

Средство защиты информации от несанкционированного доступа
«Блокхост-Сеть 3»

Руководство администратора. Система развертывания и аудита

Аннотация

Настоящее руководство предназначено для администраторов средства защиты информации от несанкционированного доступа «Блокхост-Сеть 3» и содержит описание работы с консолью «Система развертывания и аудита».

Содержание

Введение	5
1 Установка и настройка консоли СРиА.....	6
1.1 Установка консоли СРиА	6
1.2 Настройка консоли СРиА.....	6
2 Описание работы с консолью СРиА.....	13
2.1 Ролевое распределение	14
3 Раздел «Развертывание»	17
3.1 Вкладка «Агенты развертывания»	17
3.1.1 Установка агента системы развертывания.....	19
3.1.1.1 Установка из консоли СРиА.....	19
3.1.1.2 Локальная установка.....	29
3.1.1.3 Установка с использованием групповых политик	33
3.1.2 Удаление агента развертывания.....	38
3.2 Вкладка «Инсталляционные пакеты»	38
3.2.1 Создание инсталляционных пакетов	39
3.2.2 Подготовка дистрибутива для AD.....	44
3.3 Вкладка «Задачи»	46
3.3.1 Создание задачи на установку ПО	50
3.3.2 Добавление в задачу нескольких рабочих станций	56
3.3.3 Параметры перезагрузки рабочих станций	57
3.3.4 Создание задачи на удаление программы	59
3.3.4.1 Удаление клиента Блокхост-Сеть	60
3.3.4.2 Удаление программы из списка инсталляционных пакетов.....	63
3.3.4.3 Удаление программы с использованием скрипта PowerShell или командного файла Windows	65
3.3.5 Создание задачи на перезагрузку компьютеров	67
3.3.6 Запуск задачи на установку/удаление ПО	68
3.3.7 Остановка задачи	71
3.3.8 Установка клиента Блокхост-Сеть.....	73
3.3.9 Удаление агента Блокхост-Сеть с защищаемых рабочих станций.....	74
4 Раздел «Мониторинг».....	75
4.1 Дерево иерархии	76
4.2 Строка навигации	79
4.3 Настройка сбора событий в консоли управления политиками сервера.....	80
4.4 Аудит серверов.....	82
4.4.1 Вкладка «Подчиненные серверы»	82
4.4.2 Вкладка «Статистика»	85
4.4.2.1 Распределение клиентов по типу аутентификации	87
4.4.2.2 Состояние клиентов Блокхост-Сеть.....	90

4.4.2.3	Режим работы клиентов Блокхост-Сеть	92
4.4.2.4	События для рассмотрения.....	93
4.4.3	Вкладка «События»	95
4.4.3.1	Выбор типа запроса	98
4.4.3.2	Настройка параметров запроса	100
4.4.4	Контекстное меню сервера	106
4.4.5	Параметры сервера.....	107
4.4.5.1	Общая информация	108
4.4.5.2	Сбор событий с подчиненных серверов.....	109
4.4.5.3	Сбор событий с клиентов.....	113
4.4.5.4	Автоархивация событий аудита.....	115
4.4.5.5	Удаление событий аудита	117
4.4.5.6	Экспорт событий в SIEM-систему	117
4.4.5.7	Кэш событий	120
4.4.6	Запуск внеплановой загрузки событий аудита	121
4.5	Аудит групп серверов.....	123
4.6	Аудит клиентов сервера	124
4.6.1	Вкладка «События»	125
4.6.2	Контекстное меню клиентского компьютера.....	127
5	Раздел «Архивы».....	129
6	Создание и восстановление резервной копии данных сервера СРиА	134
6.1	Создание резервной копии данных сервера СРиА.....	134
6.2	Восстановление резервной копии данных сервера СРиА	136
	Перечень сокращений	141

Введение

На сервер средства защиты информации (СЗИ) от несанкционированного доступа «Блокхост-Сеть 3» одновременно с установкой серверной части СЗИ «Блокхост-Сеть 3» (далее по тексту – сервер СЗИ) устанавливается и консоль «Система развертывания и аудита» (далее по тексту — СРиА или консоль СРиА). СРиА предназначена для установки программного обеспечения, в том числе клиентской части СЗИ «Блокхост-Сеть 3» (далее по тексту — клиент Блокхост-Сеть) на рабочие станции, а также для мониторинга событий клиентов СЗИ «Блокхост-Сеть 3».

Знаки, расположенные на полях руководства, указывают на примечания.

Степени важности примечаний:



Важная информация, информация предостерегающего характера.



Дополнительная информация, примеры.

1 Установка и настройка консоли СРиА

1.1 Установка консоли СРиА

Графическая консоль СРиА позволяет управлять процессом установки программного обеспечения (в частности, клиента Блокхост-Сеть) на рабочие станции в сети и осуществлять мониторинг рабочих станций. Консоль СРиА автоматически устанавливается на **сервер безопасности** в процессе установки сервера СЗИ.

Процесс установки сервера СЗИ подробно описан в подразделе 1.3 «Порядок установки серверной части СЗИ «Блокхост-Сеть 3» документа «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Руководство по инсталляции (вариант с удаленным управлением)».

Консоль СРиА запускается из меню *Пуск: Пуск → Все программы → Блокхост-Сеть 3 → Система развертывания и аудита*.

1.2 Настройка консоли СРиА

Перед запуском консоли СРиА необходимо выполнить настройку параметров работы консоли. Запуск мастера настройки СРиА может быть выполнен автоматически по окончании процесса установки сервера СЗИ – если в окне завершения работы мастера установки отмечен параметр **Запустить мастер настройки системы развертывания и аудита**:

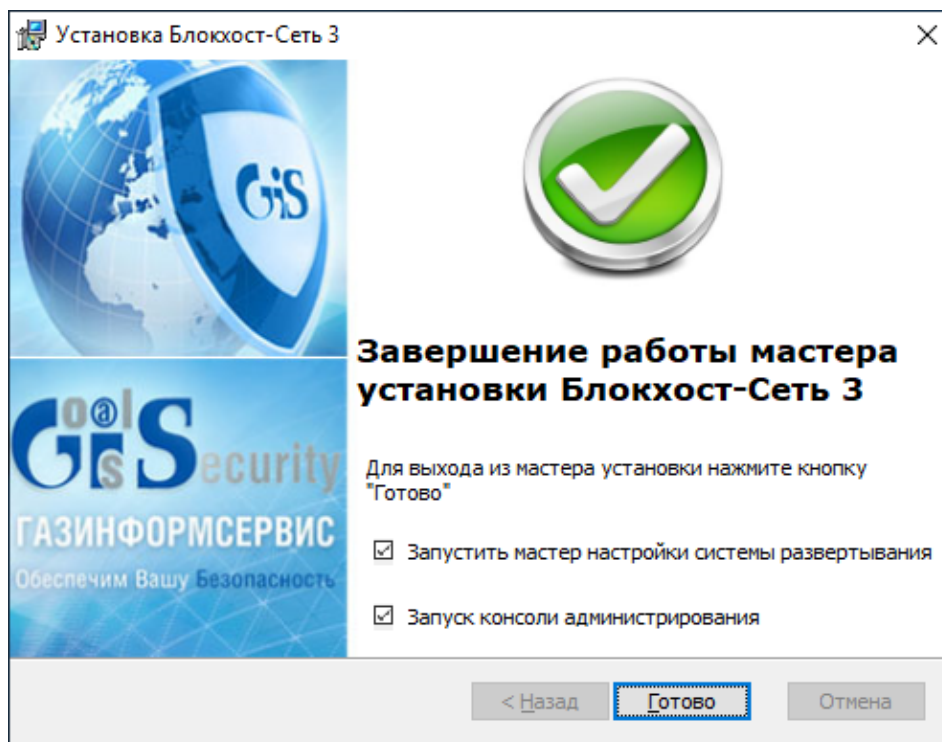


Рисунок 1.1 – Окно окончания установки сервера СЗИ

Для самостоятельного запуска мастера настройки параметров СРиА необходимо

выбрать пункт главного меню **Пуск** → **Программы** → **Блокхост-Сеть 3** → **Мастер настройки системы**.

После вызова мастера настройки СРиА откроется окно приветствия, в котором необходимо нажать кнопку **Далее**:

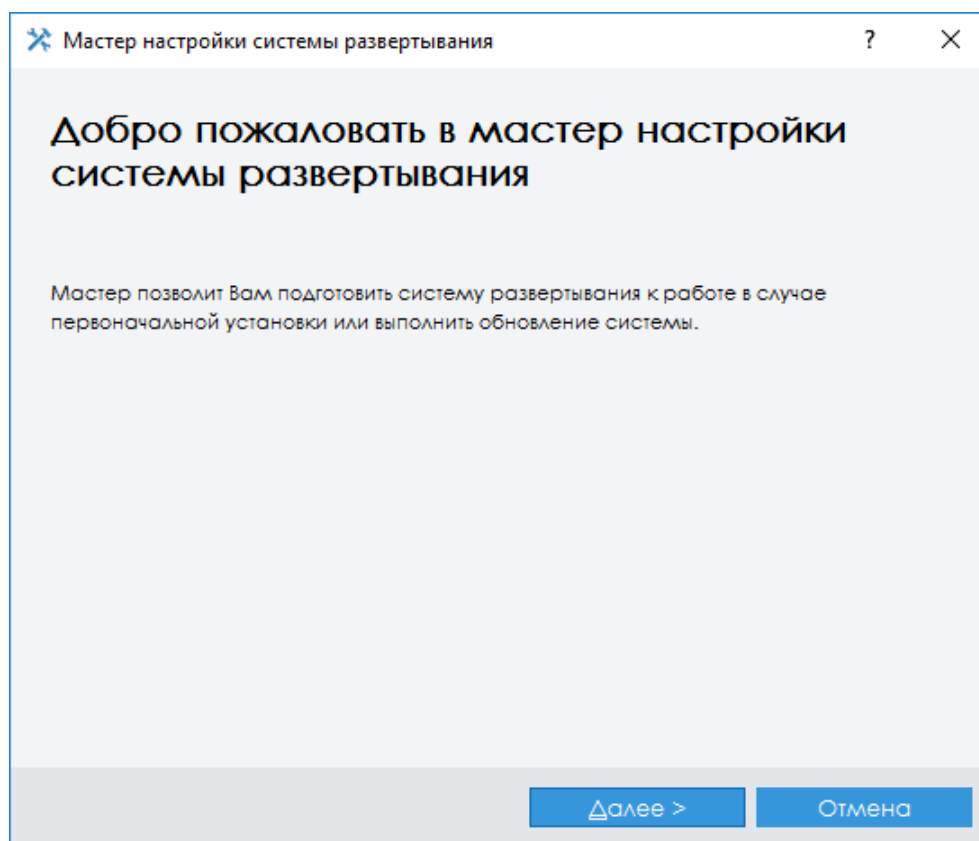


Рисунок 1.2 – Окно приветствия мастера настройки параметров СРиА

На следующем этапе работы мастера настройки СРиА необходимо задать путь к файлу инсталлятора распространяемого пакета Microsoft Visual C++ 2015 Redistributable или более поздней версии, содержащий компоненты Microsoft Visual C++ 2015 (рисунок 1.3). Наличие данного пакета является обязательным для корректной работы компонентов «Агент системы развертывания» и «Клиент Блокхост-Сеть».

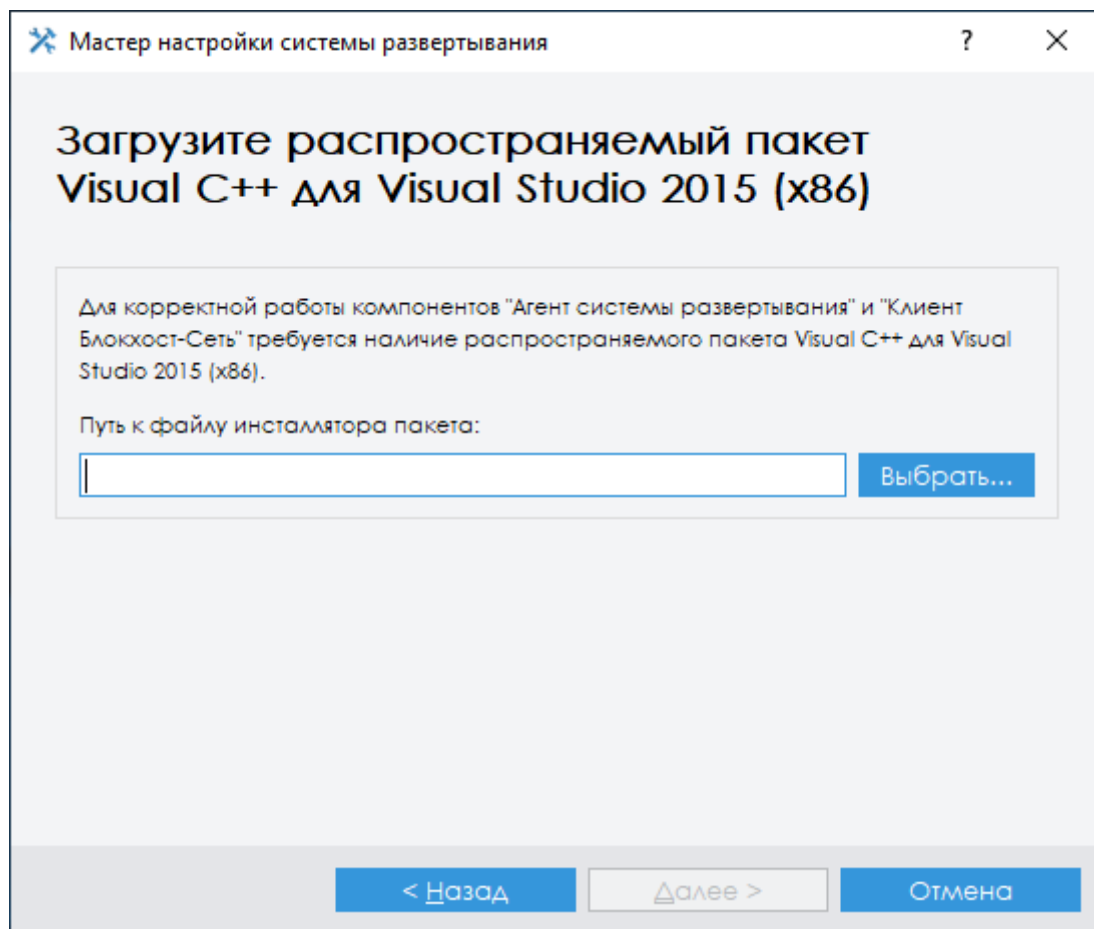


Рисунок 1.3 – Требование загрузки распространяемого пакета
Microsoft Visual C++ 2015 Redistributable

На следующем этапе работы мастера настройки СРиА (рисунок 1.4) необходимо задать параметры соединения СРиА с сервером БД¹:

- **Тип сервера базы данных** – выбирается тип СУБД: **PostgreSQL** или **встроенная база данных**;



При выборе параметра **Встроенная база данных** в выпадающем списке поля **Тип сервера базы данных** остальные параметры соединения с сервером базы данных отсутствуют.

- **Адрес сервера базы данных** – указывается IP-адрес или DNS-имя рабочей станции, на которой установлена СУБД PostgreSQL. При размещении СУБД PostgreSQL и сервера СЗИ на одной ЭВМ в поле **Адрес** можно оставить значение по умолчанию localhost;
- **Порт** – указывается значение TCP-порта, по которому осуществляется работа СУБД PostgreSQL;

¹ СЗИ «Блокост-Сеть 3» поддерживает работу с СУБД «Jatoba». Для настройки работы СРиА с СУБД «Jatoba» необходимо выбрать тип СУБД **PostgreSQL** и задать параметры соединения с сервером БД.

- **Имя пользователя** – имя пользователя СУБД PostgreSQL, обладающего полномочиями создания и редактирования баз данных;
- **Пароль** – пароль указанного выше пользователя СУБД PostgreSQL. Отмеченный параметр **Показать пароль** позволяет отобразить, введенное в поле **Пароль** значение. В противном случае в поле отображаются символы «*».

Для создания базы данных СРиА необходимо отметить параметр **Создать новую базу данных**. Если база данных уже существует, например, была перенесена с другого сервера баз данных, то параметр **Создать новую базу данных** отмечать не нужно.



|| При установке параметра **Создать новую базу данных**, существующая база данных СРиА будет уничтожена.

Рисунок 1.4 – Окно настройки параметров соединения СРиА и сервера баз данных

После ввода всех необходимых параметров соединения СРиА с СУБД необходимо нажать кнопку **Далее** – в результате откроется окно по выбору сетевого интерфейса. IP-адрес выбранного сетевого интерфейса используется для подключения агентов развертывания и клиентов Блокхост-Сеть к серверу СЗИ (рисунок 1.5). В списке сетевых интерфейсов отображаются только включенные сетевые адаптеры типа Ethernet и Wireless, имеющие IP-адреса протокола IPv4. Для выбора необходимого интерфейса следует выделить его в окне мастера настройки и нажать кнопку **Далее**.

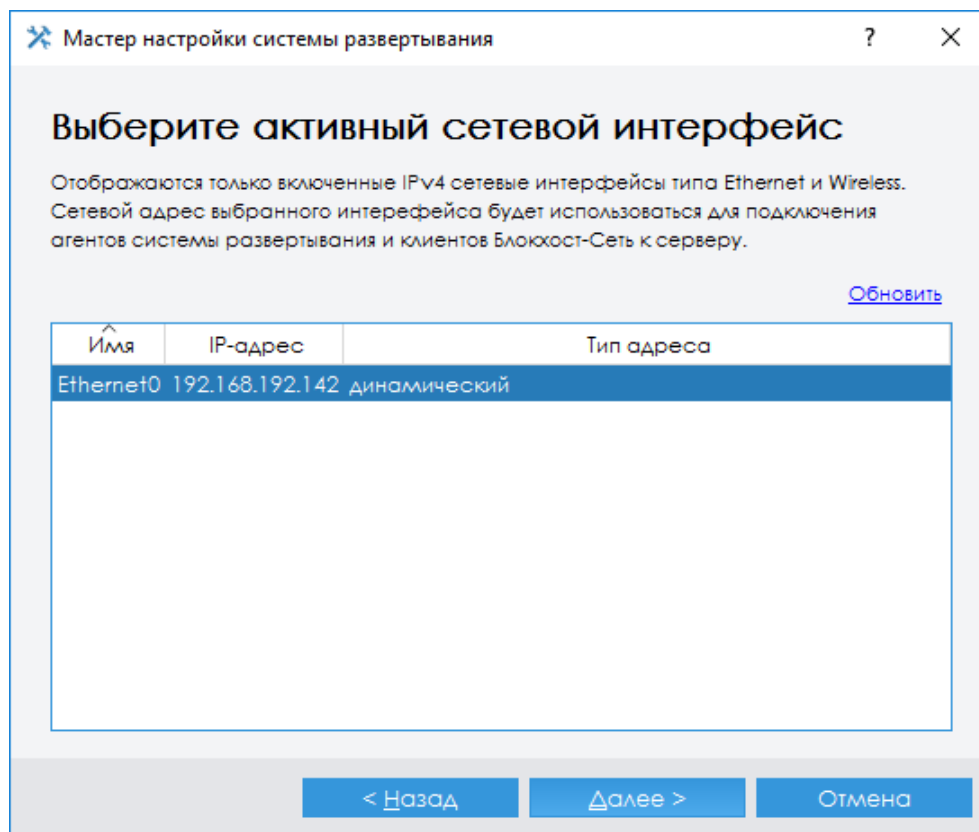


Рисунок 1.5 – Окно выбора сетевого интерфейса

На следующем шаге мастера настройки параметров СРиА откроется окно по редактированию параметров удаленного соединения агентов развертывания и клиентов Блокхост-Сеть с серверной частью СРиА (далее – сервер СРиА) (рисунок 1.6).

Для изменения установленного по умолчанию значения TCP-порта входящих соединений (25000), необходимо ввести новое значение в соответствующее поле.

Для включения механизма логирования работы следует отметить параметр **Выполнять логирование работы системы** и указать в соответствующем поле каталог, в котором будут храниться лог-файлы СРиА. Путь к каталогу можно ввести в поле вручную или выбрать его в окне **Выбор**, которое открывается после нажатия на кнопку **Выбрать**.



