параметры перезагрузки рабочих станций после выполнения задачи (подробнее в пункте ***«Параметры перезагрузки рабочих станций»***).

Введите имя создаваемой задачи (рисунок 5.12) и нажмите кнопку ***Создать.***

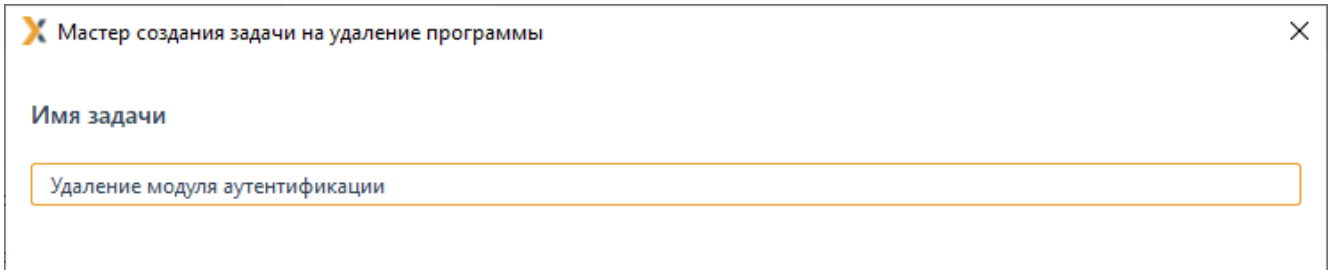


Рисунок 5.12 – Ввод наименования задачи

В случае успешного завершения создания задачи появится окно с сообщением о создании задачи на удаление модуля аутентификации.

В результате во вкладке ***Задачи*** в список задач будет добавлена новая задача, с заданными в ходе работы мастера создания задачи параметрами (рисунок 5.13).

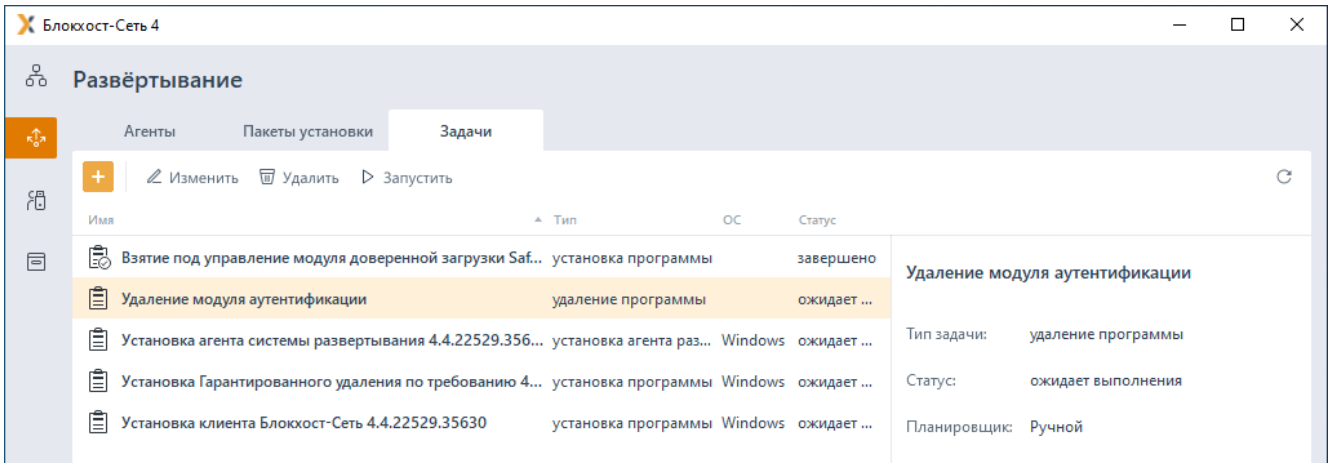


Рисунок 5.13 – Отображение в списке задачи на удаление модуля аутентификации

Окончательное удаление модуля аутентификации с рабочей станции произойдет после перезагрузки рабочих станций, в зависимости от выбранных при создании задачи на удаление модуля аутентификации параметров перезагрузки.

6 Запуск задачи

Запуск любого типа задач на выполнение возможен только на рабочих станциях с установленным агентом развертывания.

При выделении задачи в списке, в правой части вкладки отобразится подробная информация о выбранной задаче (рисунок 6.1):

– ***Тип задачи*** – какая задача была запущена на выполнение (установка агента развертывания, установка программы, удаление программы, перезагрузка компьютера, выполнение скрипта);

– ***Статус*** – в каком статусе находится выполнение задачи в данный момент времени (ожидает выполнения, выполняется, останавливается, завершено);

– ***Планировщик*** – как запланирован запуск задачи на выполнение (вручную, сразу после создания, по времени, периодически по расписанию, по завершению другой задачи);

– ***Результат выполнения задачи*** – чем завершилось выполнение задачи (требуется перезагрузка; выполняется; успешно завершено; завершено с предупреждением; завершено с ошибкой; недоступны; ожидает выполнения).

В зависимости от установленных параметров планировщика запуск задачи может быть осуществлен автоматически или вручную.

Для запуска задачи вручную выделите нужную задачу в списке и нажмите в меню кнопку ▷ Запустить или нажмите кнопку ***Запустить*** в открывшейся панели справа (рисунок 6.1).

Любую задачу, имеющую статус *Ожидает выполнения* или *Завершено*, независимо от установленных параметров планировщика, можно запустить вручную.

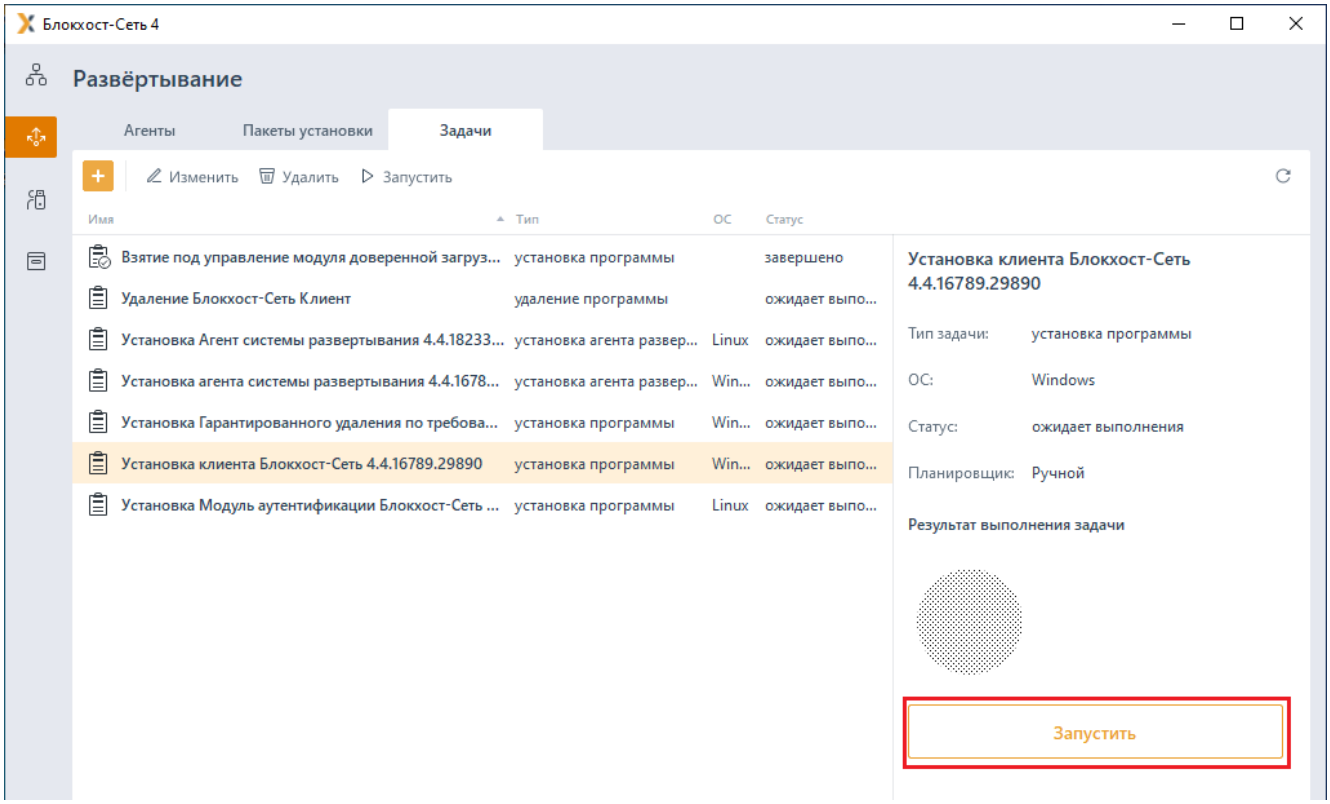


Рисунок 6.1 – Запуск задачи

6.1 Результаты выполнения задачи

Результатов выполнения задачи может быть несколько в одной задаче в зависимости от количества рабочих станций в задаче. Каждый результат является ссылкой, переход по которой открывает окно просмотра операций, выполненных в ходе выполнения задачи (рисунок 6.3). Результаты выполнения задачи и его описание, приведены в таблице 6.1.

Таблица 6.1 – Результат выполнения задачи

Результат выполнения задачи	**Описание установленного результата выполнения задачи**
Завершено с ошибкой	• выполнение задачи любого типа на рабочей станции завершилось ошибкой; • при установке клиента Блокхост-Сеть было обнаружено, что на рабочей станции не выполняются требования по установке; • выполнение задачи было остановлено (нажата кнопка ***Остановить***), когда процесс установки программы на рабочей станции уже был запущен.
Недоступны	• не удалось установить связь с рабочей станцией, чтобы начать выполнение задачи.
Завершено с предупреждением	• в параметрах перезагрузки задачи выбран параметр «не перезагружать компьютер»; после завершения инсталляции/деинсталляции программное обеспечение затребовало перезагрузку; • выполнение задачи было остановлено (нажата кнопка ***Остановить***) на этапе, когда задача для рабочей станции была завершена со статусом

	Требуется перезагрузка (установка программы на рабочей станции успешно завершена, однако, в соответствии с настройками задачи, необходима перезагрузка рабочей станции); • на рабочей станции не установлен клиент Блокхост-Сеть (возникновение события возможно при выполнении задачи на удаление клиента Блокхост-Сеть).
Успешно завершено	• выполнение задачи любого типа на рабочей станции успешно завершено.
Выполняется	• процесс выполнения задачи на рабочей станции был начат, но еще не закончен.
Требуется перезагрузка	• установлен параметр перезагрузки рабочей станции при создании задачи на установку (удаление) ПО рабочей станции ***Перезагружать компьютер как можно скорее*** или ***Уведомить пользователя о необходимости перезагрузки***.
Ожидает выполнения	• задача еще не выполнялась на рабочих станциях, имеющих данный статус; • выполнение задачи было остановлено (нажата кнопка ***Остановить***) на этапе копирования инсталляционного файла на рабочую станцию.
Останавливается	• нажата кнопка ***Остановить***; идет процесс остановки задачи.

Для отслеживания состояния задачи в ходе ее выполнения на рабочей станции, перейдите по одной из имеющихся ссылок <*статус задачи*>, либо по ссылке ***Все результаты*** (рисунок 6.2).

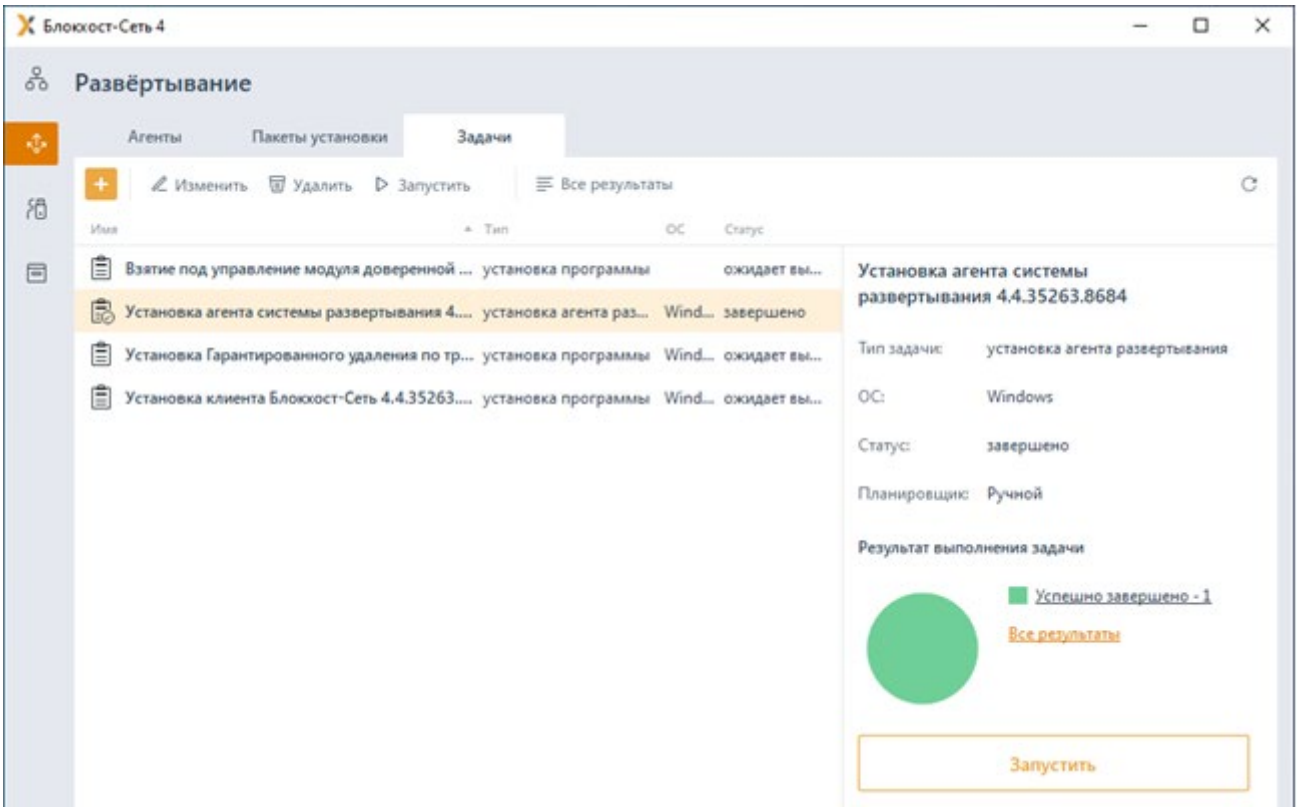


Рисунок 6.2 – Результат выполнения задачи

В верхней части окна просмотра результатов (рисунок 6.3), выделите нужную рабочую

станцию, после чего в нижней части окна отобразится история операций, выполненных на рабочей станции в ходе выполнения задачи.

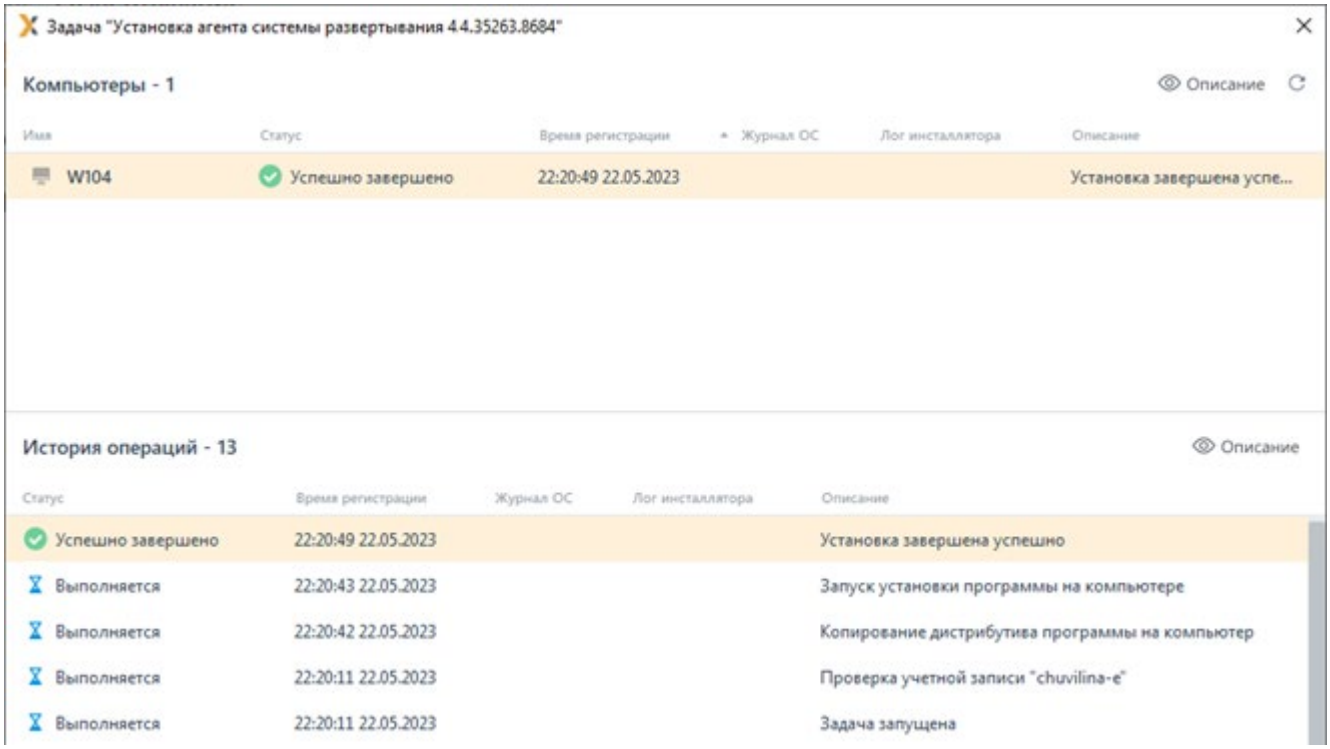


Рисунок 6.3 – Просмотр результатов выполнения задачи

По кнопке Описание в верхней части окна (рисунок 6.3) возможен просмотр статуса выполнения задачи.

При возникновении ошибки в ходе выполнения задачи на рабочей станции под управлением ОС Windows, дополнительную информацию о причине возникновения ошибки можно получить из:

– фрагмента журнала Windows, относящегося к выполняемой задаче;

– журнала файла-установщика программного обеспечения (лог инсталлятора).

Эти журналы собираются агентом развертывания на клиентской рабочей станции и передаются на сервер подсистемы развертывания.

Просмотр журналов доступен в окне просмотра результатов выполнения задачи по ссылке ***Все результаты*** (рисунок 6.2). В истории операций у операции, завершившейся ошибкой, в столбцах ***Журнал ОС*** и/или ***Лог инсталлятора*** появится индикатор , это означает возможность просмотра журнала ОС Windows и лога инсталлятора с помощью соответствующих кнопок в верхней части окна и сохранение их в указанную директорию в виде текстового файла (рисунок 6.4).

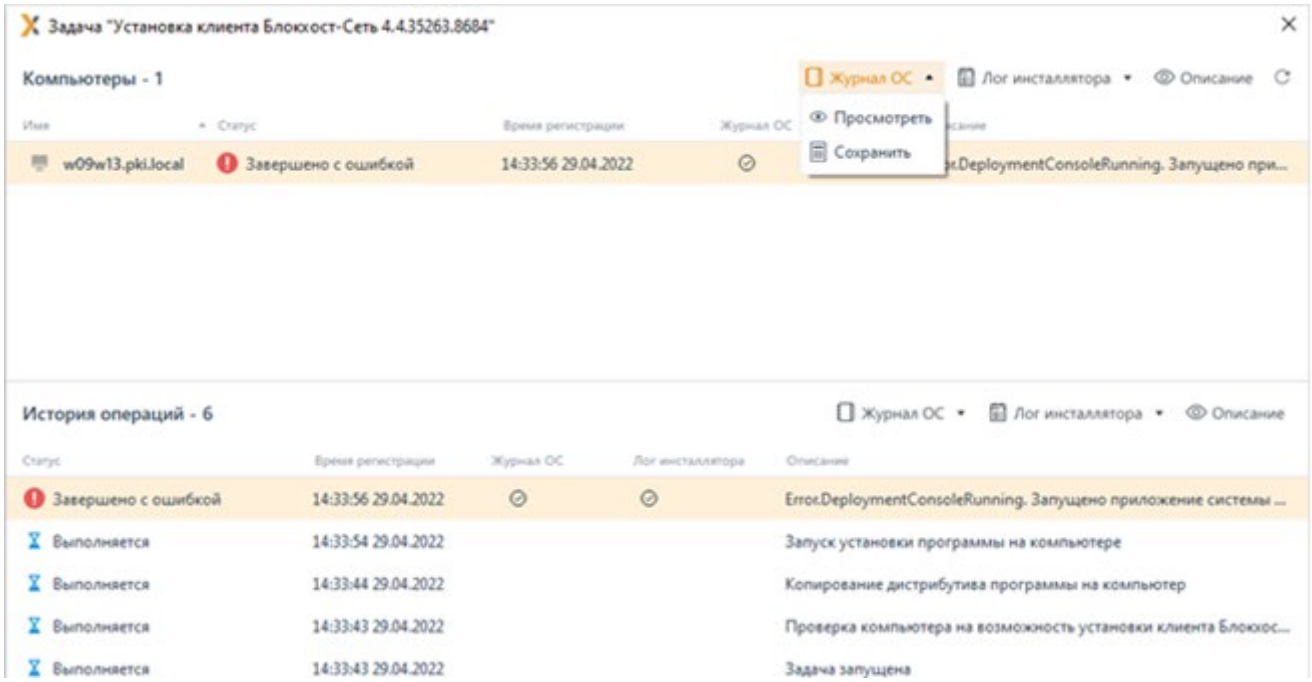


Рисунок 6.4 – Просмотр журнала ОС и лога инсталлятора в истории операций

При возникновении ошибки в ходе выполнения задачи на рабочей станции под управлением ОС Linux, дополнительную информацию о причине возникновения ошибки можно получить из журнала файла-установщика программного обеспечения (лог инсталлятора), который является объединением вывода в потоки *stdout* и *stderr*.

Эти журналы собираются агентом развертывания на клиентской рабочей станции и передаются на сервер подсистемы развертывания (рисунок 6.5).

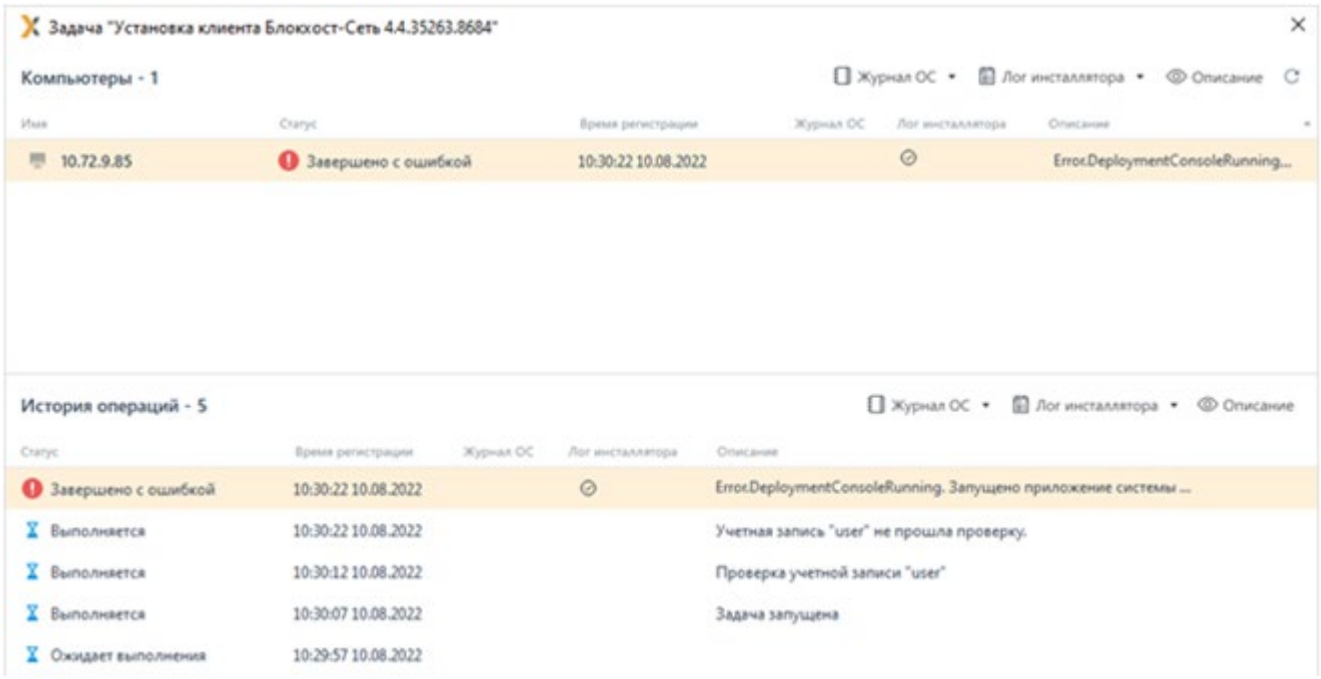


Рисунок 6.5 – Просмотр лога инсталлятора в истории операций

6.2 Остановка задачи

Выполнение задачи может быть прервано на любом этапе своего выполнения. Для остановки задачи необходимо в панели выполнения задачи нажать кнопку ***Остановить*** (рисунок 6.6).

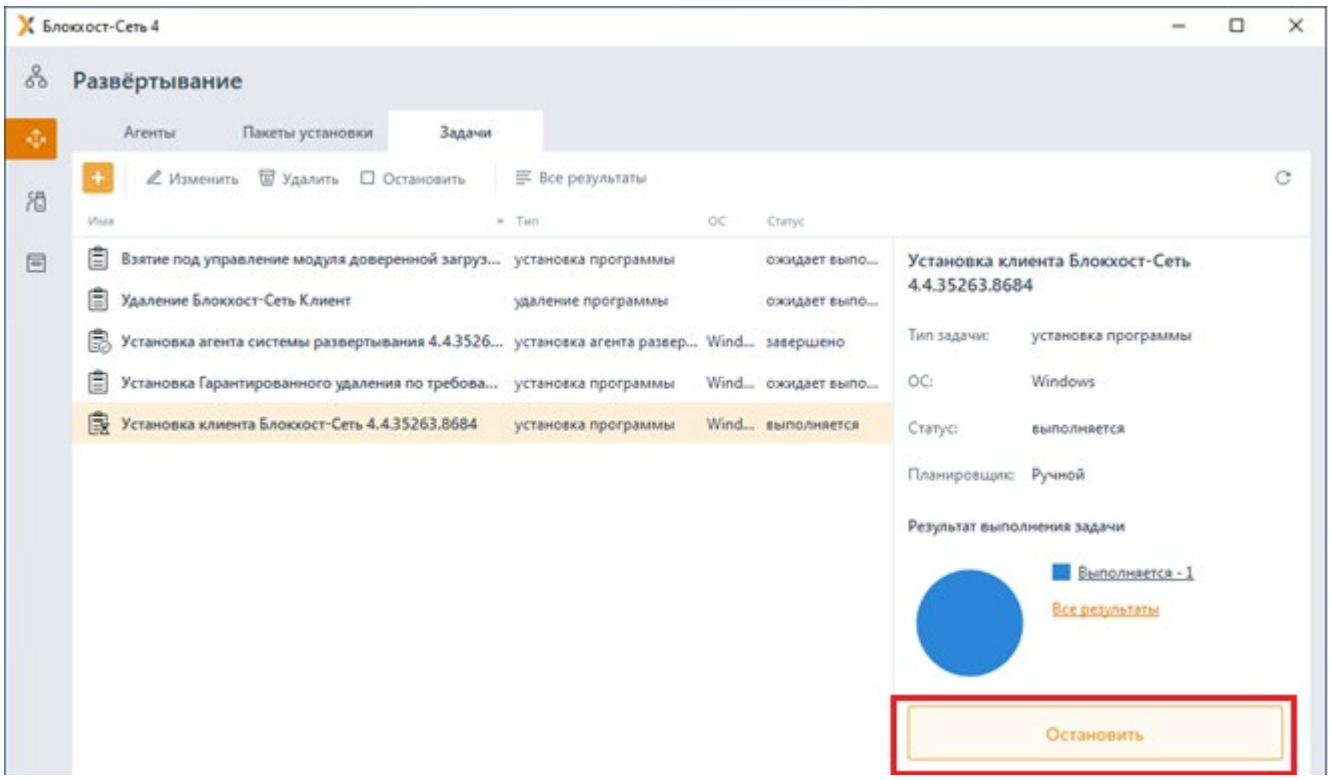


Рисунок 6.6 – Остановка задачи

В зависимости от этапа выполнения, реакция на прерывание будет различной. Описание возможных реакций приведено в таблице 6.2.

Таблица 6.2 – Остановка задачи

Операция, выполняемая на рабочей станции на момент остановки задачи	**Результат остановки задачи**
Рабочая станция ожидает своей очереди для начала выполнения задачи. Никаких операций не выполняется. Статус задачи: *ожидает выполнения*	На рабочей станции не происходит каких-либо изменений. Статус задачи: *ожидает выполнения*
На рабочую станцию выполняется копирование файла-установщика программы. Статус задачи: *выполняется*	На рабочей станции не происходит каких-либо изменений. Процесс установки программы еще не был запущен. Статус задачи: *ожидает выполнения*
На рабочей станции запущен процесс установки (удаления) программы.	Остановка задачи не приводит к прерыванию процесса установки программы на рабочей станции. Установка программы либо завершается

Статус задачи: *выполняется*	естественным путем, либо прекращается в случае превышения временного интервала, заданного в планировщике задачи ***Прервать установку программы на рабочей станции, если инсталлятор не активен дольше*** (рисунок 6.20). Статус задачи: *завершено с ошибкой*
Выполняется ожидание перезагрузки клиентской рабочей станции. Статус задачи: *требуется перезагрузка*	Остановка задачи не приводит к прерыванию выдачи уведомления пользователю о необходимости выполнения перезагрузки. Однако при назначении следующей задачи на эту же рабочую станцию параметры перезагрузки новой задачи будут иметь приоритет. Статус задачи: *завершено с предупреждением*
Установка (удаление) программы завершено. Перезагрузка, в случае необходимости ее выполнения, была выполнена. Статус задачи: *успешно завершено, завершено с ошибкой, завершено с предупреждением, недоступен*	На рабочей станции не происходит каких-либо изменений. Статус остается без изменений.

7 Вкладка «Агенты развертывания»

Во вкладке ***Агенты*** (рисунок 7.1) расположен список рабочих станций, на которых установлена и запущена служба агента подсистемы развертывания (*GIS.Client.DeploymentSystem*).

В верхней части вкладки расположены следующие элементы управления:

– кнопка позволяет обновить список рабочих станций и увидеть текущее состояние клиентских рабочих станций, на которых запущена служба агента подсистемы развертывания;

– кнопка , открывающая строку поиска, предназначенную для отбора клиентских рабочих станций, в соответствии со значением, введенным в строку поиска.

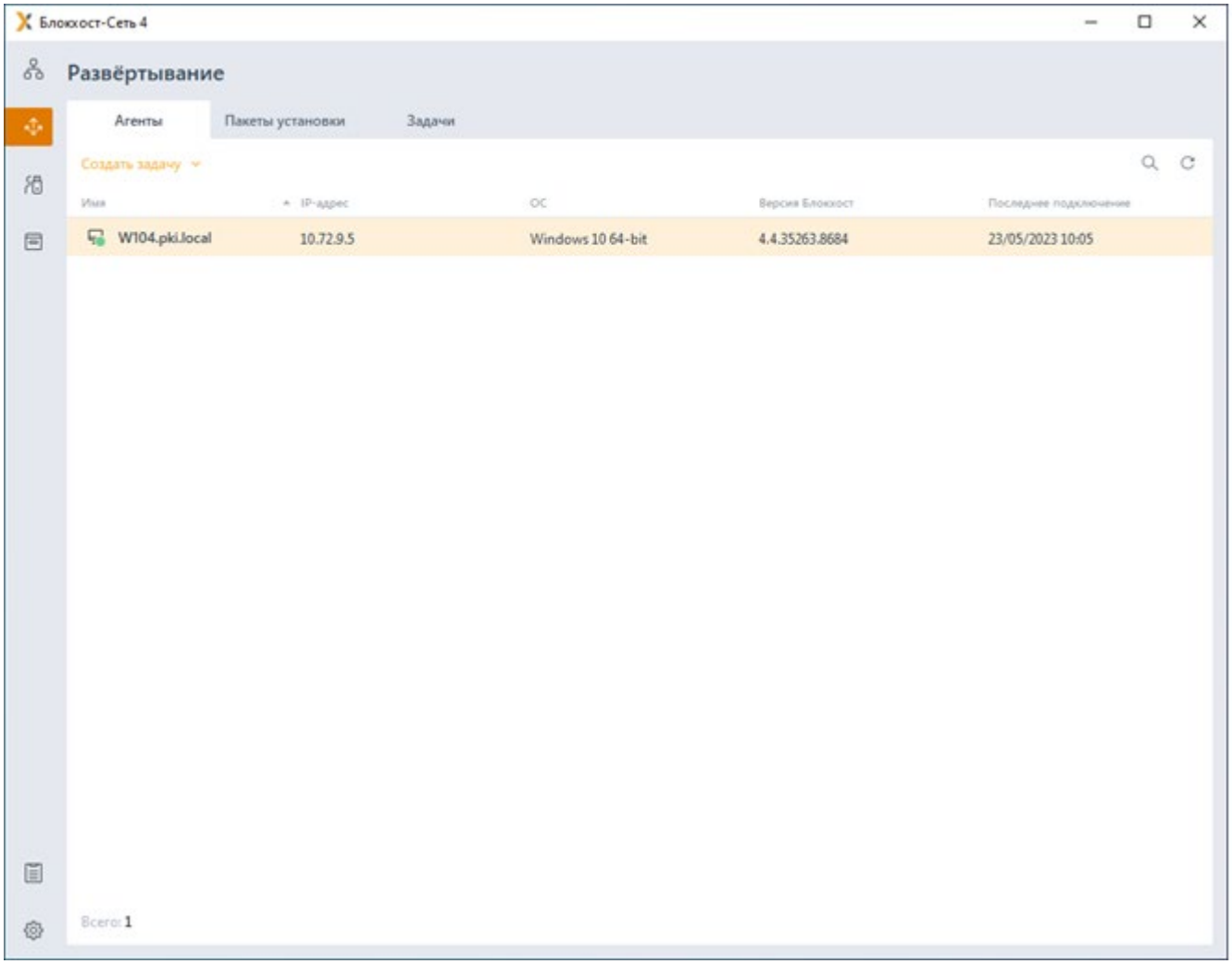


Рисунок 7.1 – Вкладка ***Агенты***

Для каждой рабочей станции из списка во вкладке ***Агенты*** доступно контекстное меню, открываемое по щелчку правой кнопкой мыши на строке с именем рабочей станции, в

котором содержатся следующие пункты (рисунок 7.2):

– ***Проверить соединение*** – проверка соединения с выбранной рабочей станцией (со службой агента развертывания);

– ***Создать задачу*** – создание задачи на установку, удаление программы, перезагрузку рабочей станции или выполнение скрипта;

– ***Копировать DNS-имя*** – копирование имени рабочей станции;

– ***Удалить*** – удаление выбранной рабочей станции из списка вкладки ***Агенты***. Рабочая станция снова появится во вкладке после ее перезагрузки или перезапуска на ней службы агента подсистемы развертывания (*GIS.Client.DeploymentSystem*).

При выделении группы рабочих станций контекстное меню содержит пункты: ***Создать задачу, Копировать*** и ***Удалить***.

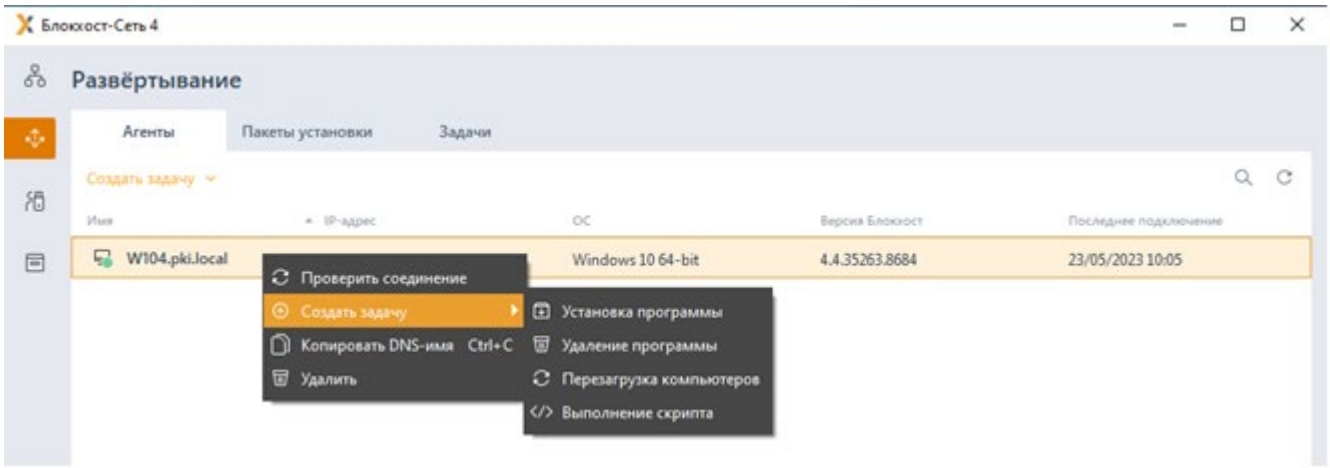


Рисунок 7.2 – Контекстное меню рабочей станции вкладки ***Агенты***

8 Вкладка «Пакеты установки»

Во вкладке ***Пакеты установки*** (рисунок 8.1) содержится список созданных в подсистеме развертывания инсталляционных пакетов ПО.

В верхней части вкладки расположены следующие элементы управления:

– кнопка + для создания нового пакета установки с помощью мастера по добавлению установщика в подсистему развертывания.

– кнопка Изменить для редактирования инсталляционных пакетов, созданных в подсистеме развертывания.

– кнопка Удалить для удаления инсталляционных пакетов, созданных в подсистеме развертывания.

– кнопка Создать автономный пакет установки позволяет подготовить файл-установщик для развертывания сторонними средствами.