В лог-файлы, связанные с работой СРиА, записывается в основном отладочная информация, которая необходима для разработчиков системы. Однако запись информации о работе СРиА поможет быстрее разобраться с возможными проблемами, возникшими в ее работе.

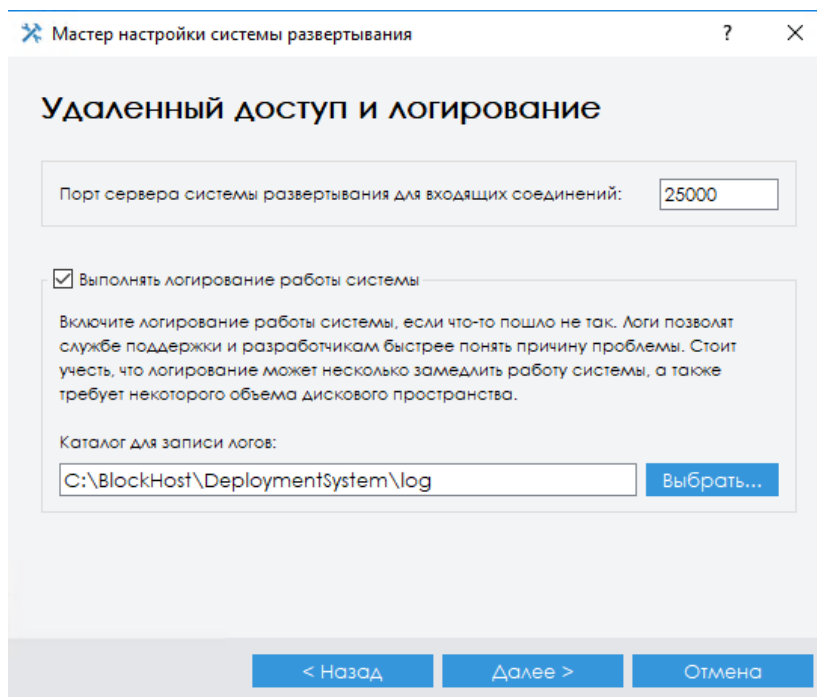


Рисунок 1.6 – Окно настройки параметров удаленного доступа и логирования сервера СРиА

Для продолжения работы по настройке СРиА необходимо нажать кнопку **Далее**.

В открывшемся окне завершения работы мастера настройки СРиА (рисунок 1.7) нажать кнопку **Готово**.

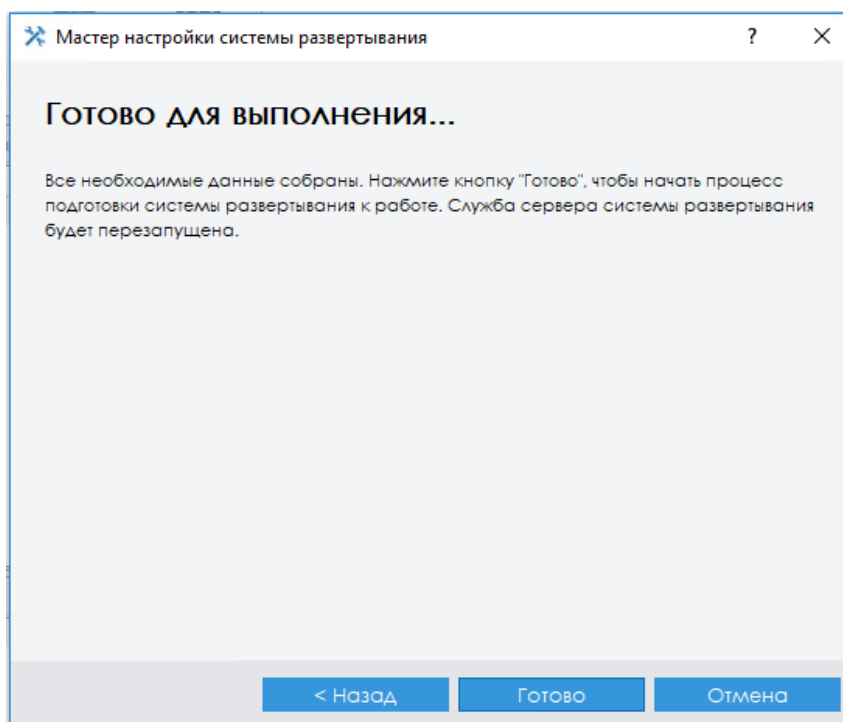


Рисунок 1.7 – Окно окончания настройки параметров сервера СРиА

Для завершения работы мастера настройки СРиА необходимо нажать кнопку

Завершить в открывшемся в окне мастера настройки (рисунок 1.8).

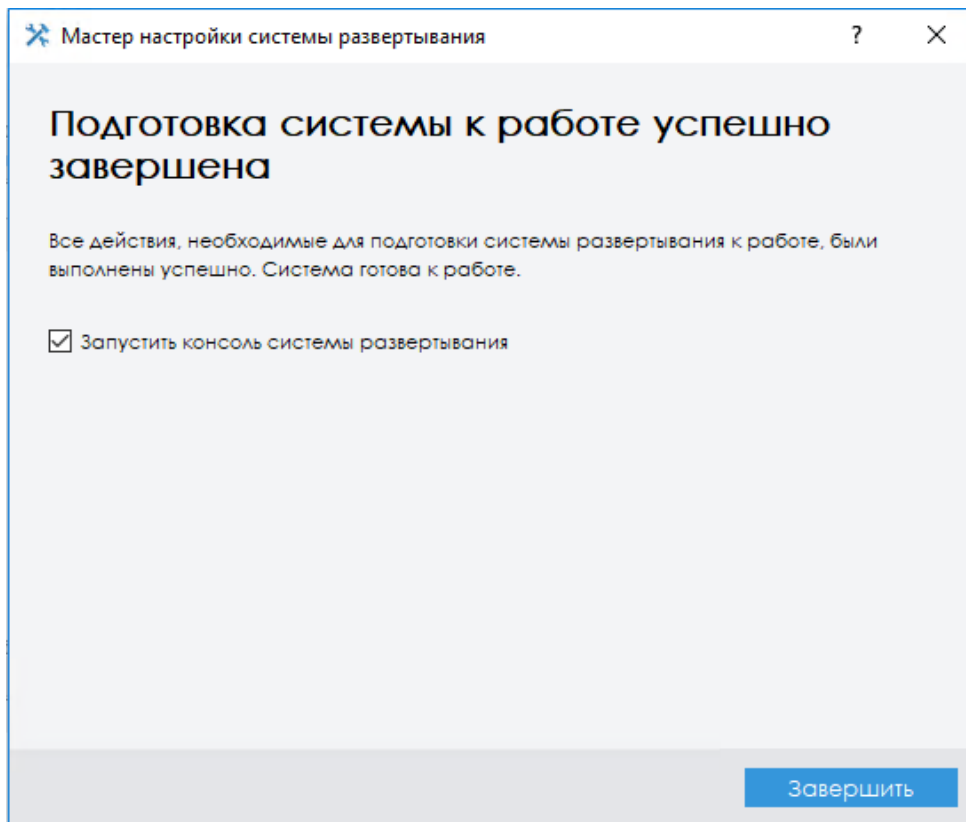


Рисунок 1.8 – Окно окончания работы мастера настройки параметров СРиА

В результате СРиА будет сконфигурирована в соответствии с параметрами, указанными в мастере настройки системы.

2 Описание работы с консолью СРиА

Для запуска консоли СРиА необходимо выбрать в меню **Пуск** пункт **Все программы** → **Блокхост-Сеть 3** → **Система развертывания и аудита** → (на рисунке 2.1 показан вызов консоли СРиА в ОС Windows 8).

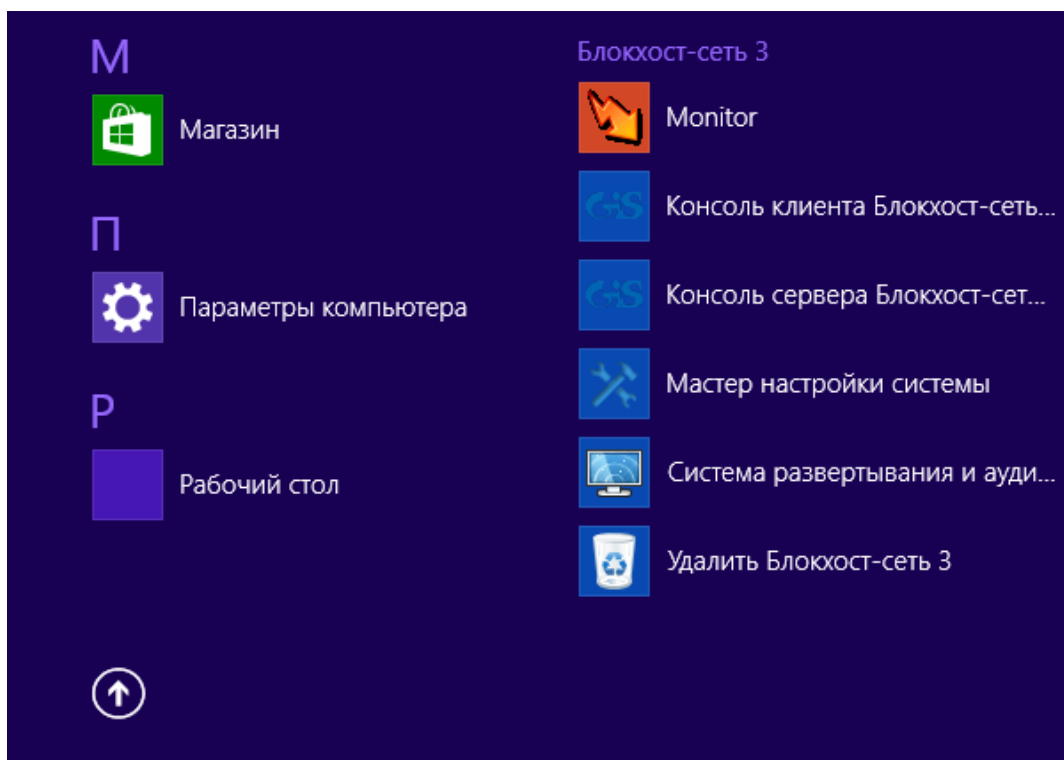


Рисунок 2.1 – Запуск консоли СРиА из меню **Пуск**

Консоль СРиА имеет вид, приведенный на рисунке 2.2. Название и описание разделов консоли приведены в таблице 2.1.

Таблица 2.1 – Разделы консоли СРиА

Наименование раздела	Описание раздела
Развертывание	Предназначается для управления процессом установки программного обеспечения, в том числе клиентов Блокхост-Сеть на рабочие станции
Мониторинг	Отслеживание событий клиентов Блокхост-Сеть (состояние клиента, тип аутентификации пользователя на клиенте, режим работы клиента, наличие неактивных шаблонов клиентов, наличие ошибок при синхронизации политик)
Архивы	Архивирование зарегистрированных событий клиентов Блокхост-Сеть

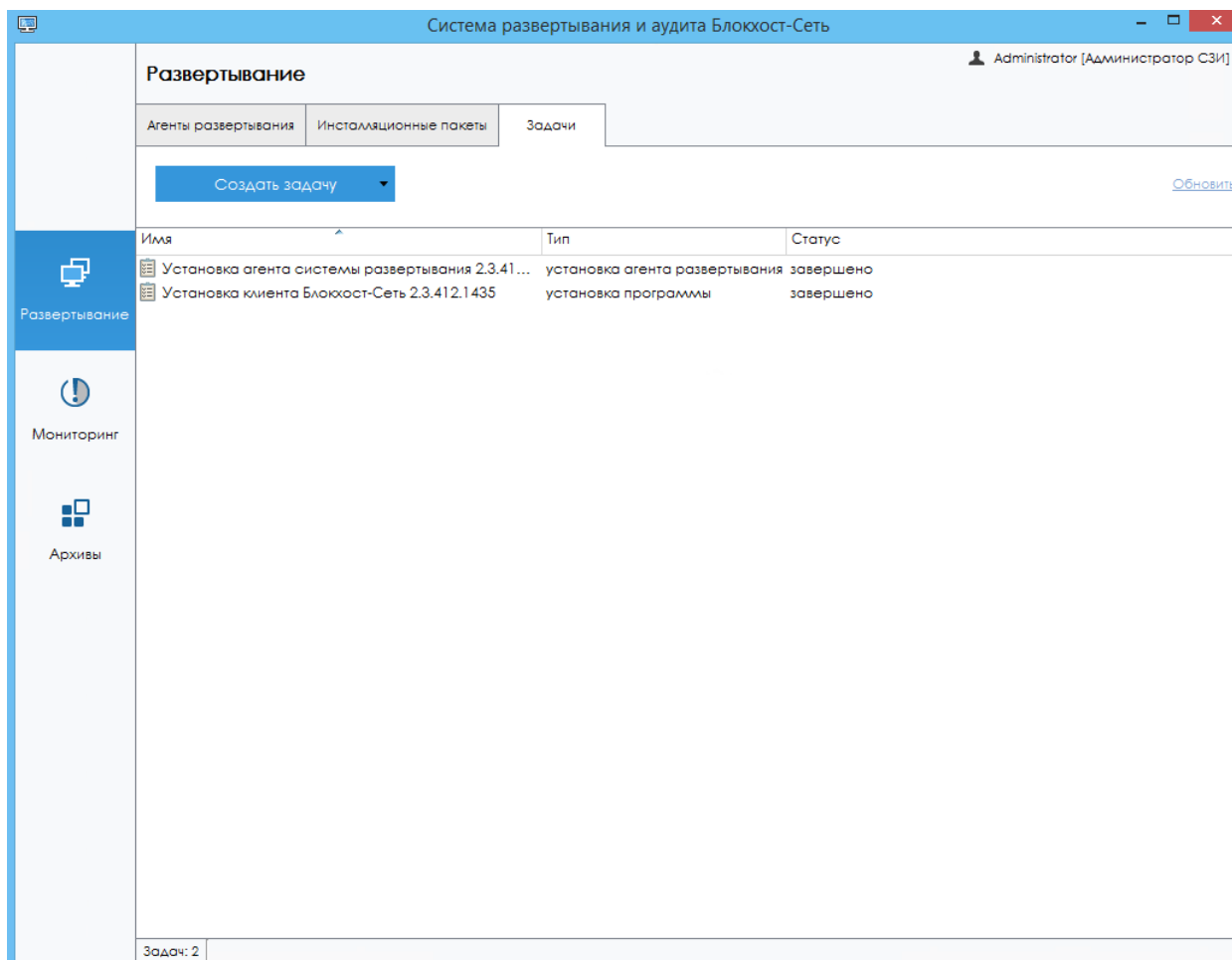


Рисунок 2.2 – Основное окно консоли СРиА

2.1 Ролевое распределение

Распределение по ролям необходимо для ограничения полномочий пользователей в отношении использования функционала СЗИ «Блокост-Сеть 3».

Для установки ролевого разграничения администратору безопасности необходимо выполнить настройки полномочий для пользователей СЗИ. Подробное описание настроек полномочий приведено в документе «Средство защиты информации от несанкционированного доступа «Блокост-Сеть 3». Руководство администратора безопасности».

Для присвоения пользователю определенной роли, администратору безопасности необходимо проверить, что пользователь:

- входит в группу «Администраторы» на локальной машине;
- добавлен в список пользователей локальной машины в политике Блокост-Сеть.

В зависимости от предоставляемых прав, пользователю могут быть присвоены роли:

- **Администратора** – предоставление пользователю прав администратора, полный доступ к функционалу СЗИ.
- **Аудитора** – предоставление пользователю прав аудитора. Пользователь имеет

доступ только к просмотру настроек СЗИ, без внесения каких-либо изменений.



Права администратора предоставляются пользователю при установке флага **Администратор** или флагов **Администратор** и **Аудитор**. Права аудитора предоставляются пользователю при установке флага **Аудитор**.



При отсутствии у пользователя одной из ролей (флаги **Администратор** и/или **Аудитор** не установлены) запуск консоли СРиА осуществлен не будет.

Пользователь с правами аудитора, в консоли СРиА не обладает правами на выполнение следующих операций в разделе **Развертывание**:

- удаление компьютера (вкладка **Агенты развертывания**);
- создание/редактирование/удаление инсталляционных пакетов;
- создание/редактирование/удаление любого типа задач;
- запуск/остановка выполняющейся задачи любого типа;
- подготовка дистрибутива для АД.



При попытке пользователя с ролью **Аудитор** выполнить одну из перечисленных операций, появится диалоговое окно с сообщением об отсутствии прав для выполнения данных операций (рисунок 2.3).

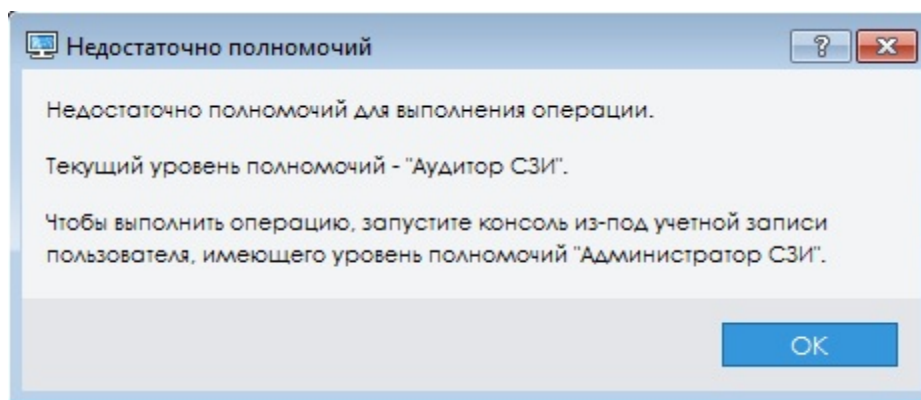


Рисунок 2.3 – Сообщение об отсутствии прав на выполнение операции

Работа с разделом **Мониторинг** предоставляется пользователю с правами аудитора в полном объеме.

Роль пользователя отображается в верхнем правом углу консоли СРиА (рисунок 2.4), при этом имя пользователя, из-под которого была запущена консоль и его роль отображается в формате:

- <имя домена>\<имя пользователя> (роль), если консоль запущена из-под доменного пользователя;
- <имя пользователя> (роль), если консоль запущена из-под локального пользователя.

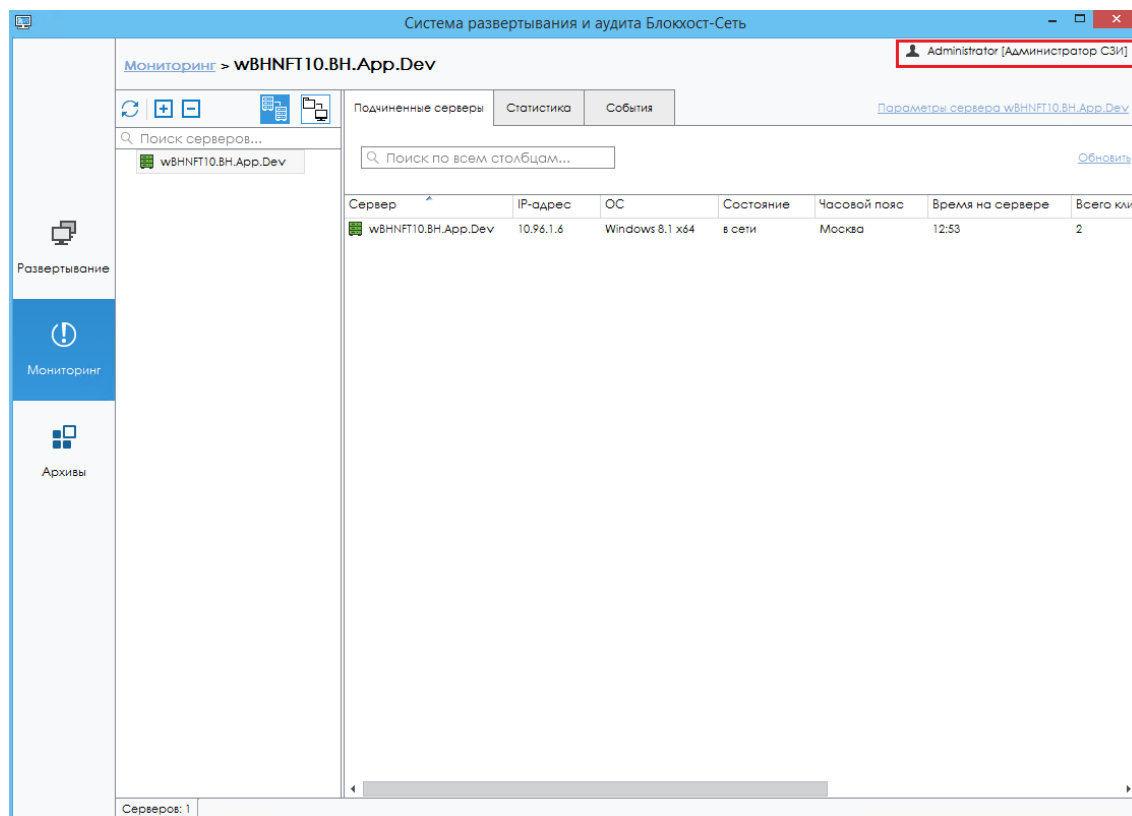


Рисунок 2.4 – Отображение роли пользователя в консоли СРиА

3 Раздел «Развертывание»

В разделе **Развертывание** консоли СРиА осуществляется управление процессом установки или удаления программного обеспечения, в том числе клиентов Блокхост-Сеть на рабочие станции (рисунок 3.1). Название и содержимое вкладок раздела приведены в таблице 3.1.

Таблица 3.1. – Вкладки раздела **Развертывание**

Наименование вкладки	Содержимое вкладки
Агенты развертывания	Отображается список рабочих станций, на которых установлены агенты (клиенты) системы развертывания
Инсталляционные пакеты	Отображается список созданных пакетов для инсталляции ПО, имеющих в консоли СРиА
Задачи	Отображается список задач по установке инсталляционных пакетов на рабочие станции, имеющих в консоли СРиА

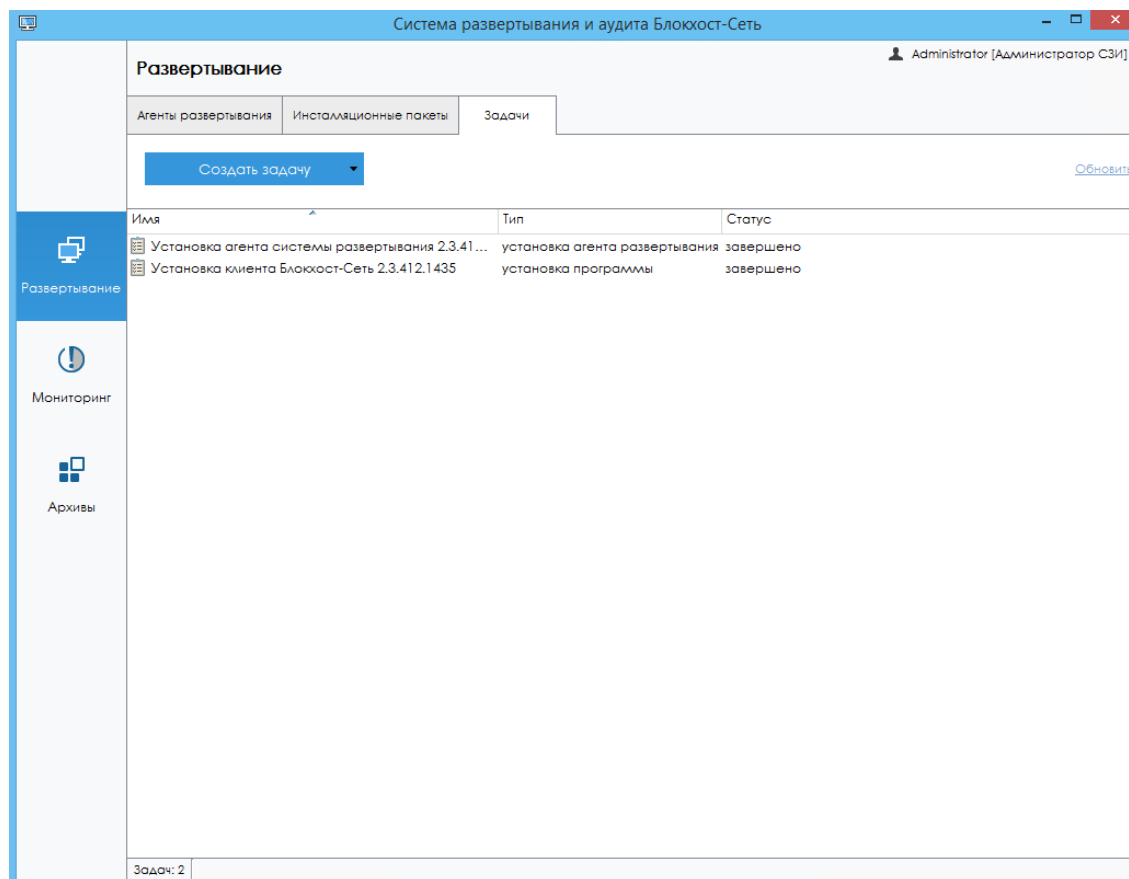


Рисунок 3.1 – Раздел «Развертывание»

3.1 Вкладка «Агенты развертывания»

Во вкладке **Агенты развертывания** (рисунок 3.2) расположен список рабочих станций, на которых запущена служба агента системы развертывания (СР) (*GIS.Client.DeploymentSystem*), а также кнопка **Обновить**, нажатие на которую позволяет обновить список подключенных к серверу СРиА рабочих станций. Иконки

рабочих станций отображаются разными цветами - в зависимости от того, как давно агент развертывания подключался к серверу: зеленый, желтый и красный.

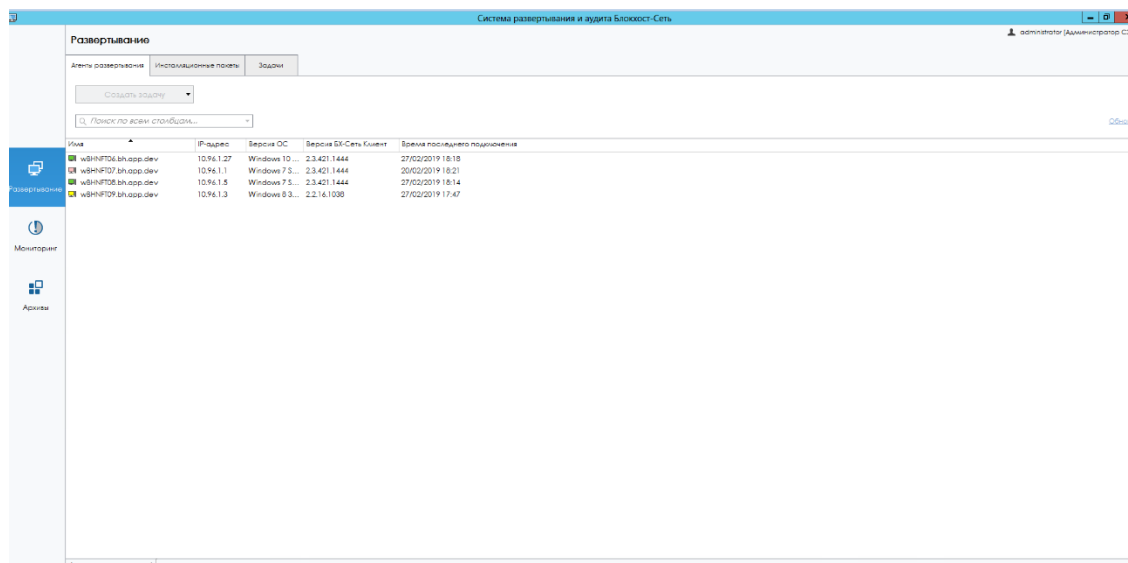


Рисунок 3.2 – Вкладка **Агенты развертывания**

Для каждой рабочей станции из списка во вкладке **Агенты развертывания** доступно контекстное меню, открываемое по щелчку правой кнопкой мыши на строке с именем рабочей станции, в котором содержатся следующие пункты (рисунок 3.3):

- **Проверить соединение со службой агента** – проверка соединения с выбранной рабочей станцией (со службой агента развертывания);
- **Создать задачу** – создание задачи на установку, удаление программы или перезагрузку рабочей станции.
- **Копировать** – копирование имени рабочей станции;
- **Удалить** – удаление выбранной рабочей станции из списка вкладки **Агенты развертывания**. Рабочая станция снова появится во вкладке **Агенты развертывания** после ее перезагрузки или перезапуска на ней службы агента CP (*GIS.Client.DeploymentSystem*).



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

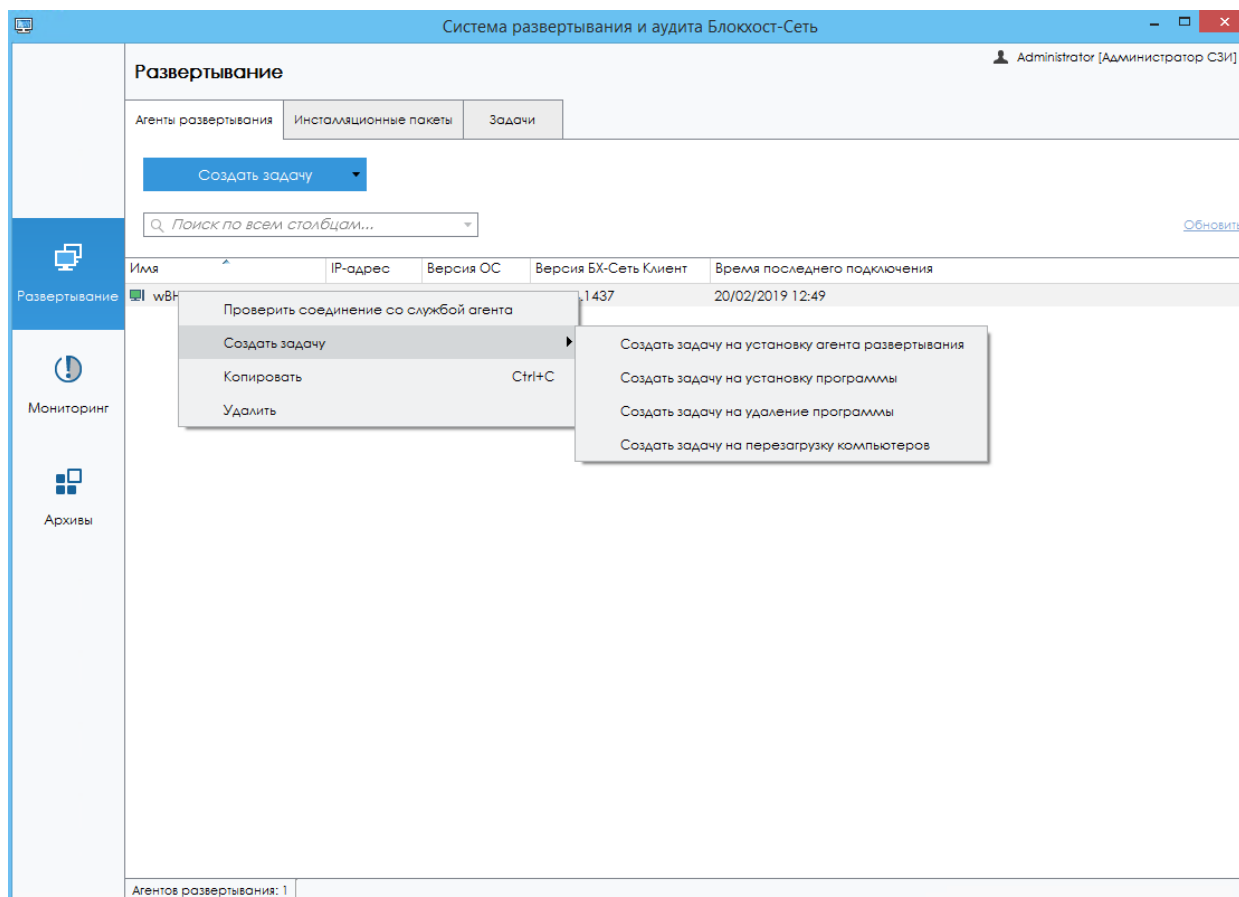


Рисунок 3.3 – Контекстное меню рабочей станции вкладки **Агенты развертывания**

3.1.1 Установка агента системы развертывания

Агент развертывания осуществляет взаимодействие между сервером СЗИ и удаленной рабочей станцией. Агент развертывания устанавливается на **рабочих станциях в сети**, на которые планируется установить программное обеспечение. Агент развертывания может быть установлен различными способами:

- с сервера СЗИ из консоли СРиА;
- вручную на рабочей станции;
- с использованием Active Directory;
- с использованием SMS;
- с использованием других программных средств, позволяющих устанавливать файлы с расширением .msi (например, антивирус Касперского и др).

Инсталляционный пакет агента развертывания входит в состав сервера СЗИ и располагается в каталоге *Агент системы развертывания* директории установки серверной части СЗИ (C:\BlockHost\DeploymentSystem\default\).

3.1.1.1 Установка из консоли СРиА

Для установки агента развертывания на рабочие станции из консоли СРиА администратору необходимо выполнить следующие действия:

1) Отредактировать параметры автоматически созданной задачи **Установка агента системы развертывания <номер версии>** по установке агента развертывания:

- сформировать список рабочих станций, на которые будет устанавливаться агент развертывания;
- указать учетные записи пользователей (локальные или доменные), обладающие административными правами на рабочих станциях, на которые будет устанавливаться агент развертывания;
- указать параметры планировщика выполнения задачи установки агента развертывания на рабочие станции.

2) Запустить задачу по установке агента системы развертывания вручную, если не настроен запуск по расписанию.



Для установки агента развертывания на рабочие станции также возможно создание новой задачи на установку программного обеспечения. Подробнее в пункте 3.3.1 «Создание задачи на установку ПО» данного документа.

Для редактирования параметров автоматически созданной задачи по установке агента системы развертывания администратору безопасности необходимо:

1) Запустить консоль СРиА и перейти в раздел **Развертывание**, во вкладку **Задачи** (рисунок 3.4).

2) Щелкнуть правой кнопкой мыши на строке с именем **Установка агента системы развертывания <номер_версии>** и выбрать в открывшемся контекстном меню пункт **Редактировать** (рисунок 3.4), выполнить двойной щелчок левой кнопкой мыши на необходимой строке.

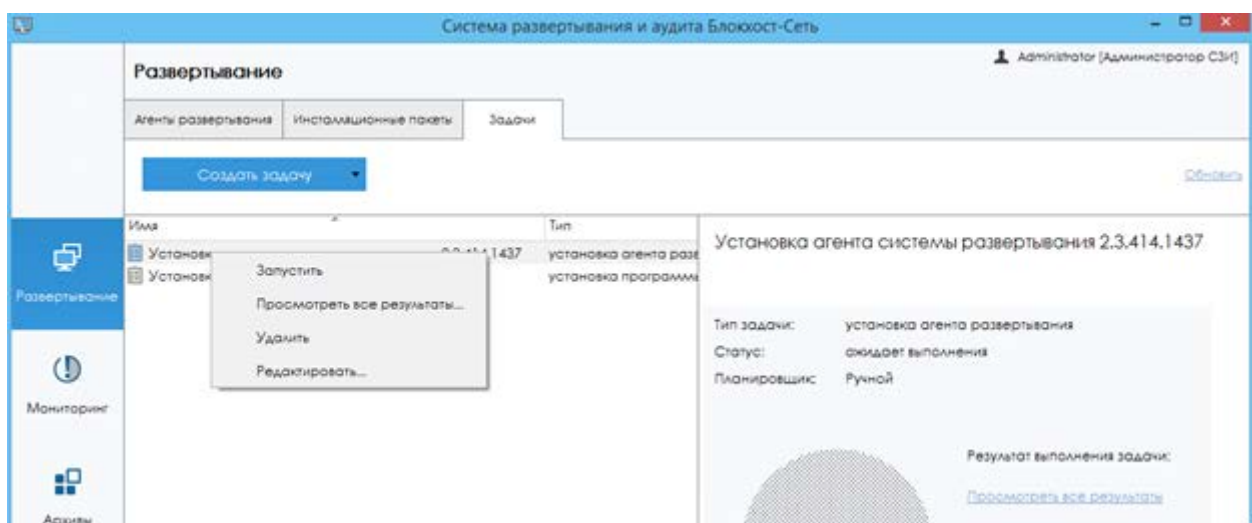


Рисунок 3.4 – Контекстное меню задачи во вкладке **Задачи**

3) В открывшемся окне редактирования задачи по установке агента системы развертывания (рисунок 3.5) перейти в раздел **Компьютеры** и сформировать список рабочих станций, на которые будет установлен агент развертывания одним из четырех способов:

Способ 1:

Нажать кнопку **Добавить**, и в открывшееся поле ввода ввести имя или IP-адрес рабочей станции и нажать клавишу <Enter>:

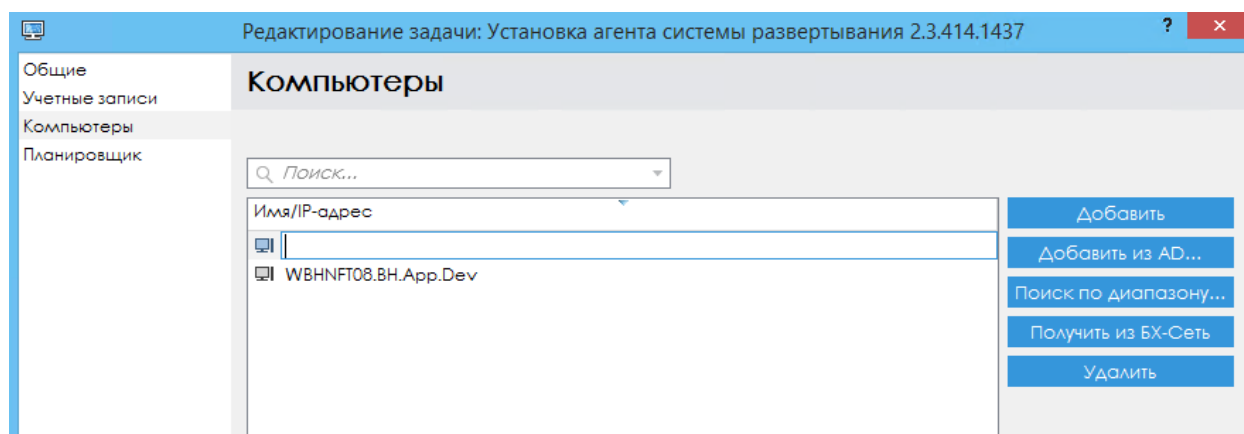


Рисунок 3.5 – Ввод имени/IP-адреса рабочей станции по кнопке **Добавить**

Способ 2:

Нажать кнопку **Добавить из AD:**

- в открывшемся окне авторизации в домене ввести имя домена, логин и пароль учетной записи пользователя домена и нажать кнопку **Подключиться** (рисунок 3.6);

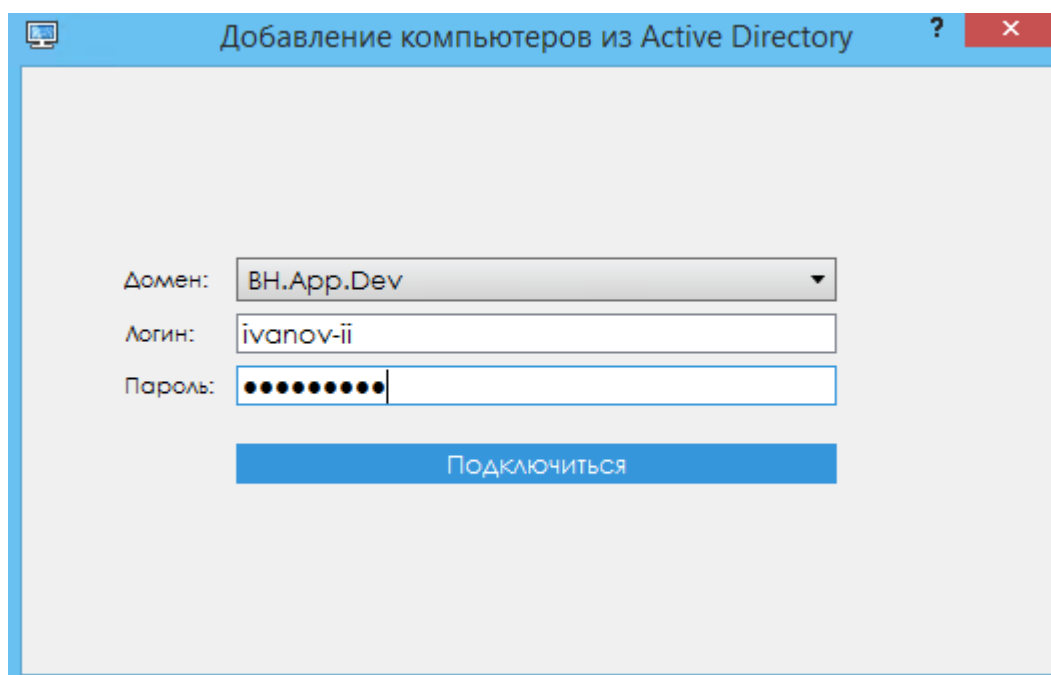


Рисунок 3.6 – Окно авторизации в домене



Если рабочая станция, на которую установлен сервер СЗИ, включена в домен, то поле **Домен** будет содержать выпадающий список всех доступных для подключения доменов

- в открывшемся окне добавления рабочих станций (рисунок 3.7) в левой части области *Компьютеры домена* отобразится структура объектов Active Directory (AD) указанного домена. Для выбора рабочих станций (серверов), на которые будет устанавливаться программное обеспечение, необходимо выделить объект структуры AD, и в правой части области *Компьютеры домена* отобразятся зарегистрированные в нем рабочие станции. Например, в структуре объектов AD домена **BH.App.Dev**, приведенной на рисунке 3.7, выделен объект **BlockHost**, и в правой части области *Компьютеры домена* отобразились все находящиеся в выделенном объекте AD сервера и рабочие станции.