– кнопка ↻ позволяет обновить список созданных в подсистеме развертывания инсталляционных пакетов.

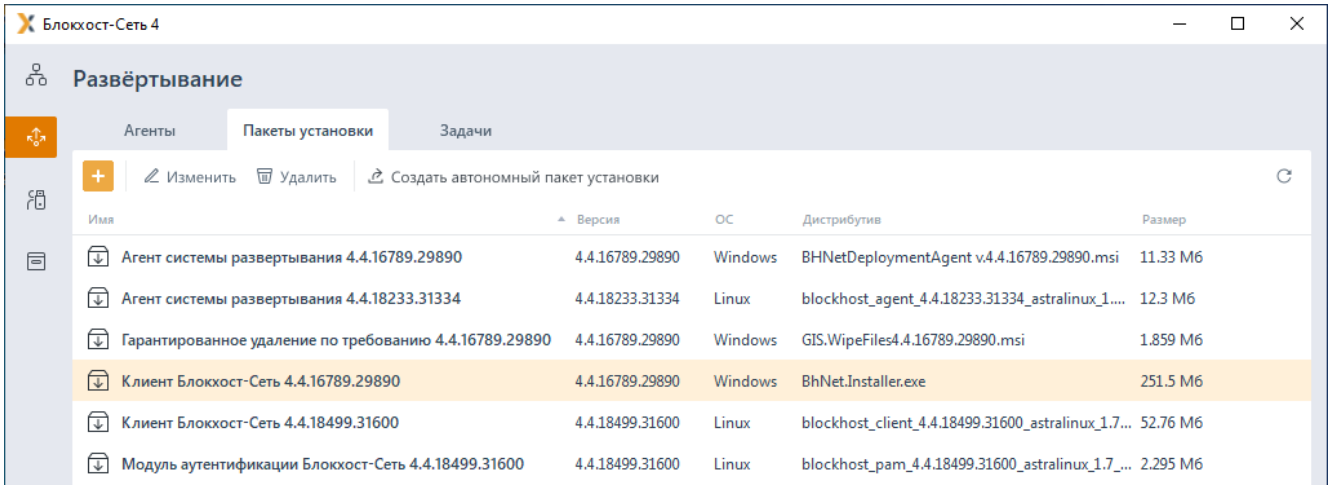


Рисунок 8.1 – Вкладка ***Пакеты установки***

При установке серверной части СЗИ во вкладке ***Пакеты установки*** автоматически создаются инсталляционные пакеты, содержащие в себе все необходимые параметры установки:

– ***Агент системы развертывания <номер_версии>;***

– ***Клиент Блокхост-Сеть <номер_версии>;***

– ***Гарантированное удаление по требованию <номер_версии>.***

Необходимо учитывать, что автоматически создаются инсталляционные пакеты для той же ОС, под управлением которой находится сервер СЗИ.

8.1 Создание инсталляционных пакетов

Перед установкой ПО на рабочие станции с помощью подсистемы развертывания, необходимо чтобы на сервере был создан инсталляционный пакет – пакет, содержащий в себе сведения о файле-установщике программного обеспечения и параметрах командной строки по установке этого программного обеспечения.

При создании инсталляционных пакетов необходимо учитывать следующее ограничение: если серверная часть Блокхост-Сеть установлена на ОС Linux, создание автономных пакетов для ОС Windows не поддерживается.

Файл-установщик программного обеспечения в обязательном порядке должен поддерживать возможность «тихой» (скрытой) установки. Установку программного обеспечения в интерактивном режиме подсистема развертывания не поддерживает.

Для создания установочного пакета перейдите во вкладку ***Пакеты установки*** и нажмите кнопку + (рисунок 8.1).

В открывшемся окне мастера по созданию пакетов установки (рисунок 8.2) нажмите кнопку ***Выбрать*** для выбора файла дистрибутива программного обеспечения с расширением **.msi*, **.msu* или **.exe*.

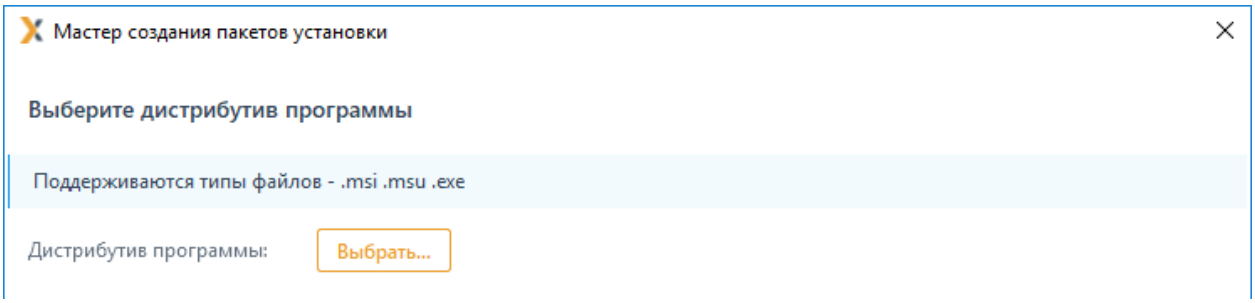


Рисунок 8.2 – Окно мастера по созданию инсталляционного пакета

После выбора файла дистрибутива программного обеспечения при необходимости, добавьте в открывшееся поле ввода параметры командной строки (рисунок 8.3).

Для файла-установщика в формате **.exe* ввод параметров «тихой» установки является обязательным – установку программного обеспечения в интерактивном режиме подсистема развертывания не поддерживает.

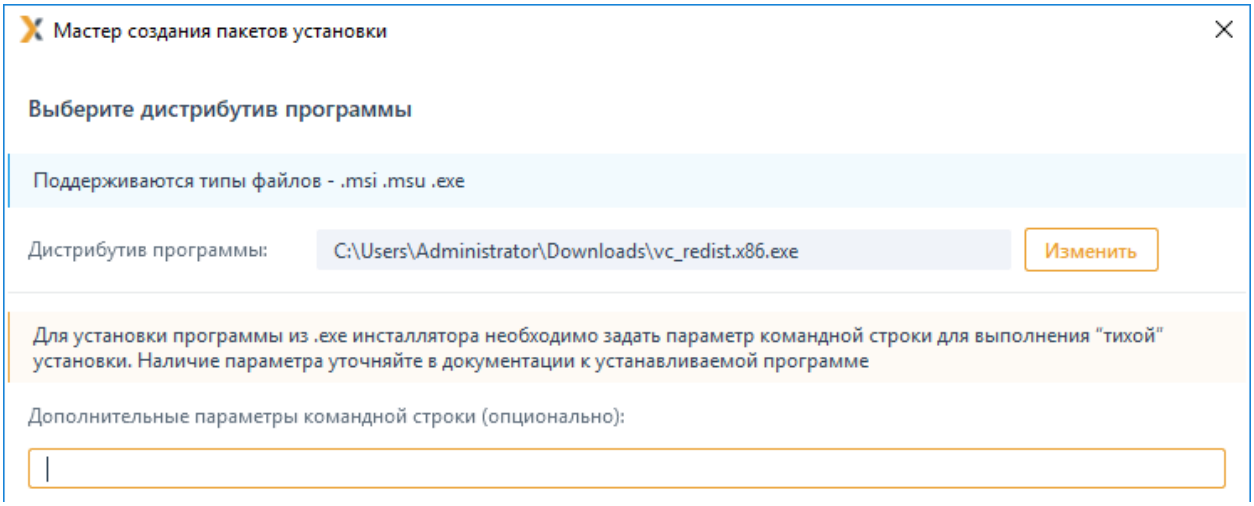


Рисунок 8.3 – Ввод дополнительных параметров установки ПО

На следующем шаге мастера по созданию пакета установки введите имя создаваемого пакета и нажмите кнопку ***Создать*** (рисунок 8.4).

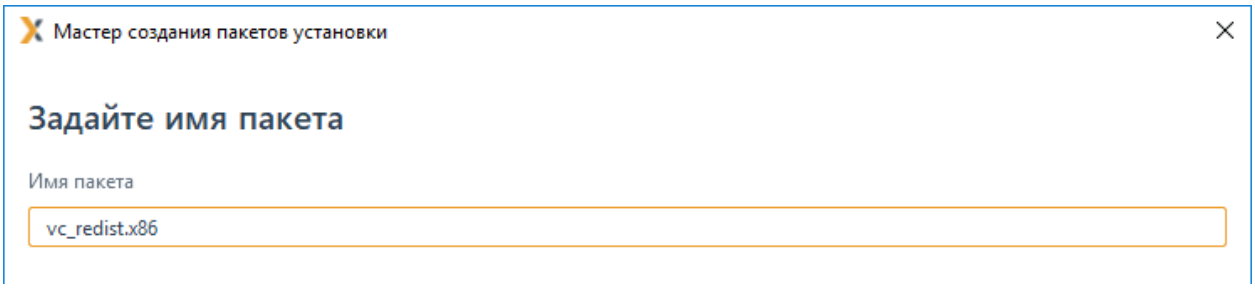


Рисунок 8.4 – Ввод имени создаваемого инсталляционного пакета

В результате успешного завершения операции по созданию пакета установки в каталоге размещения инсталляционных пакетов *C:\BlockHost\DeploymentSystem\packagestorage* будет создан каталог, в который будет скопирован выбранный файл-установщик. В окне мастера по созданию установочного пакета появится сообщение об успешном создании пакета (рисунок 8.5).

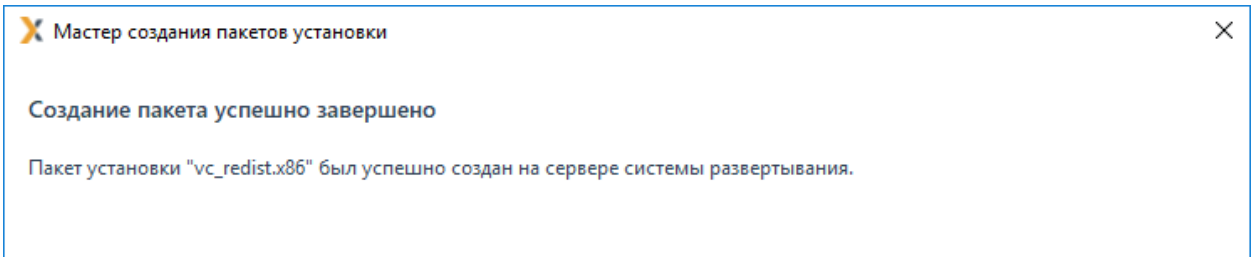


Рисунок 8.5 – Окно завершения работы мастера по созданию пакета установки

В инсталляционных пакетах, содержащих файлы-установщики агента развертывания и клиента Блокхост-Сеть, параметры командной строки задавать нельзя. Все необходимые параметры формируются подсистемой развёртывания автоматически.

8.2 Подготовка дистрибутива для сторонних систем развертывания

Формирование дистрибутивов для развертывания через сторонние системы доступно только для инсталляционных пакетов, содержащих файлы-установщики агента развертывания и клиента Блокхост-Сеть.

Для подготовки файла-установщика для развертывания сторонними средствами перейдите во вкладку ***Пакеты установки***, выберите из списка дистрибутив, содержащий установку агента развертывания или клиента Блокхост-Сеть и нажмите на кнопку Создать автономный пакет установки (рисунок 8.6).

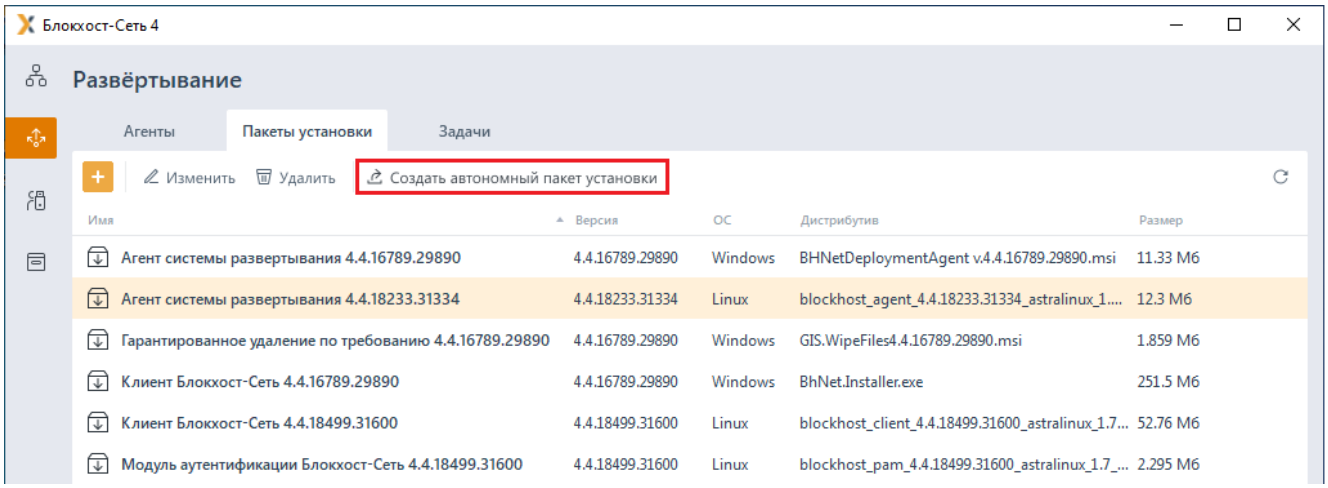


Рисунок 8.6 – Создание автономного пакета установки

В открывшемся окне (рисунок 8.7) по кнопке ***Выбрать*** укажите каталог, в который будет сохранен подготовленный пакет и нажмите кнопку ***Создать***.

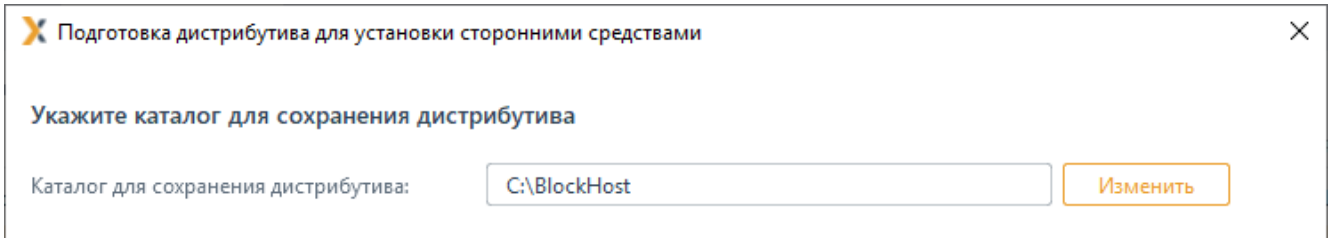


Рисунок 8.7 – Выбор каталога для сохранения автономного пакета установки

В случае успешного завершения операции подготовки дистрибутива появится окно, содержащее директорию и наименование подготовленного дистрибутива для установки сторонними средствами развертывания (рисунок 8.8). Для завершения подготовки дистрибутива для сторонних систем развертывания нажмите кнопку ***Завершить***.

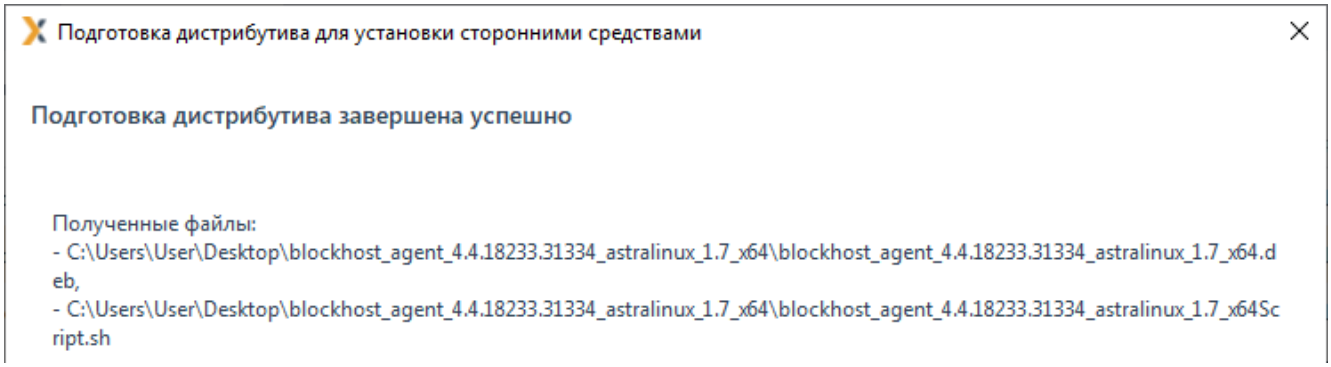


Рисунок 8.8 – Подготовленный дистрибутив для установки сторонними средствами

9 Вкладка «Задачи»

Во вкладке ***Задачи*** (рисунок 9.1) содержится список созданных в подсистеме развертывания задач.

При установке/удалении программ на клиентские рабочие станции под управлением ОС Linux задачи на установку и удаление программы могут завершиться ошибкой, если на клиентской рабочей станции запущен менеджер пакетов ***synaptic***. В этом случае закройте менеджер пакетов ***synaptic*** и выполните задачу повторно для клиентской рабочей станции, на которой задача завершилась ошибкой.

В верхней части вкладки расположены следующие элементы управления:

– кнопка + для создания следующих типов задач:

- ***Установка агента развертывания*** – создание задачи на установку агента развертывания;
- ***Установка программы*** – создание задачи на установку ПО на рабочие станции сети;
- ***Удаление программы*** – создание задачи на удаление ПО с рабочих станций сети;
- ***Перезагрузка компьютеров*** – создание задачи на перезагрузку рабочих станций сети;
- ***Выполнение скрипта*** – создание задачи для автоматического выполнения выбранного сценария на рабочей станции;
- ***Взятие под управление*** – создание задачи на взятие под управление модуля доверенной загрузки SafeNode system Loader;
- ***Поиск компьютеров без СЗИ*** – создание задачи на поиск установленных на рабочих станциях сети: агента развертывания, клиента Блокхост-Сеть и СДЗ «SafeNode System Loader»;
- ***Настройка входа по сертификатам*** – создание задачи по настройке аутентификации пользователя на клиентской рабочей станции под управлением ОС Linux с использованием токена, с записанным на нем сертификатом.

– кнопка Изменить для редактирования задач, созданных в подсистеме развертывания.

– кнопка Удалить для удаления задач, созданных в подсистеме развертывания.

– кнопка ▷ Запустить позволяет выполнить запуск задач, созданных в подсистеме развертывания.

– кнопка ↻ позволяет обновить список созданных в подсистеме развертывания задач.

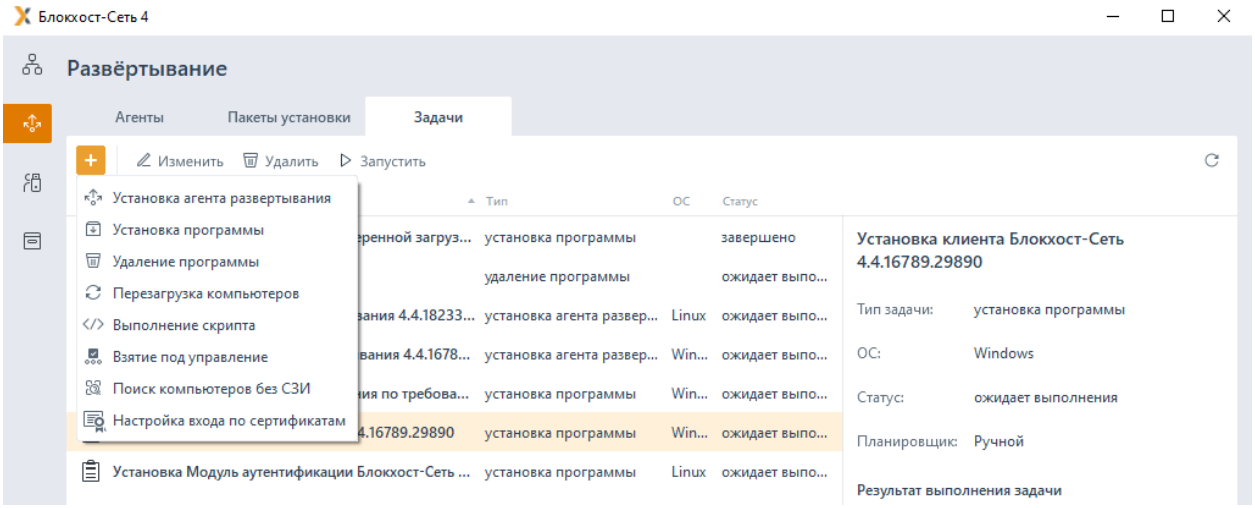


Рисунок 9.1 – Вкладка ***Задачи***

9.1 Установка агента развертывания

Описание задачи на установку агента развертывания на рабочие станции приведено в разделе «***Установка агента подсистемы развертывания***».

9.2 Установка программы

Для создания задачи на установку программного обеспечения на клиентские рабочие станции перейдите во вкладку ***Задачи***, раскройте меню создания задач по кнопке + и выберите пункт ***Установка программы*** (рисунок 9.1).

В открывшемся окне создания задачи на установку программы (рисунок 9.2) выберите пакет установки из списка имеющихся в базе данных подсистемы развертывания и нажмите кнопку ***Далее***.

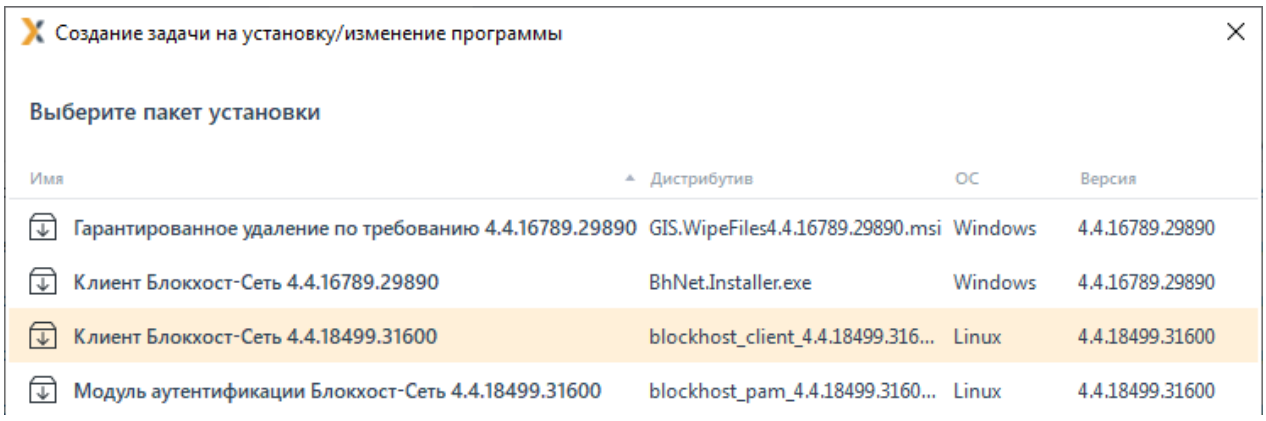


Рисунок 9.2 – Выбор пакета установки

Выберите в списке те рабочие станции, на которые необходимо выполнить установку выбранного программного обеспечения, и нажмите кнопку ***Далее*** (рисунок 9.3).

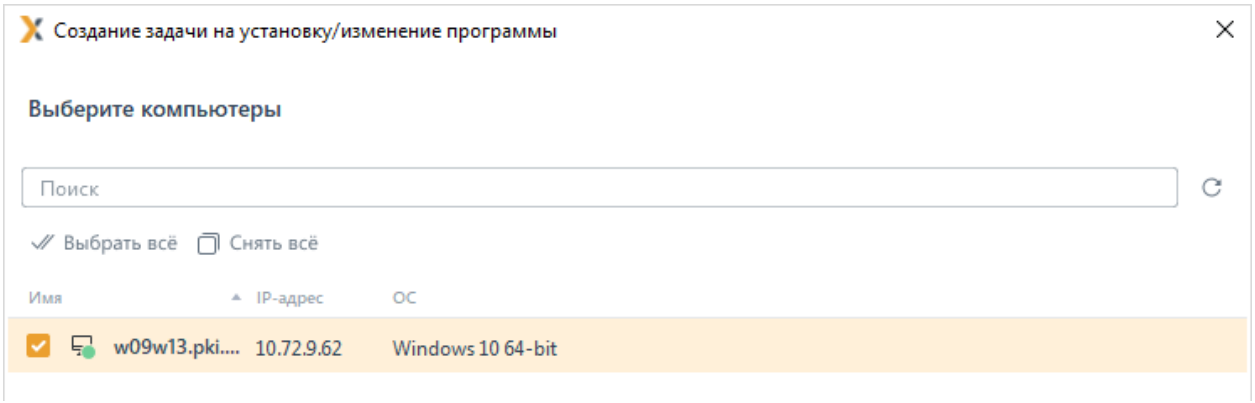


Рисунок 9.3 – Выбор рабочих станций для установки программы

Задайте параметры планировщика запуска задачи (подробнее в пункте ***«Указание параметров планировщика задачи по установке агента»***), определите интервалы времени выполнения задачи (рисунок 9.4) и нажмите кнопку ***Далее*** для продолжения создания задачи на установку программы.

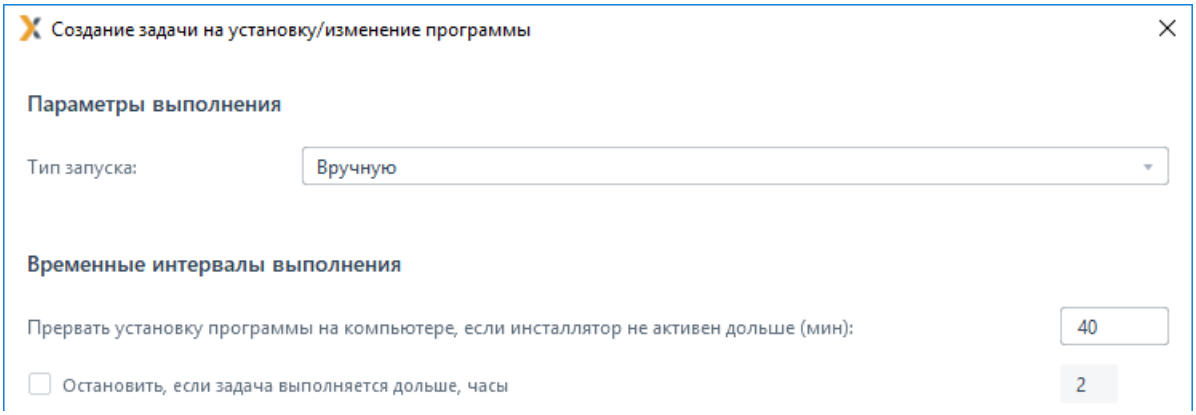


Рисунок 9.4 – Определение параметров планировщика и временных интервалов выполнения задачи

В следующем окне (рисунок 9.5) укажите параметры перезагрузки рабочих станций после выполнения задачи (подробнее в пункте ***«Параметры перезагрузки рабочих станций»***).

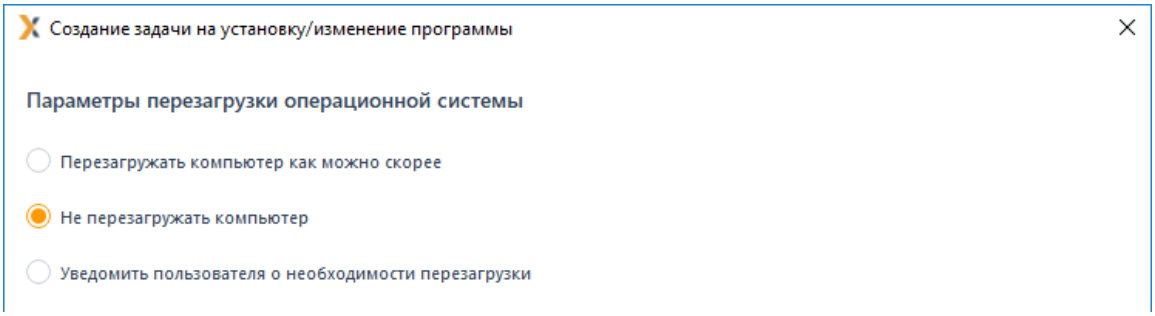


Рисунок 9.5 – Определение параметров перезагрузки рабочих станций

Введите имя создаваемой задачи и нажмите кнопку ***Создать*** (рисунок 9.6).

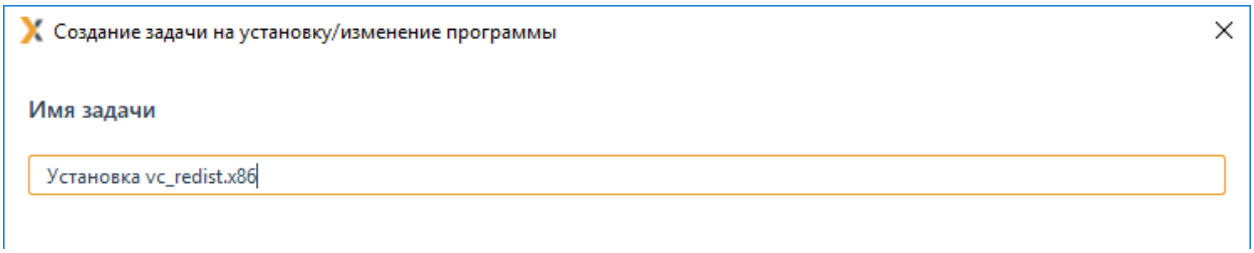


Рисунок 9.6 – Ввод имени создаваемой задачи

В случае успешного завершения создания задачи появится окно с сообщением о создании задачи на установку (рисунок 9.7).

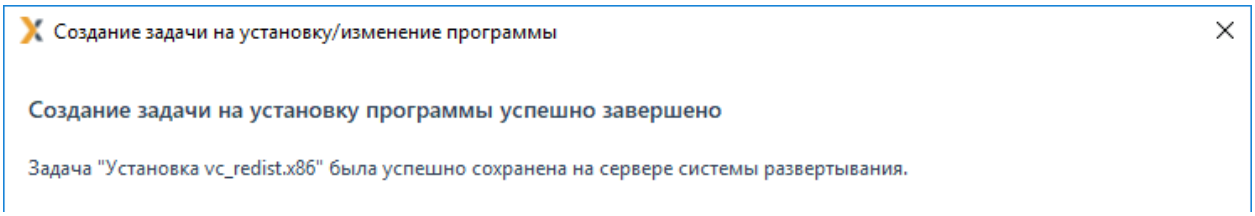


Рисунок 9.7 – Завершение создания задачи на установку программы

В результате во вкладке ***Задачи*** будет создана новая задача на установку программы с заданными в ходе работы мастера создания задачи параметрами.

9.3 Удаление программы

Для создания задачи на удаление программы на клиентских рабочих станциях перейдите во вкладку ***Задачи***, раскройте меню создания задач по кнопке + и выберите пункт ***Удаление программы*** (рисунок 9.1).

В открывшемся окне создания задачи на удаление программы (рисунок 9.8) выберите одну из подзадач:

– ***Удаление Блокхост-Сеть Клиент*** – создание задачи по удалению с рабочих станций клиента Блокхост-Сеть;

– ***Удаление программы из списка инсталляционных пакетов (только для msi-инсталляторов)*** – создание задачи на удаление программы, для которой в подсистеме развертывания создан инсталляционный пакет;

– ***Выполнение скрипта для удаления программы*** – создание задачи для запуска на рабочей станции скрипта *PowerShell* или командного (**.bat*) файла для удаления программы;

– ***Удаление модуля аутентификации (только Linux машины)*** – создание задачи для удаления модуля расширенной аутентификации на клиентских рабочих станциях под управлением ОС Linux.

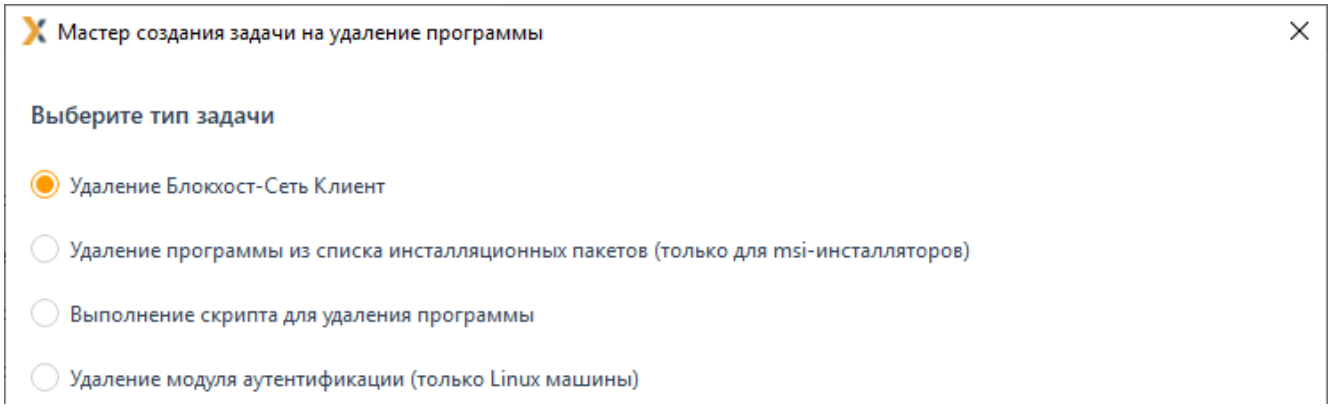


Рисунок 9.8 – Выбор типа задачи на удаление программы

Дальнейшие настройки различаются в зависимости от выбранного типа задачи на удаление. Подробнее каждый тип задачи на удаление описан в пунктах 9.3.1 - 9.3.4.

9.3.1 Удаление Блокхост-Сеть Клиент

Описание задачи на удаление клиента Блокхост-Сеть с рабочих станций приведено в разделе «***Удаление клиента Блокхост-Сеть через подсистему развертывания»***.

9.3.2 Удаление программы из списка инсталляционных пакетов

При выборе типа задачи ***Удаление программы из списка инсталляционных пакетов (только для msi-инсталляторов)*** появится окно (рисунок 9.9), в котором необходимо выбрать инсталляционный пакет из списка имеющихся по кнопке ***Выбрать*** (рисунок 9.10) и при необходимости ввести дополнительные параметры выполнения задачи по удалению выбранной программы в поле ***Дополнительные параметры команды для удаления (опционально)***.

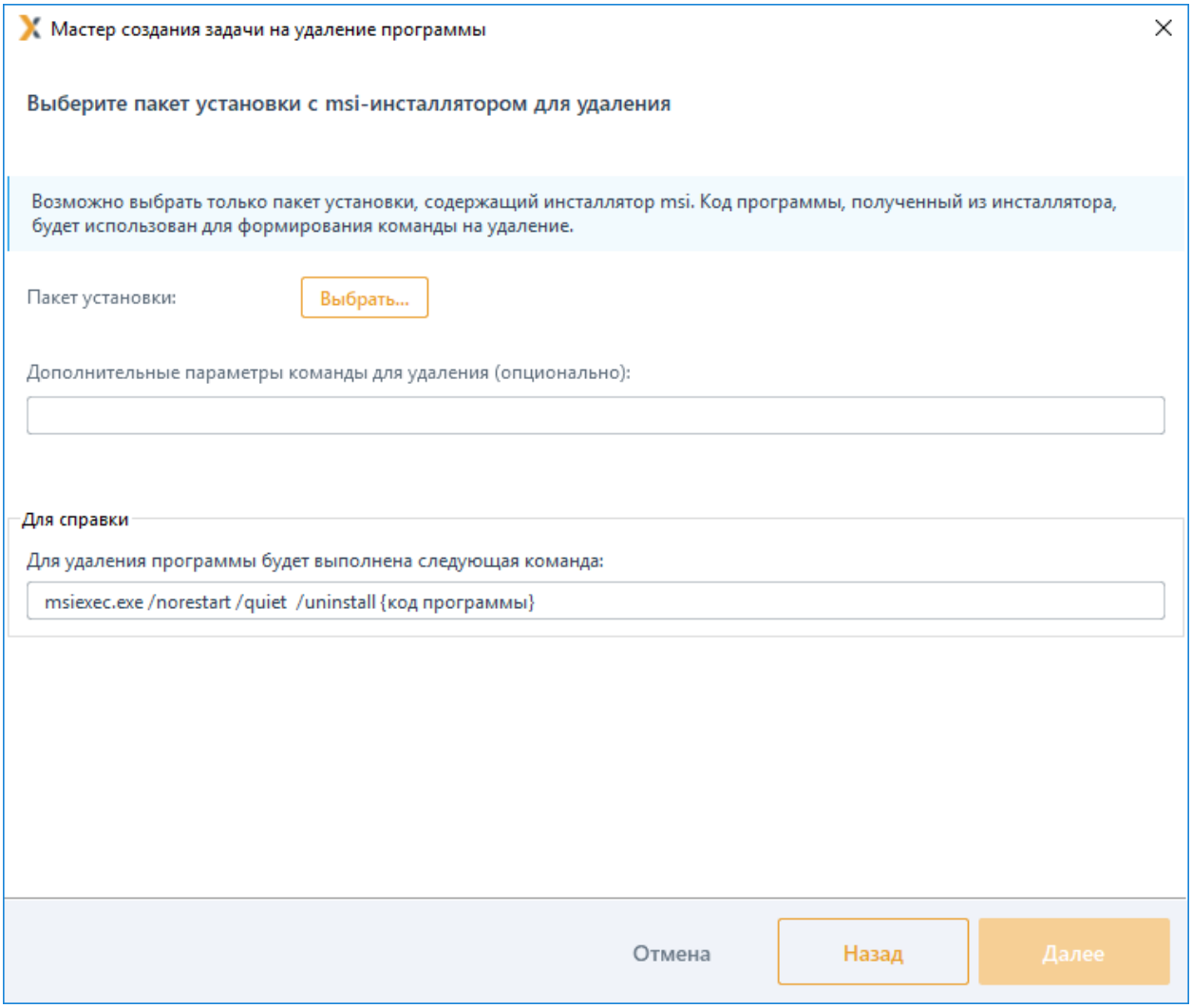


Рисунок 9.9 – Окно выбора пакета установки с msi-инсталлятором для удаления

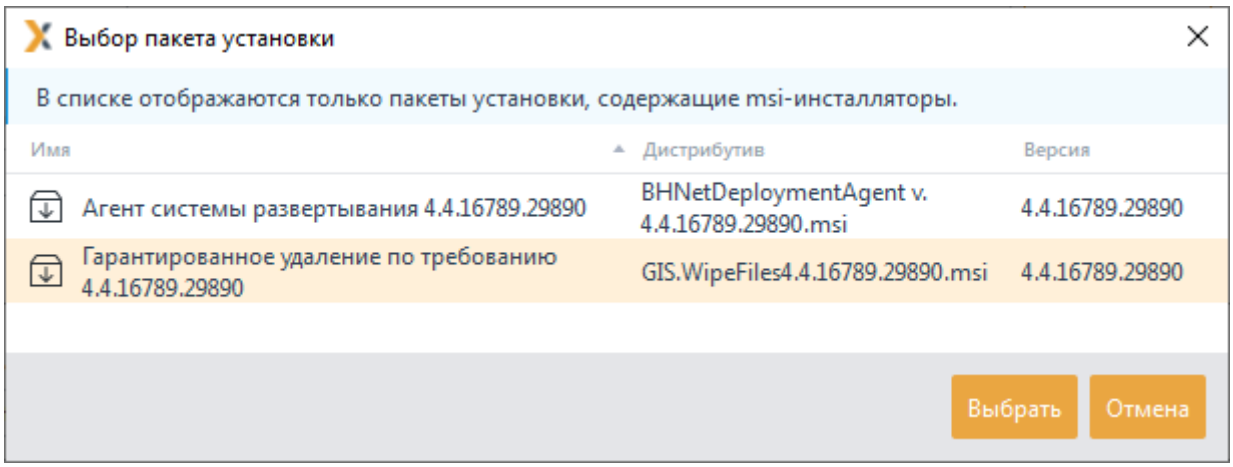


Рисунок 9.10 – Выбор пакета установки из списка

В следующем окне выберите рабочие станции, с которых будет удаляться выбранная программа (рисунок 9.11).

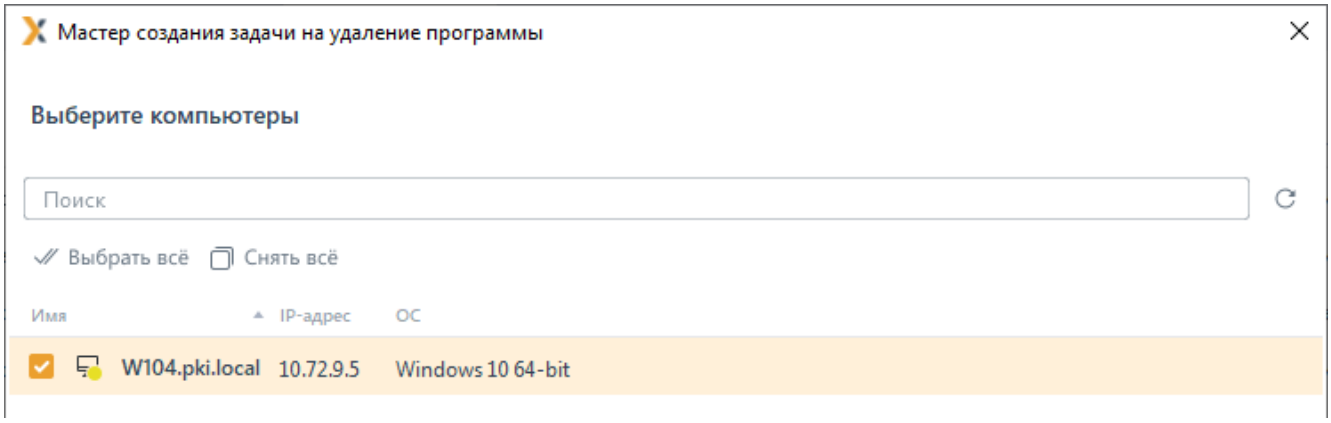


Рисунок 9.11 – Выбор рабочих станций для удаления программы

Задайте параметры планировщика запуска задачи (подробнее в пункте ***«Указание параметров планировщика задачи по установке агента»***) и определите интервалы времени выполнения задачи.

Укажите параметры перезагрузки рабочих станций после выполнения задачи (подробнее в пункте ***«Параметры перезагрузки рабочих станций»***).

Введите имя создаваемой задачи (рисунок 9.12) и нажмите кнопку ***Создать.***

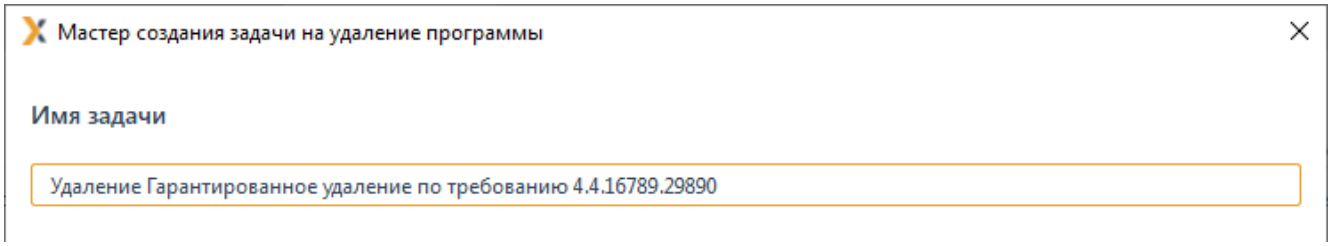


Рисунок 9.12 – Ввод имени задачи на удаление

В случае успешного завершения создания задачи появится окно с сообщением о создании задачи на удаление программы из списка инсталляционных пакетов (рисунок 9.13).

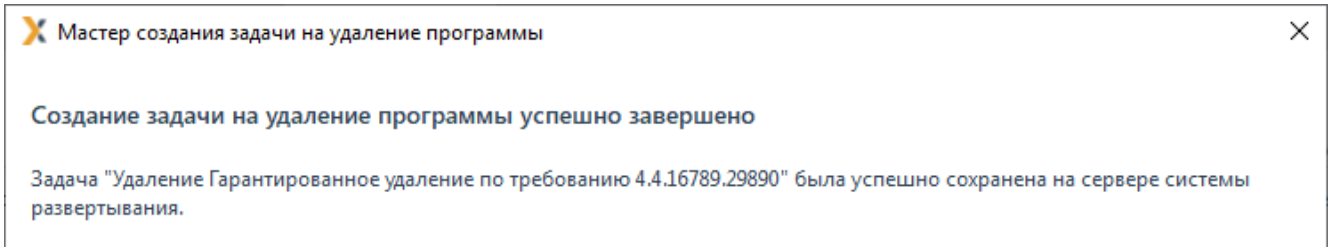


Рисунок 9.13 – Завершение создания задачи на удаление программы

В результате во вкладке ***Задачи*** будет создана новая задача на удаление программы из списка инсталляционных пакетов с заданными в ходе работы мастера параметрами (рисунок 9.14).

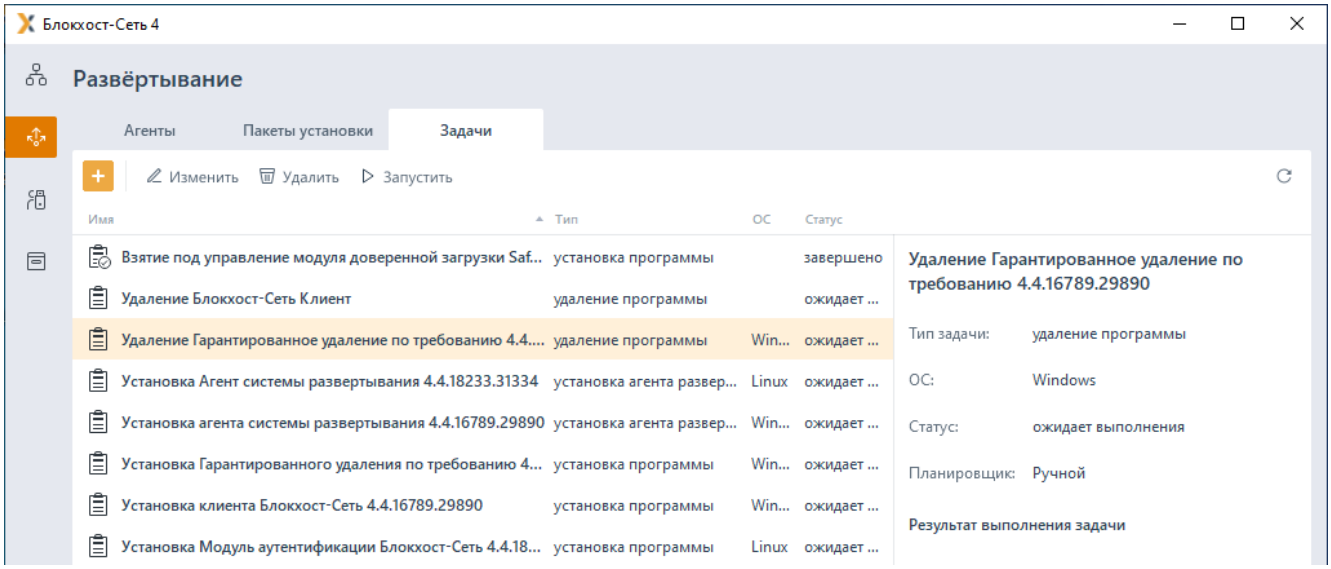


Рисунок 9.14 – Отображение в списке задачи на удаление программы

9.3.3 Удаление программы с использованием скрипта PowerShell или командного файла Windows

При выборе типа задачи на удаление ***Выполнение скрипта для удаления программы*** появится окно (рисунок 9.15), в котором необходимо выбрать файла скрипта (*.ps1) или командного файла (*.bat) по удалению программы с рабочей станции, имеющиеся по кнопке ***Выбрать*** (рисунок 9.16) и при необходимости ввести дополнительные параметры выполнения задачи по удалению в поле ***Параметры командной строки файла скрипта (опционально).***

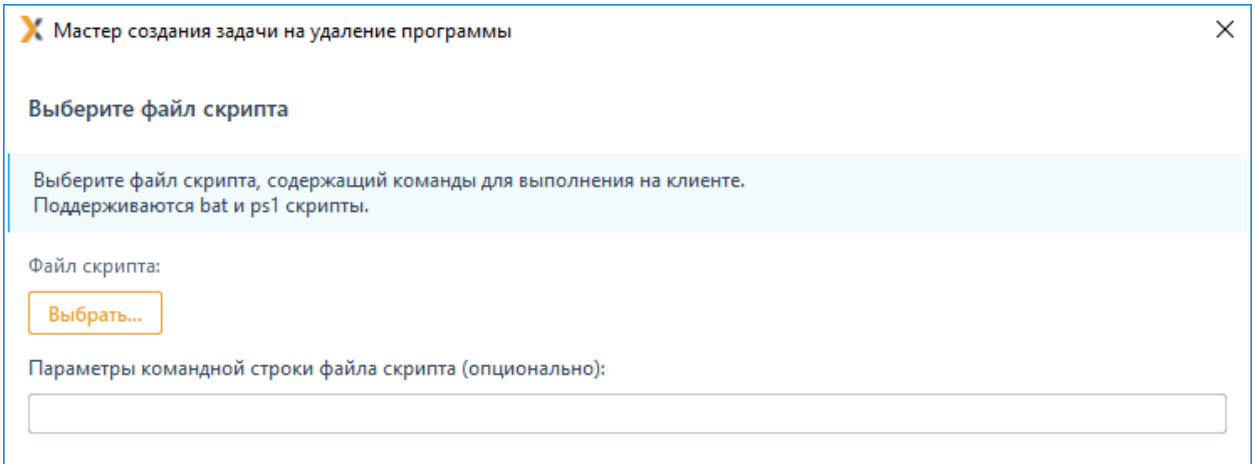


Рисунок 9.15 – Окно ввода параметров файла скрипта по удалению программы

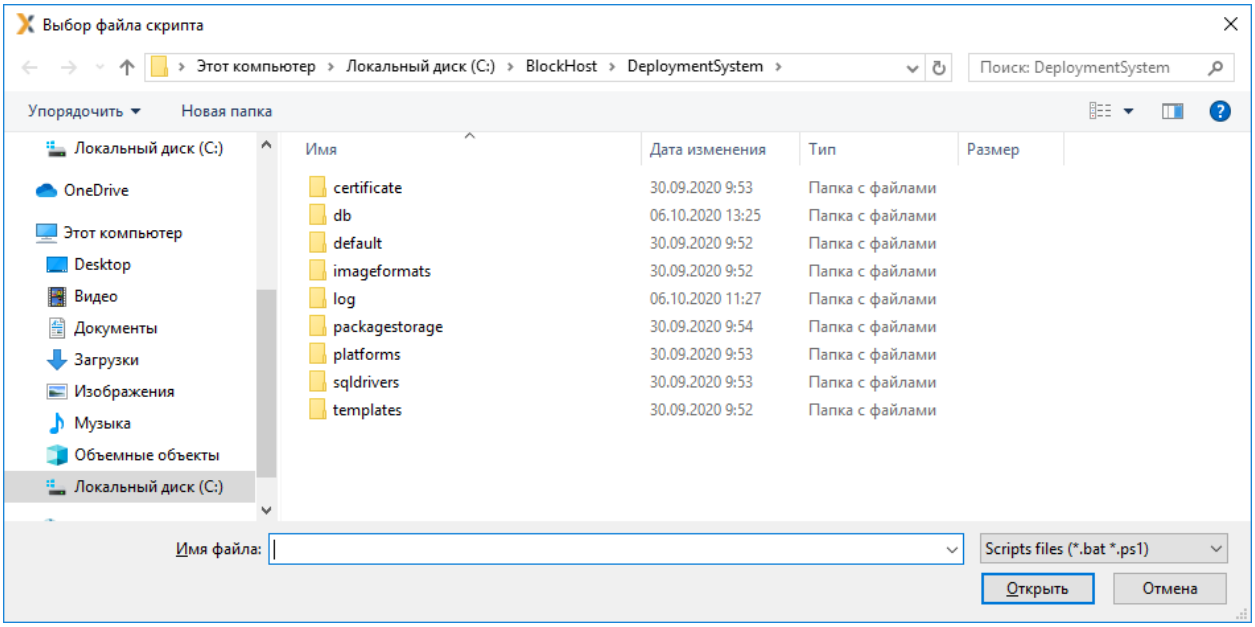


Рисунок 9.16 – Выбор файла скрипта по удалению программы

В следующем окне выберите рабочие станции, на которых будет выполнятся скрипт по удалению программы (рисунок 9.11).

Задайте параметры планировщика запуска задачи (подробнее в пункте ***«Указание параметров планировщика задачи по установке агента»***) и определите интервалы времени выполнения задачи.

Укажите параметры перезагрузки рабочих станций после выполнения задачи (подробнее в пункте ***«Параметры перезагрузки рабочих станций»***).

Введите имя создаваемой задачи (рисунок 9.12) и нажмите кнопку ***Создать.***

В случае успешного завершения создания задачи появится окно с сообщением о создании задачи на выполнение скрипта на удаление программы (рисунок 9.17).

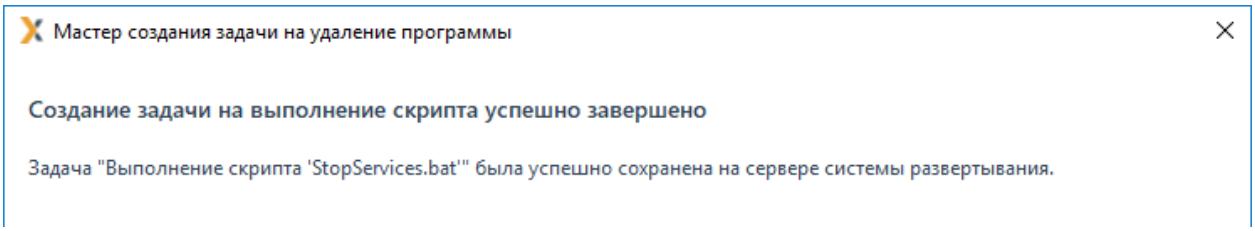


Рисунок 9.17 – Завершение создания задачи на выполнение скрипта удаления

В результате работы мастера создания задачи на удаление программы будет добавлена новая задача на удаление программы с использованием скрипта, с указанными в диалоговых окнах мастера параметрами.

9.3.4 Удаление модуля аутентификации

Описание задачи на удаление модуля аутентификации с рабочих станций под управлением ОС Linux приведено в разделе «***Удаление модуля аутентификации»***.

9.4 Перезагрузка компьютеров

Для создания задачи на перезагрузку рабочих станций перейдите во вкладку ***Задачи***, раскройте меню создания задач по кнопке + и выберите пункт ***Перезагрузка компьютеров*** (рисунок 9.1).

В открывшемся окне выберите в списке рабочие станции, которые необходимо перезагрузить и нажать кнопку ***Далее***.

Задайте параметры планировщика запуска задачи (подробнее в пункте ***«Указание параметров планировщика задачи по установке агента»***) и определите интервалы времени выполнения задачи.

Укажите параметры перезагрузки рабочих станций (подробнее в пункте ***«Параметры перезагрузки рабочих станций»***).

Введите имя создаваемой задачи и нажмите кнопку ***Создать.***

В случае успешного завершения создания задачи появится окно с сообщением о создании задачи на перезагрузку компьютеров (рисунок 9.18).

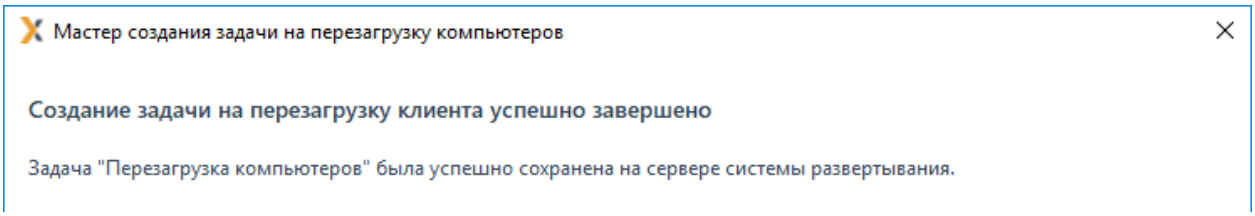


Рисунок 9.18 – Завершение создания задачи на перезагрузку компьютеров

В результате во вкладке ***Задачи*** в список задач будет добавлена новая задача, с заданными в ходе работы мастера создания задачи параметрами.

9.5 Выполнение скрипта

Для создания задачи на выполнение скрипта перейдите во вкладку ***Задачи***, раскройте меню создания задач по кнопке + и выберите пункт ***Выполнение скрипта*** (рисунок 9.1).

В открывшемся окне выберите файл скрипта (*.ps1) или командного файла (*.bat), имеющиеся по кнопке ***Выбрать*** (рисунок 9.19) и при необходимости введите дополнительные параметры выполнения задачи в поле ***Параметры командной строки файла скрипта (опционально).***

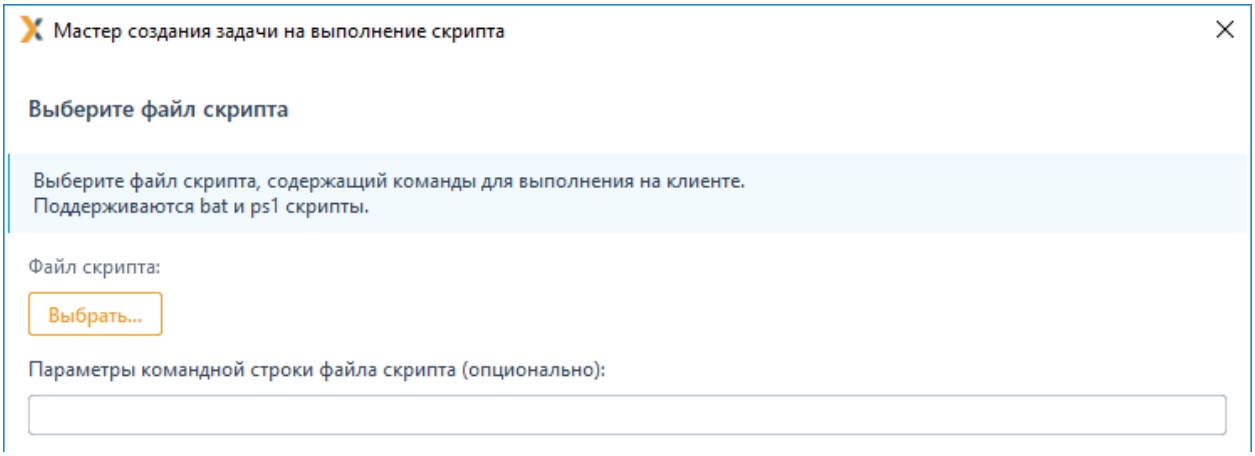


Рисунок 9.19 – Окно ввода параметров файла скрипта

В следующем окне выберите рабочие станции, на которых будет выполнятся скрипт.

Задайте параметры планировщика запуска задачи (подробнее в пункте ***«Указание параметров планировщика задачи по установке агента»***) и определите интервалы времени выполнения задачи.

Укажите параметры перезагрузки рабочих станций после выполнения задачи (подробнее в пункте ***«Параметры перезагрузки рабочих станций»***).

Введите имя создаваемой задачи и нажмите кнопку ***Создать.***

В случае успешного завершения создания задачи появится окно с сообщением о создании задачи на выполнение скрипта (рисунок 9.20).

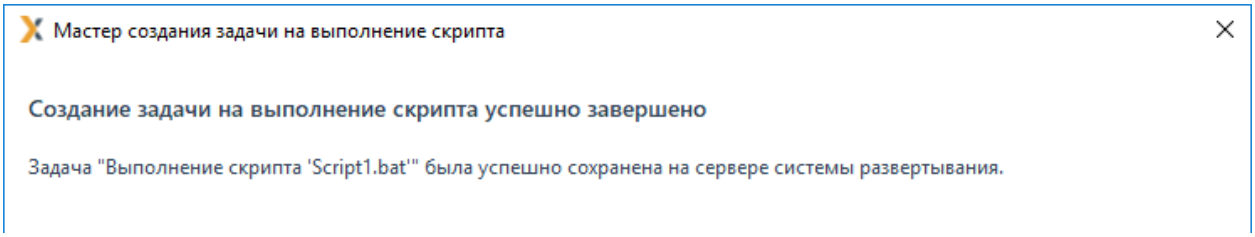


Рисунок 9.20 – Завершение создания задачи на выполнения скрипта

В результате работы мастера создания задачи будет добавлена новая задача на выполнение скрипта, с указанными в диалоговых окнах мастера параметрами.

9.6 Взятие под управление модуля доверенной загрузки «SafeNode System Loader»

Перед запуском задачи на взятие под управление модуля доверенной загрузки «SafeNode System Loader» на клиентских рабочих станциях необходимо убедиться в том, что на станциях установлены и настроены:

– клиентская часть СЗИ от НСД «Блокхост-Сеть 4»;

– средство доверенной загрузки «SafeNode System Loader».

При отсутствии на рабочих станциях СДЗ «SafeNode System Loader» выполните установку на каждой рабочей станции локально или воспользуйтесь централизованной установкой с помощью подсистемы развертывания СЗИ от НСД «Блокхост-Сеть 4» (подробнее в разделе ***«Централизованная установка СДЗ «SafeNode System Loader»»***).

9.6.1 Централизованная установка СДЗ «SafeNode System Loader»

Установка СДЗ «SafeNode System Loader» осуществляется в два этапа:

– на первом этапе происходит установка СДЗ «SafeNode System Loader» на рабочие станции без самозащиты;

– на втором этапе СДЗ «SafeNode System Loader» устанавливается с параметрами самозащиты.

Перед установкой СДЗ «SafeNode System Loader» на рабочие станции необходимо сформировать пакет установки СДЗ с помощью подсистемы развертывания.

Установка СДЗ «SafeNode System Loader» на рабочие станции под управлением ОС Windows осуществляется с помощью файла-инсталлятора ***SafeNodeSL.exe***, установка на рабочие станции под управлением ОС Linux осуществляется с помощью файлов-инсталляторов, входящих в комплект дистрибутива, ***snsl_<номер версии>_altlinux.rpm*** для ОС Альт 8 СП, ***snsl_<номер версии>.deb*** для ОС Astra Linux «Смоленск», ***snsl_<номер версии>.rpm*** для РЕД ОС.

Для формирования пакета установки перейдите во вкладку ***Пакеты установки*** по кнопке  (рисунок 9.21).

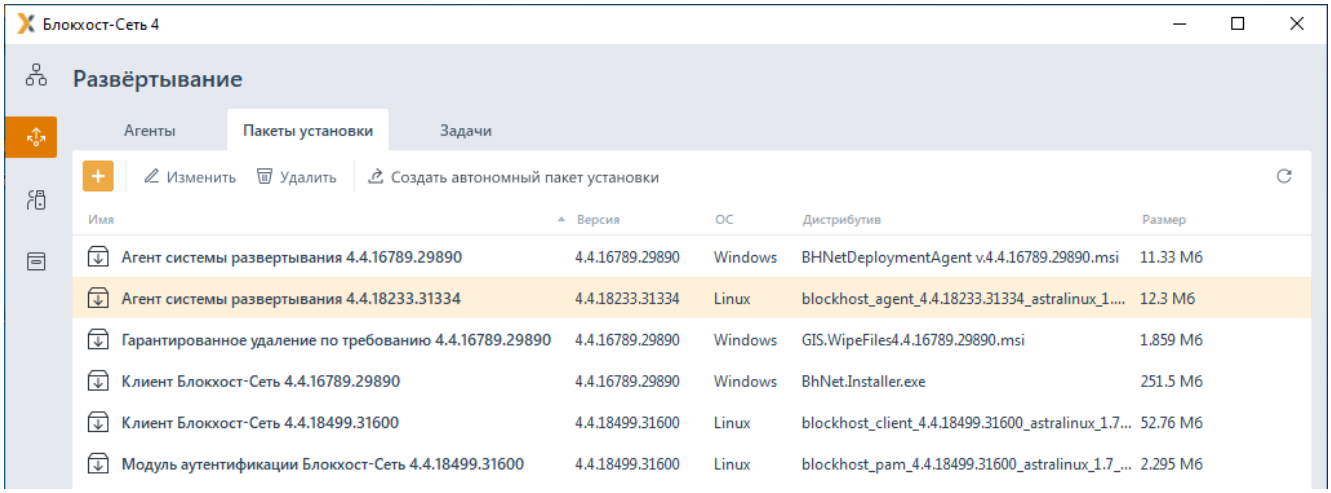


Рисунок 9.21 – Вкладка Пакеты установки

По кнопке  запустите создание пакета установки с помощью мастера создания пакетов установки (рисунок 9.22).

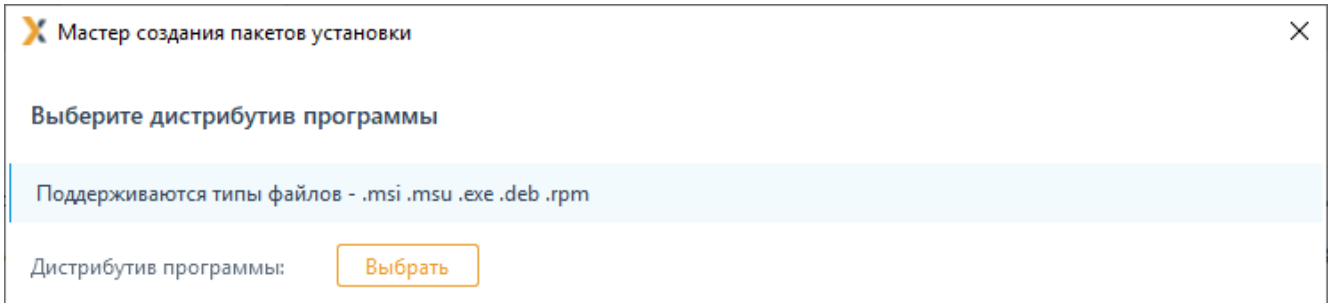


Рисунок 9.22 – Мастер создания пакетов установки

По кнопке ***Выбрать*** из списка выберите дистрибутив, содержащий установку СДЗ «SafeNode System Loader» (рисунок 9.23).

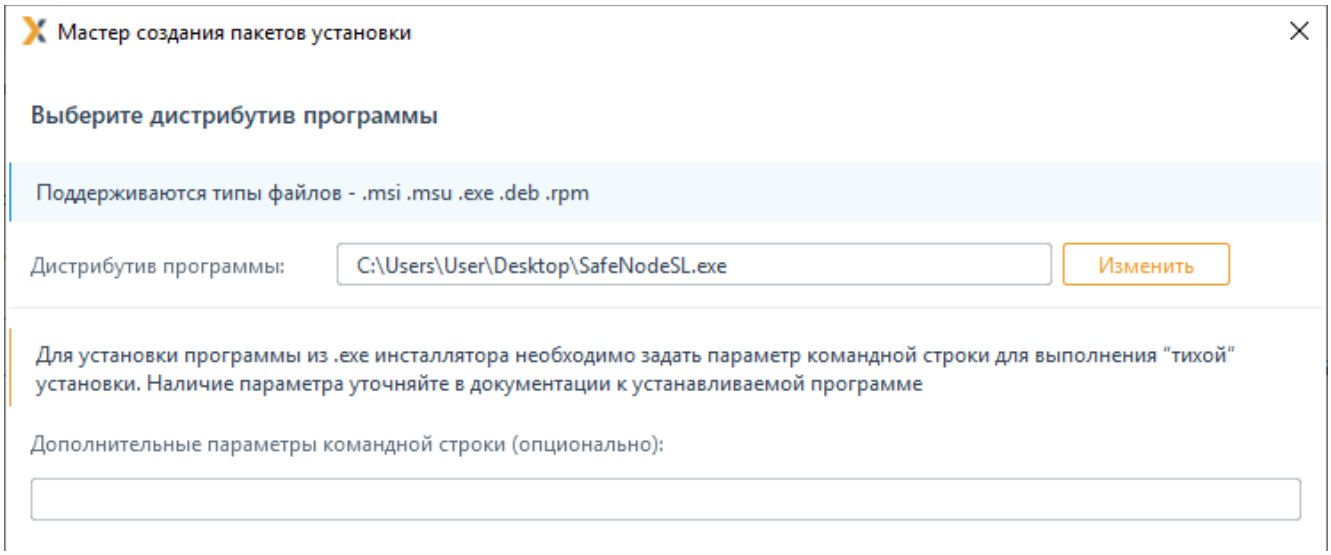


Рисунок 9.23 – Выбор пакета установки

Задайте имя создаваемого пакета (рисунок 9.24).

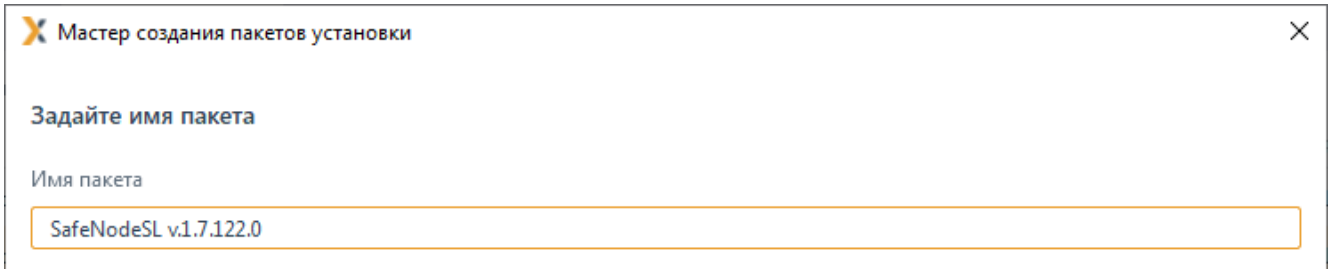


Рисунок 9.24 – Ввод имени пакета установки

По окончанию создания пакета установки, в списке появится новый пакет с заданным именем (рисунок 9.25).

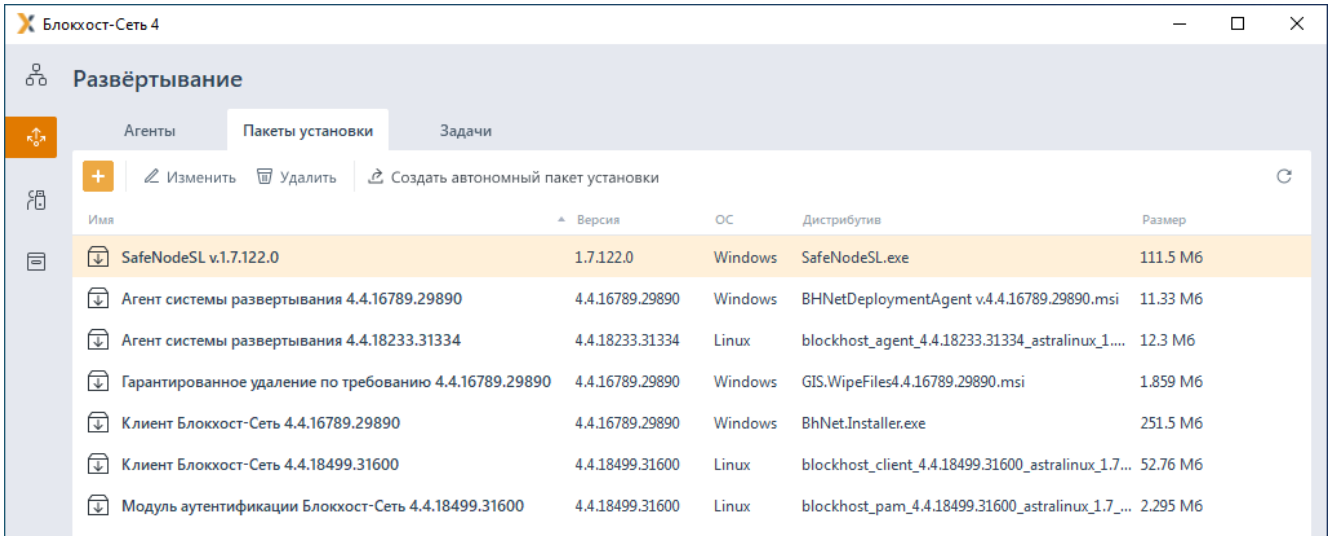


Рисунок 9.25 – Отображение созданного пакета установки в списке

Для создания задачи на установку СДЗ «SafeNode System Loader» на клиентские рабочие станции перейдите во вкладку ***Задачи***, раскройте меню создания задач по кнопке + и выберите пункт ***Установка программы*** (рисунок 9.1).

В открывшемся окне создания задачи на установку программы (рисунок 9.26) выберите пакет установки ***SafeNode System Loader*** и нажмите кнопку ***Далее***.

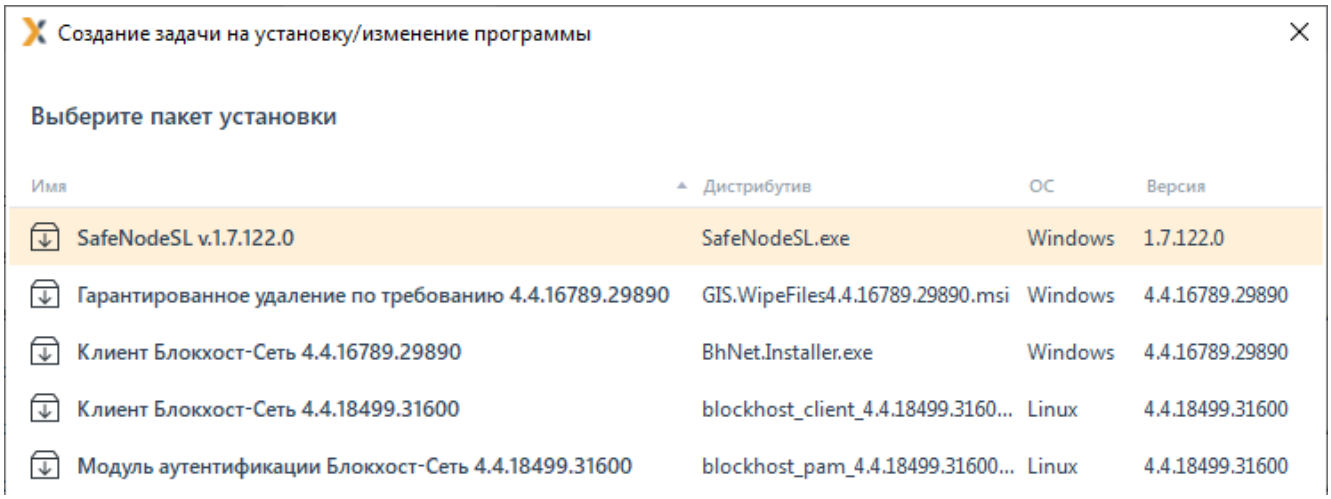


Рисунок 9.26 – Выбор пакета для создания задачи на установку ПО

Выберите в списке те рабочие станции, на которые необходимо выполнить установку выбранного программного обеспечения, и нажмите кнопку ***Далее*** (рисунок 9.3).

Задайте параметры планировщика запуска задачи (подробнее в пункте ***«Указание параметров планировщика задачи по установке агента»***), определите интервалы времени выполнения задачи (рисунок 9.4) и нажмите кнопку ***Далее*** для продолжения создания задачи на установку программы.

В следующем окне (рисунок 9.27) отобразится информация о времени перезагрузки рабочих станций после выполнения задачи. Для задачи на установку СДЗ «SafeNode

System Loader» перезагрузка рабочих станций произойдет через 5 минут после завершения задачи на установку. Пользователи не смогут отказаться или отложить перезагрузку.