При установке параметра **показывать компьютеры во вложенных Organization Unit** и выделении в левой части области *Компьютеры домена* необходимого Organization Unit, будет выведен список всех серверов и рабочих станций, находящихся в выбранном Organization Unit, а также во всех вложенных в него элементах.

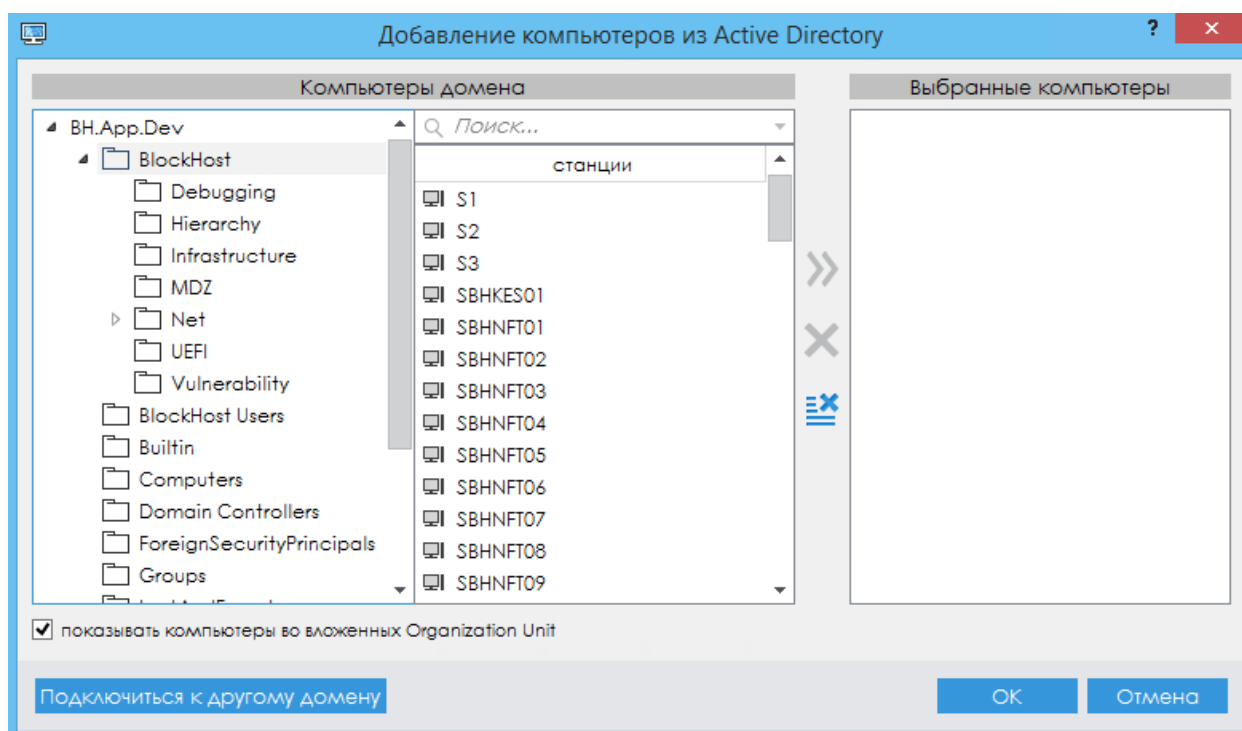


Рисунок 3.7 – Окно добавления в задачу рабочих станций из домена

- выделить одну или несколько рабочих станций (с помощью клавиш **<Ctrl>** или **<Shift>**), нажав кнопку **Добавить станцию** «**>>**» переместить их в область *Выбранные компьютеры* (добавление или удаление рабочей станции также возможно двойным щелчком левой кнопки мыши);
- после нажатия кнопки **ОК**, добавленные рабочие станции появятся во вкладке

Компьютеры окна редактирования параметров задачи:

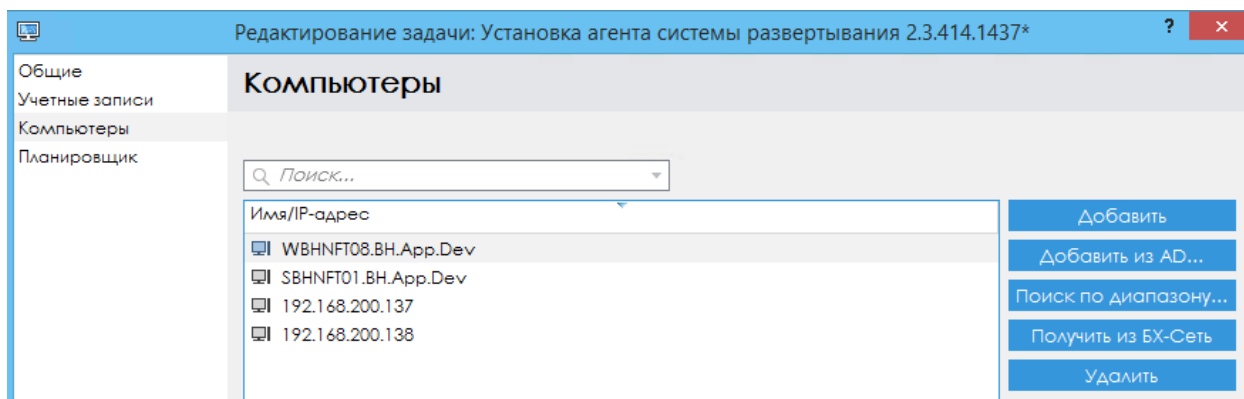


Рисунок 3.8 – Список рабочих станций для установки агента CP

Способ 3:

Нажать кнопку **Поиск по диапазону** (рисунок 3.5):

- в открывшемся окне (рисунок 3.9), для поиска IP-адресов в заданном диапазоне, необходимо ввести начальный и конечный IP-адреса в соответствующие поля и нажать кнопку **Начать поиск**;

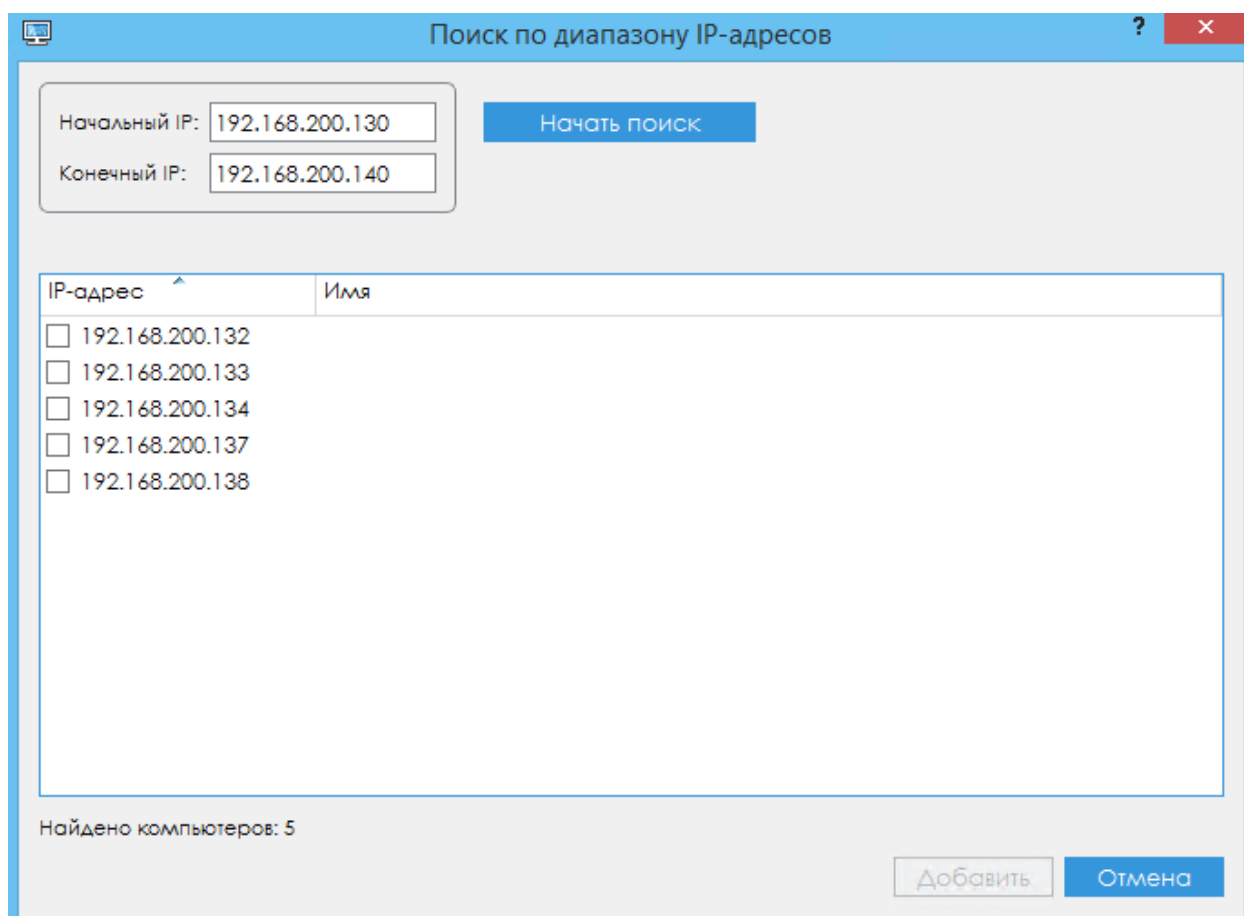


Рисунок 3.9 – Окно поиска рабочих станций по диапазону IP-адресов

- в сформированном списке выбрать рабочие станции (см. пункт 3.3.2. Добавление

в задачу нескольких рабочих станций»), и нажать кнопку **Добавить**. Каждой рабочей станции в списке соответствует строка, где указаны её IP-адрес и DNS-имя. Если не удалось определить DNS-имя добавляемой рабочей станции, то в списке будет указан только её IP-адрес (рисунок 3.8).

Способ 4:

Нажать кнопку **Получить из БХ-Сеть** (рисунок 3.5). В этом случае с сервера СЗИ будет получен список клиентов Блокхост-Сеть, зарегистрированных на сервере СЗИ. Таким образом, возможно быстро сформировать список рабочих станций для установки агента развертывания, чтобы затем с помощью СРиА выполнить обновление клиента Блокхост-Сеть.

При нажатии на кнопку будет выведено окно с пояснением выполняемой операции. Если установлен параметр **Выполнять преобразование IP-адресов в DNS-имена**, то будет произведена попытка преобразования IP-адресов в DNS-имя рабочей станции (рисунок 3.10).

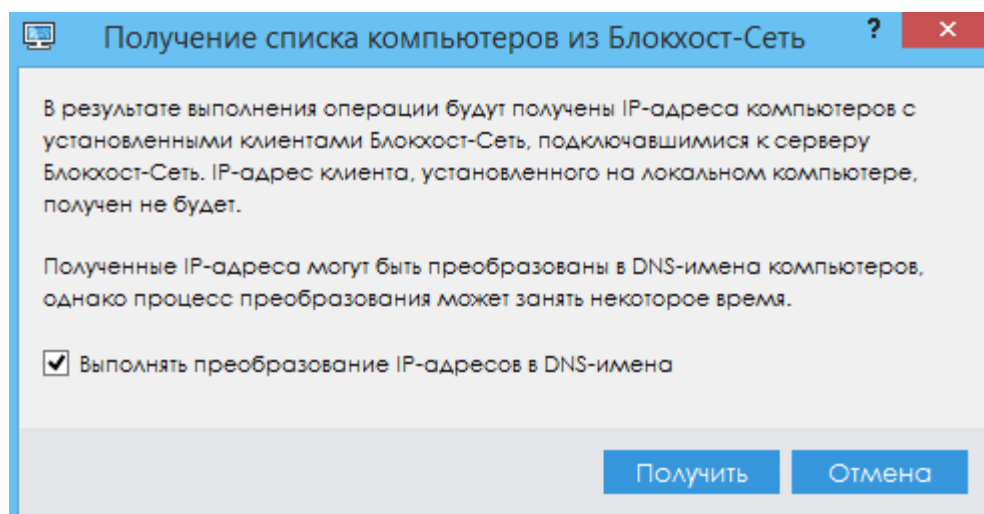


Рисунок 3.10 – Получение списка компьютеров с сервера СЗИ

4) Перейти в раздел **Учетные записи** (рисунок 3.11) и нажать кнопку **Добавить** для формирования списка учетных записей, с правами администратора на рабочих станциях, где будет устанавливаться агент развертывания.

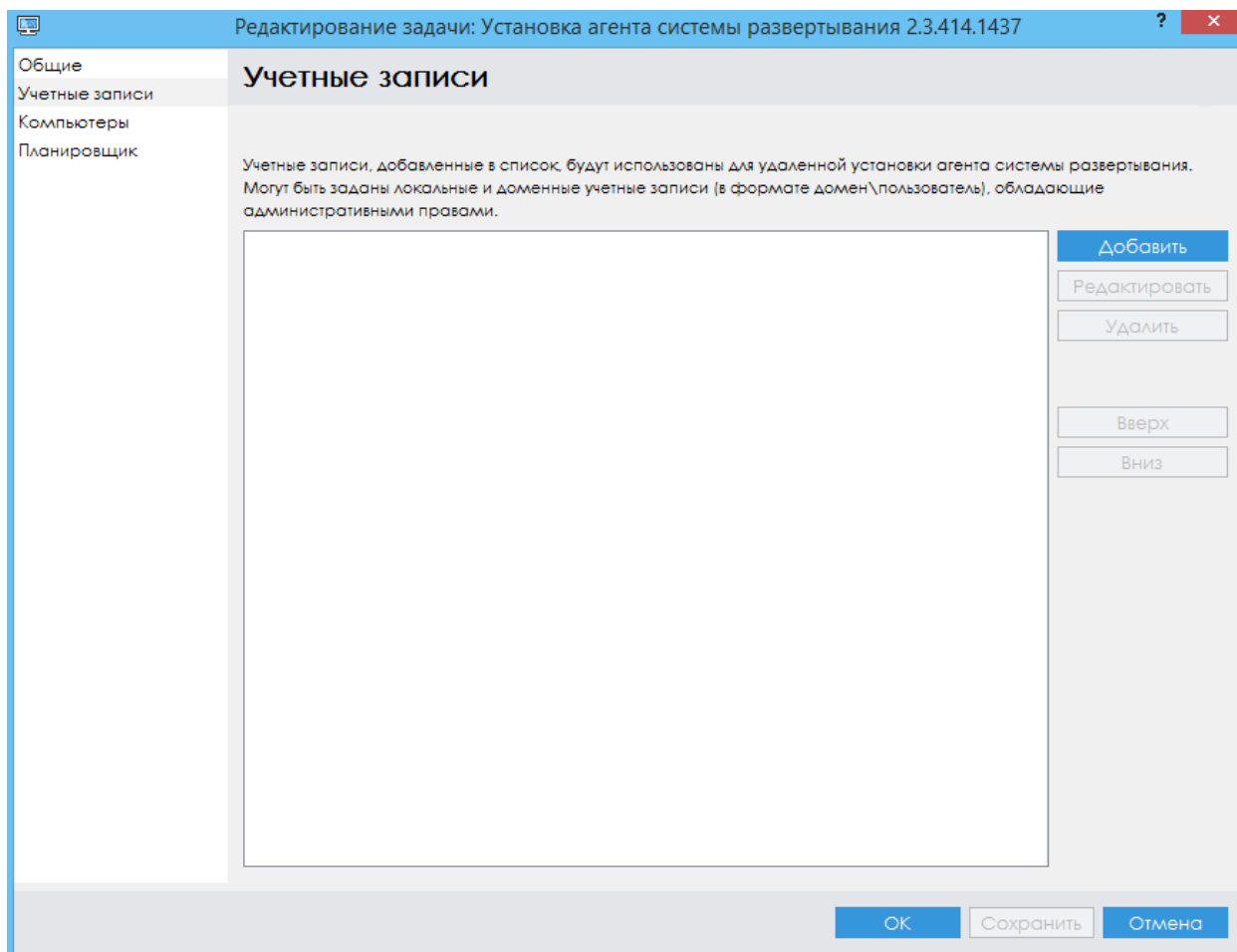


Рисунок 3.11 – Раздел **Учетные записи** окна редактирования параметров задачи

5) В открывшемся окне **«Добавление учетной записи»** (рисунок 3.12) в соответствующие поля ввести логин и пароль учетной записи, обладающей административными правами на рабочих станциях и нажать кнопку **ОК** (отмеченный параметр **показать пароль** позволяет отобразить введенный в поле пароль).

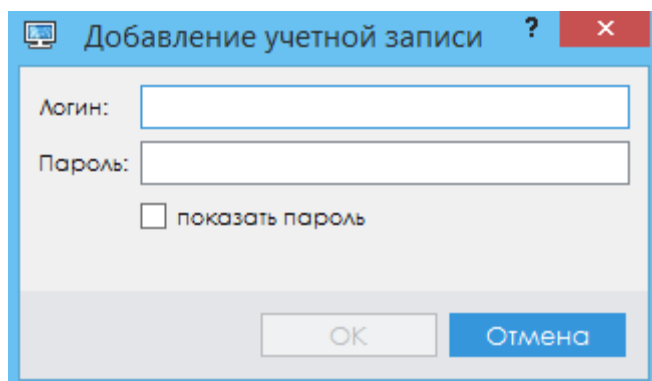


Рисунок 3.12 – Окно добавления учетной записи

6) Для добавления нескольких учетных записей необходимо повторить действия пунктов 4 и 5. В этом случае, при выполнении задачи, будет использована учетная запись из списка, и, если у данной учетной записи не будет административных прав,

будет использована следующая учетная запись в списке.

7) Перейти во вкладку **Планировщик** (рисунок 3.13) и в соответствующем поле выбрать тип запуска задачи по установке агента системы развертывания на рабочих станциях.