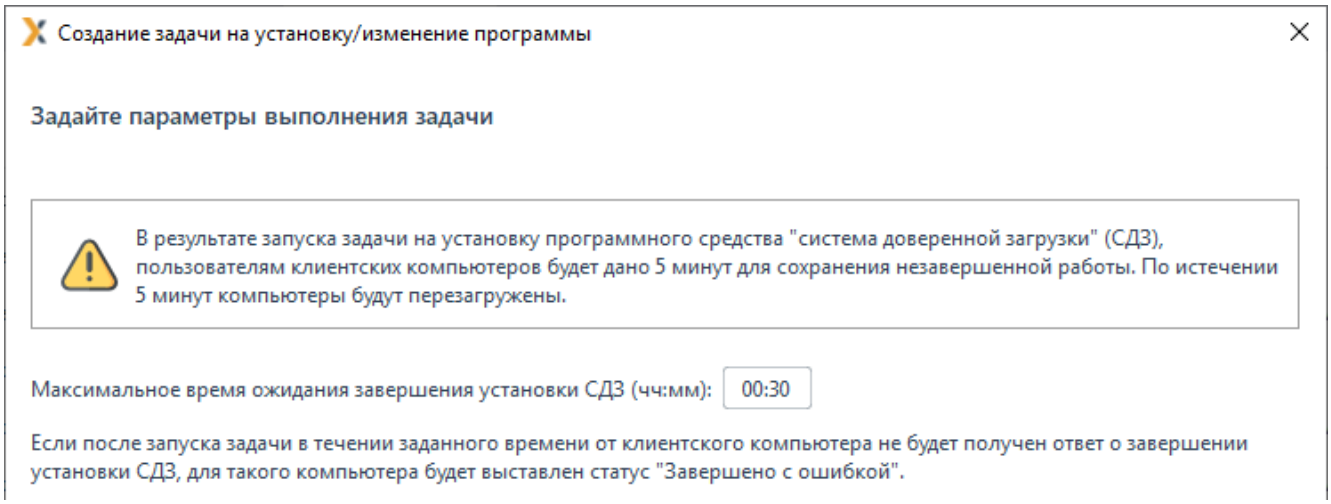


Рисунок 9.27 – Параметры перезагрузки рабочих станций

На клиентской рабочей станции появится сообщение о необходимости перезагрузки рабочей станции (рисунок 9.28).

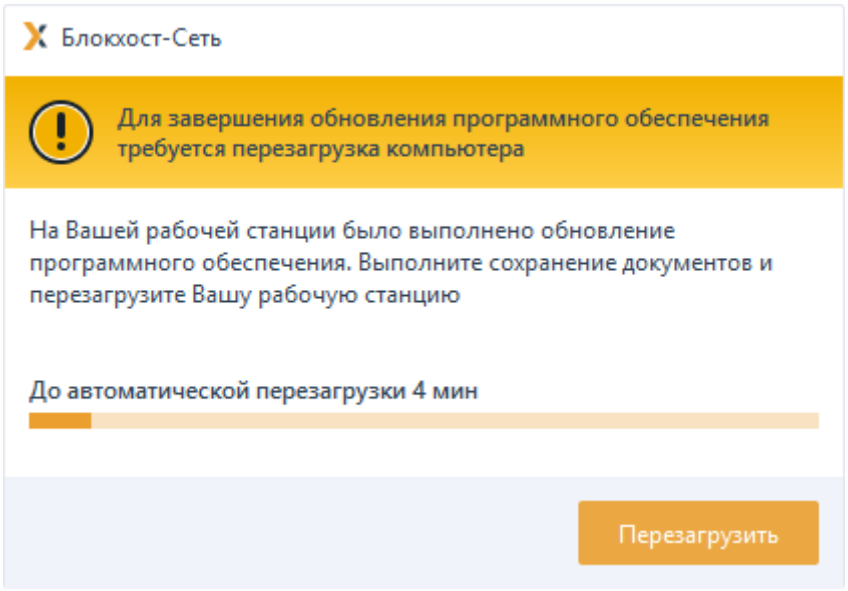


Рисунок 9.28 – Сообщение с предупреждением о перезагрузке рабочей станции

Введите имя создаваемой задачи и нажмите кнопку ***Создать*** (рисунок 9.29).

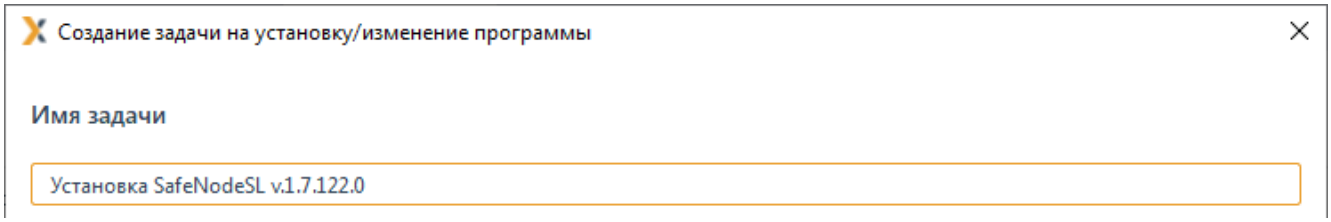


Рисунок 9.29 – Ввод имени создаваемой задачи

В случае успешного завершения создания задачи появится окно с сообщением о создании задачи на установку (рисунок 9.30).

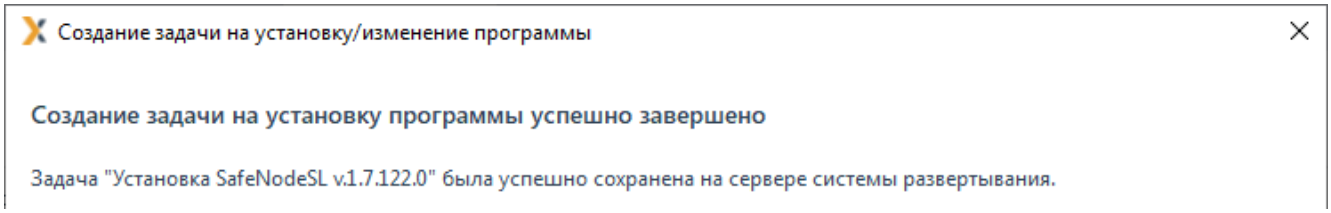


Рисунок 9.30 – Завершение создания задачи на установку программы

В результате во вкладке ***Задачи*** будет создана новая задача на установку программы с заданными в ходе работы мастера создания задачи параметрами.

В зависимости от установленных параметров планировщика запуск задачи будет осуществлен автоматически или вручную (подробнее в пункте ***«Запуск задачи»***).

Для отслеживания состояния задачи в ходе ее выполнения на рабочей станции, перейдите по ссылке ***Все результаты*** (рисунок 6.2).

По кнопке Описание в верхней части окна (рисунок 6.3) возможен просмотр статуса выполнения задачи.

В результате выполнения задачи по установке модуля SafeNode System Loader, после выполнения перезагрузки, на всех указанных в списке рабочих станциях будет установлен СДЗ «SafeNode System Loader».

После установки СДЗ «SafeNode System Loader» на рабочих станциях необходимо повторно выполнить запуск задачи на установку модуля SafeNode System Loader с дополнительными параметрами.

Для установки дополнительных параметров самозащиты перейдите во вкладку ***Пакеты установки*** по кнопке в строку с созданным пакетом установки ***SafeNode System Loader*** и нажмите кнопку Изменить (рисунок 9.25).

В открывшемся окне (рисунок 9.31) введите в строке ***Дополнительные параметры командной строки (опционально)*** следующие параметры:

```
ADMINNAME=admin PASSHASH=29ac25660e3078e87e3097d3822e50d7 ADDLOCAL=InstallToBIOS
```

где:

ADMINNAME – имя предустановленной учетной записи администратора;

PASSHASH – хеш-значение от пароля администратора по умолчанию («12345678»);

ADDLOCAL – параметр, включающий запись в BIOS.

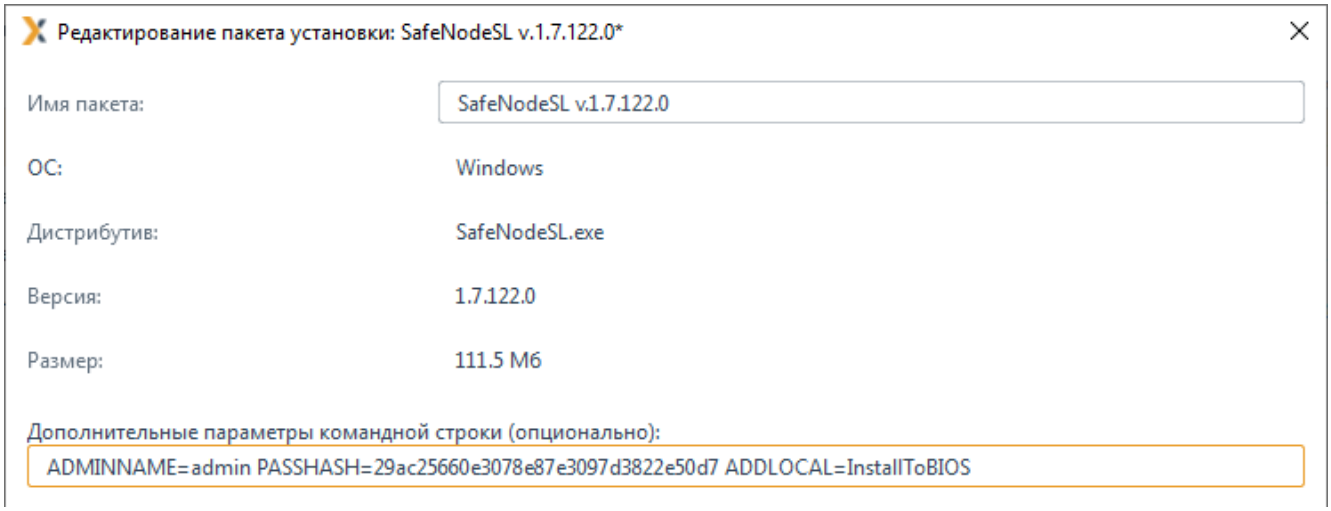


Рисунок 9.31 – Установка дополнительных параметров СДЗ «SafeNode System Loader»

Нажмите ***Применить*** для сохранения изменений в пакете установки.

Перейдите во вкладку ***Задачи*** в строку с созданной задачей на установку ***SafeNode System Loader*** и повторно выполните запуск задачи по кнопке ▷ Запустить (рисунок 9.32).

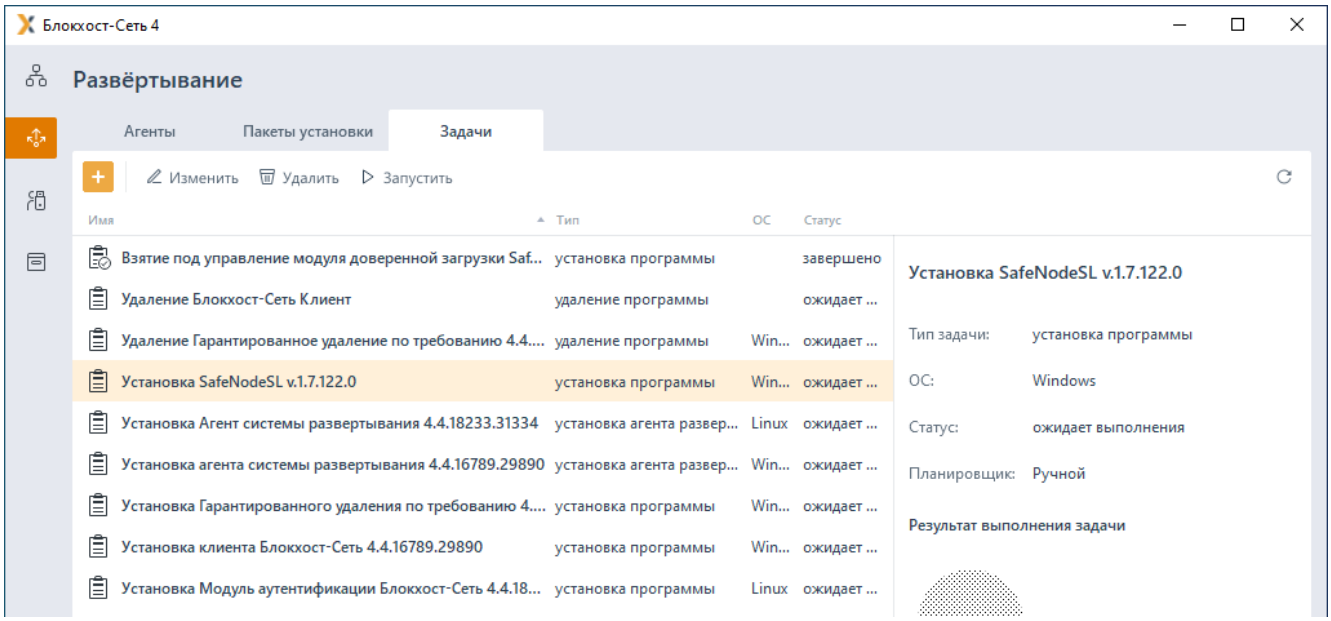


Рисунок 9.32 – Повторный запуск задачи на установку ПО

Если задача по установке ***SafeNode System Loader*** с самозащитой завершилась ошибкой (рисунок 9.33) необходимо последовательно выполнить следующие пункты документа «Средство доверенной загрузки «SafeNode System Loader». Руководство по эксплуатации. Часть 1. Руководство по установке»:

– чтение файла образа BIOS (п. 4.1);
– копирование модулей изделия (п. 4.2);

Обратите внимание, скрипт копирования файлов (01_copy.nsh)

запускать не нужно!

– модификация образа BIOS (п.4.3);

– запись модифицированного образа BIOS (п.4.4).

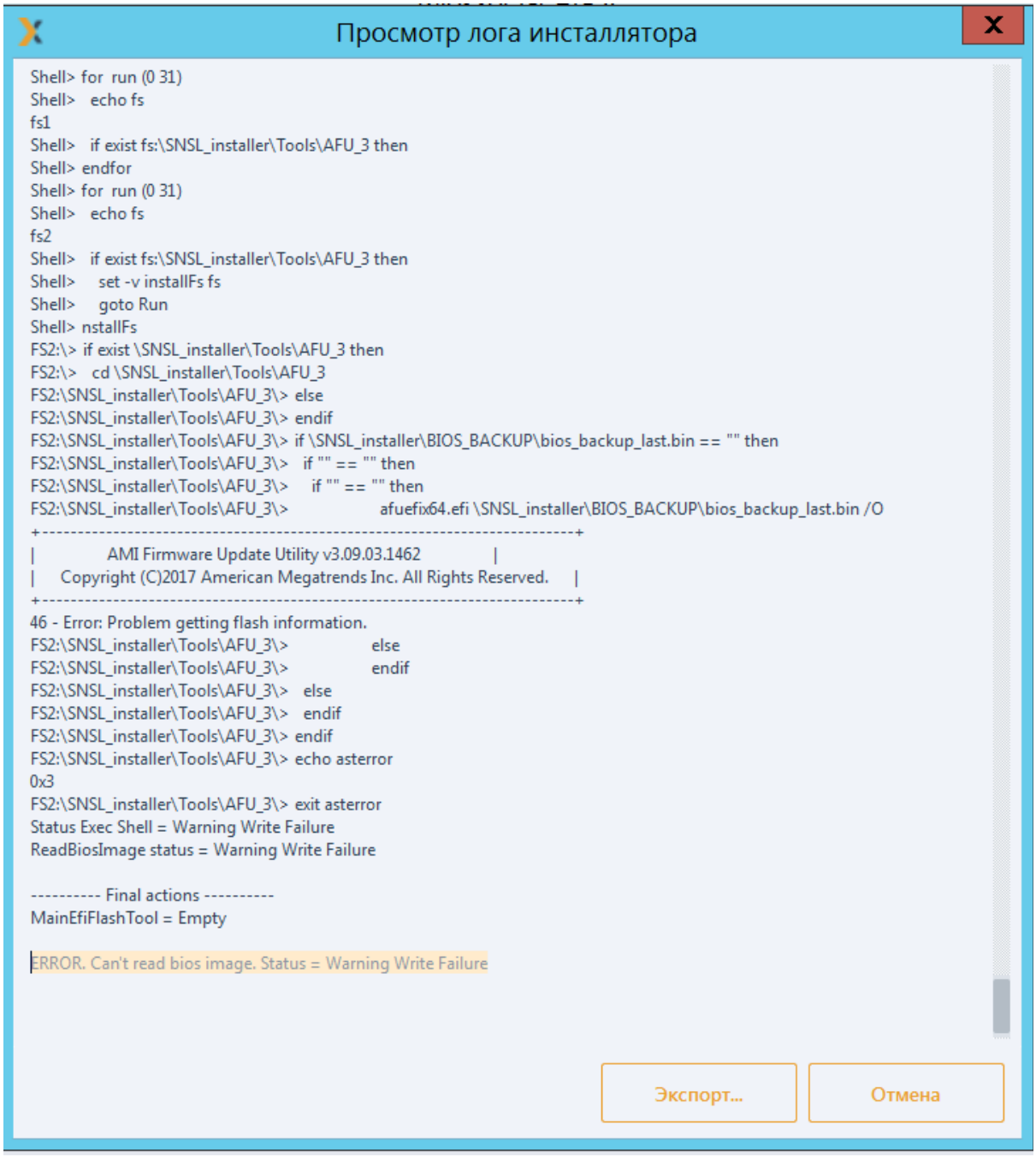


Рисунок 9.33 – Завершение задачи по установке ***SafeNode System Loader*** с ошибкой

9.6.2 Взятие под управление СДЗ «SafeNode System Loader» через предустановленную задачу

Для взятия под управление рабочих станций с установленным СДЗ «SafeNode System Loader» перейдите во вкладку ***Задачи*** и внесите корректировки в параметры автоматически созданной задачи ***Взятие под управление модуля доверенной***

загрузки SafeNode System Loader, открыв задачу на редактирование по кнопке Изменить в меню или с помощью контекстного меню (рисунок 9.34).

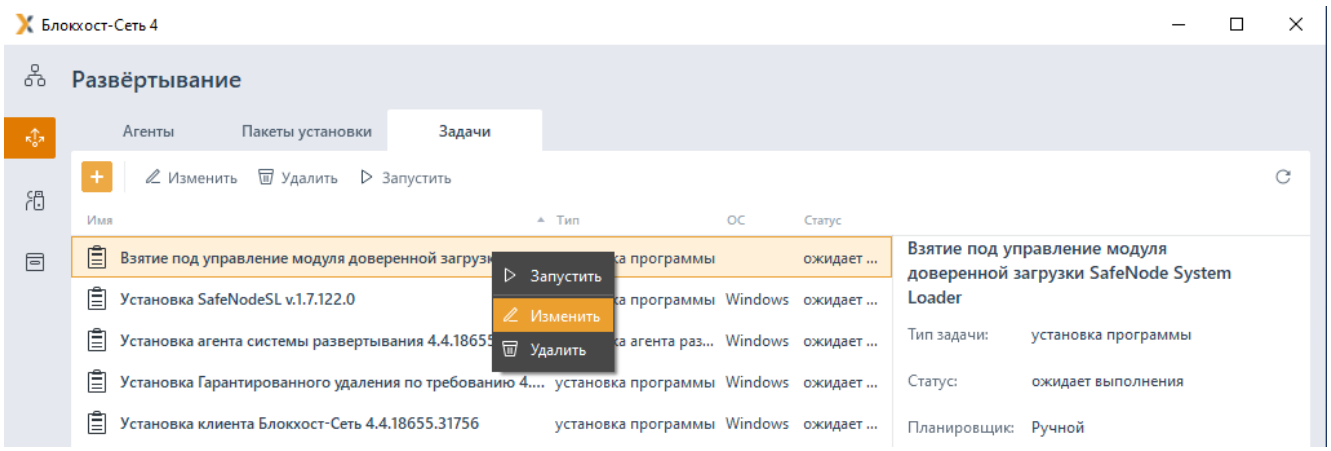


Рисунок 9.34 – Изменение задачи на взятие под управление модуля доверенной загрузки

В появившемся окне (рисунок 9.35) перейдите во вкладку ***Компьютеры*** (рисунок 9.36) и сформируйте список рабочих станций с установленным СДЗ «SafeNode System Loader», на которых необходимо выполнить задачу на взятие под управление.

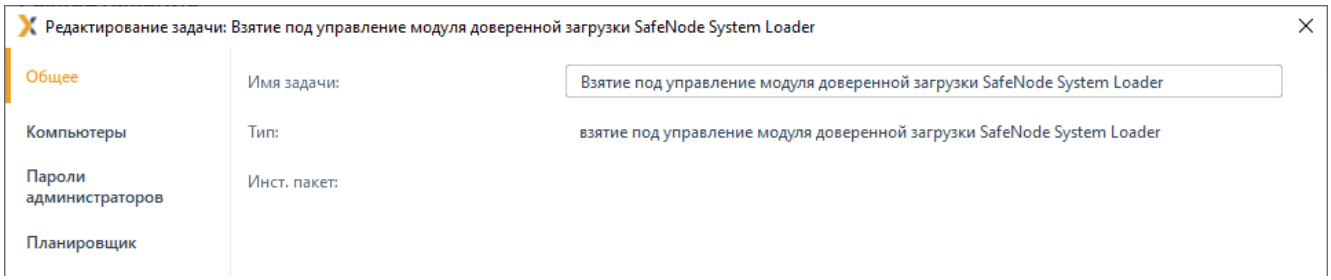


Рисунок 9.35 – Редактирование задачи на взятие под управление СДЗ «SafeNode System Loader»

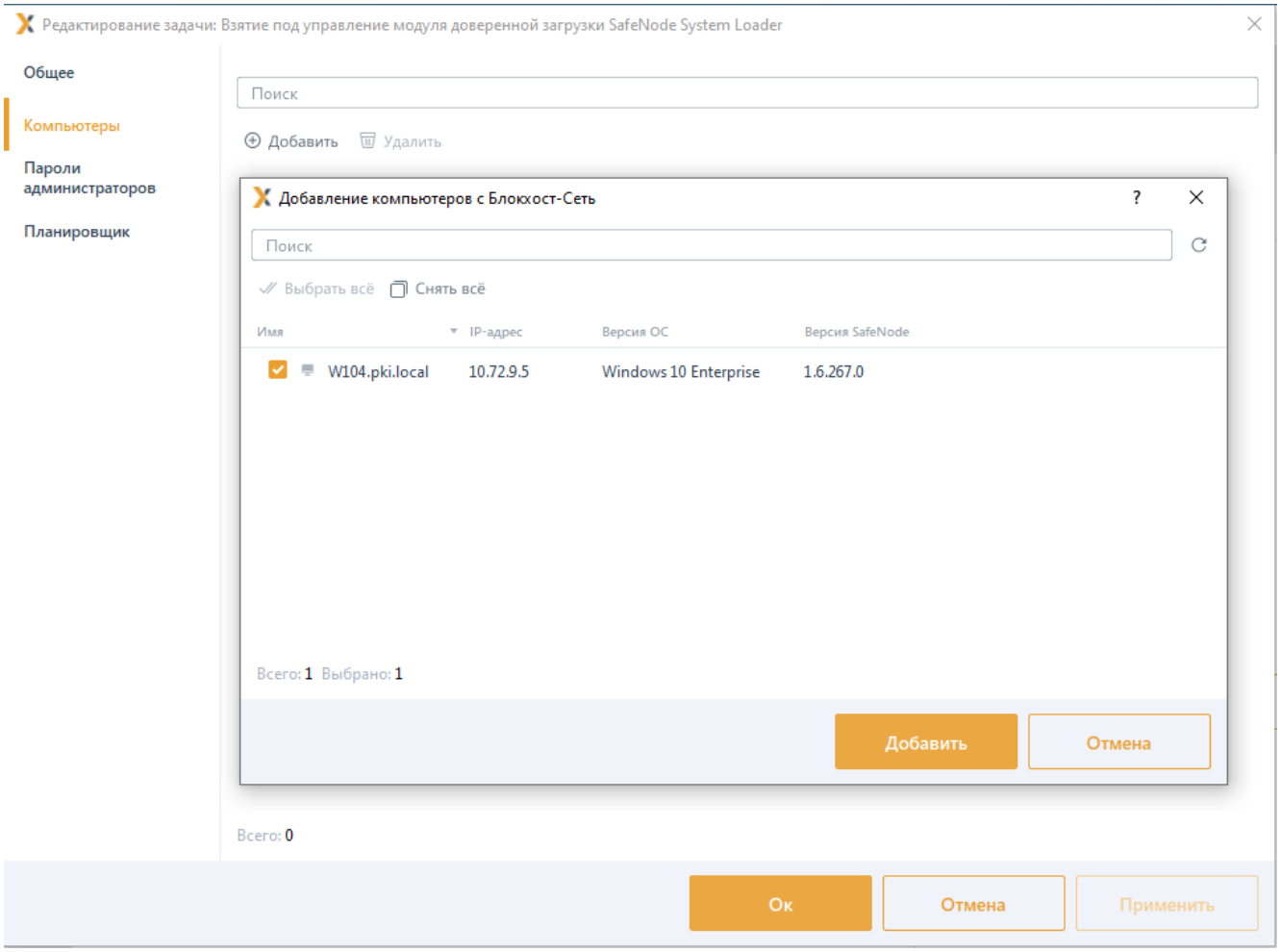


Рисунок 9.36 – Добавление рабочих станций на взятие под управление СДЗ «SafeNode System Loader»

Список рабочих станций, доступных для взятия под управление СДЗ «SafeNode System Loader» формируется из рабочих станций, на которых уже установлен агент развертывания и СДЗ «SafeNode System Loader».

Во вкладке ***Пароли администраторов*** задайте пароли локальных администраторов от всех добавленных в список рабочих станций для подтверждения прав на управление СДЗ «SafeNode System Loader» (рисунок 9.37).

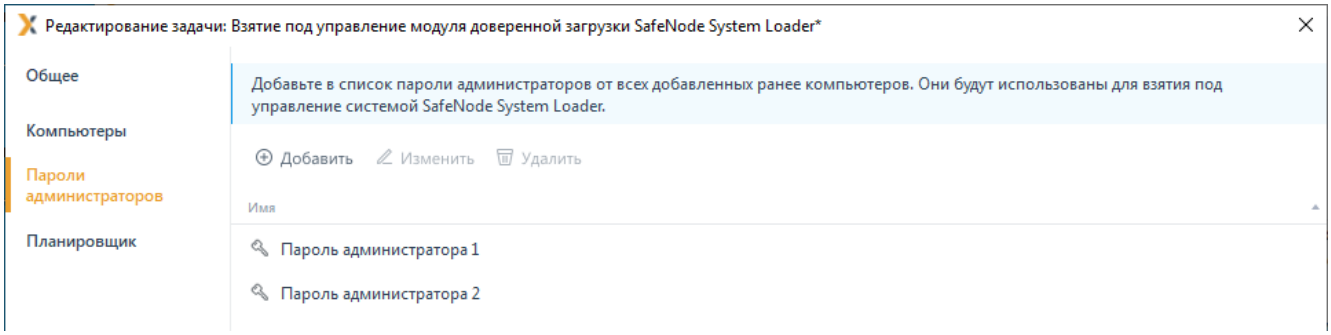


Рисунок 9.37 – Ввод паролей локальных администраторов СДЗ

Во вкладке ***Планировщик*** задайте параметры планировщика запуска задачи (подробнее в пункте ***«Указание параметров планировщика задачи по установке агента»***) и определите интервалы времени выполнения задачи (рисунок 9.38).

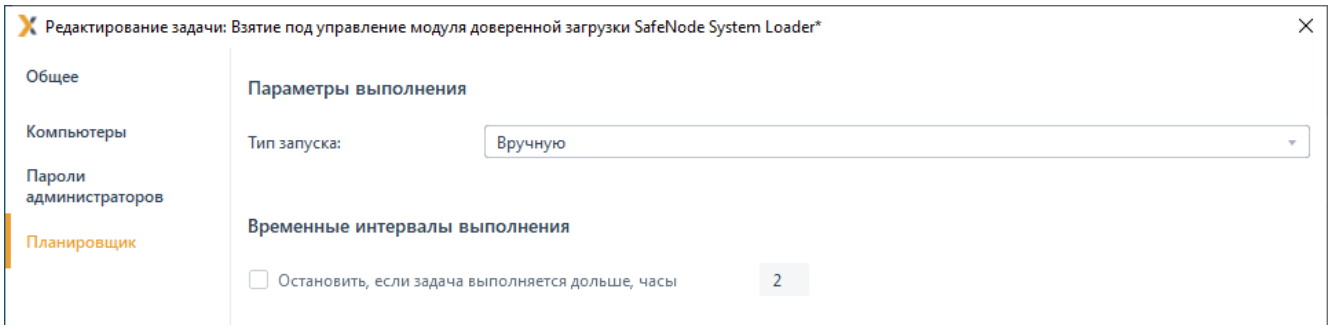


Рисунок 9.38 – Определение параметров планировщика и временных интервалов выполнения задачи

Для сохранения внесенных в задачу последовательно нажмите кнопки ***Применить*** и ***ОК*** (рисунок 9.39).

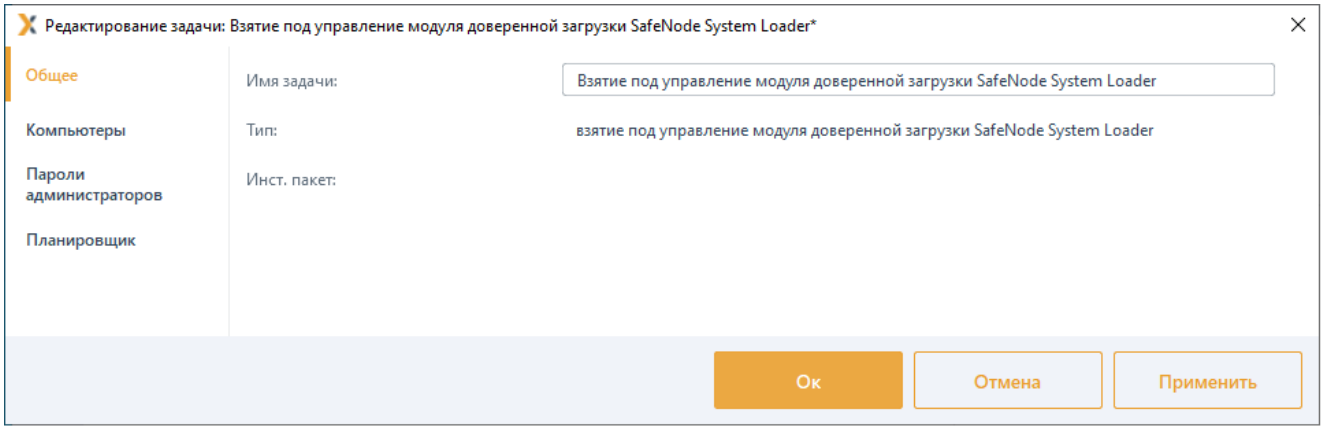


Рисунок 9.39 – Сохранение изменений в задаче

В зависимости от установленных параметров планировщика запуск задачи будет осуществлен автоматически или вручную (подробнее в пункте ***«Запуск задачи»***).

Для отслеживания состояния задачи в ходе ее выполнения на рабочей станции, перейдите по ссылке ***Все результаты*** (рисунок 6.2).

По кнопке Описание в верхней части окна (рисунок 6.3) возможен просмотр статуса выполнения задачи.

В результате выполнения задачи на взятие под управление модуля доверенной загрузки на всех указанных в списке рабочих станциях будет взят под управление СЗИ модуль доверенной загрузки «SafeNode System Loader».

9.6.2.1 Смена пароля администратора при взятии под управление

При необходимости смены пароля администратора после взятия под управление

установите флаг ***Заменять на новый пароль при взятии компьютеров под управление*** (рисунок 9.40).

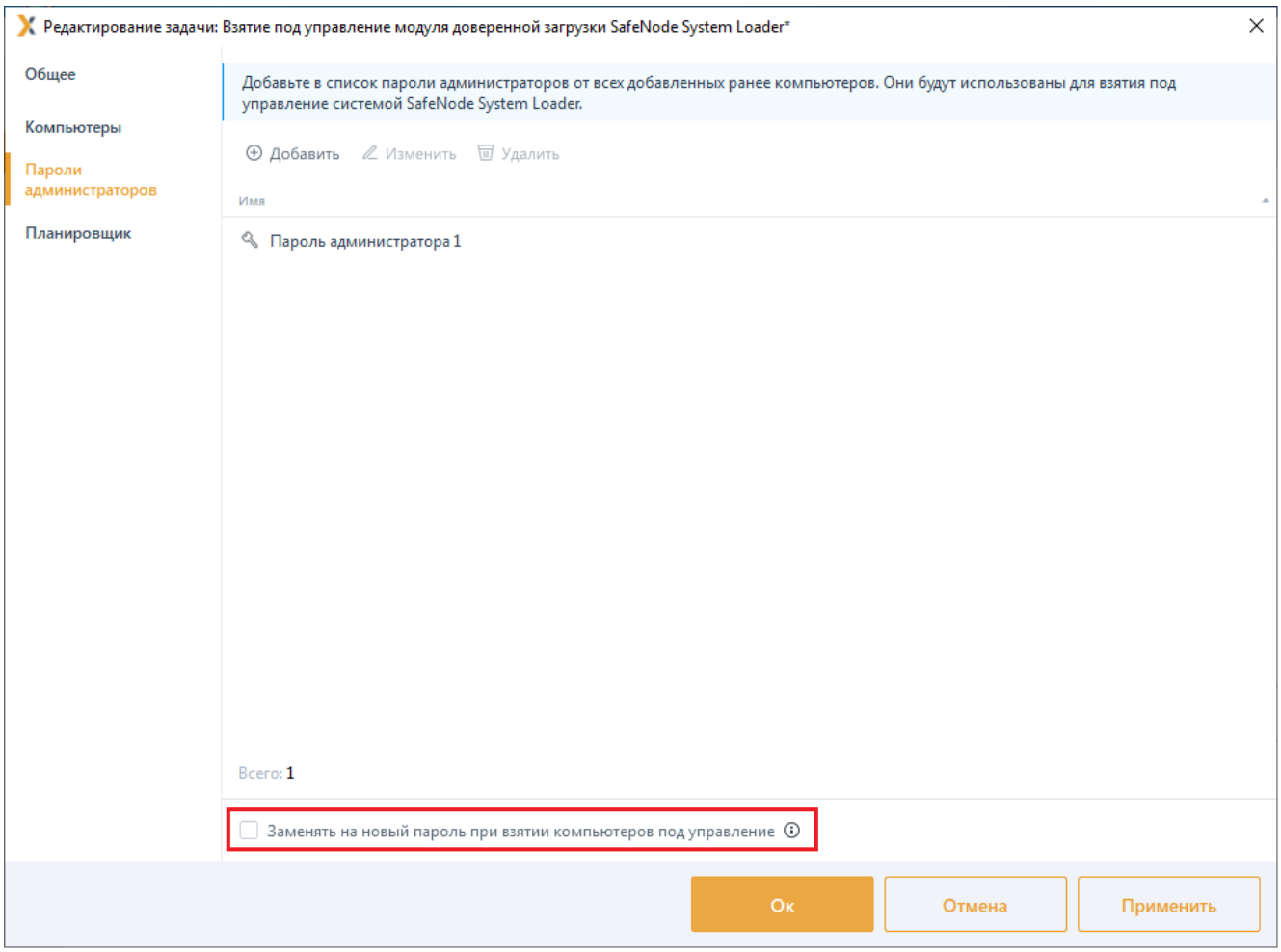


Рисунок 9.40 – Установка замены пароля при взятии компьютера под управление

После установки флага появится окно задания пароля (рисунок 9.41) с подсказкой по требованиям, предъявляемым к паролю:

– Пароль должен содержать от 10 до 32 символов.
– Пароль должен содержать символы из групп в списке ниже:
  - символы верхнего регистра (A-Z, А-Я);
  - символы нижнего регистра (a-z, а-я);
  - цифры (0-9);
  - специальные символы (! @ # $ % ^ & * ( ) _).
– Пароль не должен содержать неподдерживаемые символы Юникода.

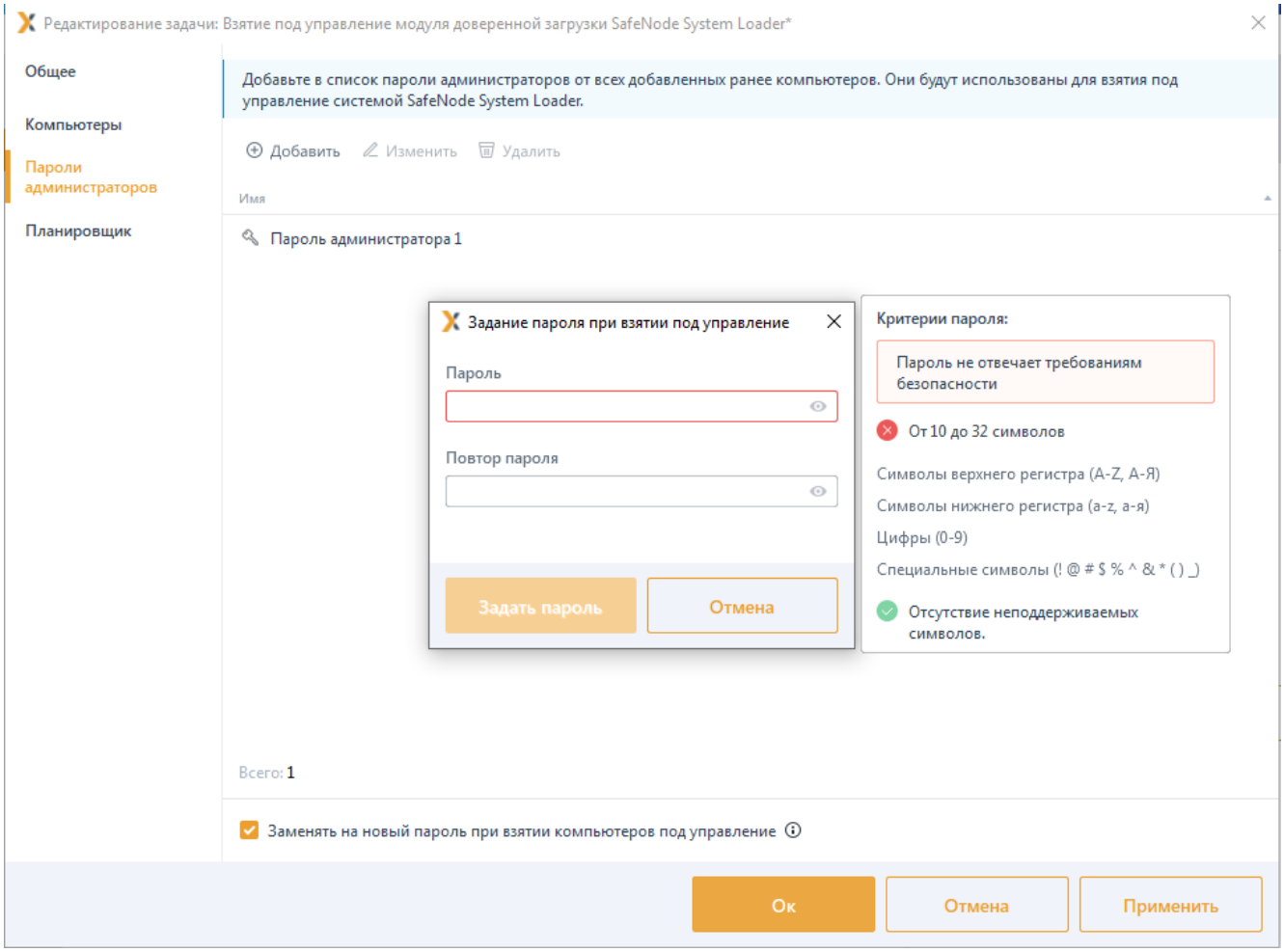


Рисунок 9.41 – Задание пароля при взятии под управление

После нажатия кнопки ***Задать пароль***, под флагом появится сообщение о том, что пароль задан с возможностью его изменить по кнопке Изменить (рисунок 9.42).

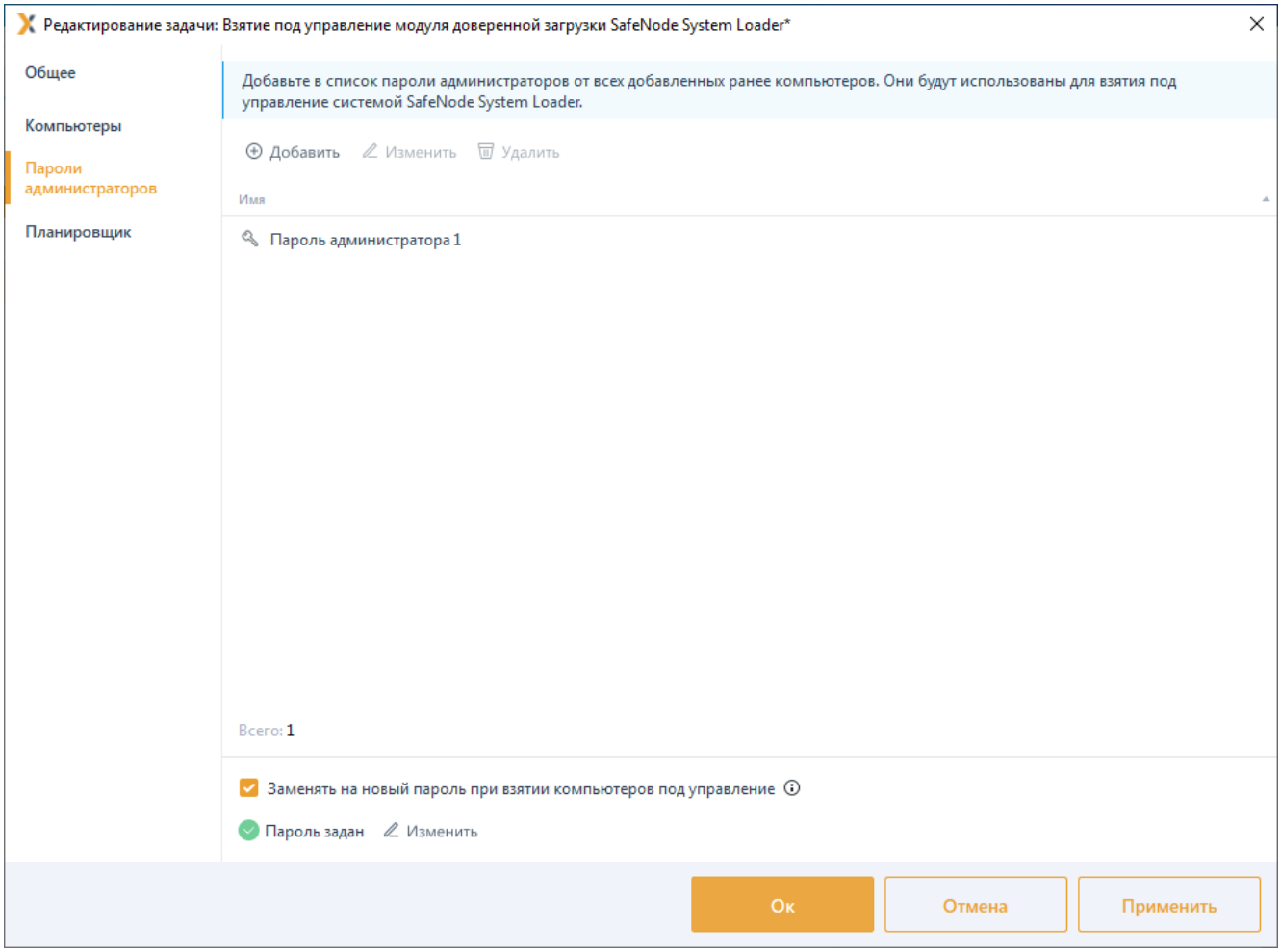


Рисунок 9.42 – Отображение заданного пароля администратора

После сохранения изменений в предустановленной задаче по взятию под управление «SafeNode System Loader» новый пароль будет добавлен в список паролей администраторов «SafeNode System Loader» (рисунок 9.43).

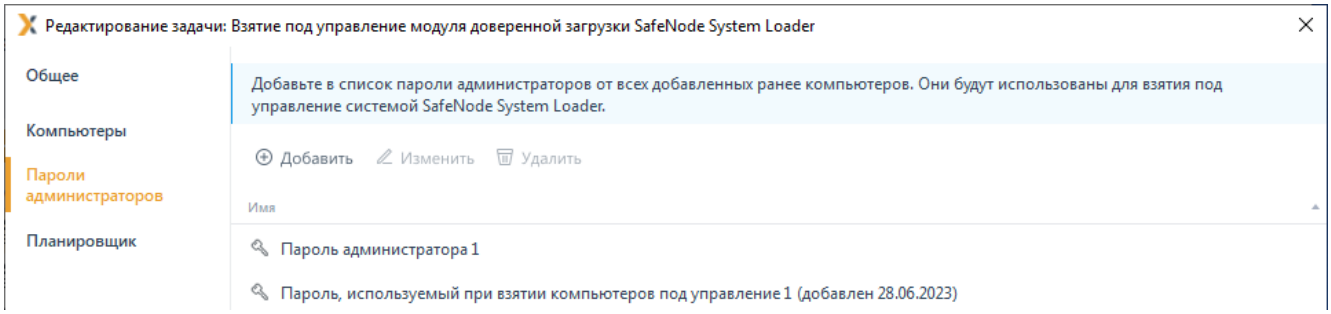


Рисунок 9.43 – Добавление нового пароля администратора в список паролей

9.6.3 Удаление СДЗ «SafeNode System Loader»

Перед осуществлением централизованного удаления изделия необходимо убедиться, что на всех рабочих станциях для администратора безопасности установлен *единый пароль.*

Перед запуском задачи на удаление изделия нужно подготовить скрипт для удаления. Для этого администратору безопасности необходимо выполнить следующие действия:

1) Создать командный файл (*.bat) содержащий:

msiexec.exe /norestart /quiet /uninstall {0AFB6386-F211-4639-A3D1-55EF122915F8} ADMINNAME=admin PASSHASH=29ac25660e3078e87e3097d3822e50d7,

где:

{0AFB6386-F211-4639-A3D1-55EF122915F8} – значение строкового параметра ***UninstallString*** объекта реестра на рабочей станции;

ADMINNAME – имя предустановленной учетной записи администратора;

PASSHASH – хеш-значение от пароля администратора по умолчанию («12345678»).

2) Перейти в ***Редактор реестра*** (***Win + R → regedit***) для получения ***UninstallString.***

3) В ***Редакторе реестра*** перейти по пути: \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ и найти раздел, содержащий информацию о СДЗ «SafeNodeSystemLoader» (рисунок 9.44).

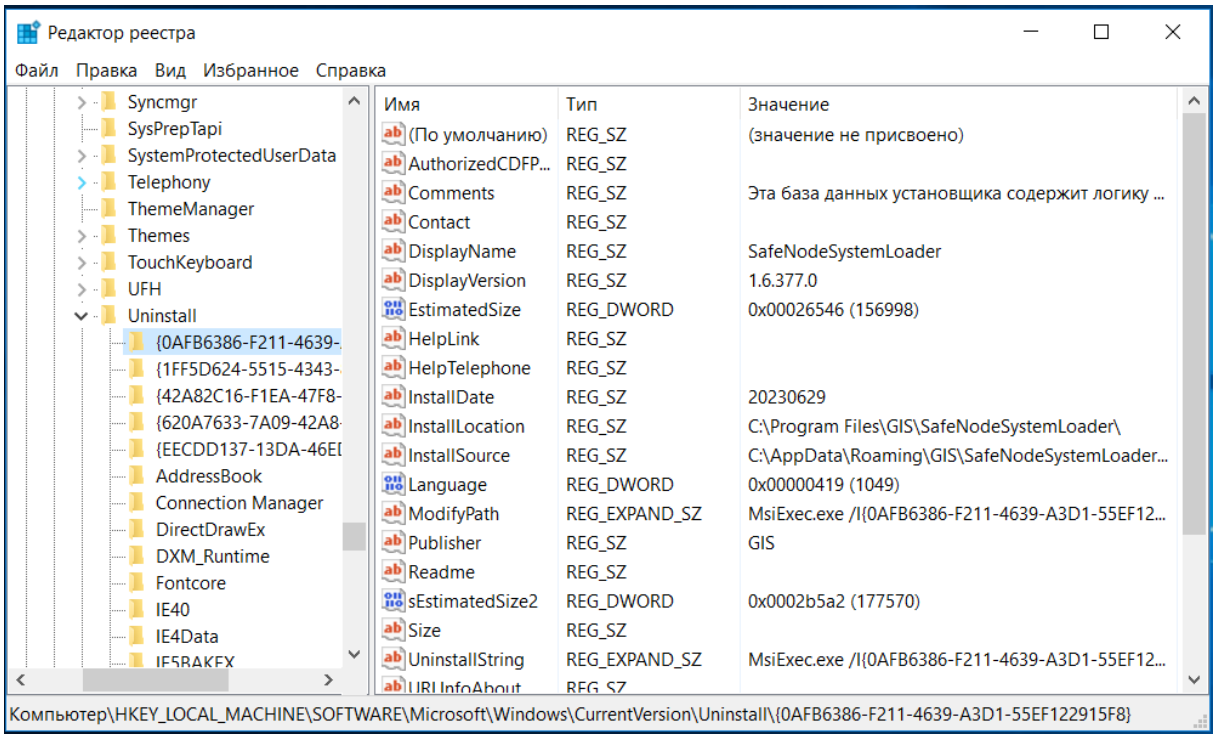


Рисунок 9.44 – Раздел, содержащий информацию о СДЗ «SafeNodeSystemLoader»

Для запуска мастера по созданию задачи на удаление программы с рабочих станций администратору безопасности необходимо в консоли управления выполнить следующие

действия.

1) Перейти в раздел **Развертывание** во вкладку **Задачи** и, нажав кнопку +, выбрать пункт ***Удаление программы*** (рисунок 9.45).

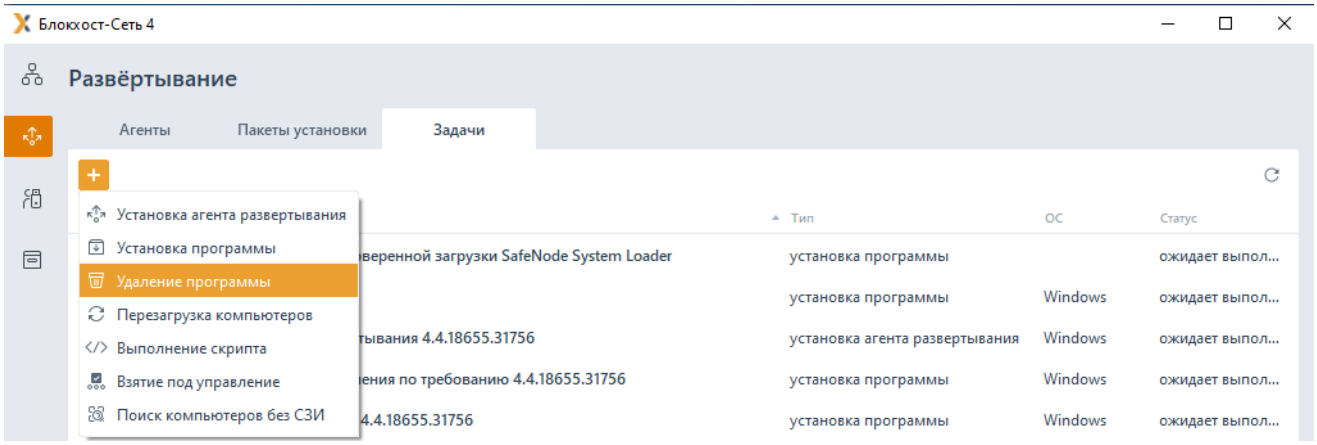


Рисунок 9.45 – Выбор задачи на удаление программы

2) В открывшемся окне мастера создания задачи на удаление программы (рисунок 9.46) выбрать подзадачу ***Выполнение скрипта для удаления программы***.

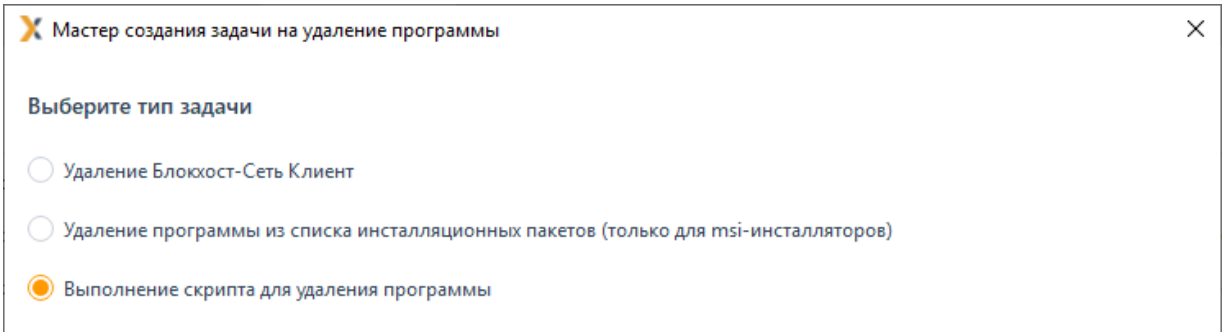


Рисунок 9.46 – Выбор параметра **Выполнение скрипта для удаления программы**

При выборе пункта **Выполнение скрипта для удаления программы** выполняется запуск мастера по созданию задачи на удаление программы (рисунок 9.47).

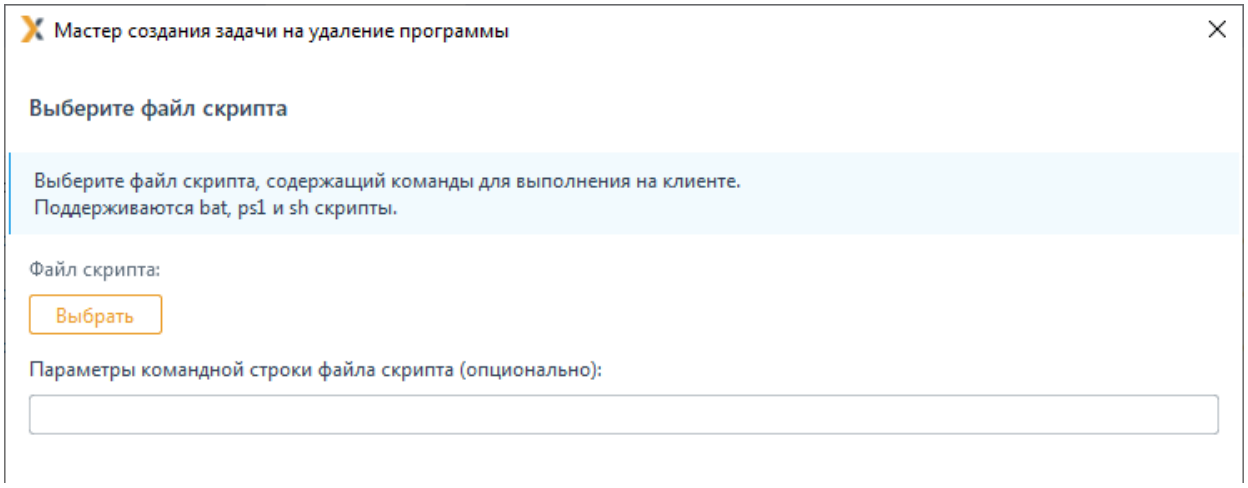


Рисунок 9.47 – Окно ввода параметров инсталляционного пакета для удаления

Администратору безопасности необходимо выполнить следующие действия:

1) На этапе выбора файла скрипта в окне мастера создания задачи на удаление программы (рисунок 9.47) выбрать ранее созданный файл (*.bat):

- в окне мастера создания задачи на удаление программы нажать кнопку ***Выбрать***;
- в открывшемся окне (рисунок 9.48) выбрать ранее созданный файл скрипта и нажать кнопку ***Открыть***.

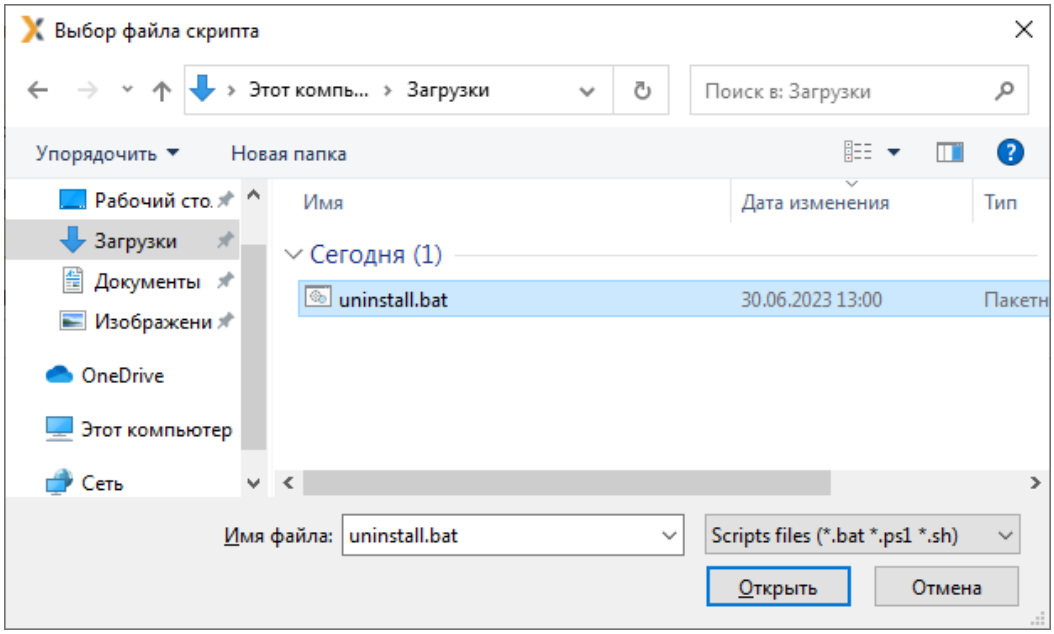


Рисунок 9.48 – Окно выбора файла скрипта

2) После успешного выбора файла (*.bat) нажать кнопку ***Далее*** для продолжения создания задачи на удаление программы.

3) На следующем шаге мастера создания задачи на удаление программы необходимо отметить рабочие станции, с которых будет удаляться выбранная

программа (рисунок 9.49) и нажать кнопку ***Далее***.

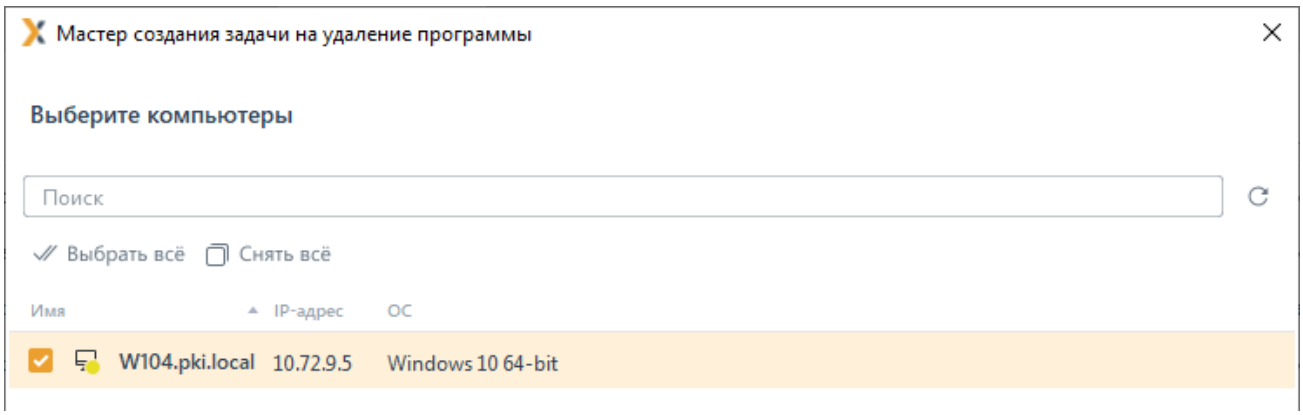


Рисунок 9.49 – Выбор рабочих станций, с которых будет произведено удаление

4) На следующем шаге мастера создания задачи на удаление программы задать параметры планировщика запуска задачи (подробнее в пункте ***«Указание параметров планировщика задачи по установке агента»***) и определить интервалы времени выполнения задачи. Для продолжения нажать кнопку ***Далее***.

5) В следующем окне мастера создания задачи на удаление программы указать параметры перезагрузки рабочей станции после удаления с нее ПО и нажать кнопку ***Далее*** (подробнее в пункте ***«Параметры перезагрузки рабочих станций»***).

Рекомендуется установить параметр ***Уведомить пользователя о необходимости перезагрузки***. После завершения задачи по установке/удалению ПО на рабочей станции откроется окно с сообщением о необходимости перезагрузки рабочей станции (рисунок 9.28).

В окне расположена кнопка ***Перезагрузить сейчас***, нажатие на которую приведет к немедленной перезагрузке рабочей станции. У пользователя не будет возможности отложить выполнение перезагрузки, когда до истечения временного интервала перезагрузки останется менее 5 минут (кнопка ***Отложить*** будет не активна).

Отмеченный параметр ***Выводить уведомление каждые (чч:мм)*** (рисунок 9.50) позволит выводить информационное сообщение через указанный промежуток времени, если пользователь закрыл его нажав кнопку ***Отложить***.

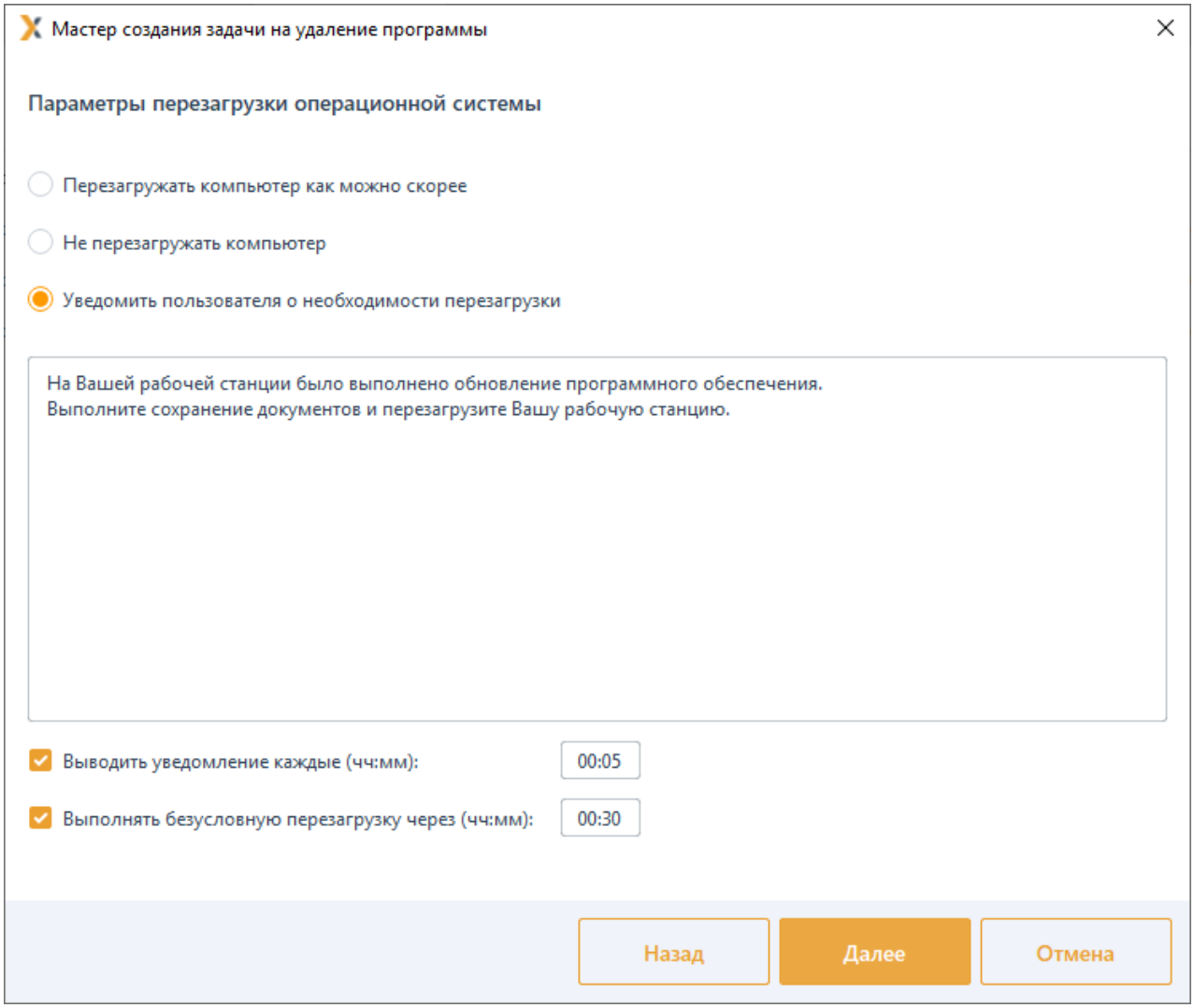


Рисунок 9.50 – Задание параметров перезагрузки ОС

6) На следующем шаге мастера создания задачи на удаление программы необходимо ввести имя создаваемой задачи и нажать кнопку ***Создать***.

7) В окне завершения работы мастера создания задачи на удаление программы нажать кнопку ***Закрыть***.

В результате работы мастера создания задачи на удаление программы в список задач будет добавлена новая задача с указанными в диалоговых окнах мастера параметрами.

Для запуска задачи необходимо выделить созданную раннее задачу в списке и нажать кнопку ***Запустить*** (рисунок 9.51). С этого момента начнется фактическое удаление изделия с рабочих станций сети.

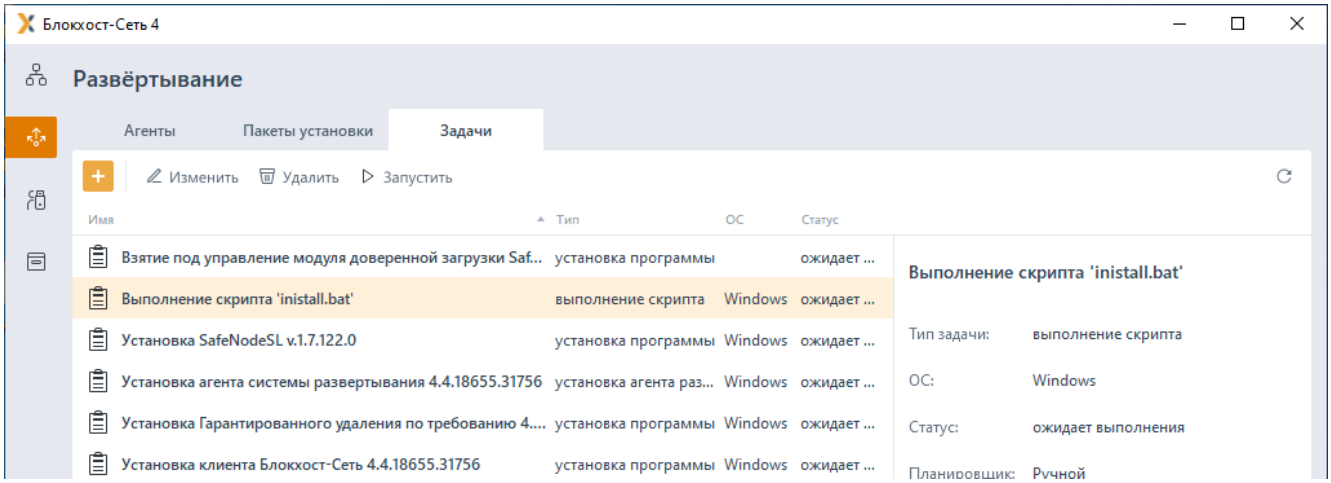


Рисунок 9.51 – Запуск задачи на удаление программы

9.7 Поиск компьютеров без СЗИ

Для создания задачи на определение наличия установленных на клиентских рабочих станциях программ: агента развертывания, клиента Блокхост-Сеть и СДЗ «SafeNode System Loader» перейдите во вкладку ***Задачи***, раскройте меню создания задач по кнопке + и выберите пункт ***Поиск компьютеров без СЗИ*** (рисунок 9.1).

В открывшемся окне создания задачи на определение наличия установленных программ (рисунок 9.52) выберите нужный домен (возможно выбрать несколько доменов) или, при отсутствии необходимого домена в списке, добавьте его по кнопке Добавить домен.

Подключение к системному домену происходит из-под текущей учетной записи или, в случае неудачи, запрашивается логин/пароль для подключения.
При подключении к пользовательскому всегда запрашивается логин/пароль для подключения (попытка подключения из-под текущей учетной записи не выполняется).

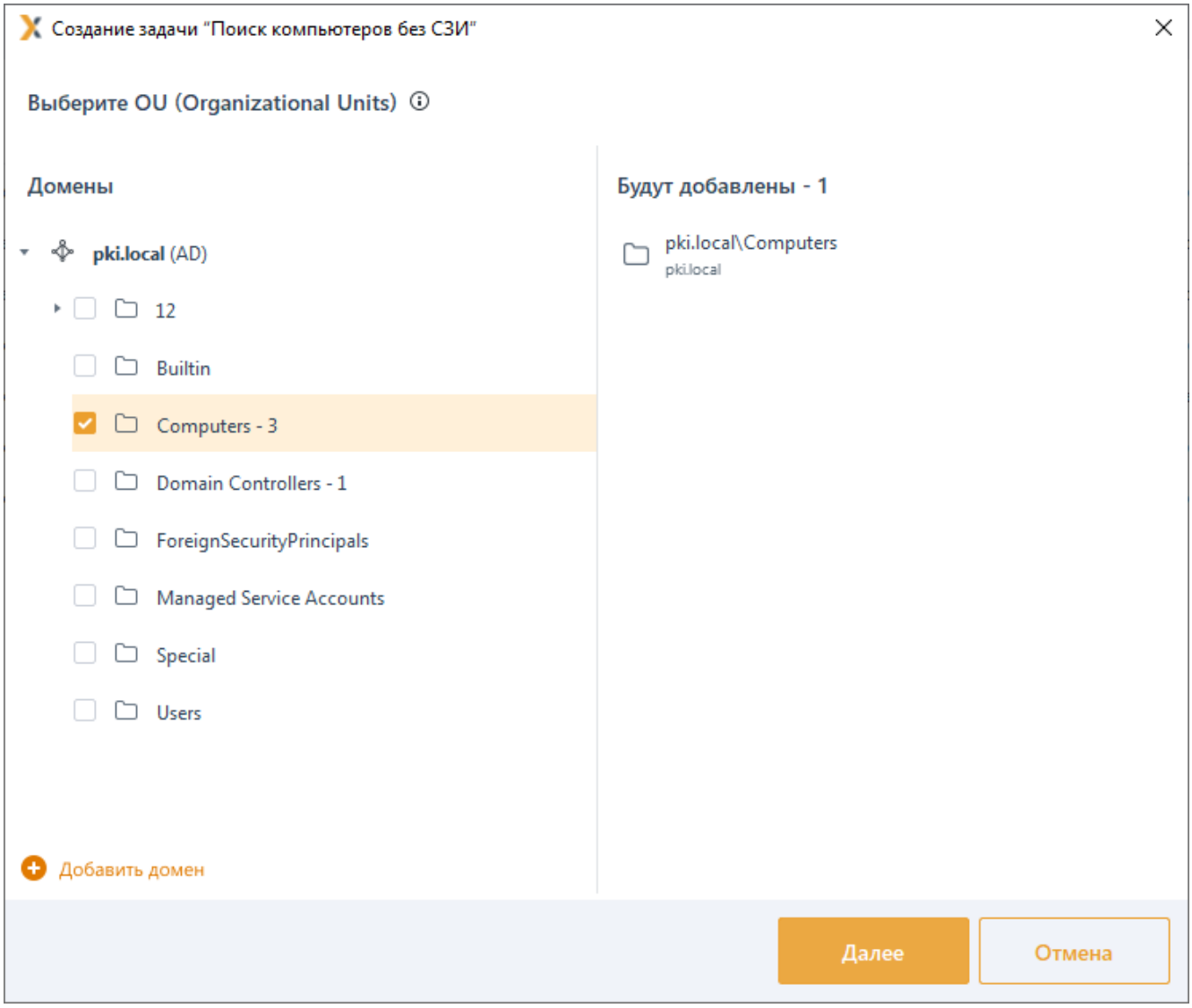


Рисунок 9.52 – Выбор домена для поиска

Укажите список *Organization Unit* в которых будет осуществляться поиск рабочих станций, на наличие установленных на них программ: агента развертывания, клиента Блокхост-Сеть и СДЗ «SafeNode System Loader», и нажмите кнопку ***Далее.***

Введите логин и пароль учетной записи, имеющей доступ к выбранному домену, и нажмите кнопку ***Далее*** (рисунок 9.53).

Если выбрано несколько доменов, необходимо ввести аутентификационные данные каждой учетной записи для доступа к выбранным доменам.

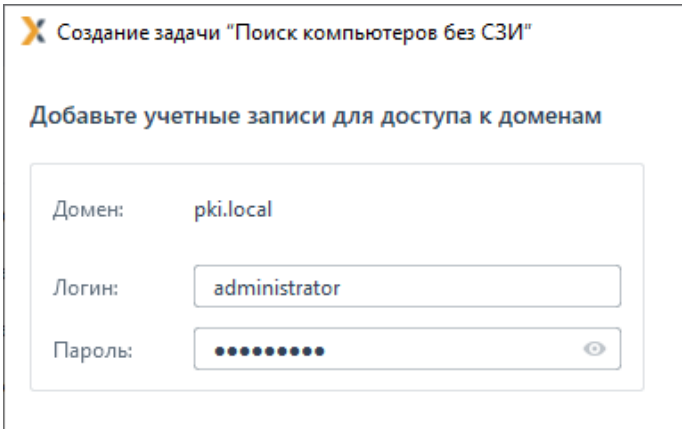


Рисунок 9.53 – Ввод аутентификационных данных учетной записи для подключения к домену

В следующем окне (рисунок 9.54) по кнопке + добавьте учетные записи пользователей (локальные или доменные), обладающие административными правами на рабочих станциях, на которых выполняется определение наличия установленных программ: агента развертывания, клиента Блокхост-Сеть и СДЗ «SafeNode System Loader».

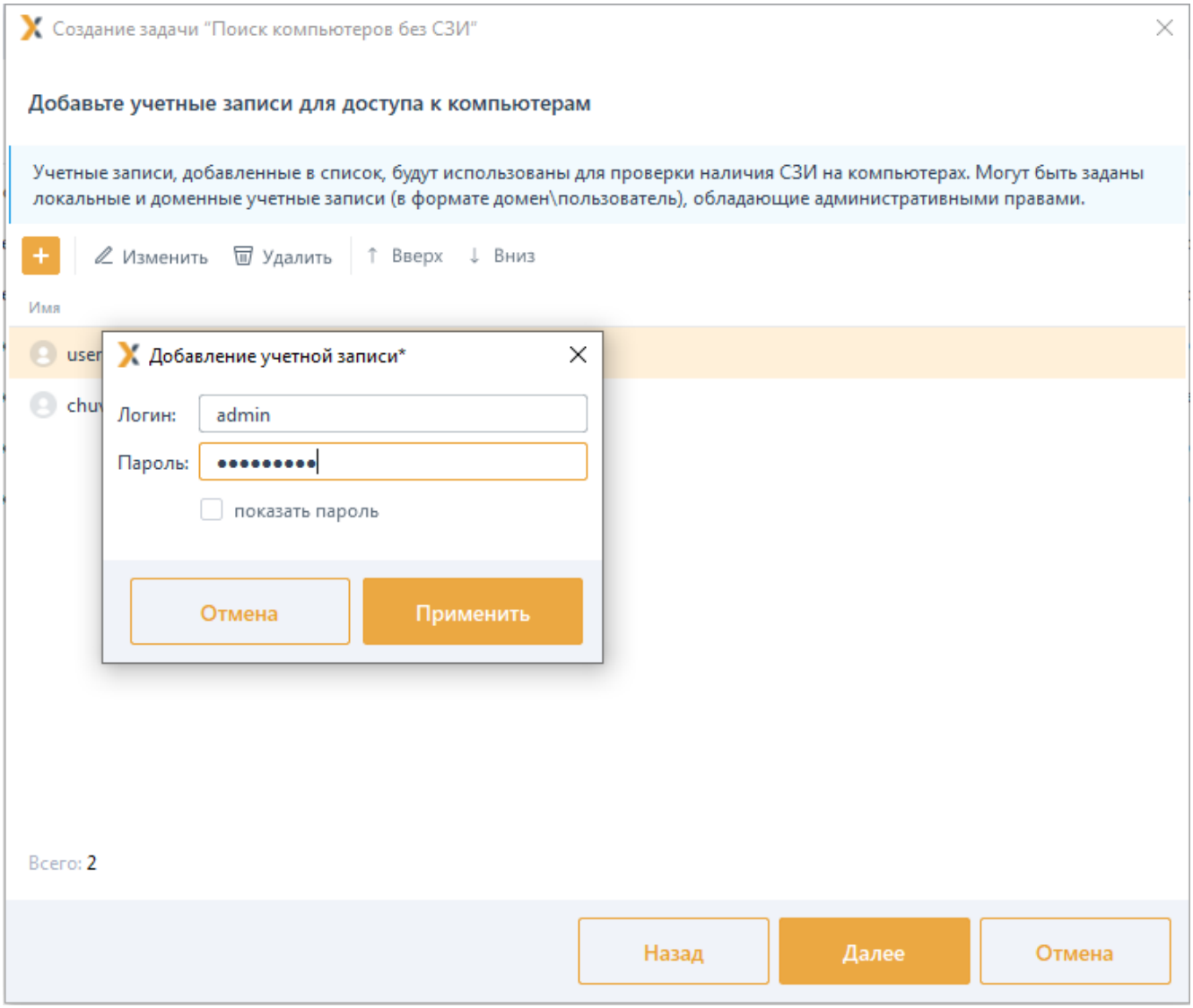


Рисунок 9.54 – Добавление учетных записей с административными правами

В следующем окне (рисунок 9.55) укажите программы: агент развертывания, клиент Блокхост-Сеть или СДЗ «SafeNode System Loader» на наличие которых будет осуществляться проверка.