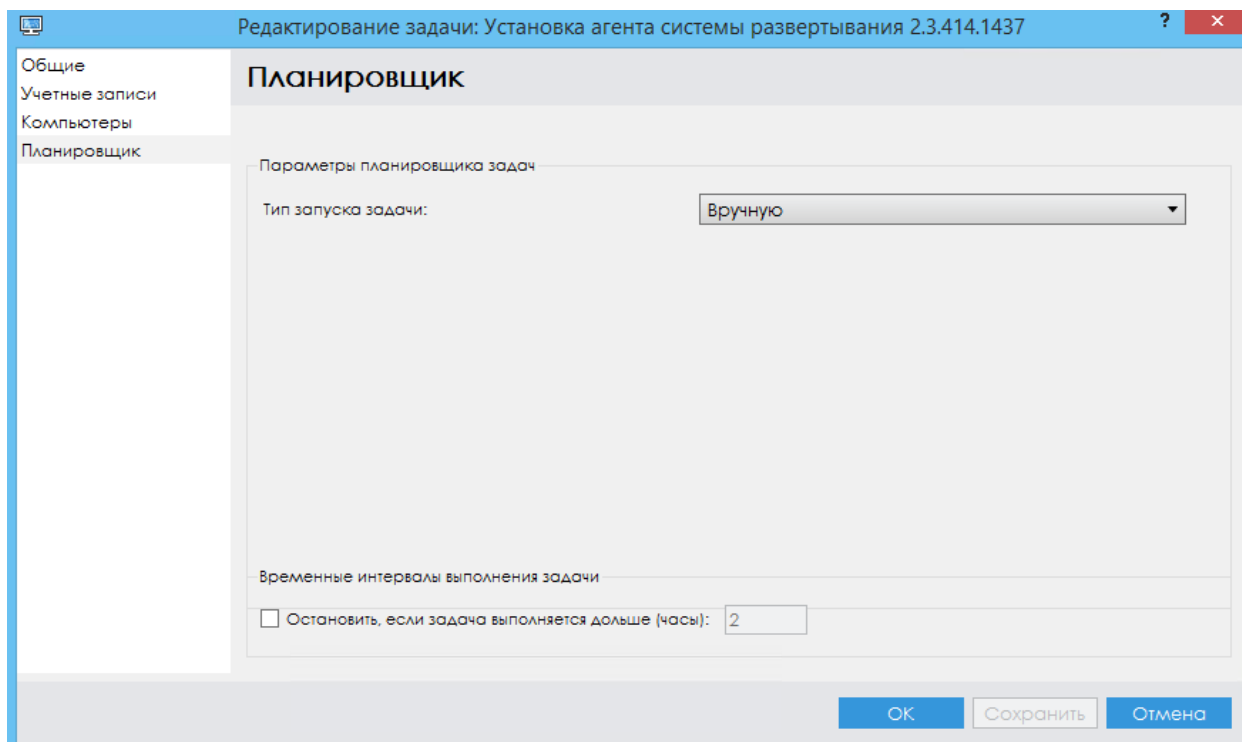


Рисунок 3.13 – Раздел **Планировщик** окна редактирования параметров задачи

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

- **Вручную** – задача запускается администратором безопасности из консоли СРиА;
- **Сразу после создания/редактирования задачи** – задача запустится, как только будет закрыто окно ее редактирования;
- **Однократно в заданное время** – в соответствующих полях указывается дата и время запуска задачи (рисунок 3.14, а);
- **По расписанию** – указывается дата и время первого запуска задачи, интервал запуска, параметры повторного запуска задачи и время окончания действия расписания (рисунок 3.14, б):
 - о *дату первого запуска задачи* и ее окончания можно ввести вручную или выбрать из календаря, раскрывающегося при нажатии на кнопку раскрытия списка;
 - о *время первого запуска* и окончания задачи также можно указать, введя его значение вручную или установив курсор на необходимый параметр (часы, минуты, секунды) откорректировать его значение с помощью кнопок

прокрутки;

- o *интервал запуска* повторного запуска задачи указывается в формате дни:часы, максимальное количество дней – 99, часов – 23. Минимальный интервал – 1 час, интервал, установленный по умолчанию – 1 день;
- o для рабочих станций задачи, имеющих статус «ожидает выполнения», повторный запуск задачи выполняется всегда;
- o 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** – задача будет запущена после того, как завершится предыдущая задача (рисунок 3.14, в). Для выбора задачи, после которой будет запущена текущая, необходимо нажать кнопку **Выбрать**, и в открывшемся окне (рисунок 3.15) выделить необходимую задачу и нажать кнопку **Выбрать**.

Планировщик

Параметры планировщика задач

Тип запуска задачи:	Однократно в заданное время ▼
Дата:	25.05.2018 ▼
Время:	11:35:12 ⌵

а)

Планировщик

Параметры планировщика задач

Тип запуска задачи: По расписанию

Время первого запуска: 20.02.2019 13:31:07

Интервал запуска (дни:часы) 1 00

Момент времени, после которого периодический запуск задачи прекращается: 22.02.2019 13:31:07

Выполнять периодический запуск задачи для компьютеров (опционально):
☐ недоступных
☐ с ошибками

i Каждый следующий периодический запуск задачи будет выполнен для компьютеров, добавленных в задачу после завершения ее предыдущего запуска. Кроме того, опционально возможно периодически запускать задачу для компьютеров, с которыми не удалось установить соединение при предыдущем запуске задачи, либо выполнение задачи для которых завершилось ошибкой.

б)

Планировщик

Параметры планировщика задач

Тип запуска задачи: После завершения другой задачи

Связанная задача:

[Выбрать...](#)

в)

Рисунок 3.14 – Параметры типа запуска задачи

Выберите связанную задачу

Выберите связанную задачу

Имя	Тип
Установка клиента Блокост-Сеть 2.3.414.1437	установка программы

[Выбрать](#) [Отмена](#)

Рисунок 3.15 – Окно выбора связанной задачи

Также во вкладке **Планировщик** можно указать параметры прекращения выполнения «зависшей» задачи (если задача выполняется длительное время) – отметить параметр **Остановить, если задача выполняется дольше (часы)** (рисунок 3.13) и ввести в открывшееся поле ввода необходимое значение в часах (см. пункт 3.3.7 Остановка задачи»).

8) Сохранить внесенные в задачу по установке агента системы развертывания изменения, последовательно нажав кнопки **Сохранить** и **ОК** (рисунок 3.13). Нажатие на кнопку **Отмена** до нажатия на кнопки **Сохранить** или **ОК** позволит выйти из окна редактирования параметров задачи без внесения изменений.



При выборе варианта запуска задачи **Вручную**, запустить задачу по установке агента системы развертывания на выполнение, можно нажатием кнопки **Запустить**, расположенную в нижней части области дополнительной информации выделенной задачи (рисунок 3.38).

3.1.1.2 Локальная установка

Для локальной установки агента развертывания на рабочие станции администратору необходимо выполнить следующие действия:

1) Скопировать с сервера СЗИ на рабочую станцию (или съемный носитель) инсталляционный пакет агента (*BHNetDeploymentAgent <номер_версии>.msi*) и запустить его на выполнение.



По умолчанию инсталляционный пакет агента расположен в каталоге установки СРиА (*C:\BlockHost\DeploymentSystem\default\Агент Системы развертывания*).

2) В открывшемся окне приветствия мастера установки агента развертывания нажать кнопку **Далее**:

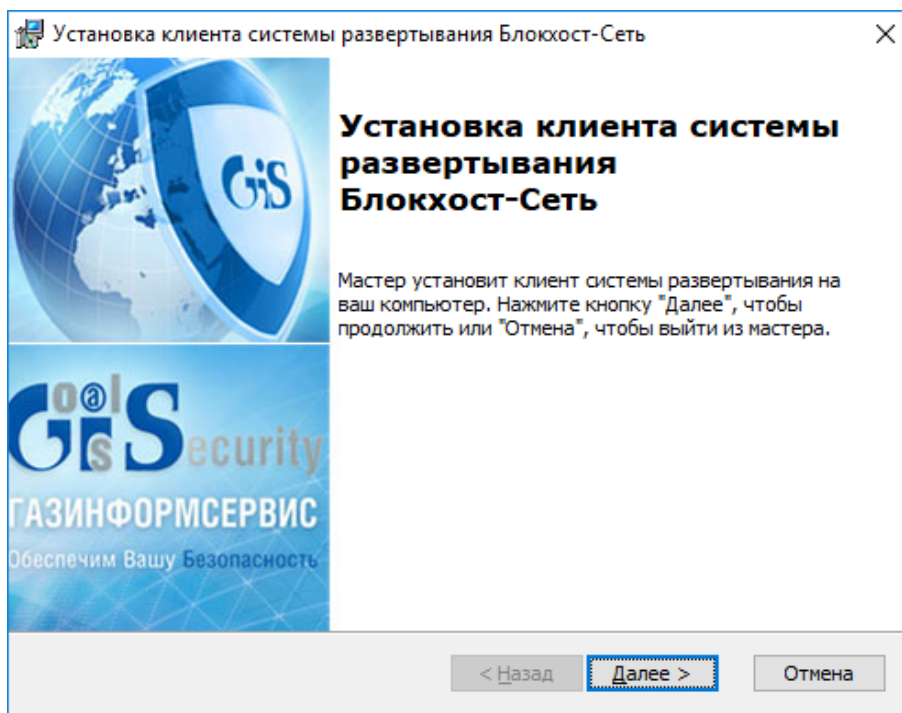


Рисунок 3.16 – Окно мастера установки агента развертывания

На любом этапе работы мастера установки агента развертывания можно нажать кнопку **Отмена**. На экране появится окно, показанное на рисунке 3.17. При нажатии кнопки **Да** установка будет прервана. При нажатии кнопки **Нет** установка будет продолжена.

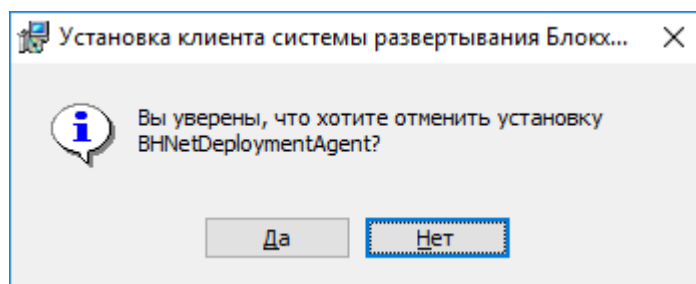


Рисунок 3.17 – Окно прекращения установки

3) В следующем диалоговом окне мастера установки (рисунок 3.18) можно изменить указанный по умолчанию каталог установки программы. Необходимый путь можно ввести в поле ввода вручную или указать его в окне выбора каталога (рисунок 3.19), открываемом при нажатии на кнопку **Обзор**. Для продолжения установки – нажать кнопку **Далее**.

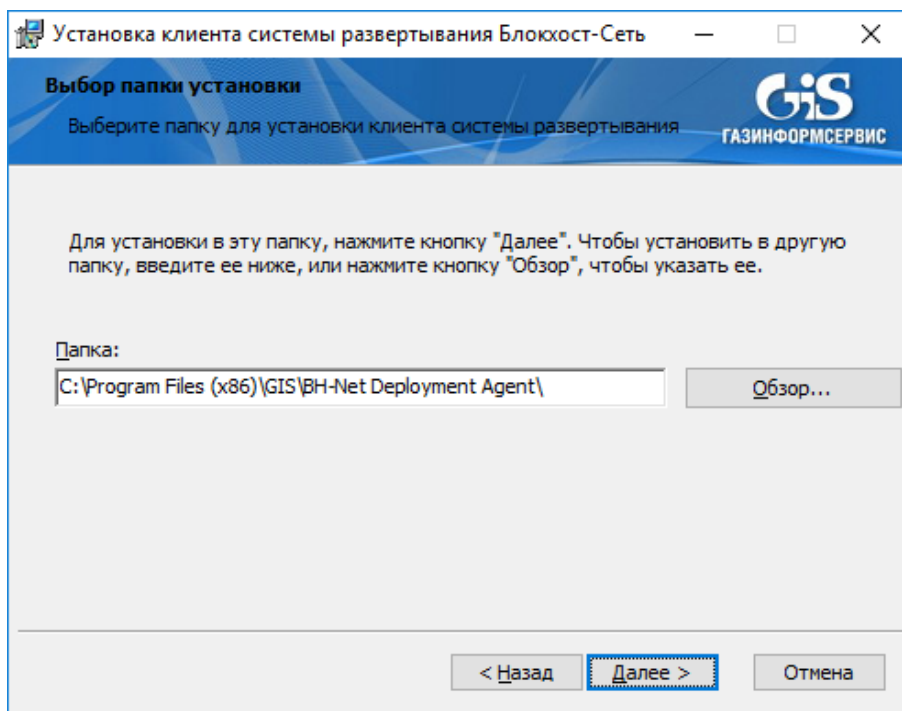


Рисунок 3.18 – Диалоговое окно выбора каталога установки программы

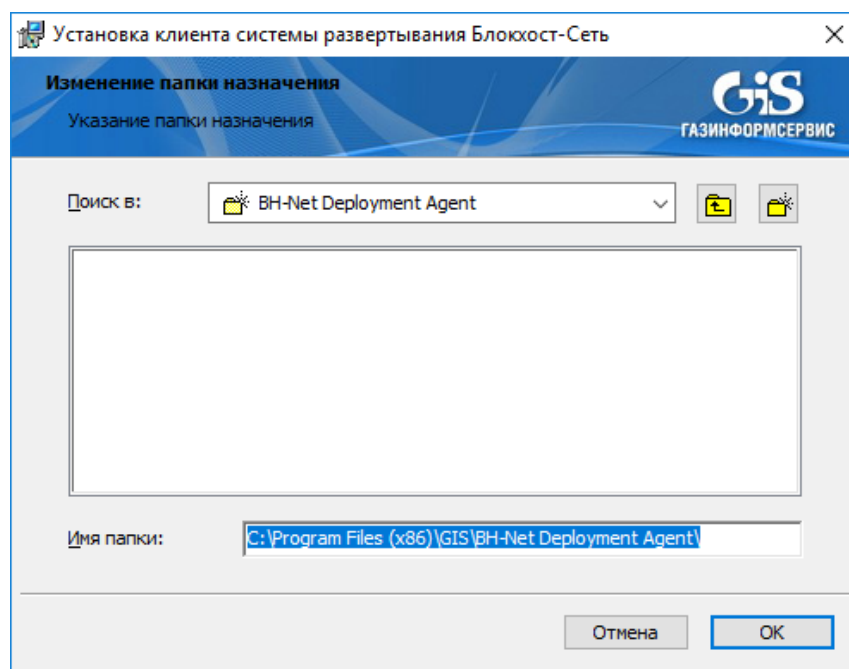


Рисунок 3.19 – Диалоговое окно изменения каталога установки программы

4) В открывшемся окне настройки параметров подключения агента развертывания к серверу СЗИ (рисунок 3.20) необходимо указать IP-адрес и TCP-порт сервера СЗИ, к которому будет подключаться агент. По умолчанию в окне указан локальный адрес серверной рабочей станции, на которой был сгенерирован инсталляционный пакет, и TCP-порт сервера СЗИ. После ввода необходимых значений нажать кнопку **Далее** для продолжения установки.



Если инсталляционный пакет не был сгенерирован в СРиА (см. пункт 3.2.2 «Подготовка дистрибутива для AD»), то по умолчанию в окне указаны IP адрес сервера 127.0.0.1, порт подключения 25000.

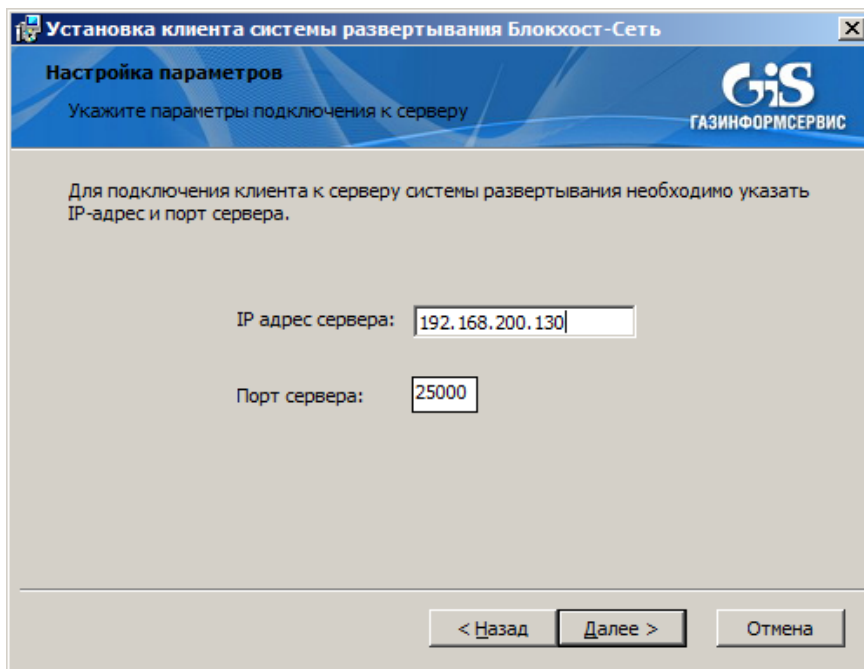


Рисунок 3.20 – Диалоговое окно ввода параметров подключения агента к серверу СЗИ

5) Откроется диалоговое окно готовности мастера к установке:

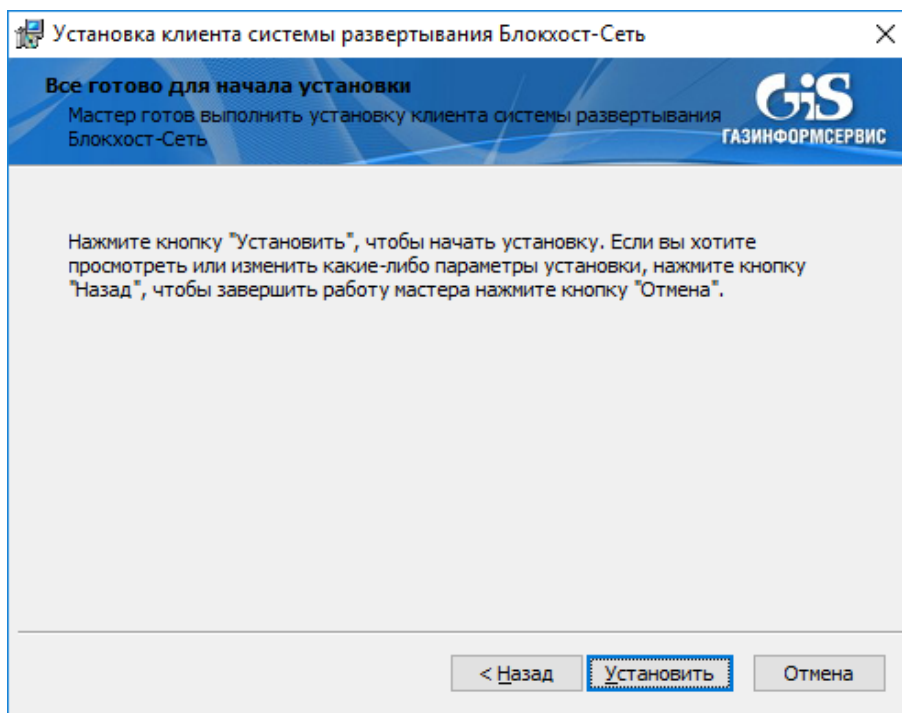


Рисунок 3.21 – Диалоговое окно готовности мастера к установке

6) После нажатия кнопки **Установить** начнется фактическая установка агента

развертывания на рабочую станцию.

7) Об окончании установки будет свидетельствовать появление окна завершения работы мастера установки, в котором необходимо нажать кнопку **Готово**:

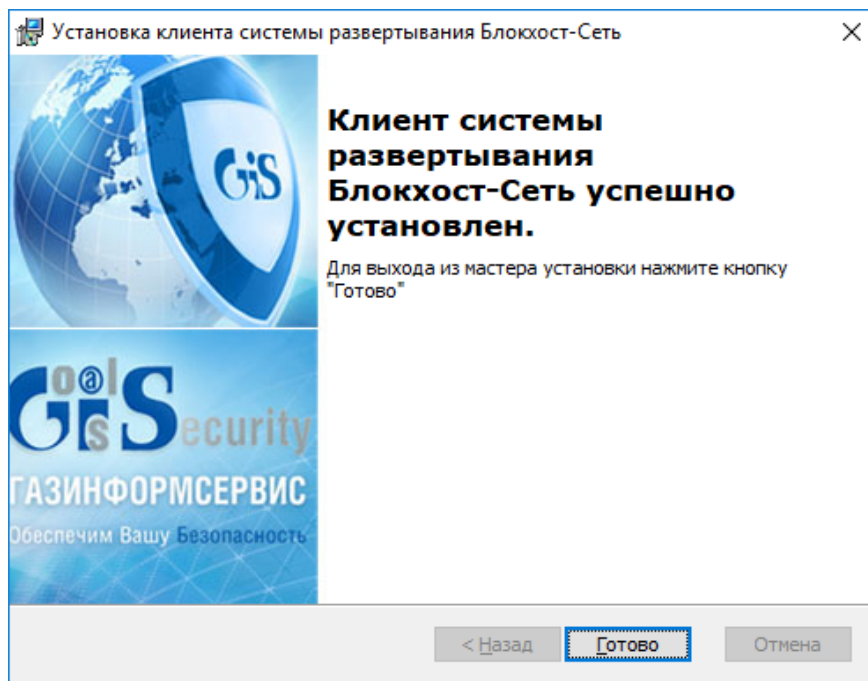


Рисунок 3.22 – Окно завершения установки агента развертывания

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

3.1.1.3 Установка с использованием групповых политик

Для установки агента развертывания с использованием групповых политик Active Directory необходимо выполнить следующие действия на контроллере домена (приведено описание настройки групповых политик для контроллера домена с ОС Windows Server 2012R2):

1) Поместить msi-файл установщика агента развертывания в папку с общим доступом (например, %WINDIR%\SYSVOL\domain\scripts).