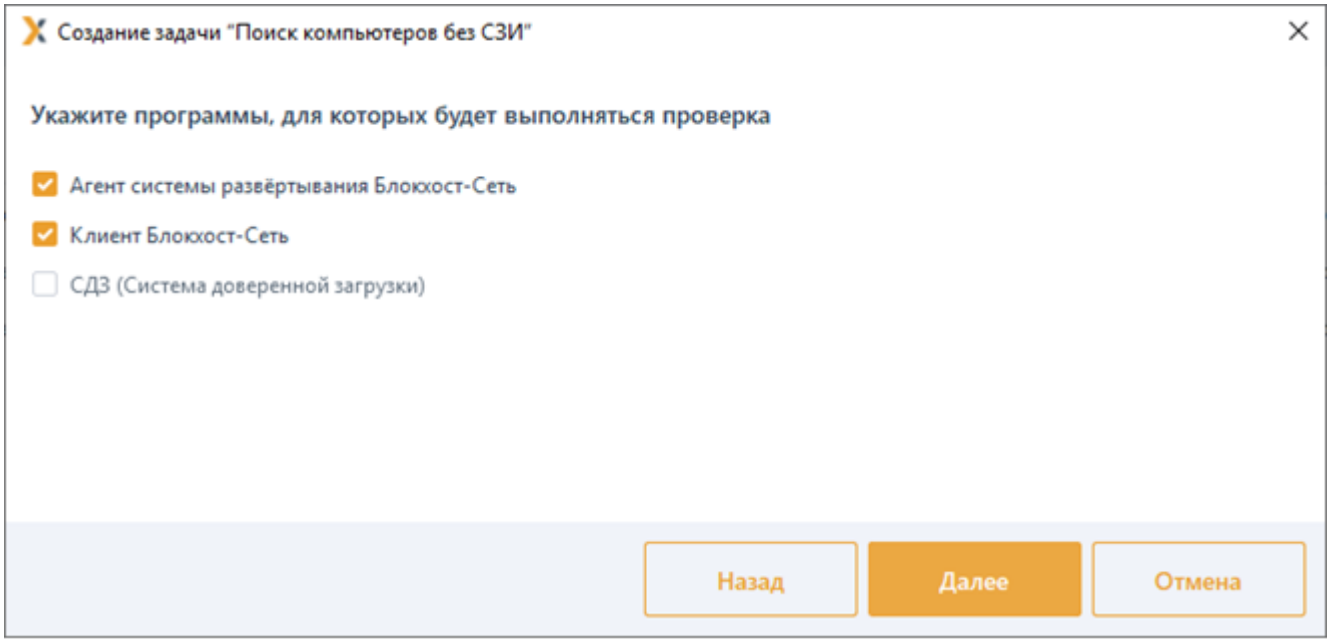


Рисунок 9.55 – Выбор программ для поиска

Задайте параметры планировщика запуска задачи (подробнее в пункте ***«Указание параметров планировщика задачи по установке агента»***) и нажмите кнопку ***Далее*** для продолжения создания задачи (рисунок 9.56).

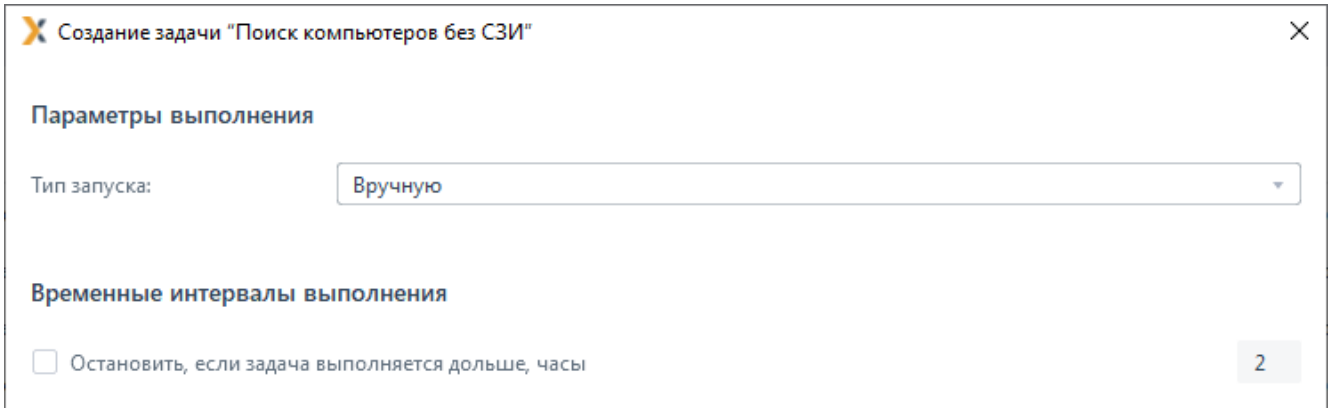


Рисунок 9.56 – Определение параметров планировщика выполнения задачи

Введите имя создаваемой задачи и нажмите кнопку ***Создать*** (рисунок 9.57).

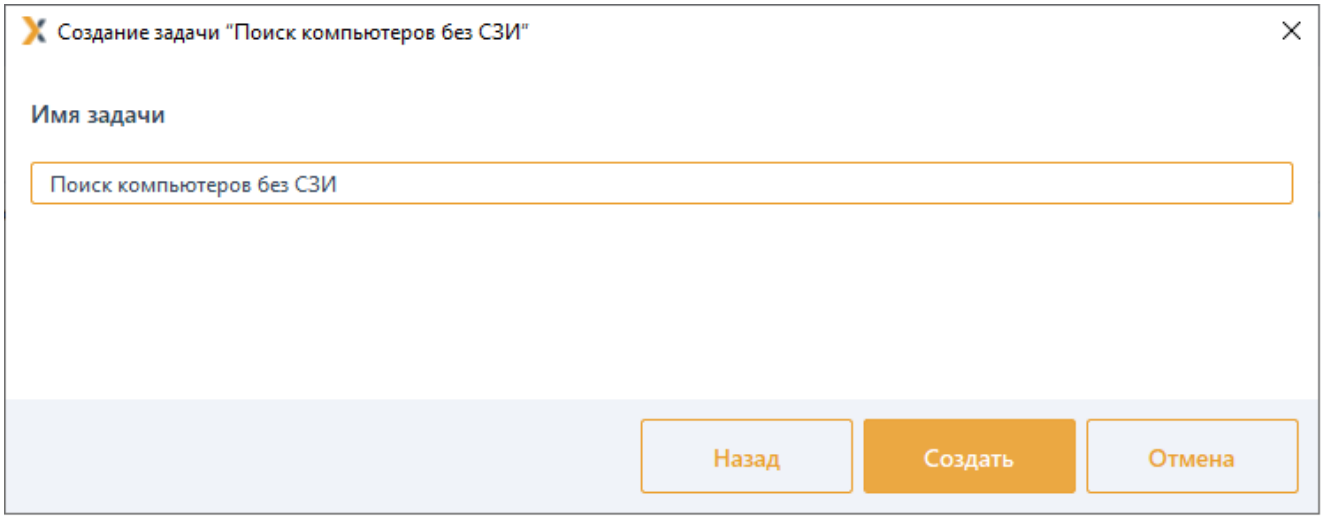


Рисунок 9.57 – Ввод имени создаваемой задачи

В случае успешного завершения создания задачи появится окно с сообщением о создании задачи «Поиск компьютеров без СЗИ» (рисунок 9.58).

Рисунок 9.58 – Завершение создания задачи «Поиск компьютеров без СЗИ»

В результате во вкладке ***Задачи*** будет создана новая задача «Поиск компьютеров без СЗИ» с заданными в ходе работы мастера создания задачи параметрами.

9.7.1 Результаты выполнения задачи на определение наличия установленных программ

Результатов выполнения задачи на определение наличия установленных программ (агента развертывания, клиента Блокхост-Сеть и СДЗ «SafeNode System Loader») может быть несколько в одной задаче в зависимости от количества рабочих станций в задаче.

Каждый результат является ссылкой, переход по которой открывает окно просмотра операций, выполненных в ходе выполнения задачи (рисунок 9.59). Результаты выполнения задачи и их описание, приведены в таблице 9.1.

Таблица 9.1 – Результат выполнения задачи на определение наличия установленных программ

Результат выполнения задачи	**Описание установленного результата выполнения задачи**
Выполняется	Клиентская рабочая станция найдена в OU, но процесс определения наличия/версий установленных на ней программ (агент/клиент/СДЗ) еще не был запущен.
Установлено	На рабочей станции установлены **все искомые** программы, выбранные при

	создании задачи (рисунок 9.55).
Не установлено	На рабочей станции установлены **не все искомые** программы , выбранные при создании задачи (рисунок 9.55).
Завершено с ошибкой	Статус может быть выведен для: • OU, если в процессе подключения к соответствующему домену возникла ошибка (например, задана некорректная учетная запись для доступа к домену); • рабочей станции, если на каком-либо этапе процесса определения наличия/версий установленных на нем программ возникла ошибка (например, задана некорректная учетная запись для доступа к рабочей станции).
Недоступны	Статус может быть выведен для • OU, если к соответствующему домену не удалось получить доступ (например, контроллер домена выключен). • рабочей станции, если к найденной рабочей станции не удалось подключиться (например, рабочая станция выключена).
Не завершено	Статус выводится для найденных в OU компьютеров, на которых процесс определения наличия и версий установленных программ не был завершен из-за преждевременной остановки задачи.

Для просмотра отчета с результатами выполнении задачи на рабочей станции, перейдите по одной из имеющихся ссылок <*статус задачи*>, либо по ссылке ***Все результаты*** (рисунок 9.59).

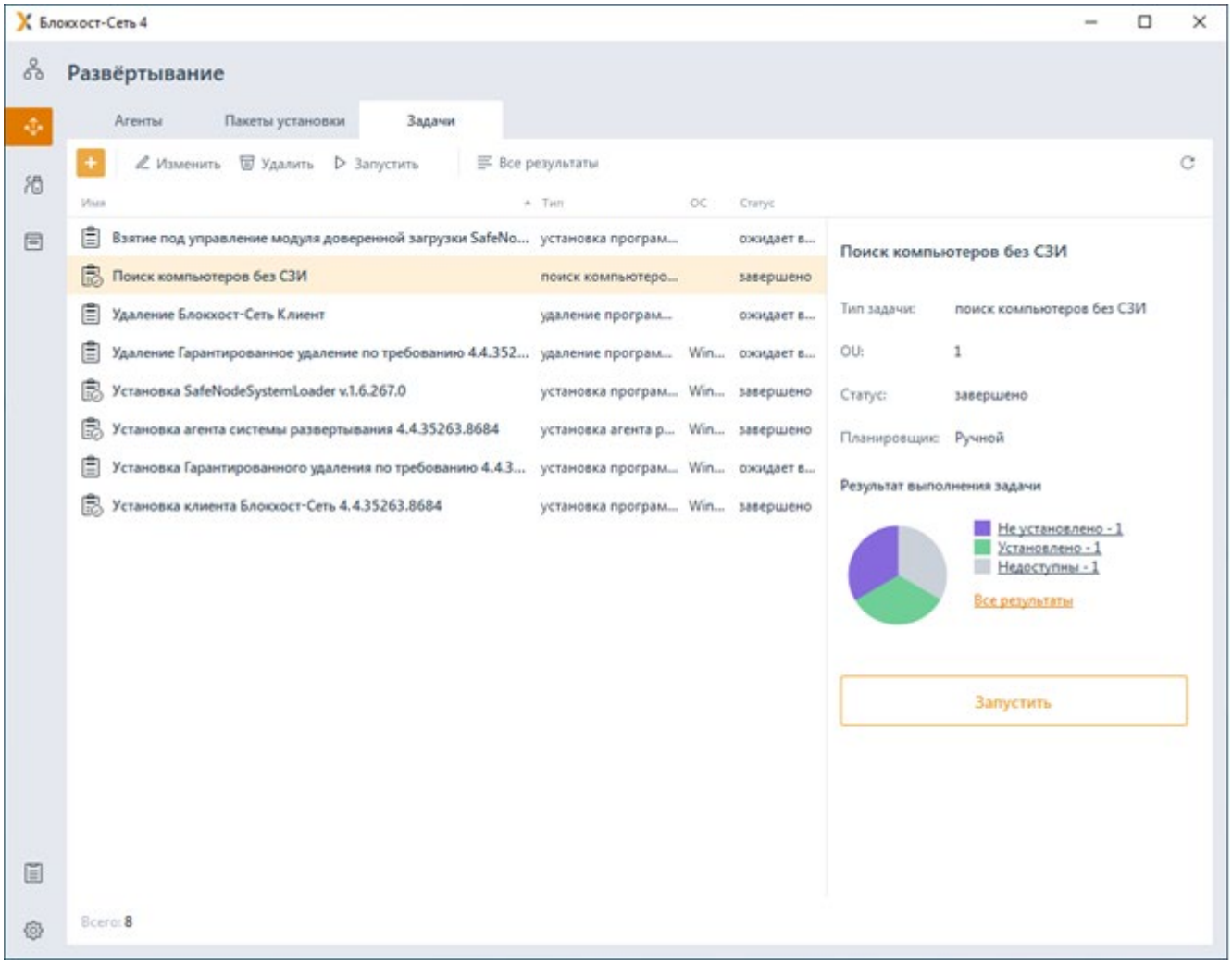


Рисунок 9.59 – Результат выполнения задачи

В окне просмотра результатов (рисунок 9.60) будет отображен перечень рабочих станций, на которых осуществлялся процесс определения наличия установленных программ: агента развертывания, клиента Блокхост-Сеть или СДЗ «SafeNode System Loader»:

– ***Статус*** – результат выполнения задачи на определение наличия установленных программ (см. в таблице 9.1);

– ***ОС*** – тип операционной системы рабочей станции;

– ***Агент*** – наличие агента развертывания на рабочей станции (при наличии определяется версия установленного агента);

– ***Блокхост-Сеть*** – наличие клиента Блокхост-Сеть на рабочей станции (при наличии определяется версия установленного клиента);

– ***СДЗ*** – наличие СДЗ «SafeNode System Loader» на рабочей станции (при наличии определяется версия установленного СДЗ);

– ***Описание*** – дополнительное пояснение, если задача завершилась с ошибкой.

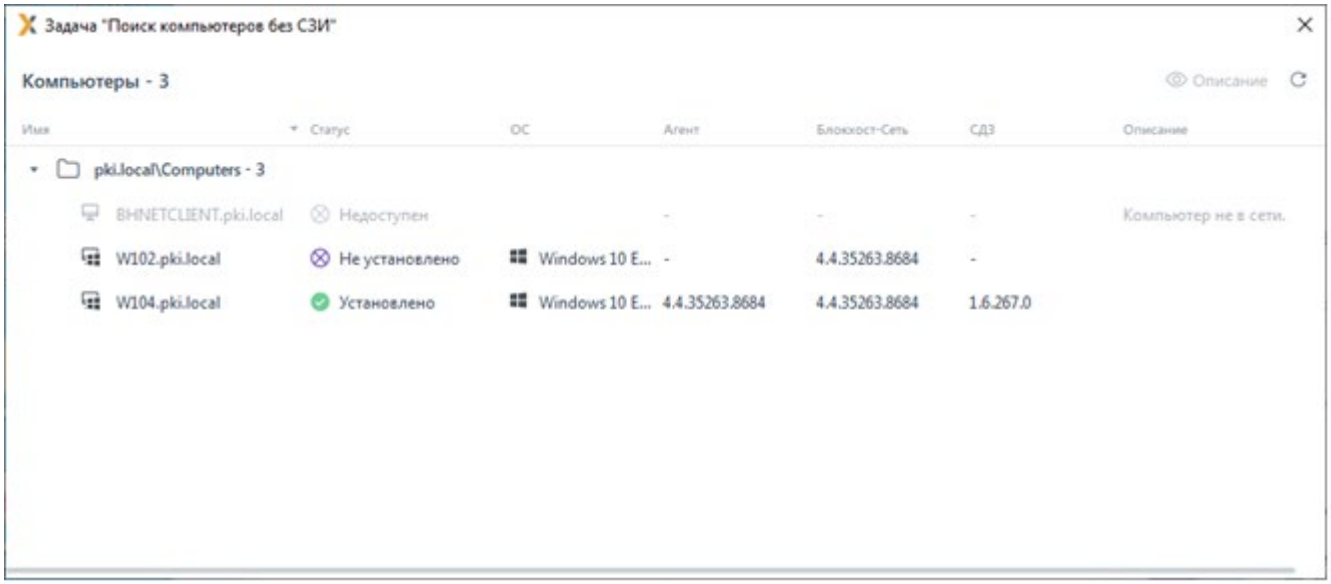


Рисунок 9.60 – Отчет с результатами выполнения задачи

9.8 Настройка входа по сертификатам

Описание задачи по настройке аутентификации пользователя на клиентской рабочей станции под управлением ОС Linux с использованием токена, с записанным на нем сертификатом, приведено в документах «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора. Часть 3. Настройка подсистемы управления токенами, ЦС Microsoft CA» и «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора. Часть 4. Настройка подсистемы управления токенами, ЦС DogTag».

10 Подсистема сбора событий

Основная работа с подсистемой сбора событий аудита осуществляется во вкладках ***Статистика*** и ***События***, доступных по кнопке  .

Подсистема сбора событий аудита предназначена для сбора событий аудита с клиентских рабочих станций, формирования сводных отчетов с информацией о состоянии клиентов, подключенных к серверам иерархии, просмотра и фильтрации событий аудита, собранных с клиентских компьютеров на сервер, а также напрямую из журнала клиентского компьютера.

Во вкладке ***Статистика*** отображается сводная статистика только по выбранному серверу или с учетом всех подчиненных серверов, находящимся в прямом или косвенном подчинении выбранному серверу.

Вкладка ***События*** предназначена для отслеживания событий, заданных политиками и настройками сервера или клиентского компьютера, происходящих на подчиненных серверах или зафиксированных на выбранном клиентском компьютере.

10.1 Вкладка «Статистика»

Во вкладке ***Статистика*** отображается сводная статистика только по текущему серверу или с учетом всех подчиненных серверов, находящимся в прямом или косвенном подчинении выбранному серверу (рисунок 10.1).

Сводная статистика только по текущему серверу предполагает отображение событий аудита, в соответствии с заданными политиками и настройками сервера, собранных только с клиентских компьютеров текущего сервера, подчиненных ему напрямую.

Сводная статистика с учетом всех подчиненных серверов предполагает отображение событий аудита, в соответствии с заданными политиками и настройками сервера, собранных и с клиентских компьютеров текущего сервера и со всех подчиненных серверов, находящихся на любом нижестоящем уровне иерархии по отношению к текущему серверу.

Клиентские компьютеры подчиненных серверов, находящихся в состоянии ***офлайн***, не учитываются в сводной статистике.

При переходе подчиненного сервера из состояния ***офлайн*** в состояние ***онлайн*** необходимо обновить информацию во вкладке по кнопке , для включения собранных данных в сводную статистику.

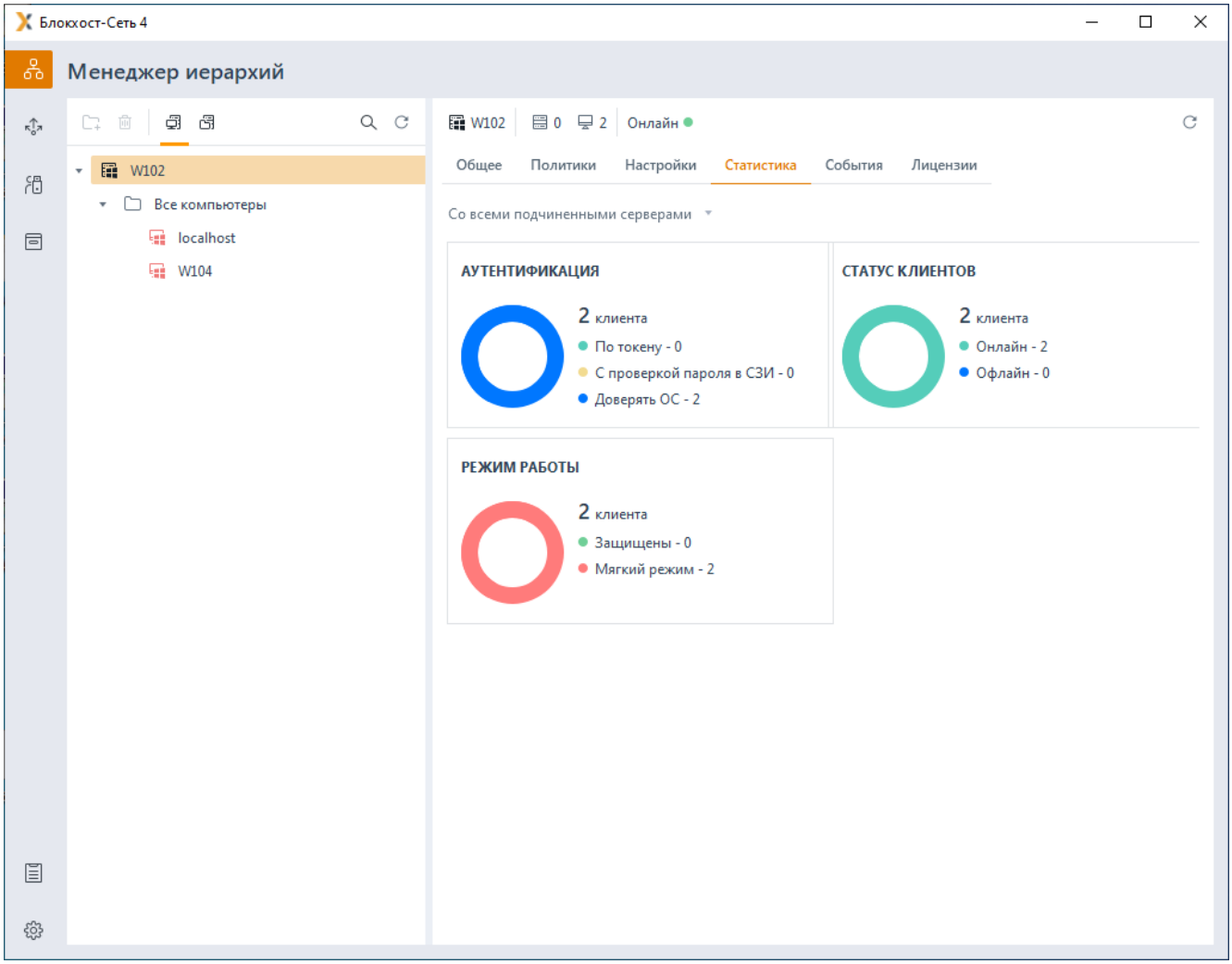


Рисунок 10.1 – Вкладка ***Статистика***

По умолчанию, во вкладке ***Статистика*** отображается сводная статистика с учетом всех подчиненных серверов. Для просмотра сводной статистики только по текущему серверу, необходимо раскрыть список в верхней части вкладки и выбрать ***Только для текущего сервера*** (рисунок 10.2).

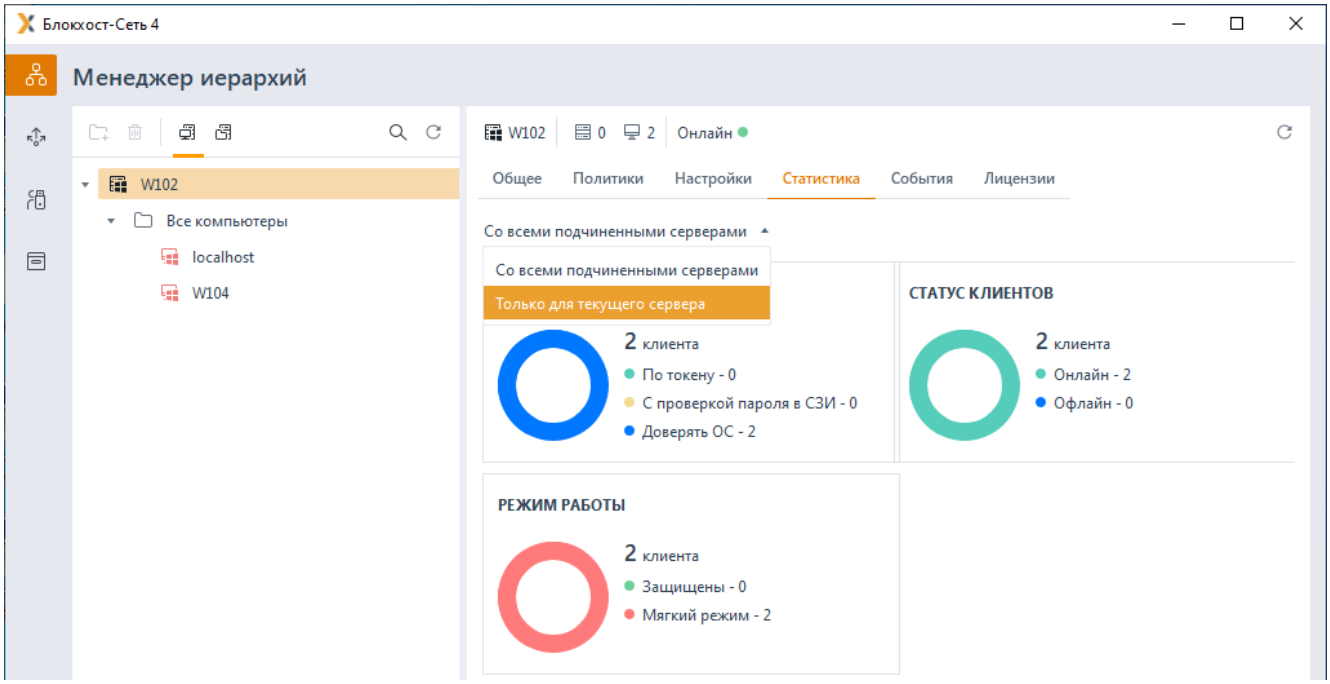


Рисунок 10.2 – Статистика только для текущего сервера

События во вкладке ***Статистика***, поделены на три области:

– ***Аутентификация*** – сводная статистика по клиентам в зависимости от типа аутентификации;

– ***Статус клиентов*** – сводная статистика по клиентам в зависимости от состояния клиентов;

– ***Режим работы*** – сводная статистика по клиентам в зависимости от их режима работы.

Все перечисленные области имеют схожую структуру и содержат общие элементы (рисунок 10.3):

1) Диаграмму, наглядно демонстрирующую пропорциональное соотношение распределения возможных значений контролируемого параметра на клиентских компьютерах.

2) Общее количество клиентских компьютеров.

3) Возможные значения, которые может принимать контролируемый параметр аудита и количество клиентов, с тем или иным значением параметра.

4) Кнопку ⋮, открывающую окно, содержащее полный список клиентских компьютеров и детальную информацию по каждому контролируемому параметру.

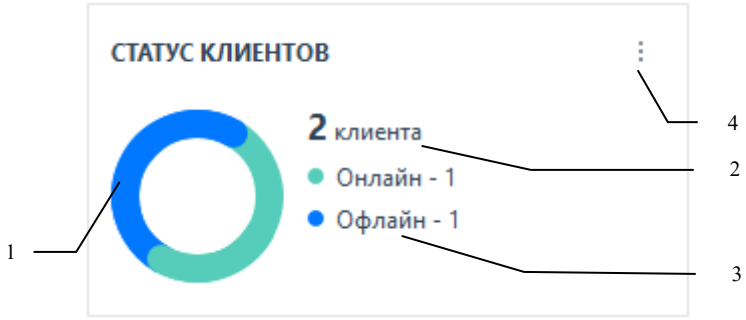


Рисунок 10.3 – Общая схема отображения сводных данных аудита

10.1.1 Сводная статистика по типу аутентификации

В области ***Аутентификация*** отображается информация о типе аутентификации пользователей на клиентских компьютерах (рисунок 10.4).

Возможны следующие варианты аутентификации пользователей:

– по токену (двухфакторная аутентификация с применением аппаратного идентификатора);

– с проверкой пароля в СЗИ (аутентификация с использованием механизма Блокхост-Сеть – проверка введенного пароля с паролем пользователя, хранящимся в БД);

– доверять ОС (аутентификация стандартными средствами операционной системы).

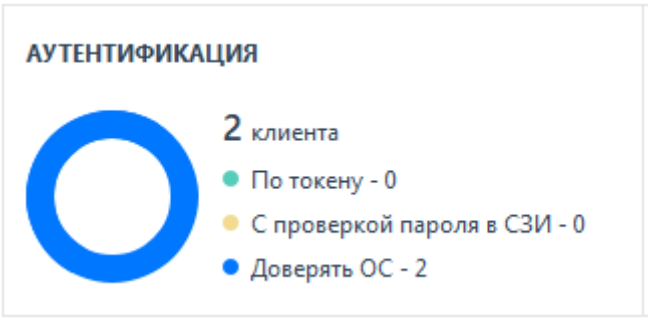


Рисунок 10.4 – Сводная статистика по типу аутентификации на клиентах

Необходимо учитывать, что в итоговой статистике учитывается только последний тип аутентификации пользователя на клиентском компьютере.

Для просмотра статистики по всем серверам, являющимся подчиненными по отношению к текущему, перейдите в окно ***Статистика подчиненных серверов по типу аутентификации*** по кнопке (рисунок 10.5).

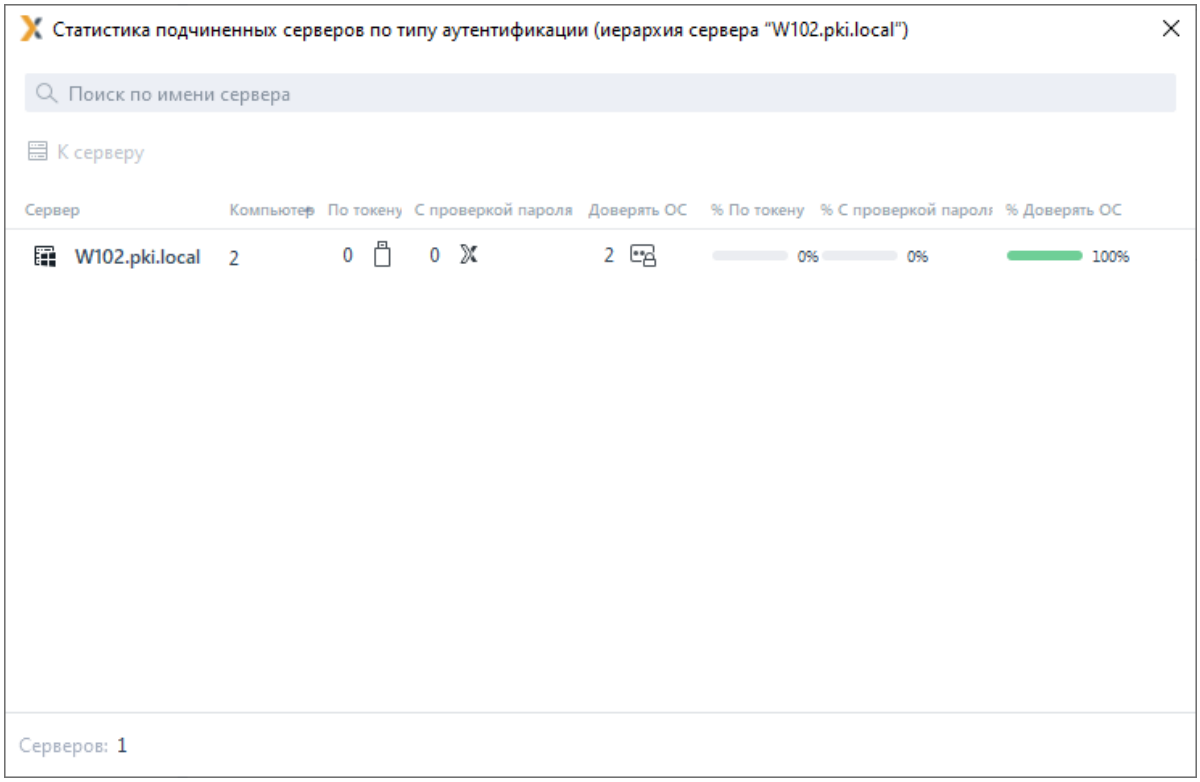


Рисунок 10.5 – Распределение клиентов по типу аутентификации

Для каждого сервера в списке в окне ***Статистика подчиненных серверов по типу аутентификации*** отображается информация:

– *Сервер* - DNS-имя сервера;

– *Компьютер* – общее количество клиентских компьютеров сервера;

– *По токену* – количество клиентов с аутентификацией пользователей с применением аппаратного идентификатора;

– *% По токену* – процентное соотношение количества клиентов с аутентификацией по токену к общему числу клиентов;

– *С проверкой пароля в СЗИ* – количество клиентов с аутентификацией пользователей с использованием механизма Блокхост-Сеть;

– *% С проверкой пароля в СЗИ* – процентное соотношение количества клиентов с аутентификацией с использованием Блокхост-Сеть к общему числу клиентов;

– *Доверять ОС* – количество клиентов с аутентификацией пользователей стандартными средствами ОС;

– *% Доверять ОС* – процентное соотношение количества клиентов с аутентификацией стандартными средствами ОС к общему числу клиентов.

10.1.2 Сводная статистика по статусу клиентов

В области ***Статус клиентов*** отображается информация о нахождении клиентских компьютеров в сети (онлайн или офлайн) (рисунок 10.6).

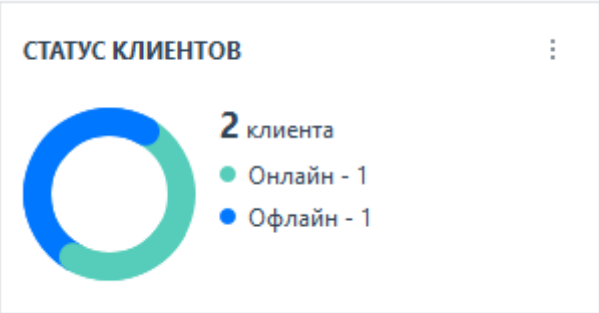


Рисунок 10.6 – Статус клиентов в сети

Для просмотра статистики по всем серверам, являющимся подчиненными по отношению к текущему, перейдите в окно ***Статистика подчиненных серверов по статусу*** по кнопке (рисунок 10.7).

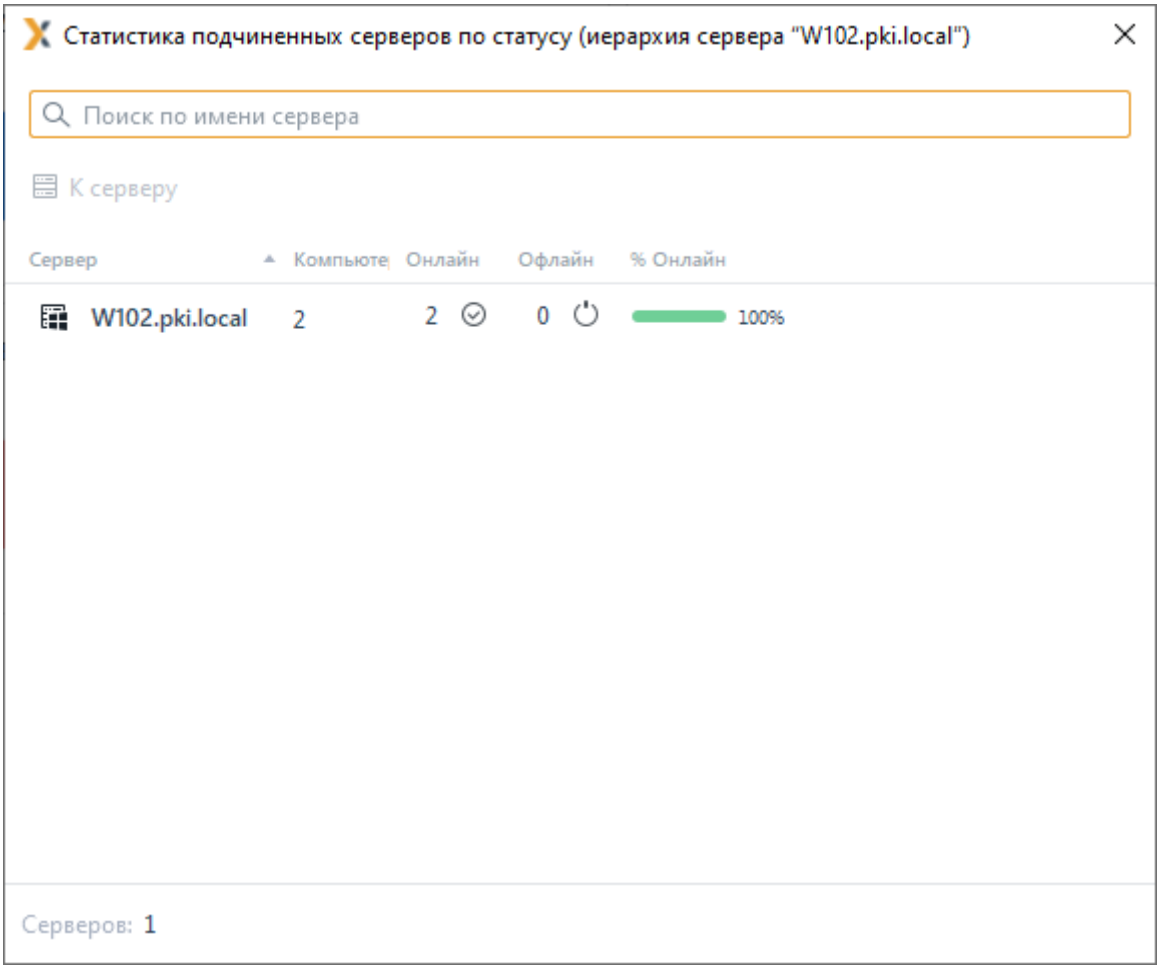


Рисунок 10.7 – Статистика клиентов в сети

Для каждого сервера в окне ***Статистика подчиненных серверов по статусу*** отображается информация:

– *Сервер* – DNS-имя сервера;

– *Компьютер* – общее количество клиентских компьютеров сервера;

– *Онлайн* – общее количество клиентов сервера в состоянии онлайн;

– *Офлайн* – общее количество клиентов сервера в состоянии офлайн;

– *% Онлайн* – процентное соотношение количества клиентов, находящихся в состоянии онлайн, к общему количеству клиентов (округление производится в меньшую сторону при >= 50%, в большую сторону при < 50%);

10.1.3 Сводная статистика по режиму работы клиентов

В области ***Режим работы*** отображается информация о режиме работы клиентских компьютеров (рисунок 10.8).

Возможные режимы работы клиентов:

– ***защищены*** – все настроенные механизмы защиты, функционируют в полном объеме;

– ***мягкий режим*** – доступ пользователей к запрещенным ресурсам разрешен; осуществляется только регистрация событий, связанных с попытками доступа к запрещенной информации.

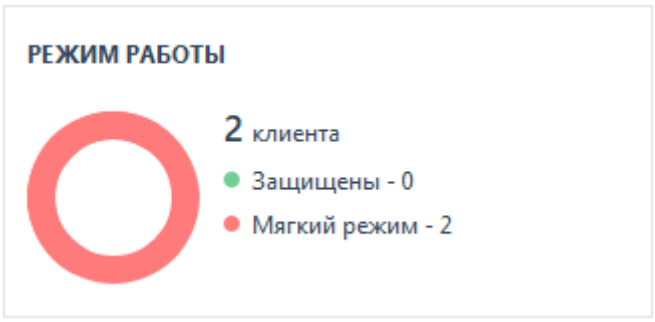


Рисунок 10.8 – Режим работы клиентов

Для просмотра статистики по всем серверам, являющимся подчиненными по отношению к текущему, перейдите в окно ***Статистика подчиненных серверов по режиму работы*** по кнопке (рисунок 10.9).

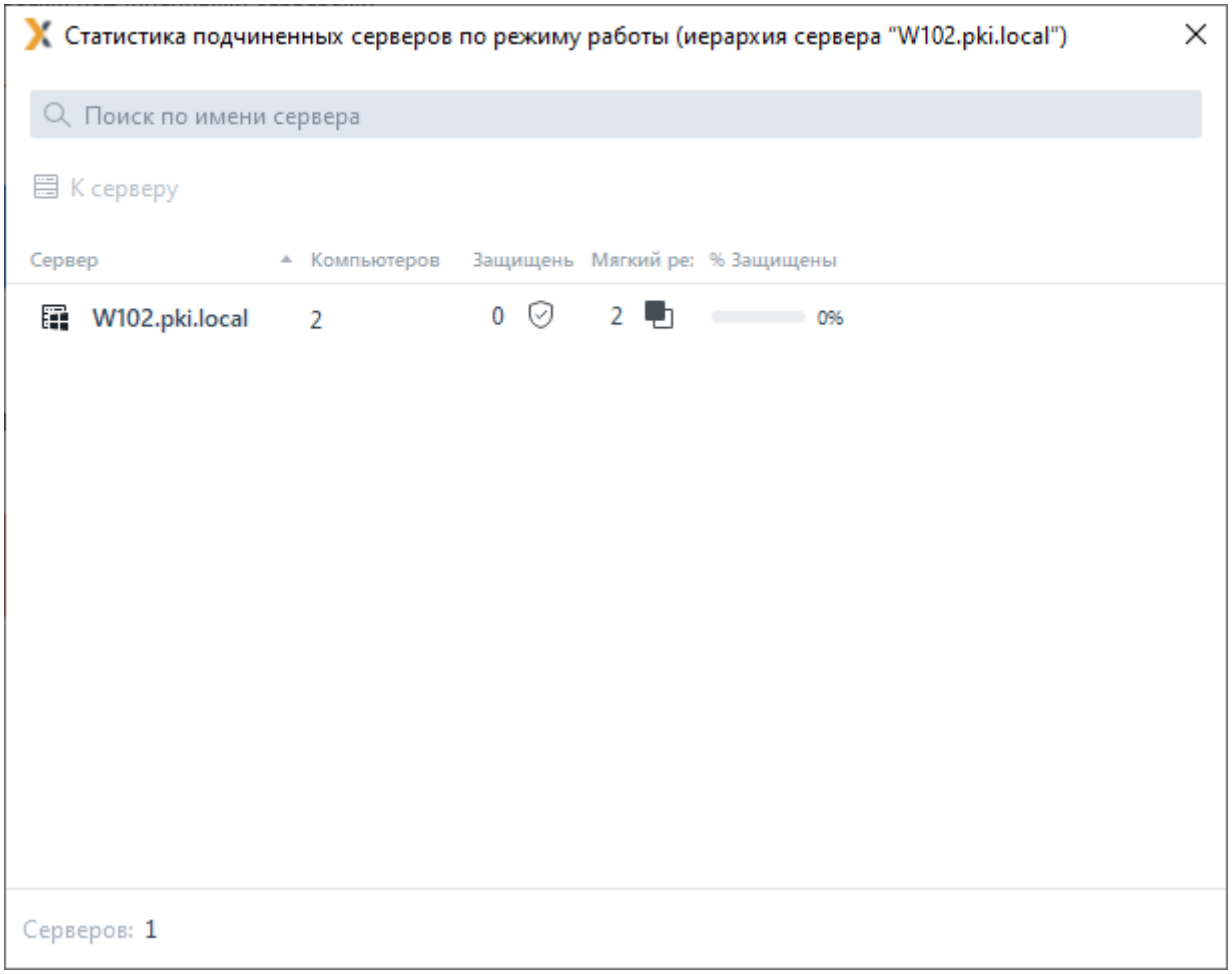


Рисунок 10.9 – Статистика клиентов по режиму работы

Для каждого сервера в окне ***Статистика подчиненных серверов по режиму работы*** отображается информация:

– *Сервер* – DNS-имя сервера;

– *Компьютер* – общее количество клиентских компьютеров сервера;

– *Защищены* – общее количество клиентов сервера, функционирующих в защищенном режиме;

– *Мягкий режим* – общее количество клиентов сервера, функционирующих в мягком режиме;

– *% Защищены* – процентное соотношение количества клиентов, функционирующих в защищенном режиме, к общему количеству клиентов.

10.2 Вкладка «События» сервера

Вкладка ***События*** предназначена для отслеживания событий, заданных политиками и настройками сервера, происходящих на подчиненных серверах.

Основная часть вкладки ***События*** предназначена для отображения списка событий, полученных в результате выполнения запроса (до выполнения запроса в основной части вкладки выводится сообщение с пояснением дальнейших действий).

В правой части вкладки доступна форма для задания параметров выполняемого запроса (рисунок 10.10).

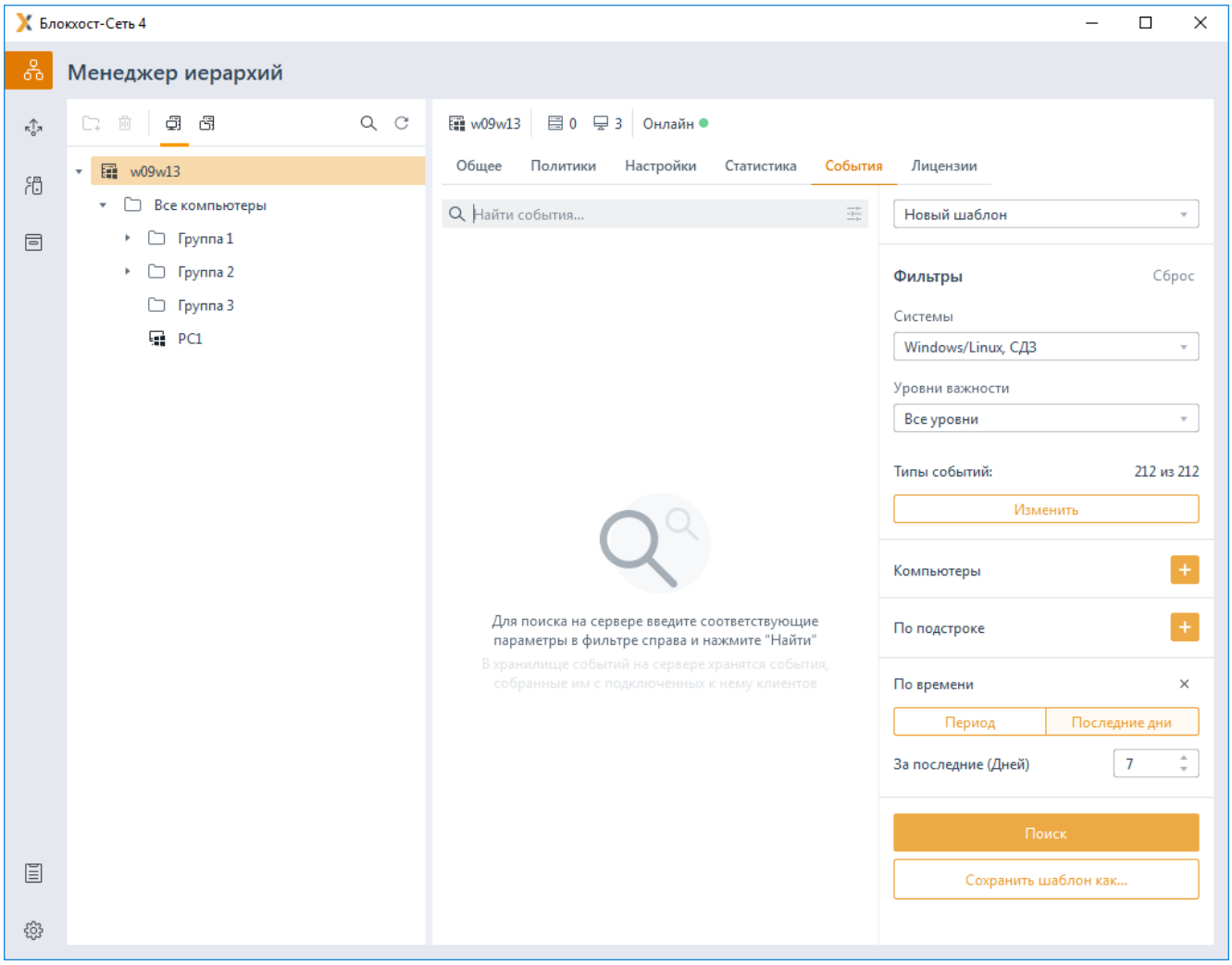


Рисунок 10.10 – Вкладка ***События***

Обновление списка событий происходит при выполнении запроса и содержит информацию (рисунок 10.11):

– ***Уровень важности*** – уровень важности зафиксированного события (сведения , предупреждения или ошибка);

– ***Событие*** – краткое описание зафиксированного события (полный перечень фиксируемых событий приведен в Приложении 1 к настоящему документу);

– ***Компьютер*** – DNS-имя компьютера;

– ***Источник событий*** – операционная система, на которой зафиксировано событие;

– ***Время*** – дата и время момента фиксации произошедшего события;

– ***Категория*** – категория, которой принадлежит зафиксированное событие;

– ***Код*** – код события.

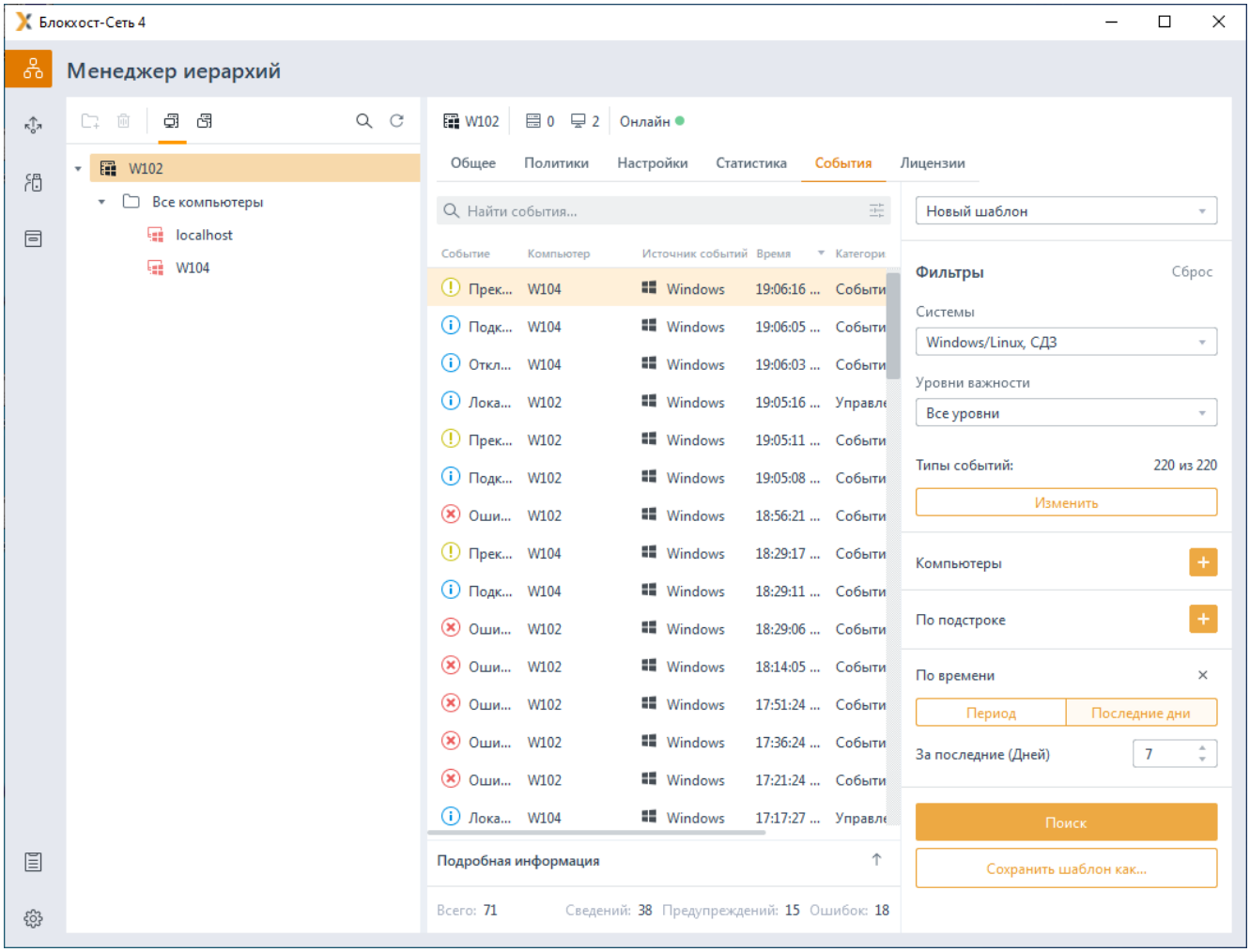


Рисунок 10.11 – Список событий после выполнения запроса

В верхней части окна, над списком событий, располагается поле ввода критериев отбора событий из списка ***Найти события…***. Проверка соответствия введенного в поле ввода значения осуществляется по значениям сразу всех колонок (рисунок 10.11).

При двойном щелчке мыши на выбранном событии в списке, внизу списка отобразится подробная информация о событии (рисунок 10.12).

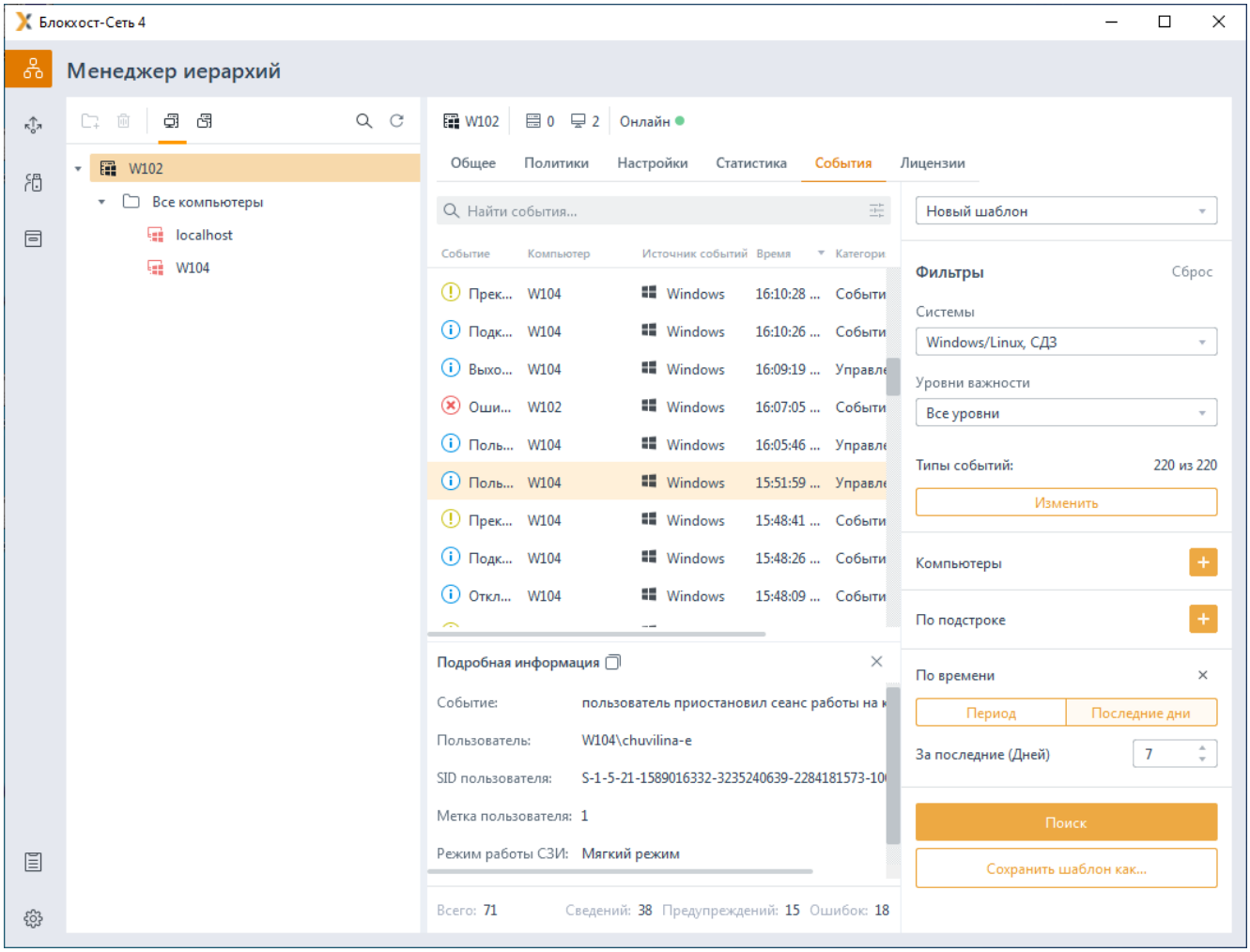


Рисунок 10.12 – Подробная информация о выбранном событии

В правой части вкладки доступна форма настройки параметров для выборки событий с серверов, при этом возможно создание новых запросов или использование запросов, сохраненных ранее.

10.2.1 Выбор шаблона

В области выбора шаблона доступен:

– ***Новый шаблон*** – новая выборка по событиям серверов, при этом доступна настройка всех параметров запроса и шаблон доступен к сохранению.

– ***Сохраненный шаблон*** – позволяет выбрать и выполнить запрос, сохраненный ранее (рисунок 10.13).

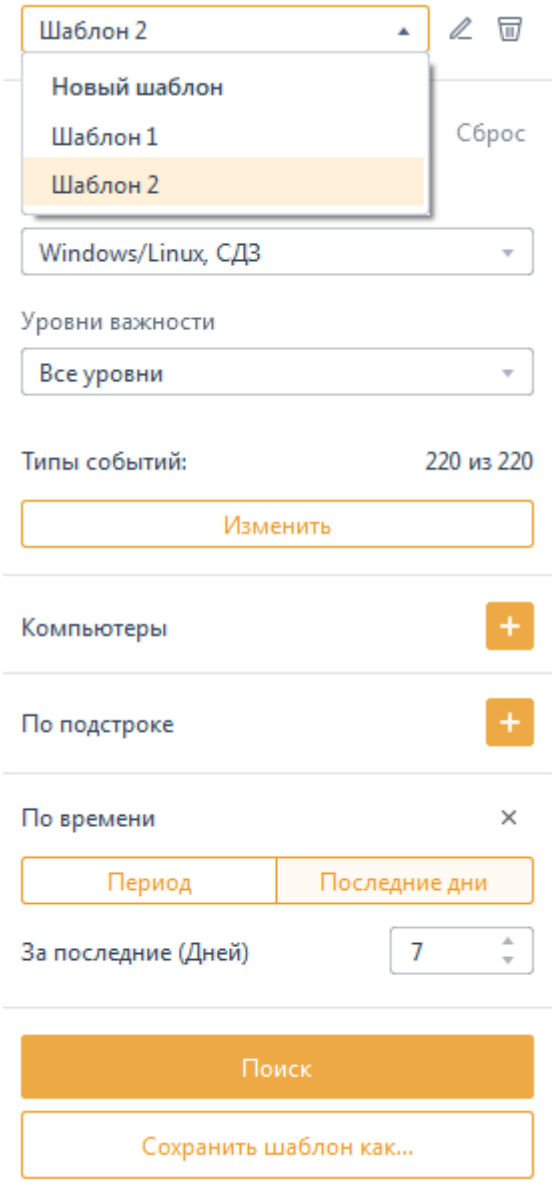


Рисунок 10.13 – Выбор шаблона

Сохраненные шаблоны можно удалить по кнопке в строке выбора шаблона.

После выбора шаблона в области фильтрации списка событий отобразятся все параметры выбранного шаблона (рисунок 10.14).

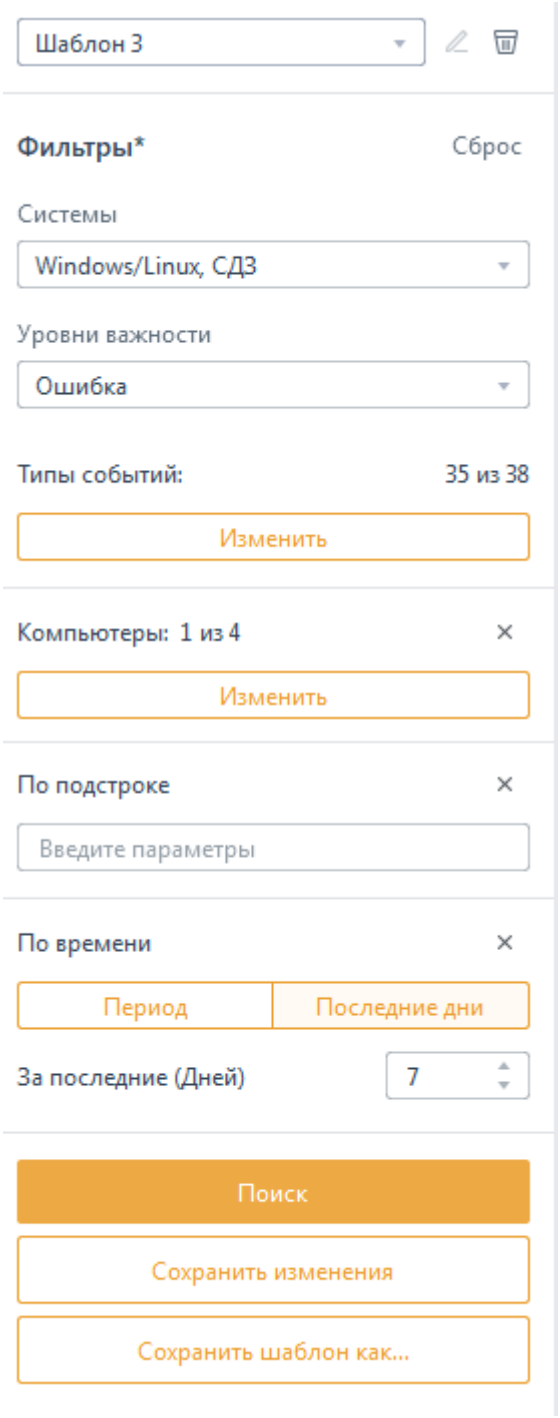


Рисунок 10.14 – Отображение параметров сохраненного шаблона

10.2.2 Настройка параметров запроса

В области ***Фильтры*** доступен выбор параметров запроса:

– ***Системы*** – выборка событий по ОС Windows/Linux, на которой зафиксировано событие, или событий СДЗ (рисунок 10.15):

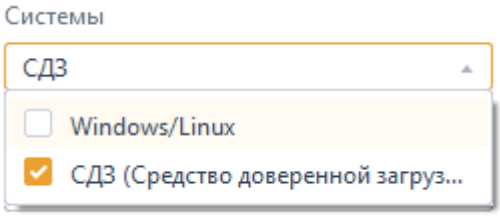


Рисунок 10.15 – Фильтр событий по системе

– ***По уровню важности*** – выборка событий по уровню важности:

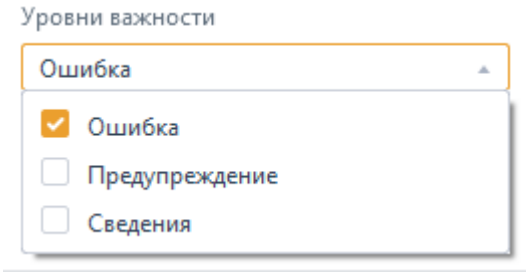


Рисунок 10.16 – Фильтр событий по уровню важности

– ***По типу событий*** – выборка событий определенного типа (по умолчанию выбраны все типы событий). По кнопке ***Изменить*** (рисунок 10.17) появится окно со списком событий, возможных к выбору (рисунок 10.18). В списке отображается тип события, система, уровень важности события и присвоенный событию код.

Рисунок 10.17 – Фильтр событий по категории

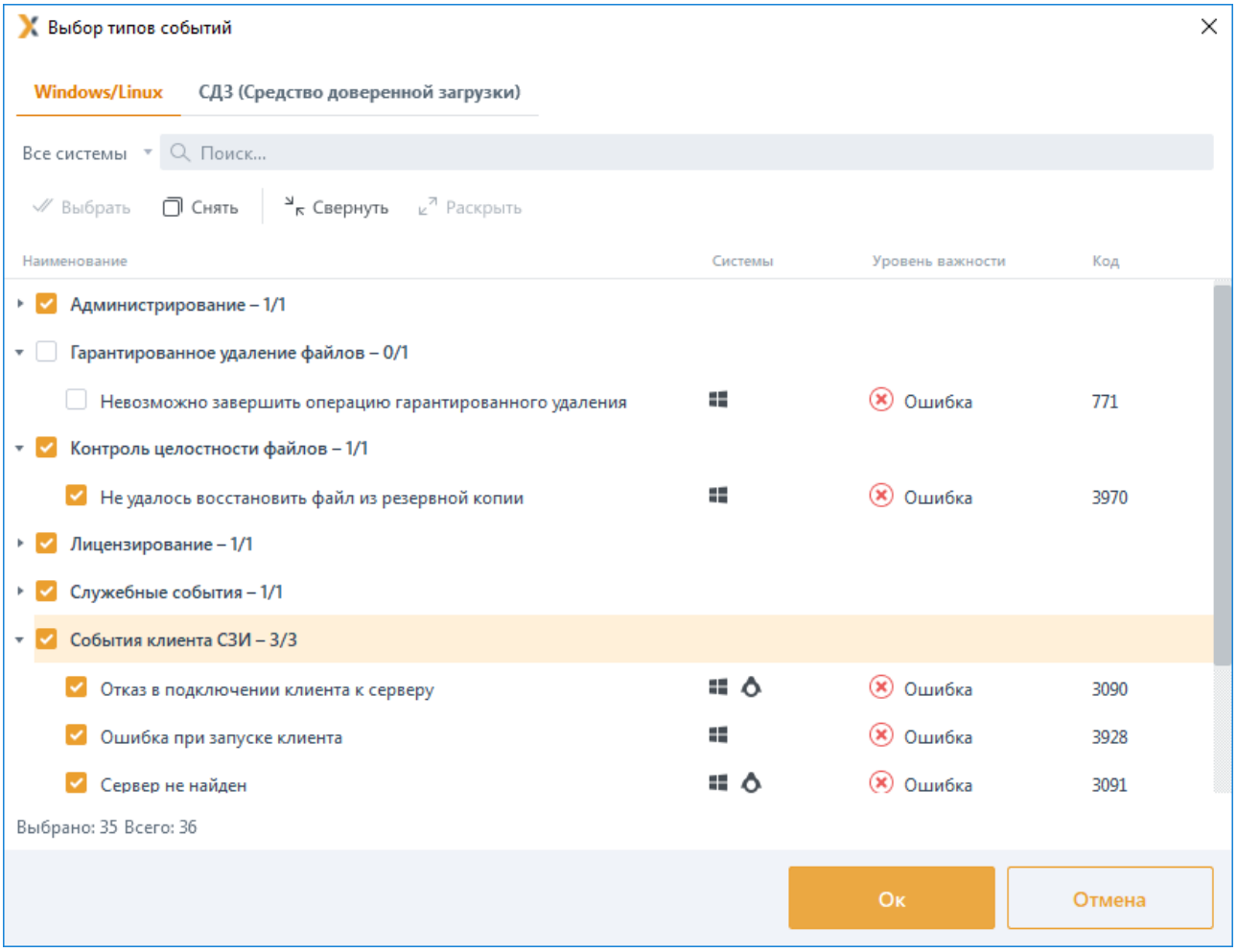


Рисунок 10.18 – Фильтр событий по типу события

Полный перечень событий приведен в Приложении 1 к настоящему документу.

– ***Компьютеры*** – фильтрация событий по клиентским рабочим станциям. По кнопке ***Изменить*** (рисунок 10.19) появится окно со списком рабочих станций, возможных к выбору (рисунок 10.20). В списке отображается имя компьютера и IP-адрес.

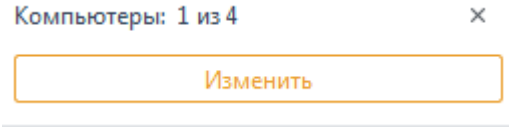


Рисунок 10.19 – Фильтр по компьютерам

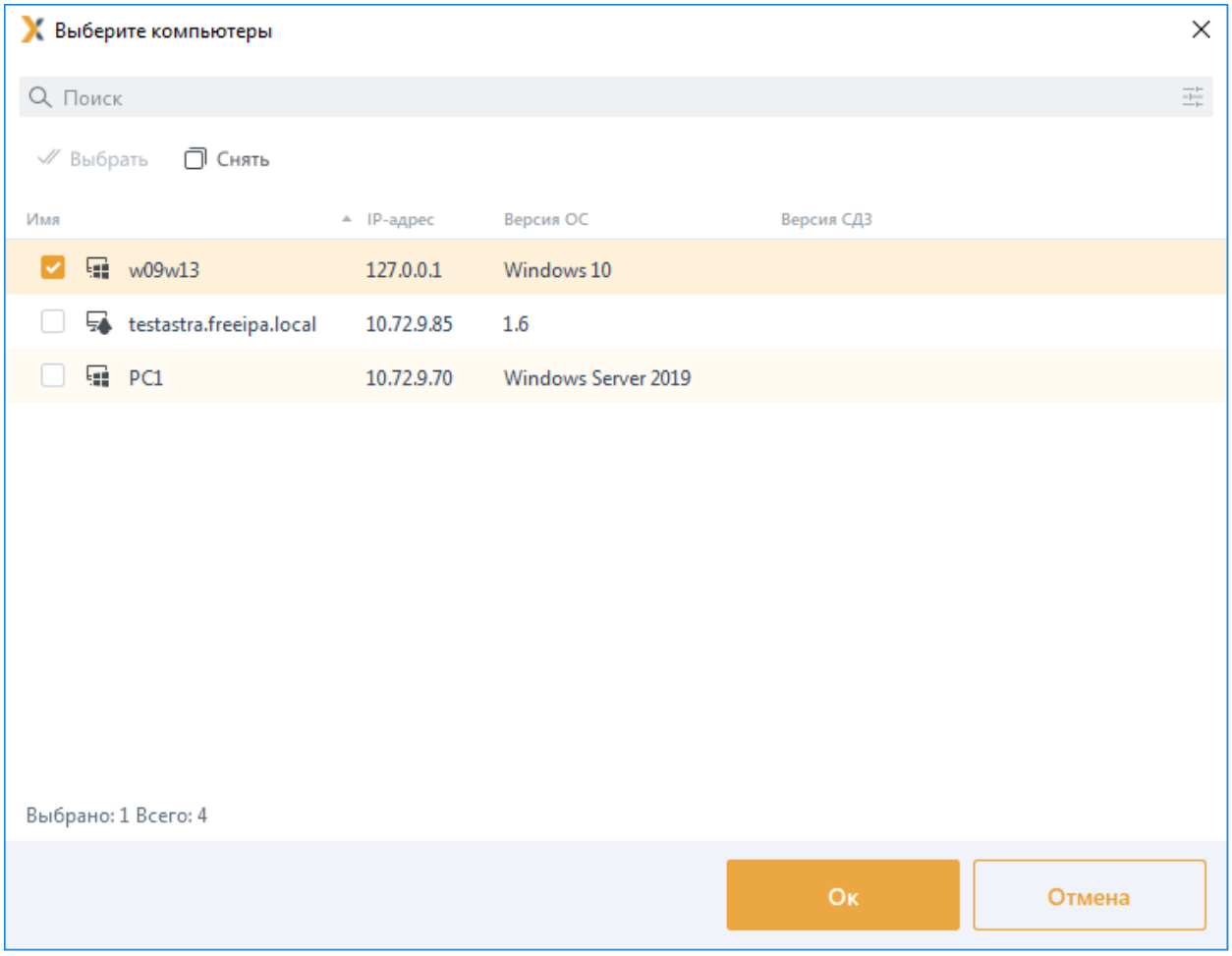


Рисунок 10.20 – Список компьютеров сервера

– ***По подстроке*** – выборка по подробной информации о событии. При нажатии на кнопку появится строка, в которой можно указать дополнительные параметры поиска (рисунок 10.21).

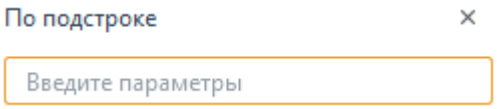
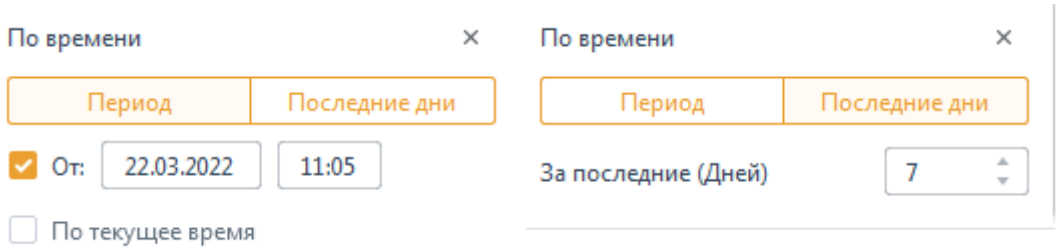


Рисунок 10.21 – Фильтр по подстроке

При вводе символов кириллицы в данное поле учитывается регистр вводимых символов.

– ***По времени*** – выборка событий за определенный период времени:



а) б)

Рисунок 10.22 – Фильтр по времени

При выборе фильтра по времени ***Период*** (рисунок 10.22 а) в поле ***От*** вводится дата начала выборки событий, в поле ***До*** вводится дата окончания выборки:

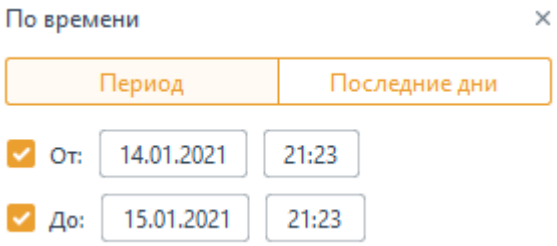


Рисунок 10.23 – Фильтр событий за период времени

- При снятии флага в поле ***От***, выборка будет осуществлена с самого первого события, имеющегося в системе:

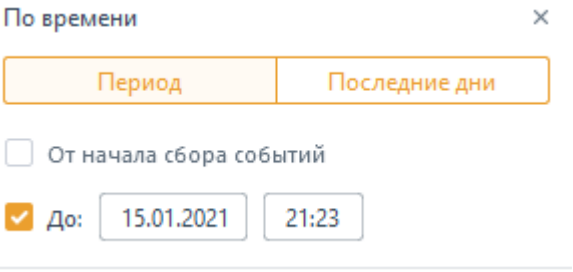


Рисунок 10.24 – Фильтр от начала сбора событий

- При снятии флага в поле ***До***, выборка будет осуществлена по текущее время (рисунок 10.22 а).

При выборе фильтра по времени ***Последние дни*** (рисунок 10.22 б) вводится количество дней, предшествующих текущему, за которые осуществляется выборка.

Необходимо учитывать, что сбор событий начинается со времени начала суток (дд.мм.гг. 00:00) вне зависимости от времени установки значения параметра. Например, при установке значения фильтра «1», сбор информации будет осуществлен начиная с 00:00 текущих суток.

10.2.3 Выполнение запроса

После выбора всех необходимых параметров запроса или после ввода сохраненного

запроса, для выборки событий необходимо нажать кнопку ***Поиск***. При этом список в основной части вкладки ***События*** обновится в соответствии с введенными параметрами запроса.

При отсутствии на сервере событий, соответствующих заданным фильтрам, в основной части вкладки ***События*** появится сообщение вида:

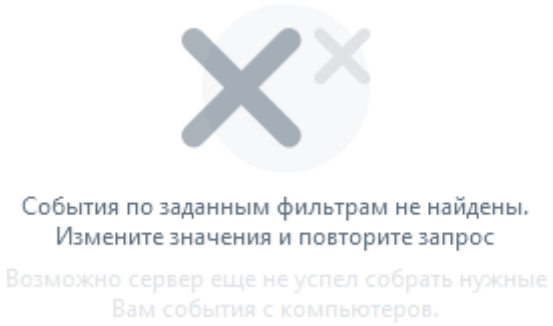


Рисунок 10.25 – Сообщение об отсутствии событий, соответствующих фильтрам

Для сброса параметров фильтрации нажмите кнопку ***Сброс***, расположенную в правом верхнем углу области ***Фильтры*** (рисунок 10.10).