К каталогу должен быть предоставлен доступ на **Чтение** и **Выполнение** для учетных записей рабочих станций.

Для этого необходимо выбрать пункт контекстного меню **Свойства (Properties)** для каталога с размещенным в нем файлом-установщика, в открывшемся окне свойств каталога перейти на вкладку **Безопасность (Security)** и добавить группу рабочих станций, на которые планируется осуществить установку клиента. Для добавленных учетных записей компьютеров (группы) установить значение **Чтение и выполнение (Read & Execute)**, нажать кнопку **ОК**.

2) Запустить консоль управления групповой политикой (**Group Policy Management**): **Пуск** → **Администрирование** → **Редактор групповой политики** (**Start** → **Administrative Tools** → **Group Policy Management**).

3) В открывшемся окне «**Управление групповой политикой**» (**Group Policy Management**) (рисунок 3.23) раскрыть дерево домена, выделить объект Active Directory Подразделение (Organizational Unit) или домен, щелкнуть на нем правой кнопкой мыши и выбрать пункт контекстного меню **Создать объект групповой политики в этом домене и связать его здесь же** (**Create a GPO in this domain, and Link it here**).

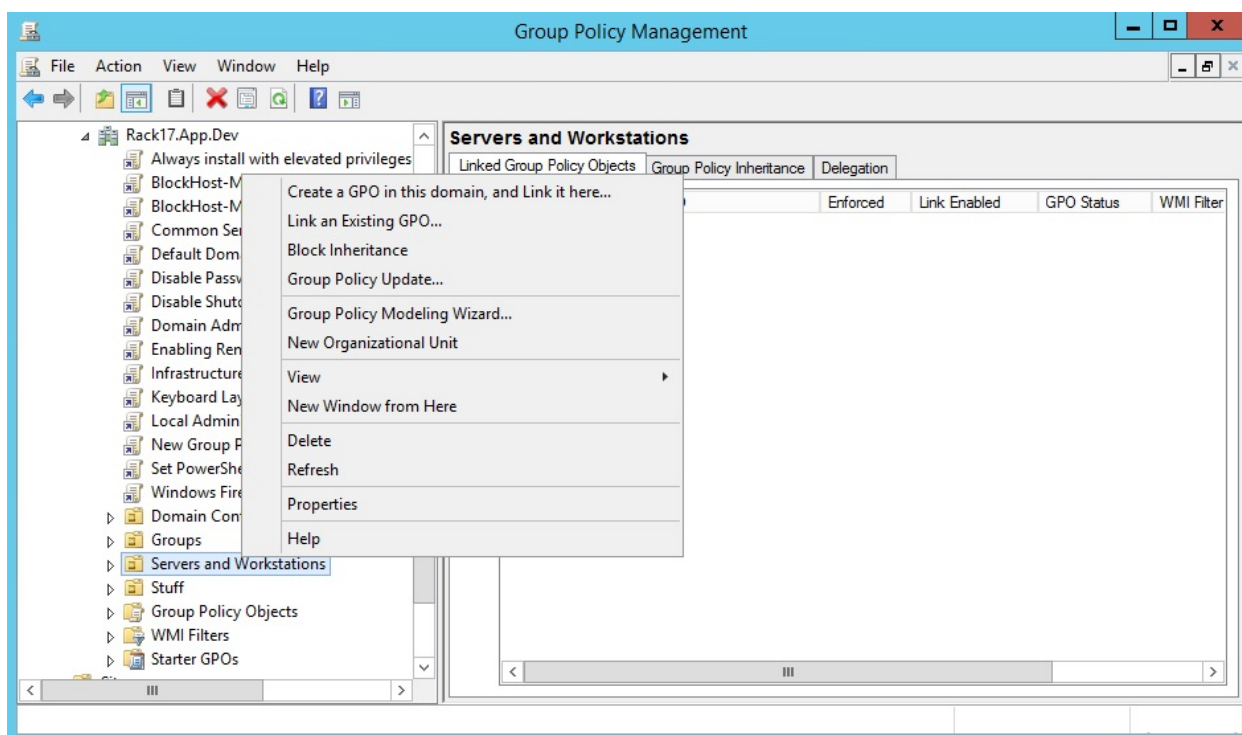


Рисунок 3.23 – Меню создания объекта групповой политики

4) Ввести описательное имя объекта групповой политики в поле **Имя** (Name) диалогового окна **Новый объект групповой политики** (New Group Policy Object) и нажать кнопку **ОК**:

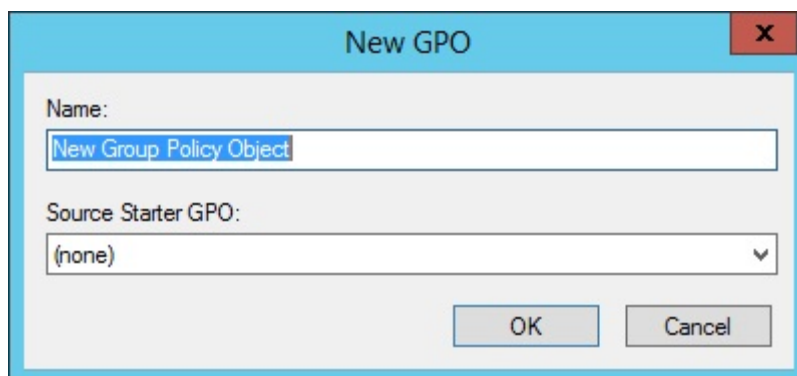


Рисунок 3.24 – Окно создания объекта групповой политики

5) Выделить созданный объект групповой политики (рисунок 3.25), щелкнуть на нем правой кнопкой мыши и выбрать пункт контекстного меню **Изменить (Edit)** для редактирования этого объекта.

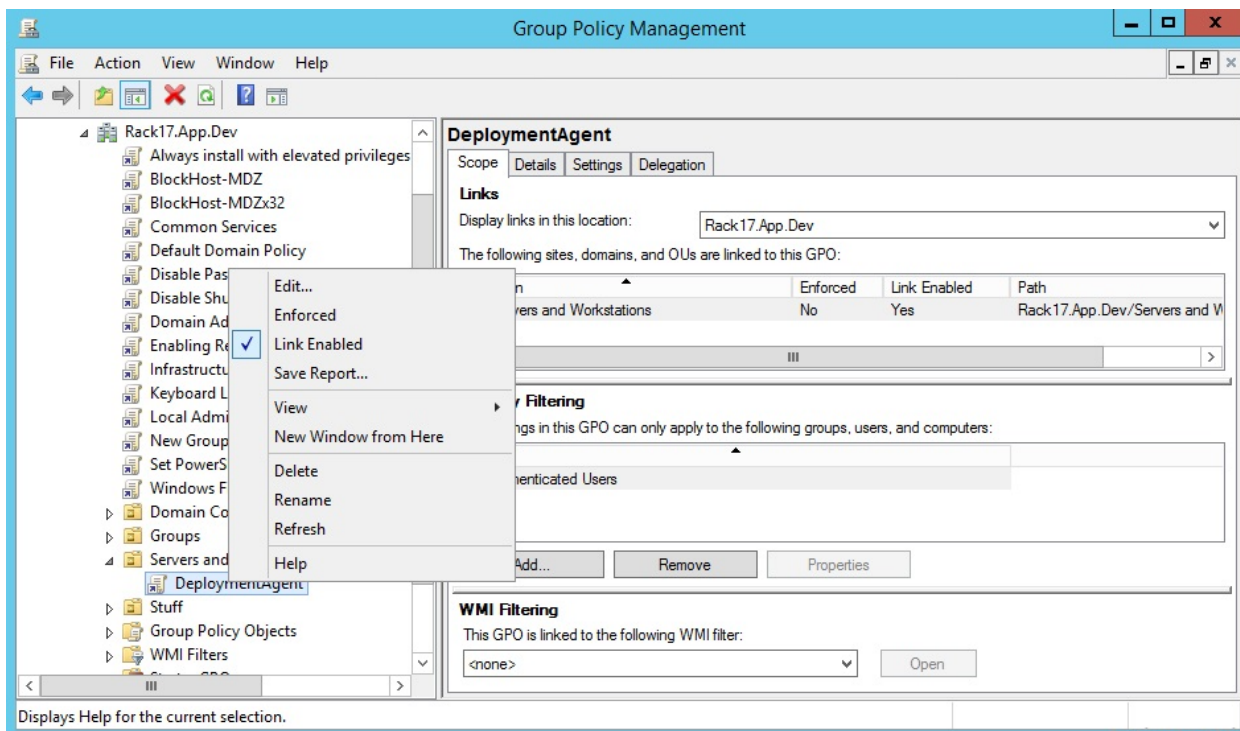


Рисунок 3.25 – Меню вызова редактора групповой политики

6) В окне **Редактор объектов групповой политики (Group Policy Management Editor)** (рисунок 3.26) перейти к пункту **Сценарии (Запуск/Завершение) (Scripts (Startup/Shutdown))**, раскрыв дерево **Конфигурация компьютера → Политики → Конфигурация Windows (Computer Configuration → Policies → Windows Settings)**. В открывшейся вкладке **Сценарии (Запуск/Завершение) (Scripts (Startup/Shutdown))** щелкнуть два раза левой кнопкой мыши на параметре **Автозагрузка (Startup)**.

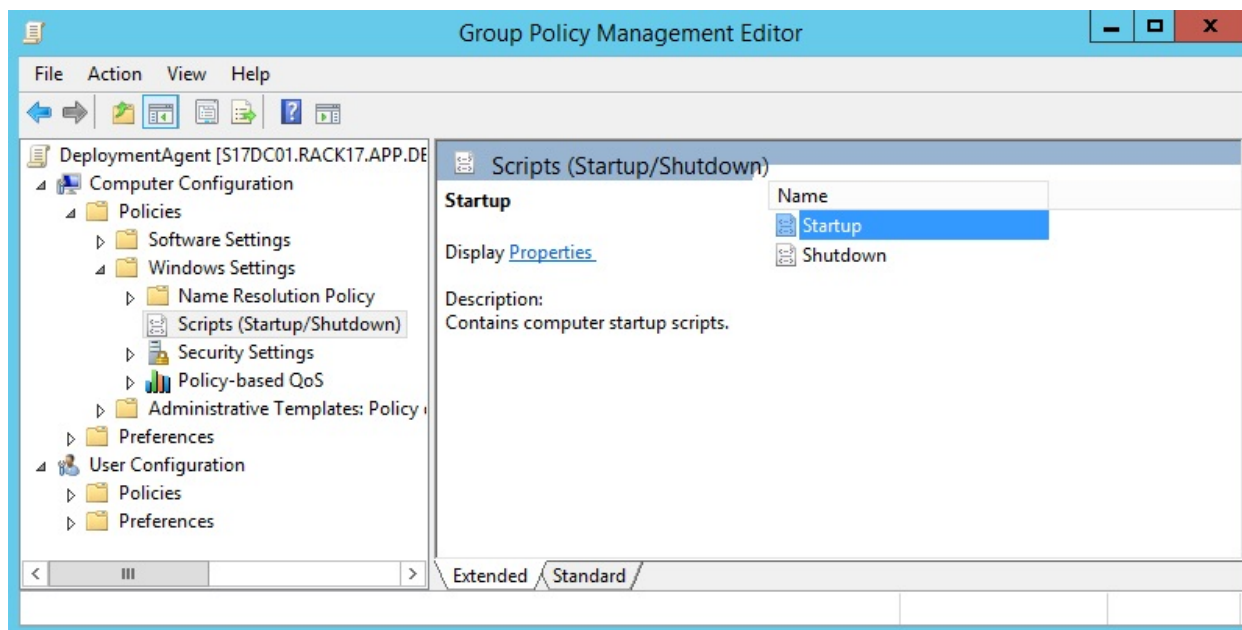


Рисунок 3.26 – Окно редактора групповой политики

- 7) В открывшемся окне **«Свойства: Автозагрузка» (Startup Properties)** (рисунок 3.27) нажать кнопку **Добавить (Add)**.

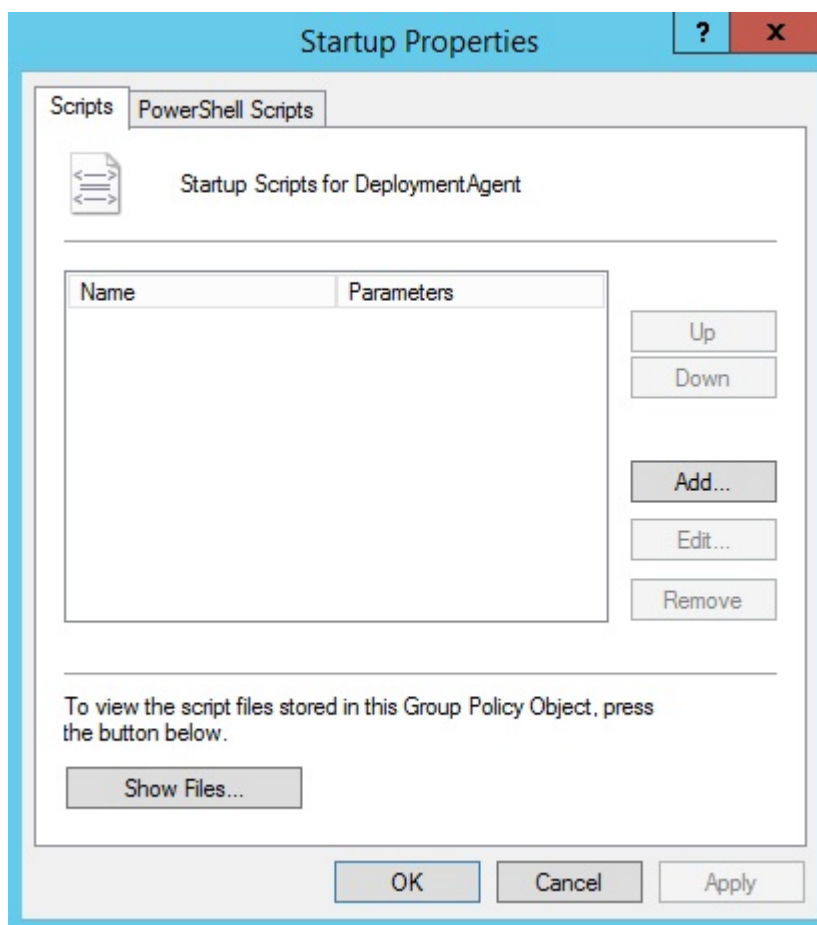


Рисунок 3.27 – Окно свойств сценария автозагрузки

8) В открывшемся окне **Добавление сценария (Add a script)** (рисунок 3.28):

- в поле **Имя сценария (Script Name)** необходимо указать путь к дистрибутиву агента развертывания. Путь можно ввести вручную или воспользовавшись кнопкой **Обзор (Browse)**, указать месторасположение файла-установщика с помощью стандартного окна Windows **Обзор (Browse)**;



Путь к файлу-установщику должен быть задан в формате UNC, например:
`\\server_name\share_name\BHNetDeploymentAgent.msi`.

- в поле **Параметры сценария (Script Parameters)** необходимо ввести ключ установки программного обеспечения (далее по тексту- ПО) в скрытом режиме (**/qn**) и параметры подключения агента развертывания к серверу СЗИ: **server_ip** – IP-адрес сервера СЗИ и **server_port** – номер TCP-порта сервера СЗИ, по которому осуществляется взаимодействие сервера и агентов развертывания (по умолчанию 25000), например:

`/qn server_ip=192.168.192.155 server_port=25000;`

- нажать кнопку **OK**.

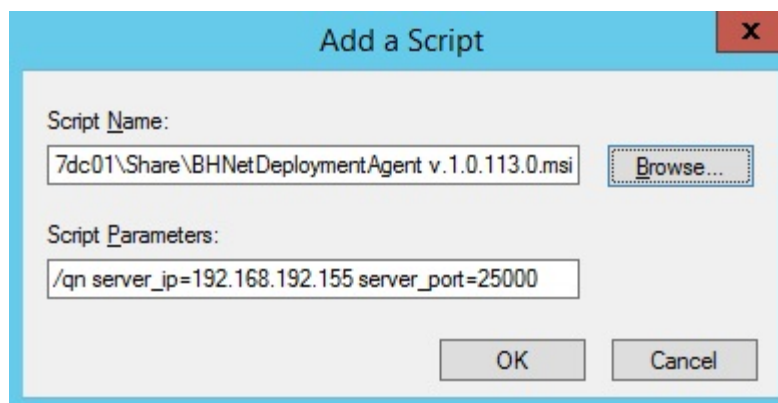


Рисунок 3.28 – Окно добавления сценария

- 9) Нажать кнопку **OK** в окне «**Свойства: Автозагрузка (Startup Properties)**» (рисунок 3.26).
- 10) Закрыть окно редактора объектов групповой политики (рисунок 3.26).
- 11) Закрыть консоль управления групповой политикой.



В дальнейшем, созданную групповую политику для установки агента развертывания можно применить и к другим организационным объектам Active Directory (*Подразделение/Organizational Unit*). Для этого следует выделить необходимый объект AD и выбрать пункт его контекстного меню **Связать существующий объект групповой политики/Link an existing GPO**. В открывшемся окне выбора групповой политики выделить имя необходимой политики и нажать **ОК**.

Также следует учитывать, что примененная к объекту AD политика наследуется всеми входящими в него подразделениями (доменами).

В результате выполнения созданных групповых политик, при входе пользователя на рабочую станцию начнется процесс установки агента развертывания с указанными в сценарии установки параметрами подключения к серверу СЗИ.

3.1.2 Удаление агента развертывания

Для удаления агента развертывания с рабочих станций администратору необходимо выполнить следующие действия:

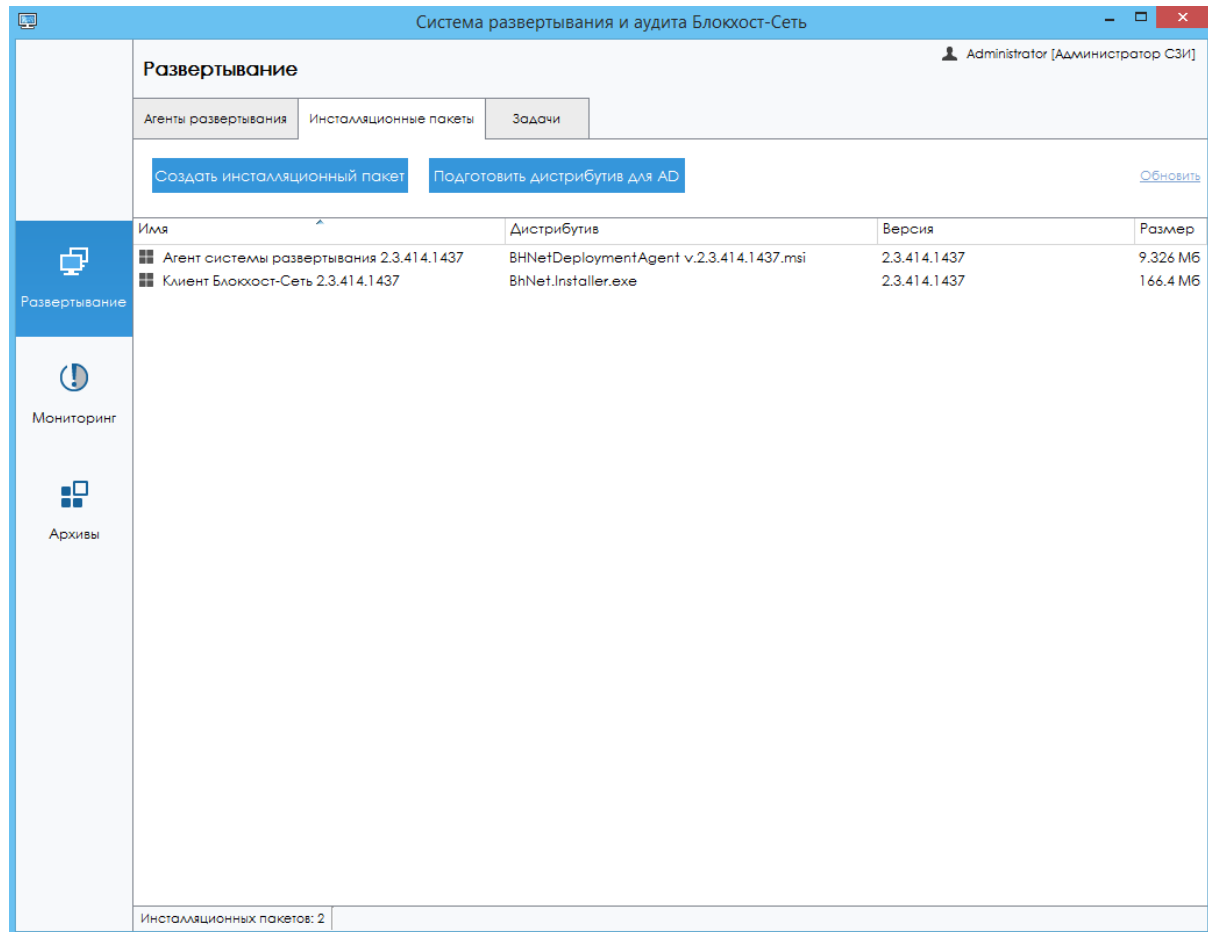
- запустить **Панель управления** и выполнить щелчок левой кнопки мыши на параметре **Программы и компоненты**;
- в списке установленных программ рабочей станции выбрать **VNNetDeploymentAgent** и нажать кнопку **Удалить**;
- в открывшемся окне подтвердить операцию удаления агента развертывания, нажав кнопку **Да**.

3.2 Вкладка «Инсталляционные пакеты»

Во вкладке **Инсталляционные пакеты** (рисунок 3.29) расположен список созданных в СРиА инсталляционных пакетов ПО. Также во вкладке имеются кнопки:

- **Создать инсталляционный пакет** – для запуска мастера по добавлению установщика в СРиА;
- **Подготовить дистрибутив для AD** – создание инсталляционных пакетов для установки клиента Блокхост-Сеть и клиента СРиА с использованием групповых политик.

Кнопка **Обновить**, расположенная в правой части вкладки, позволяет обновить список инсталляционных пакетов во вкладке.

Рисунок 3.29 – Вкладка **Инсталляционный пакеты**

При первом запуске консоли СРиА автоматически будут созданы два инсталляционных пакета: **Агент системы развертывания <номер_версии>** и **Клиент Блокхост-Сеть <номер_версии>**, содержащие, соответственно, файл-установщик агента развертывания и файл-установщик клиента Блокхост-Сети. Добавленные автоматически инсталляционные пакеты содержат в себе все необходимые параметры установки.

3.2.1 Создание инсталляционных пакетов

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



Файл-установщик программного обеспечения в обязательном порядке должен поддерживать возможность «тихой» (скрытой) установки – установку программного обеспечения в интерактивном режиме СРиА не поддерживает.

Для создания инсталляционного пакета администратору безопасности необходимо

выполнить следующие действия в консоли СРиА:

- 1) Перейти в раздел **Развертывание** во вкладку **Инсталляционные пакеты** и нажать кнопку **Создать инсталляционный пакет** (см. пример на рис 3.29).
- 2) В открывшемся окне мастера по созданию инсталляционных пакетов нажать кнопку **Выбрать**:

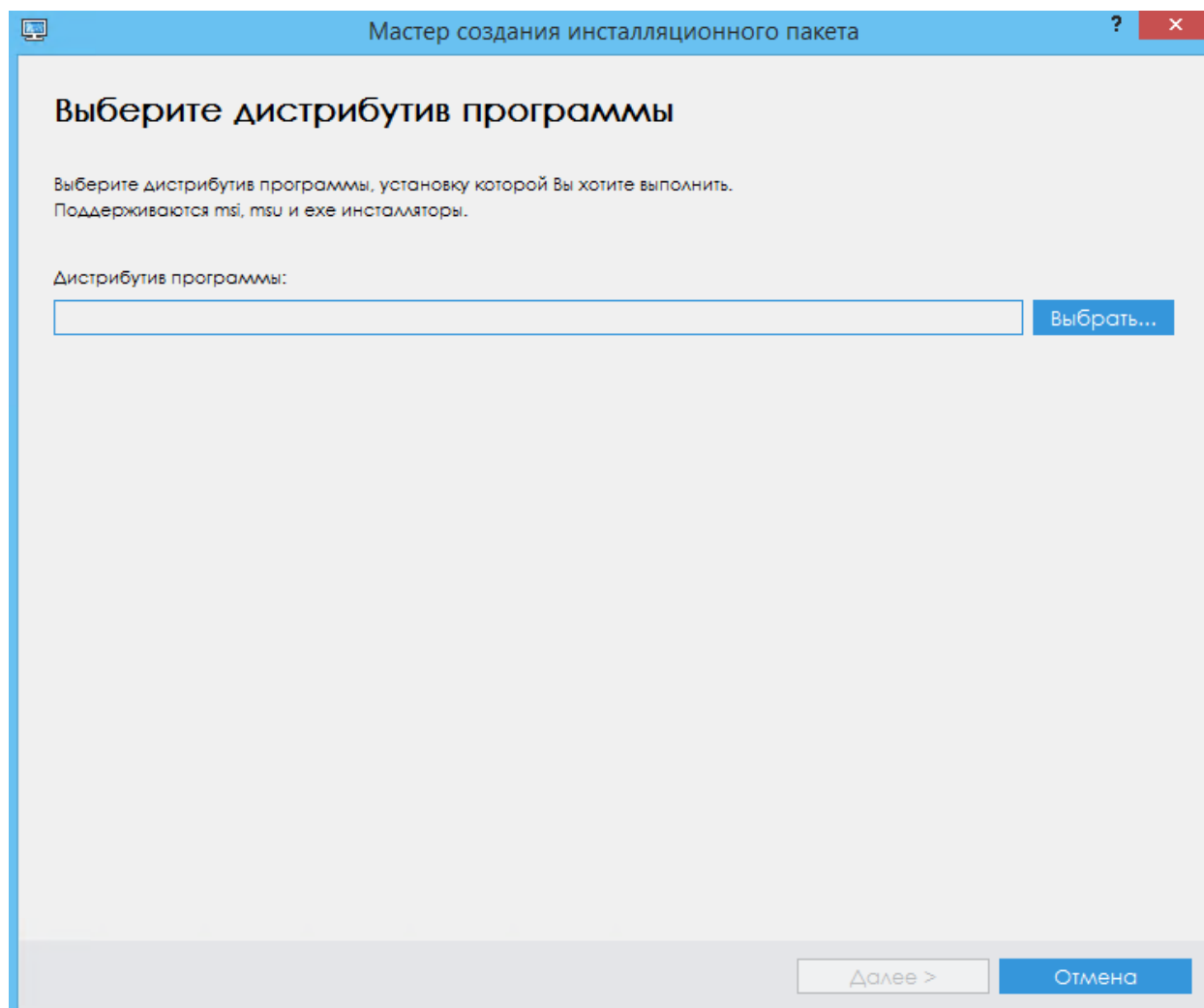


Рисунок 3.30 – Окно мастера по созданию инсталляционного пакета

- 3) В открывшемся окне выбора файла дистрибутива программного обеспечения выбрать необходимый файл-установщик (с расширением *.msi, *.msu или *.exe) и нажать кнопку **Открыть** (рисунок 3.31).

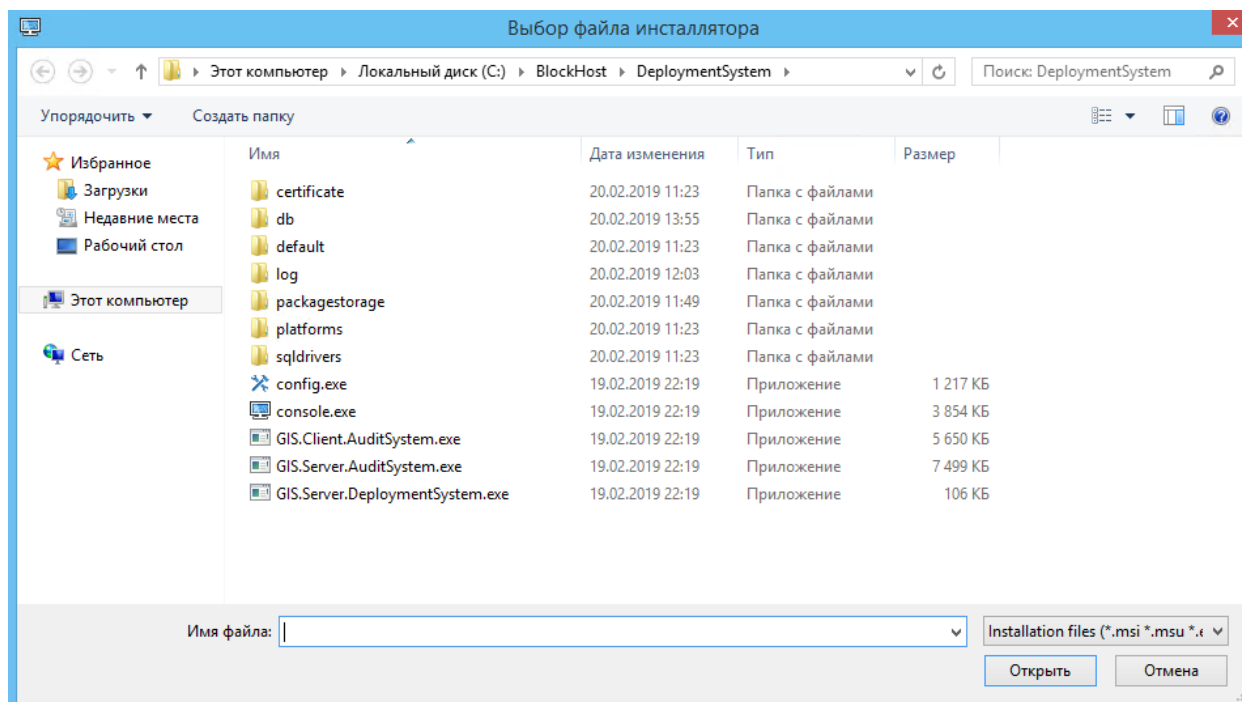


Рисунок 3.31 – Выбор файла дистрибутива устанавливаемого ПО

- 4) При необходимости, в окне мастера по созданию инсталляционного пакета ввести в открывшееся поле ввода параметры командной строки (рисунок 3.32).



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

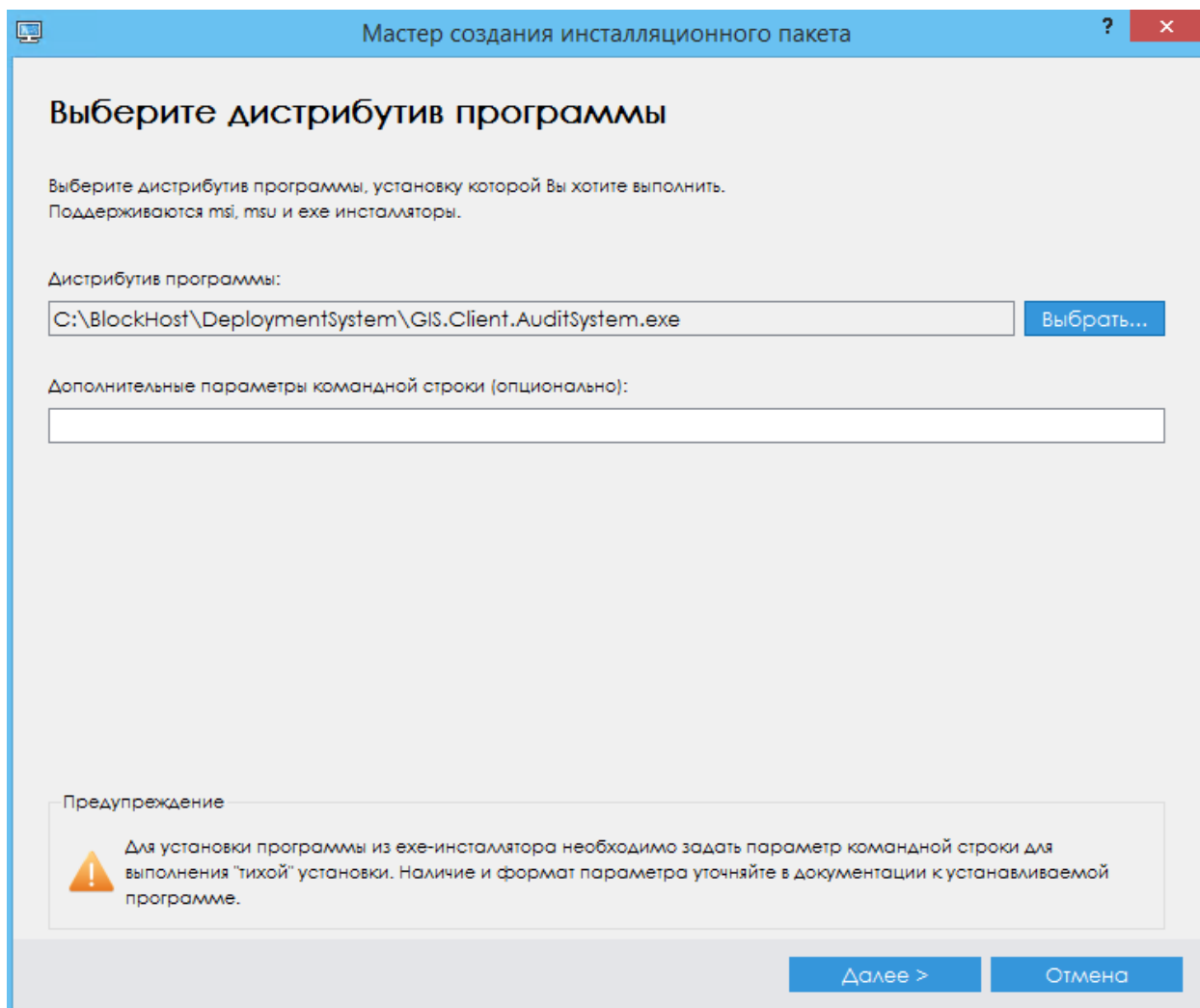


Рисунок 3.32 – Ввод дополнительных параметров установки ПО

- 5) На следующем шаге мастера по созданию инсталляционного пакета необходимо ввести имя создаваемого пакета и нажать кнопку **Создать**:

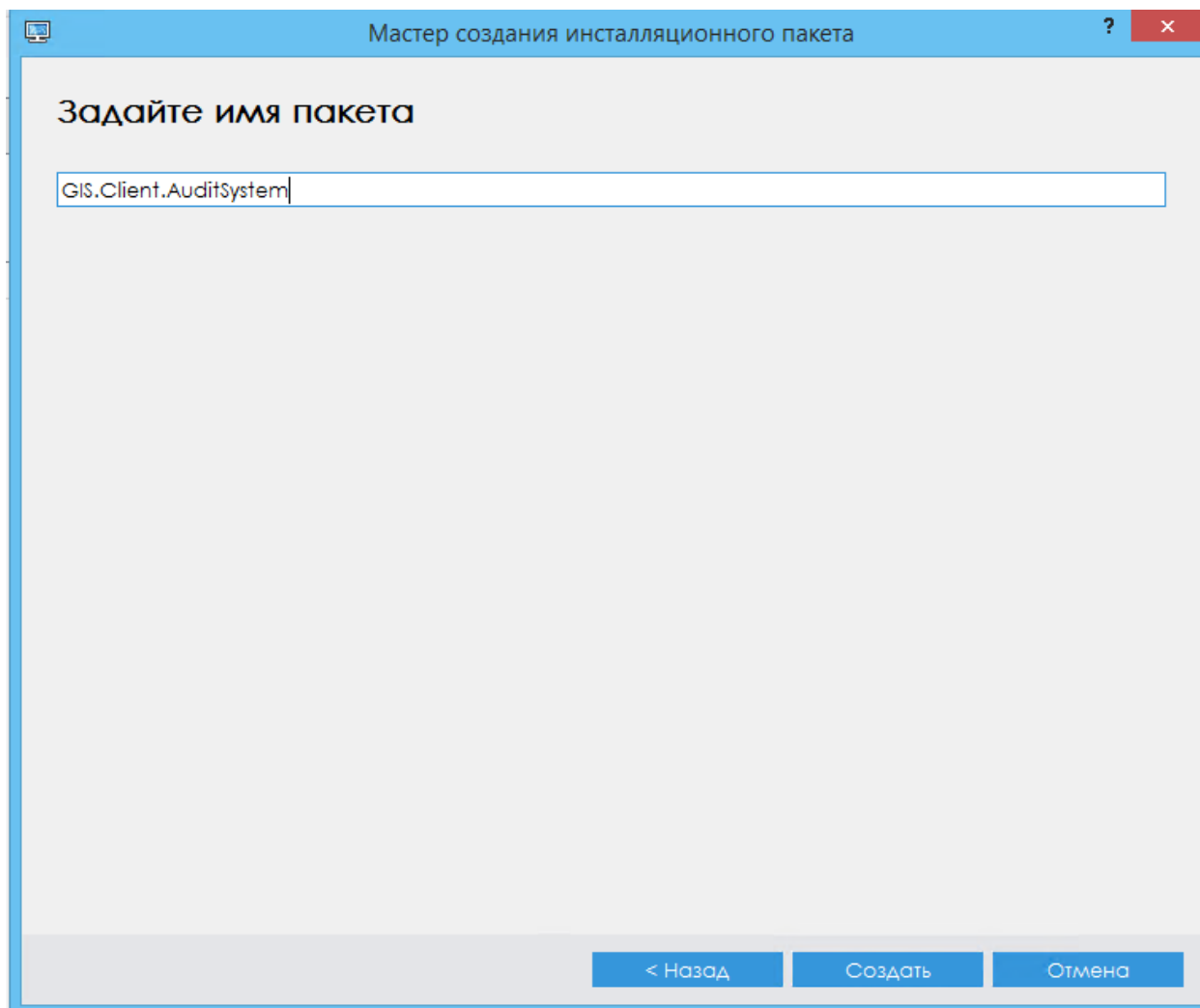


Рисунок 3.33 – Ввод имени создаваемого инсталляционного пакета

- 6) В окне завершения работы мастера по созданию инсталляционного пакета (рисунок 3.34) нажать кнопку **Заккрыть**.