10.2.4 Сохранение запроса

Кнопка ***Сохранить изменения*** (рисунок 10.14) доступна только при выборе сохраненного шаблона, после внесения изменений в значение какого-либо параметра в выбранном запросе. При этом изменения вносятся в имеющийся запрос.

Кнопка ***Сохранить шаблон как...*** (рисунок 10.14) доступна при выборе нового или сохраненного шаблона. При нажатии кнопки, открывается окно, в котором необходимо ввести имя создаваемого запроса в поле ***Имя шаблона*** (рисунок 10.26):

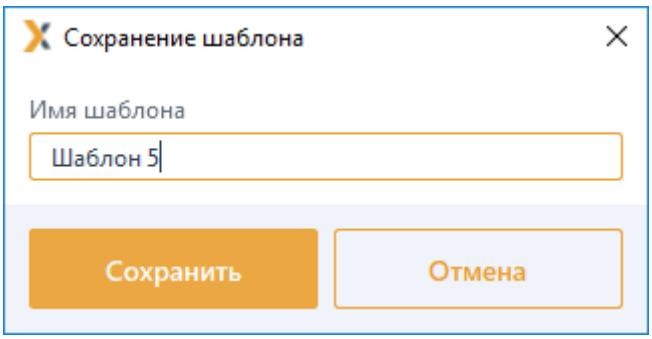


Рисунок 10.26 – Окно сохранения шаблона

10.3 Вкладка «События» клиента

Вкладка ***События*** предназначена для выполнения запросов и отслеживания всех событий, зафиксированных на выбранной в иерархии рабочей станции.

Основная часть вкладки ***События*** предназначена для отображения списка событий, полученных в результате выполнения запроса (до выполнения запроса в основной части вкладки выводится сообщение с пояснением дальнейших действий).

В правой части вкладки доступна форма для задания параметров выполняемого запроса (рисунок 10.27).

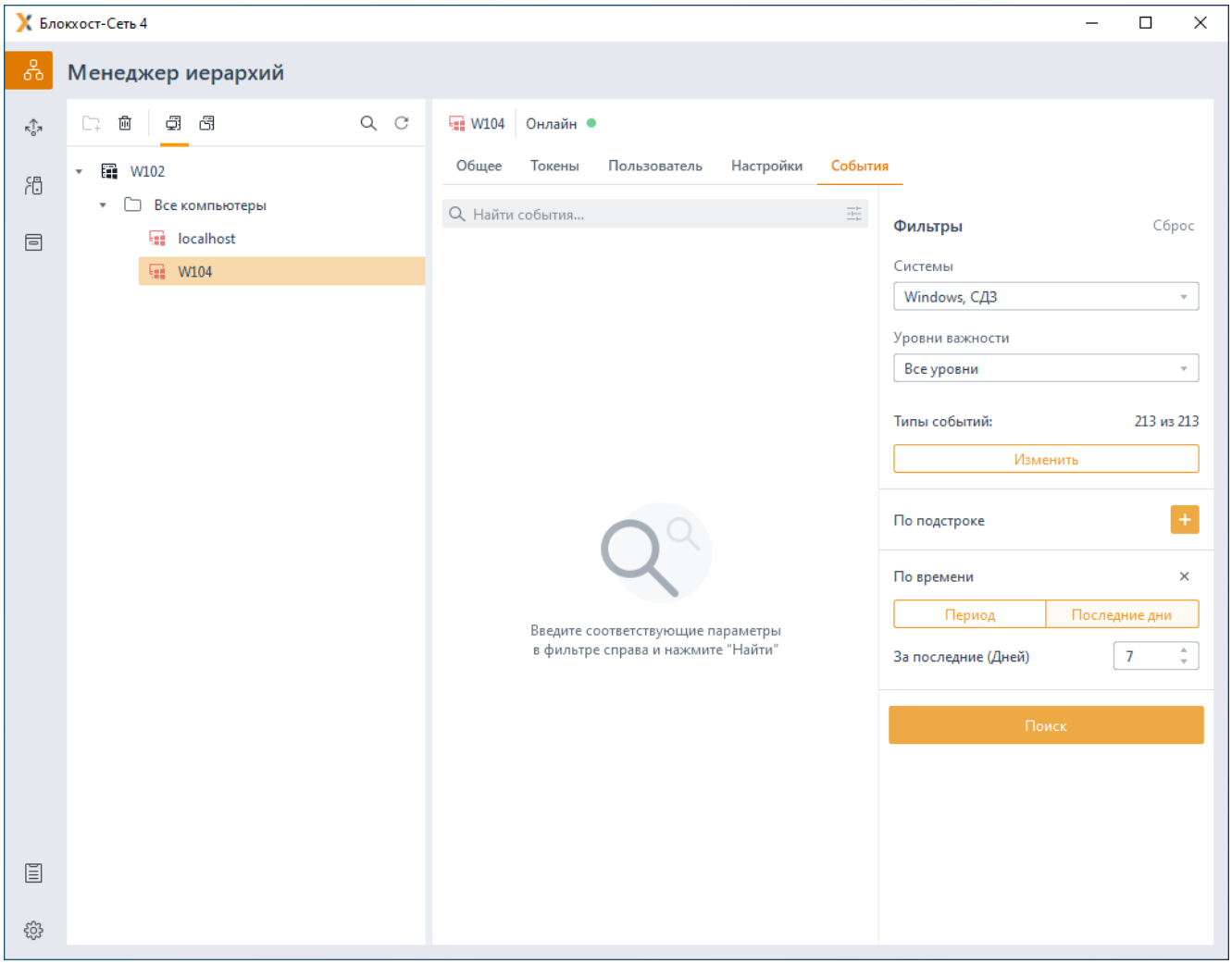


Рисунок 10.27 – Вкладка ***События*** клиента

Обновление списка событий происходит при выполнении запроса и содержит информацию (рисунок 10.28):

– ***Уровень важности*** – уровень важности зафиксированного события (сведения , предупреждения или ошибка);

– ***Событие*** – краткое описание зафиксированного события (полный перечень фиксируемых событий приведен в Приложении 1 к настоящему документу);

– ***Время*** – дата и время момента фиксации произошедшего события;

– ***Категория*** – категория, которой принадлежит зафиксированное событие;

– ***Код*** – код события.

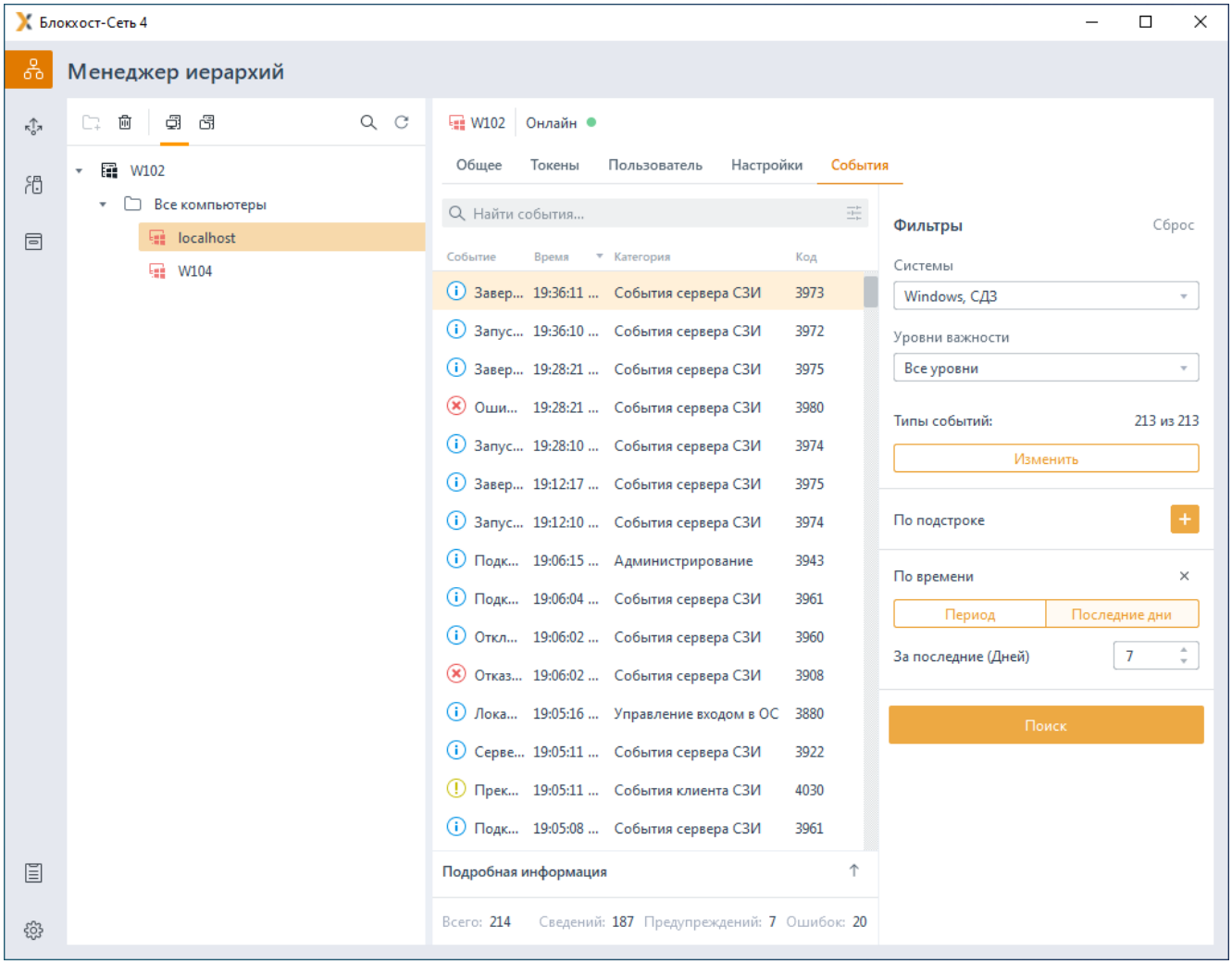


Рисунок 10.28 – Список событий после выполнения запроса

В верхней части окна, над списком событий, располагается поле ввода критериев отбора событий из списка ***Найти события…***. Проверка соответствия введенного в поле ввода значения осуществляется по значениям сразу всех колонок (рисунок 10.11).

При двойном щелчке мыши на выбранном событии в списке, внизу списка отобразится подробная информация о событии (рисунок 10.12).

В правой части вкладки доступна форма настройки параметров для выборки событий с клиентской рабочей станции.

Для выполнения запроса необходимо в области ***Фильтры*** ввести данные о параметрах запроса (по каким параметрам будет осуществляться выборка событий). Доступна фильтрация:

- ***По системе;***
- ***По уровню важности;***
- ***По типу событий;***

– ***По подстроке;***

– ***По времени.***

Подробное описание параметров фильтрации описано в разделе ***«Настройка параметров запроса»***.

После выбора всех необходимых параметров запроса для выборки событий необходимо нажать кнопку ***Поиск***. При этом список в основной части вкладки ***События*** обновится в соответствии с введенными параметрами запроса.

10.4 Запуск внеплановой загрузки событий аудита

Запуск внеплановой загрузки событий аудита доступен при выборе в иерархии сервера в контекстном меню ***Запустить внеплановую загрузку событий аудита*** (рисунок 10.29).

Внеплановая загрузка событий возможна:

– ***С клиентских компьютеров*** – для внепланового сбора событий аудита с клиентских компьютеров выбранного сервера;

– ***С подчиненных серверов*** – для внепланового сбора событий аудита с подчиненных серверов.

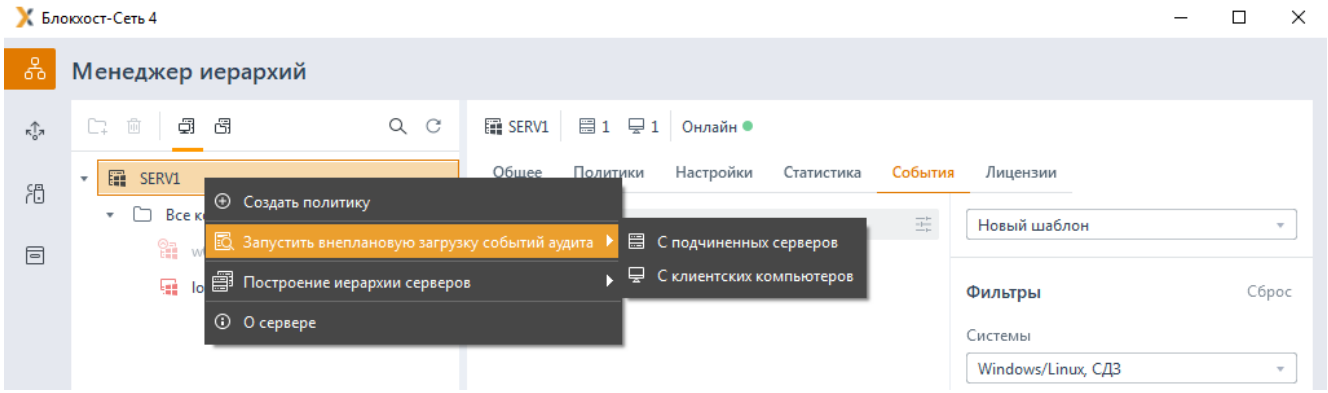


Рисунок 10.29 –Запуск внеплановой загрузки событий аудита

Если запуск внепланового цикла опроса может быть выполнен, пользователю выдается уведомление об успешности запуска (рисунок 10.30).

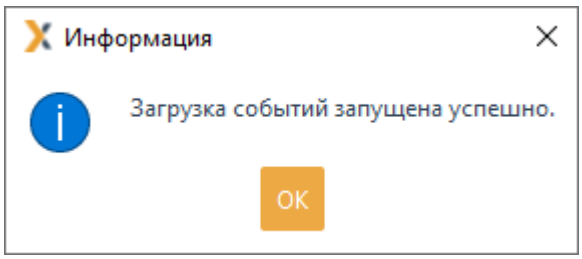


Рисунок 10.30 – Уведомление об успешности запуска внеплановой загрузки событий

Запуск внепланового цикла опроса не будет произведен при:

- выполнении в то же время планового цикла опроса;
- выполнении внепланового цикла опроса, запущенного ранее.

Логика выполнения запуска внепланового цикла опроса в зависимости от включения/отключения передачи данных аудита в SIEM-систему на выбранном сервере различна:

- **Экспорт в SIEM-систему включен**:
  - выполняется загрузка событий с подчиненных серверов/клиентских компьютеров текущего сервера;
  - загруженные события экспортируются в SIEM;
  - передача собранных данных на родительский сервер, в случае его наличия, не выполняется.
- **Экспорт в SIEM-систему выключен:**
  - выполняется загрузка событий с подчиненных серверов/клиентских компьютеров текущего сервера;
  - выполняется передача собранных данных на родительский сервер;
  - загруженные события не экспортируются в SIEM.

11 Архивы

Управление архивами доступно по кнопке  (рисунок 11.1). В разделе **Архивы** осуществляется работа с созданными ранее архивами событий аудита с возможностью выбора событий при помощи фильтрации.

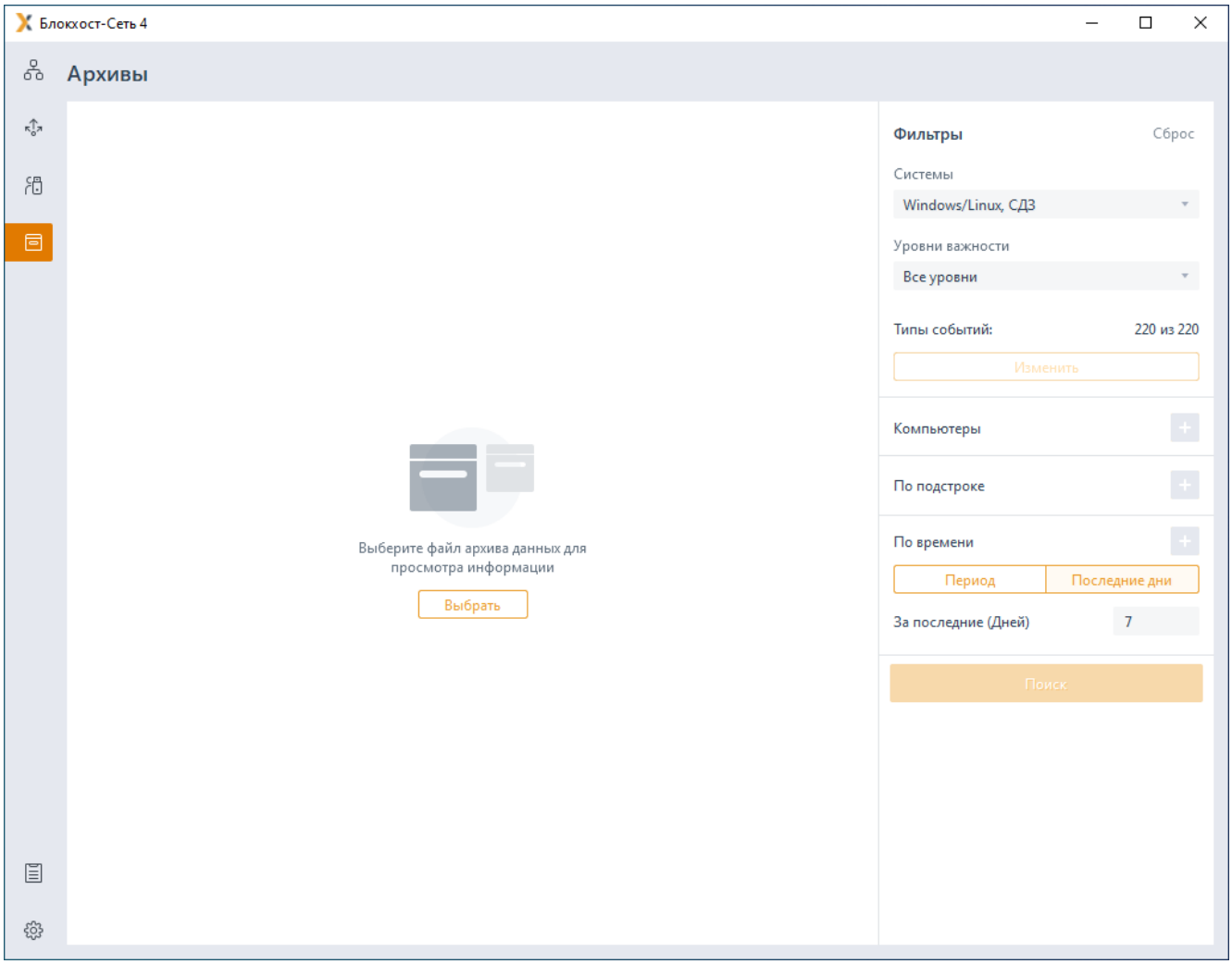


Рисунок 11.1 – Раздел **Архивы**

Основная часть раздела **Архивы** предназначена для отображения списка событий, полученных в результате выполнения запроса (до выполнения запроса в основной части раздела выводится сообщение с пояснением дальнейших действий).

В правой части доступна форма для задания параметров выполняемого запроса (рисунок 11.1).

Для начала работы с архивом событий аудита необходимо по кнопке ***Выбрать*** загрузить файл архива (рисунок 11.2), содержащий требуемую информацию.

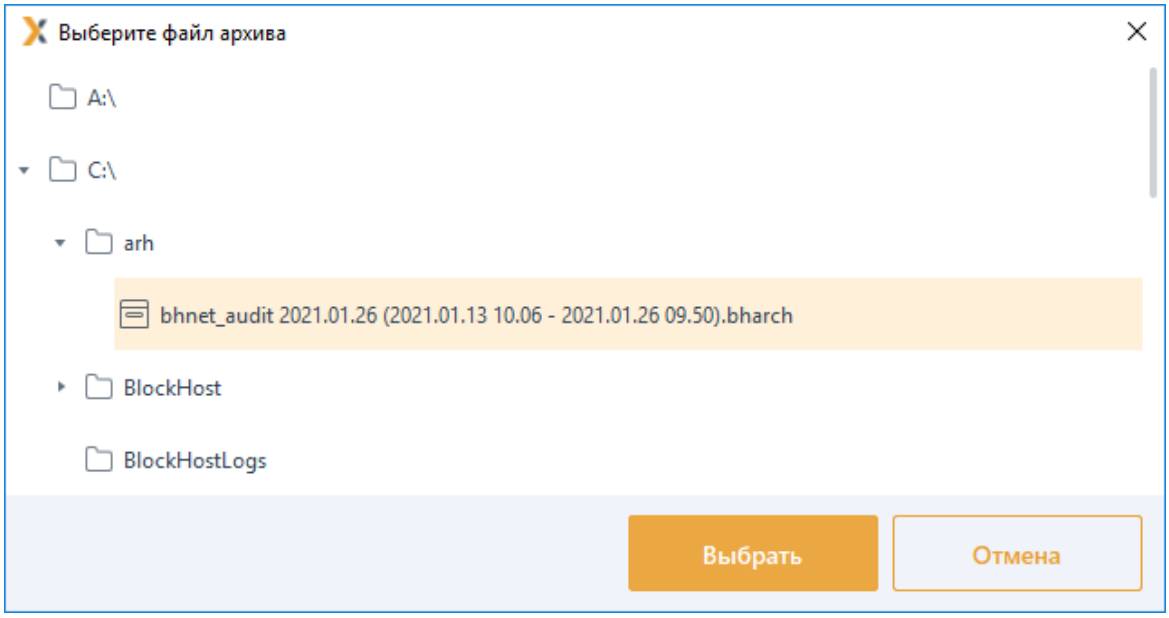


Рисунок 11.2 – Выбор файла архива

После выбора файла архива правая часть раздела, содержащая параметры выполняемого запроса, становится доступной для выполнения фильтрации по выбранному архиву. В верхней части раздела указано наименование выбранного архива (рисунок 11.3).

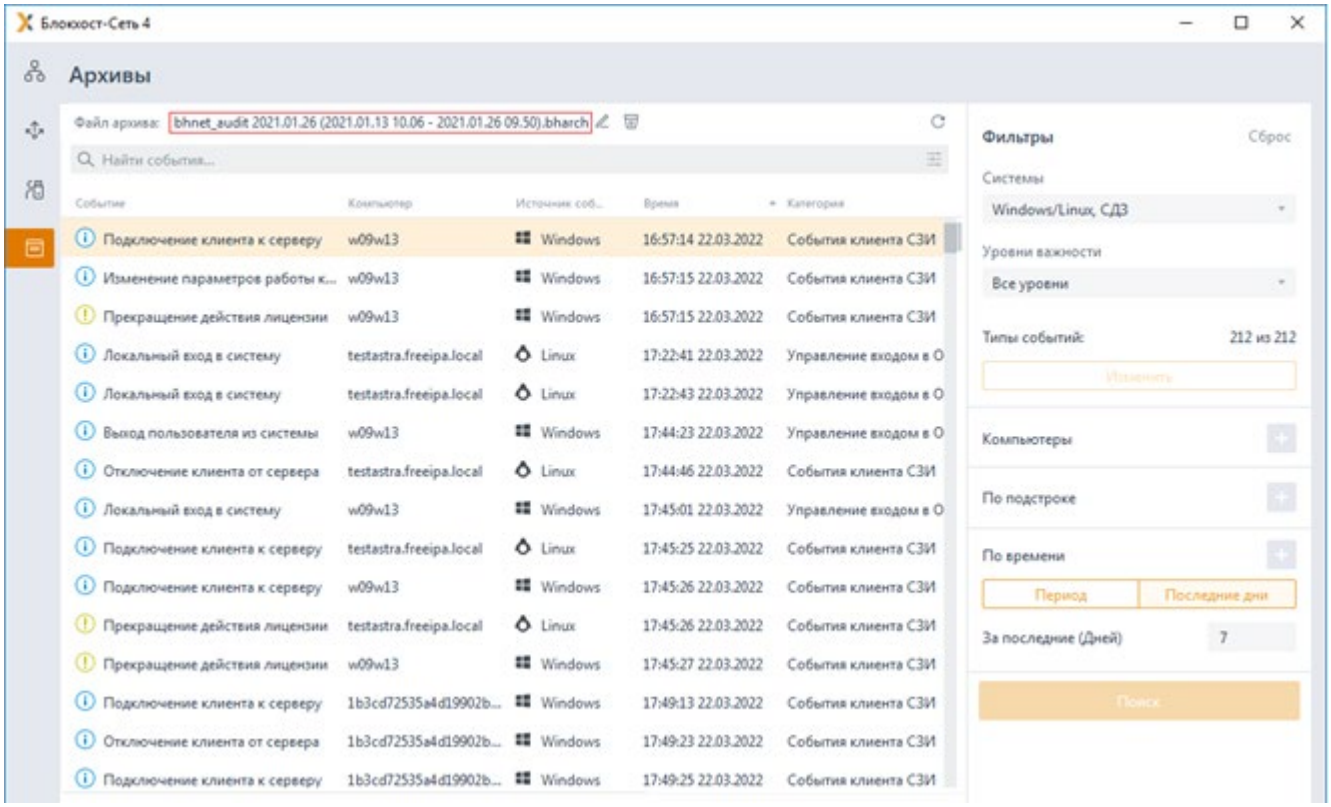


Рисунок 11.3 – Отображение содержания выбранного архива

По каждому событию в архиве отображается информация:

– ***Уровень важности*** – уровень важности зафиксированного события (сведения , предупреждения или ошибка);

– ***Событие*** – краткое описание зафиксированного события (полный перечень фиксируемых событий приведен в Приложении 1 к настоящему документу);

– ***Компьютер*** – DNS-имя компьютера;

– ***Время*** – дата и время момента фиксации произошедшего события;

– ***Категория*** – категория, которой принадлежит зафиксированное событие;

– ***Код*** – код события.

В верхней части окна, над списком событий, располагается поле ввода критериев отбора событий из списка ***Найти события…***. Проверка соответствия введенного в поле ввода значения осуществляется по значениям сразу всех колонок.

При двойном щелчке мыши на выбранном событии в списке, внизу списка отобразится подробная информация о событии (рисунок 10.12).

Для выполнения запроса необходимо в области ***Фильтры*** ввести данные о параметрах запроса (по каким параметрам будет осуществляться выборка событий). Доступна фильтрация:

– ***По системе;***

– ***По уровню важности;***

– ***По типу событий;***

– ***По компьютерам;***

– ***По подстроке;***

– ***По времени.***

Подробное описание параметров фильтрации описано в разделе ***«Настройка параметров запроса»***.

После выбора всех необходимых параметров запроса для выборки событий из архива необходимо нажать кнопку ***Поиск***. При этом список событий архива обновится в соответствии с введенными параметрами запроса.

При отсутствии в архиве событий, соответствующих заданным фильтрам, в основной части раздела ***Архивы*** появится сообщение об отсутствии в архиве таких событий (рисунок 10.25).

Для сброса параметров фильтрации нажмите кнопку ***Сброс***, расположенную в правом верхнем углу области ***Фильтры*** (рисунок 11.3).

12 Фиксация событий клиентов в приложении «ServerTrayMonitor»

В комплект поставки СЗИ от НСД «Блокхост-Сеть 4» входит приложение «**ServerTrayMonitor**», которое устанавливается одновременно с установкой серверной части СЗИ. Приложение «**ServerTrayMonitor**» предназначено для интерактивного слежения за выборочными событиями клиентских компьютеров СЗИ от НСД «Блокхост-Сеть 4».

12.1 «ServerTrayMonitor» в ОС Windows

Вызов приложения «**ServerTrayMonitor**» доступен из меню ***Пуск*** → ***Программы*** → ***Блокхост-Сеть 4*** → ***Monitor*** или в панели быстрого запуска по кнопке  .

После запуска приложения отрывается основное окно (рисунок 12.1), в котором отображается список событий, регистрируемых на клиентах Блокхост-Сеть. Для каждого события фиксируется следующая информация:

- «№ пп.» - номер события в списке;
- «Время» - время фиксации события;
- «IP адрес (DNS имя)» - IP адрес и DNS имя клиентского компьютера;
- «Тип события» - тип фиксируемого события;
- «Сообщение» - краткое описание фиксируемого события.

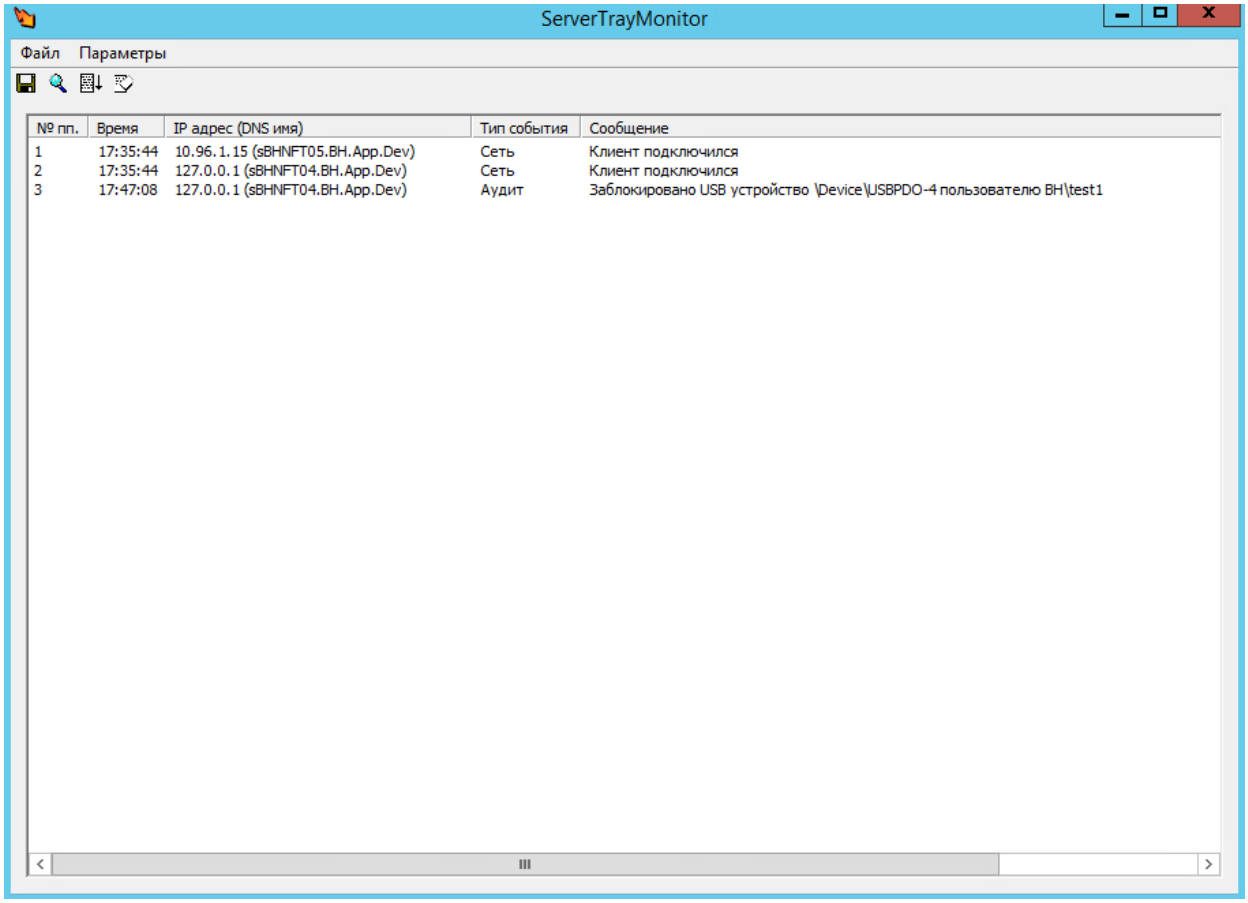


Рисунок 12.1 – Окно приложения «ServerTrayMonitor»

События клиентских компьютеров, фиксируемые приложением «**ServerTrayMonitor**»:

- подключение/отключение клиентских компьютеров;
- блокировка подключаемых USB-устройств (при установленном запрете доступа к USB-устройствам в политике ***Контроль устройств*** (подпункт 7.3.1 «Разграничение доступа к USB-устройствам» документа «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 1. Управление политиками»).

Для сохранения событий администратору безопасности необходимо нажать кнопку ***Сохранить***  , расположенную в левом верхнем углу основного окна приложения (рисунок 12.1) и выбрать директорию и имя создаваемого лог-файла.

Кнопка ***Очистить***  позволяет выполнить очистку всех событий, зафиксированных в приложении.

12.2 «ServerTrayMonitor» в ОС Linux

Вызов приложения «**ServerTrayMonitor**» доступен через терминал с помощью команды:

```
sudo journalctl -f | grep BlockHost-INFO
```

В результате выполнения команды появится список событий, регистрируемых на клиентах Блокхост-Сеть (рисунок 12.2). Для каждого события фиксируется следующая информация:

- «Время» - время фиксации события;
- «IP адрес (DNS имя)» - IP адрес и DNS имя клиентского компьютера;
- «Тип события» - тип фиксируемого события;
- «Сообщение» - краткое описание фиксируемого события.

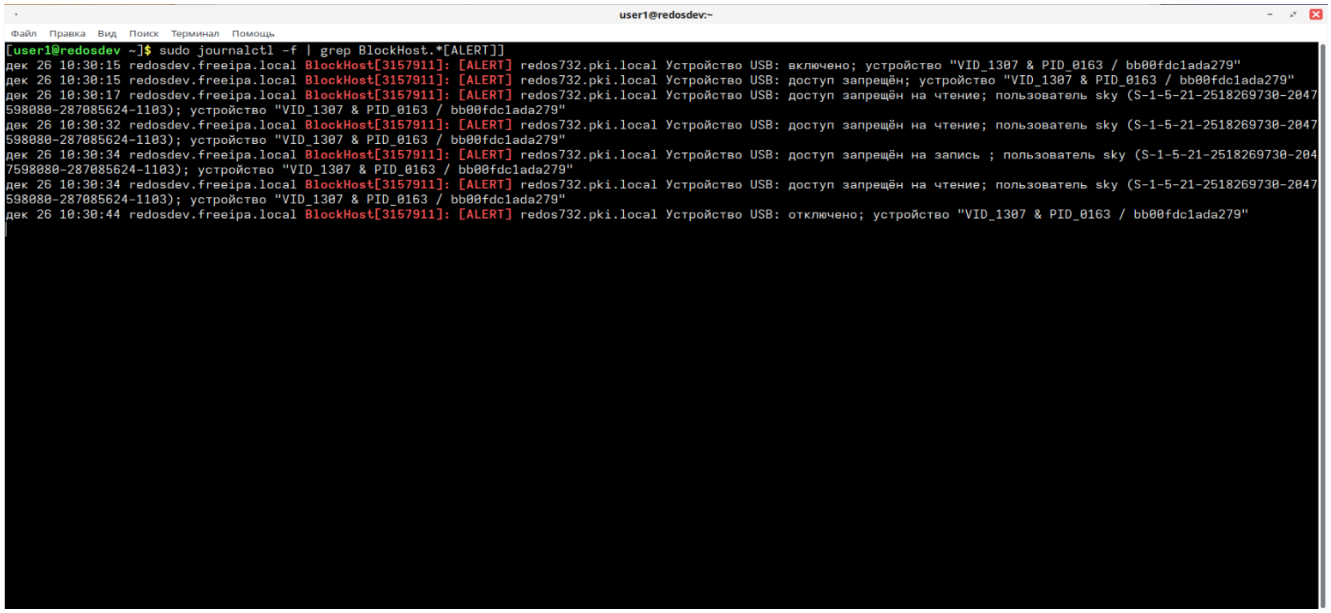


Рисунок 12.2 – Вывод событий «ServerTrayMonitor»

События клиентских компьютеров, фиксируемые приложением «**ServerTrayMonitor**»:

- внесение изменений в политику контроля устройств;
- подключение/отключение USB-устройств;
- разрешение/запрет доступа к USB-устройствам;
- разрешение/запрет доступа на чтение/ запись USB-устройств.

События, фиксируемые приложением «**ServerTrayMonitor**», могут быть отфильтрованы, например, события контроля устройств, с помощью команды:

```
sudo journalctl -f | grep BlockHost.*[ALERT]]
```

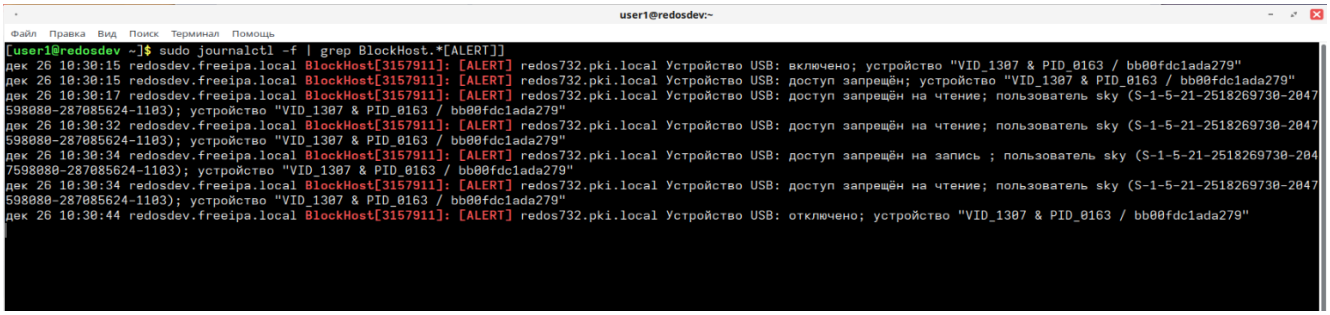


Рисунок 12.3 – Фильтрация событий «ServerTrayMonitor»

Перечень сокращений

AD	–	Active Directory (службы каталогов для операционных систем семейства Windows Server)
DNS	–	Domain Name System (система распределения имен доменов)
SIEM	–	Security Information and Event Management (управление информацией о безопасности и управление событиями безопасности)
TCP/IP	–	Transmission Control Protocol/Internet Protocol (протокол управления передачей данных)
БД	–	База данных
НСД	–	Несанкционированный Доступ
ОС	–	Операционная Система
ПК	–	Программный Комплекс
ПО	–	Программное Обеспечение
СЗИ	–	Средство Защиты Информации