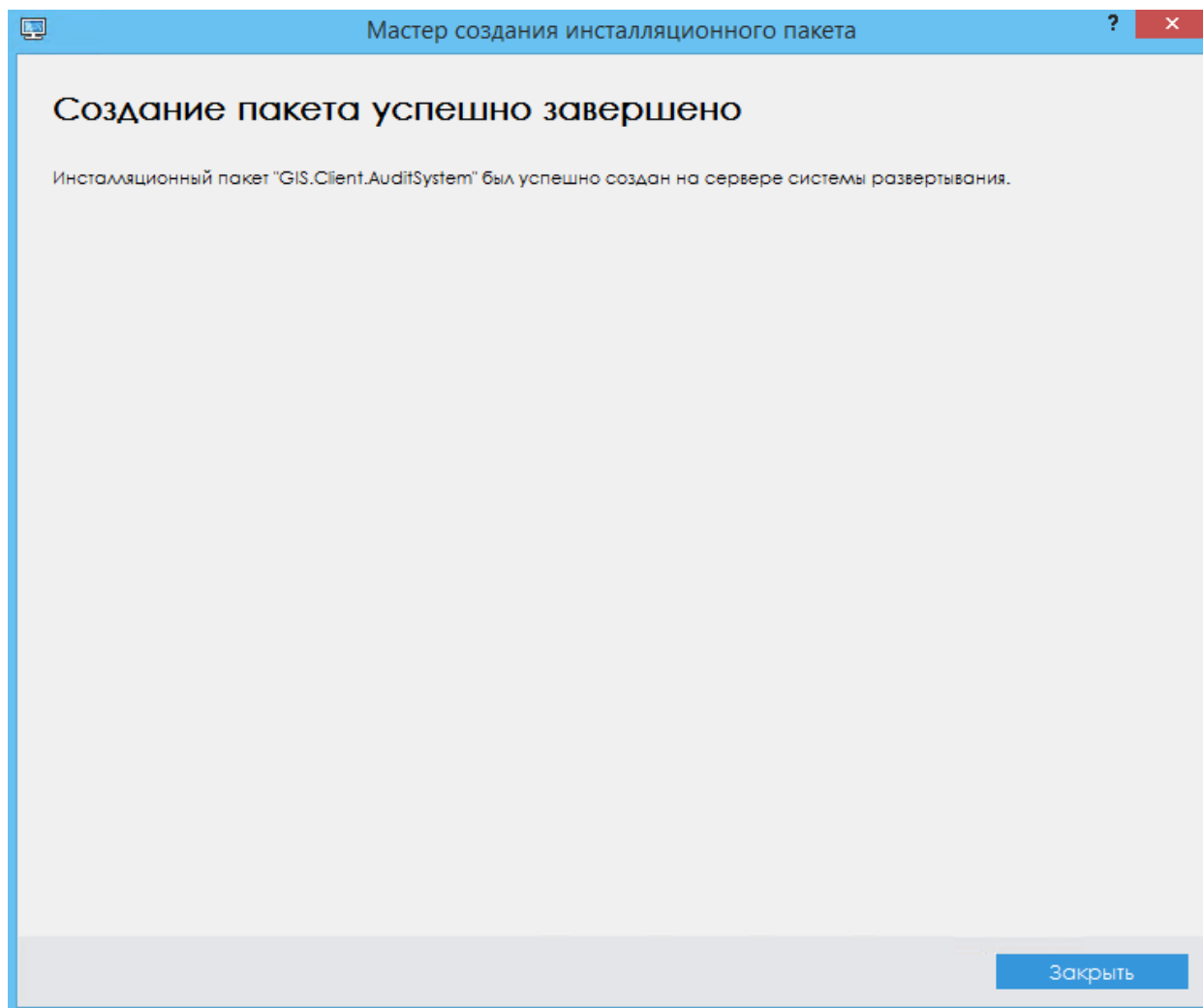


Рисунок 3.34 – Окно завершения работы мастера по созданию инсталляционного пакета

В результате работы мастера по созданию инсталляционного пакета в каталоге размещения инсталляционных пакетов в СРиА (*C:\BlockHost\DeploymentSystem\packagestorage*) будет создан каталог, в который будет скопирован выбранный в пункте 3 файл-установщик ПО.



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

3.2.2 Подготовка дистрибутива для AD



Функционал формирования дистрибутивов для развертывания через AD доступен только для инсталляционных пакетов, содержащих файлы-установщики агента развертывания и клиента Блокхост-Сеть.

При подготовке файла-установщика для развертывания средствами AD администратору

безопасности необходимо выполнить следующие действия:

- 1) Перейти в раздел **Развертывание** во вкладку **Инсталляционные пакеты**, выбрать из списка необходимый для настройки пакет и нажать кнопку **Подготовить дистрибутив для AD** (рисунок 3.29).
- 2) В открывшемся окне нажать кнопку **Выбрать** и указать каталог, в который будет сохранен подготовленный инсталляционный пакет (рисунок 3.35).

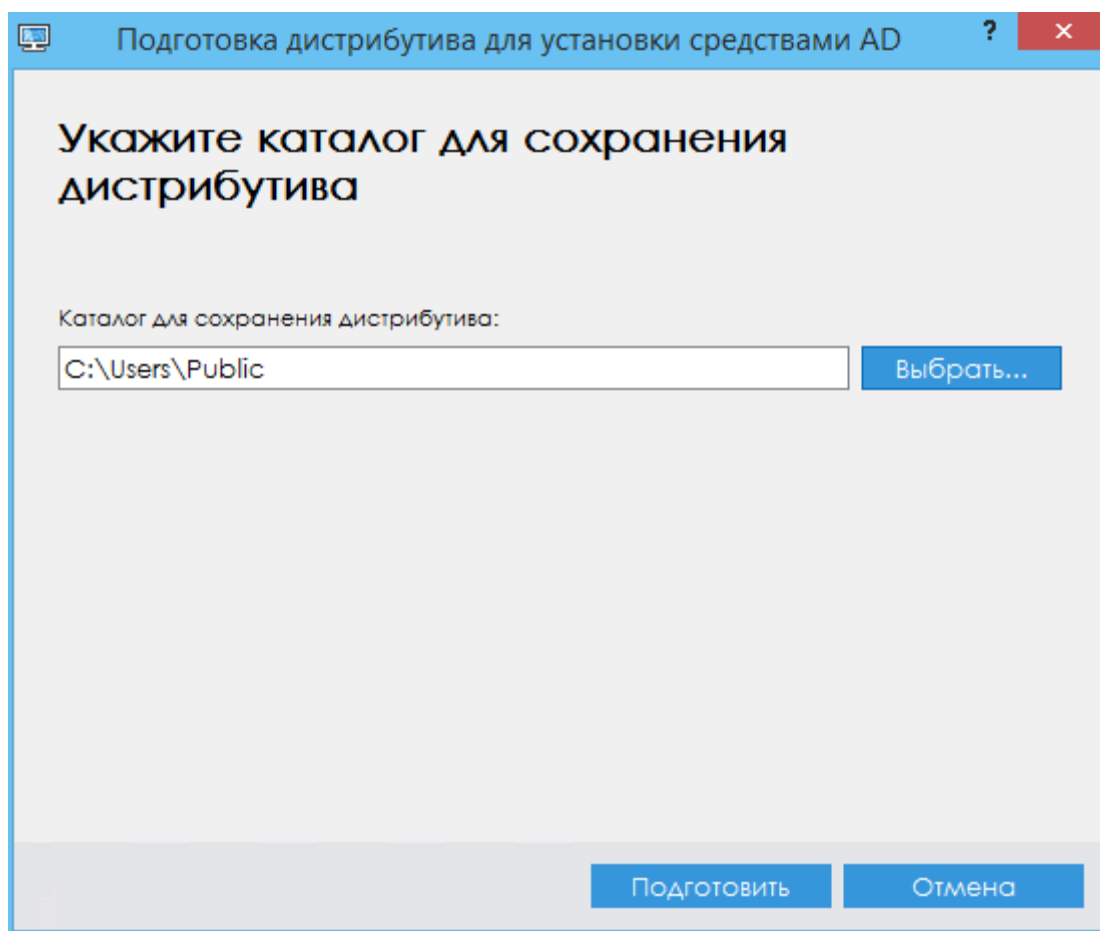


Рисунок 3.35 – Окно мастера подготовки дистрибутива для установки средствами AD

- 3) Подтвердить выполнение операции, нажав кнопку **Подготовить** (рисунок 3.35).
- 4) В окне завершения подготовки инсталляционного пакета (рисунок 3.36) нажать кнопку **Завершить**.

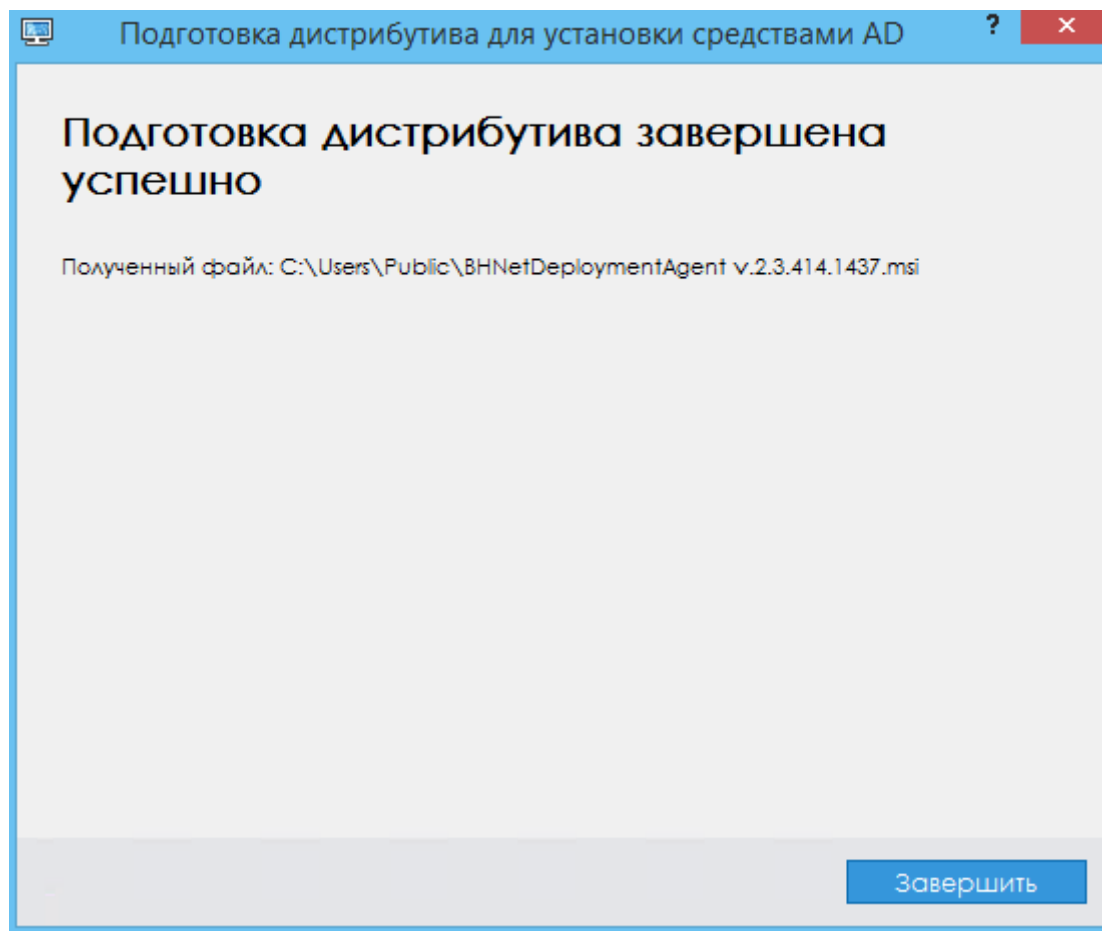


Рисунок 3.36 – Окно завершения подготовки инсталляционного пакета

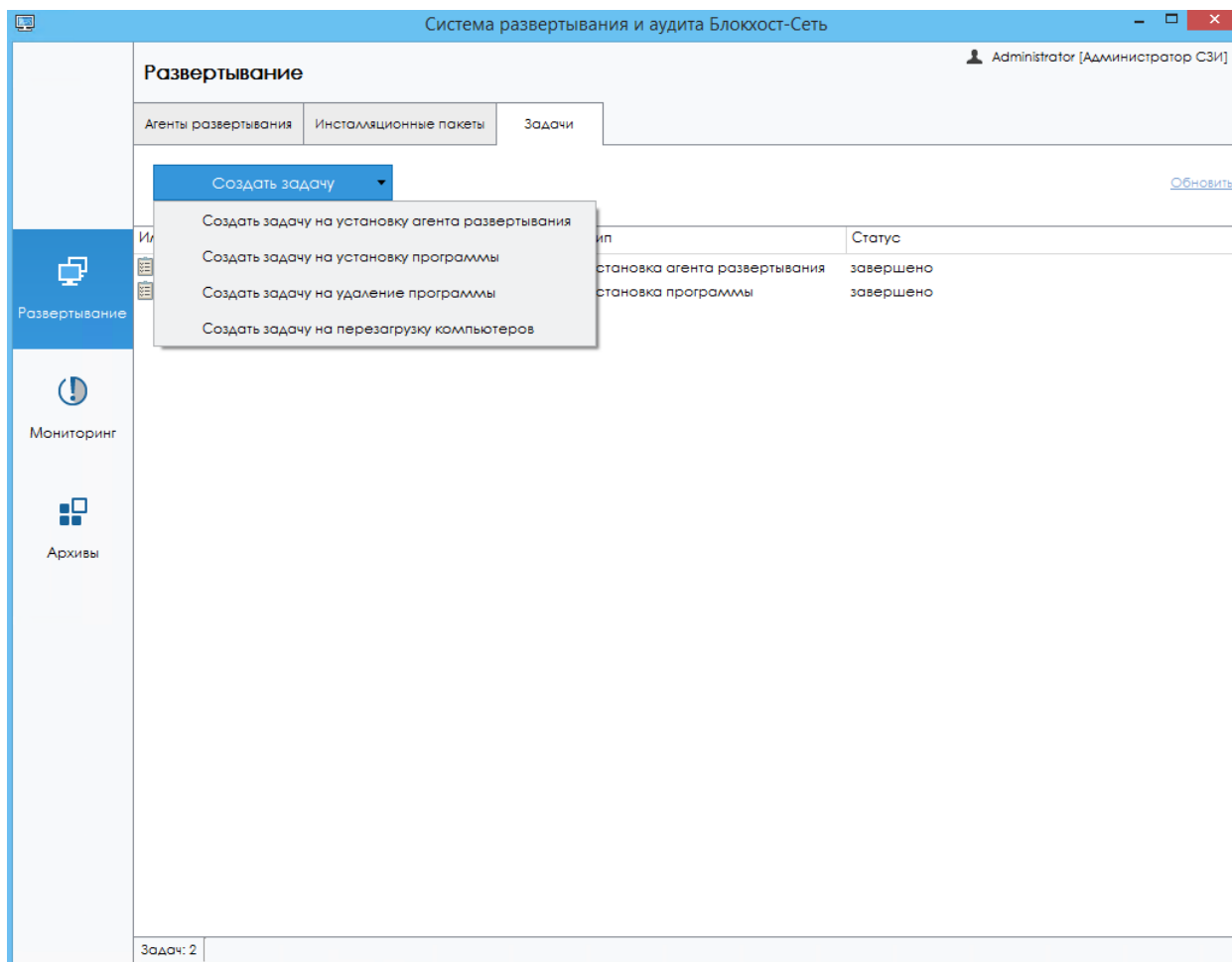
В результате работы мастера в указанном каталоге будет создан подготовленный дистрибутив для установки средствами AD.

3.3 Вкладка «Задачи»

Во вкладке **Задачи** (рисунок 3.37) расположен список созданных в СРиА задач по установке ПО. Также во вкладке имеются кнопка **Создать задачу**, нажатие на которую открывает список возможных действий:

- **Создать задачу на установку агента развертывания** – создание задачи для установки агента развертывания;
- **Создать задачу на установку программы** – создание задачи на установку ПО на рабочие станции сети;
- **Создать задачу на удаление программы** – создание задачи на удаление ПО с рабочих станций сети;
- **Создать задачу на перезагрузку компьютеров** – создание задачи на перезагрузку рабочих станций сети.

Кнопка **Обновить**, расположенная в правой части вкладки, позволяет обновить список задач во вкладке.

Рисунок 3.37 – Вкладка **Задачи**

При первом запуске консоли СРиА будут автоматически созданы две задачи: **Установка агента системы развертывания <номер_версии>** и **Установка клиента Блокхост-Сеть <номер_версии>**, для установки на рабочие станции, соответственно, агента развертывания и клиента Блокхост-Сеть.

Во вкладке **Задачи** отображаются основные сведения о задаче и информация о ходе ее выполнения. При выделении задачи в списке, в правой части вкладки отобразится подробная информация о выбранной задаче (рисунок 3.38):

- **Тип задачи:** установка агента развертывания, установка программы, удаление программы, перезагрузка компьютера;
- **Статус:** ожидает выполнения, выполняется, останавливается, завершено;
- **Планировщик:** Ручной, Сразу после создания, По времени, Периодически, По завершению задания;
- **Результат выполнения задачи:** Требуется перезагрузка; Выполняется; Успешно завершено; Завершено с предупреждением; Завершено с ошибкой;

Недоступны; Ожидает выполнения. Результатов выполнения задачи может быть несколько – отображение возможных результатов зависит от количества рабочих станций в задаче. Каждый результат является ссылкой, переход по которой открывает окно просмотра операций, выполненных в ходе выполнения задачи (рисунок 3.40).

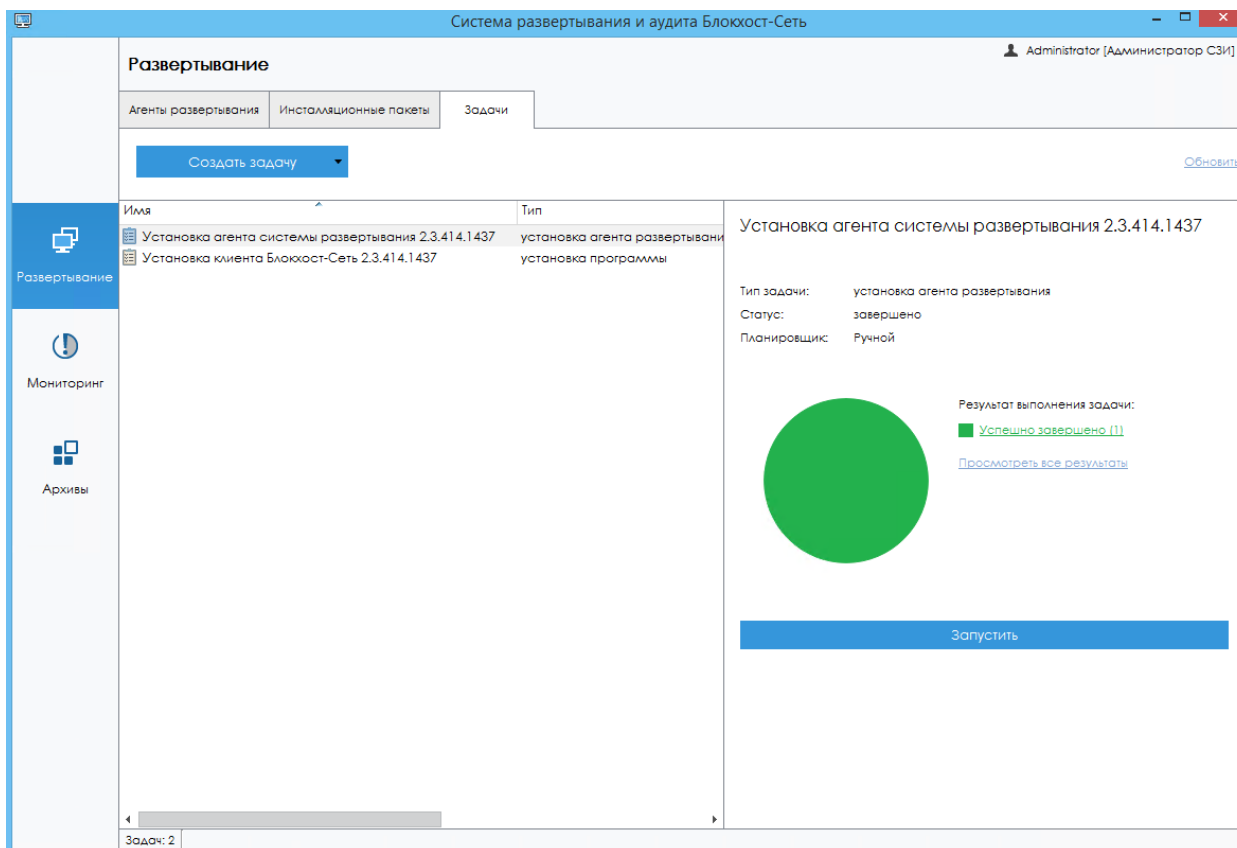


Рисунок 3.38 – Отображение дополнительных сведений о задаче и ходе ее выполнения

Статус рабочей станции в задаче зависит от вариантов событий, описанных в таблице 3.2.

Таблица 3.2 – Статусы, в которых могут находиться рабочие станции

Статус рабочей станции в задаче	Событие, в результате которого рабочая станция переходит в данный статус
Завершено с ошибкой	• выполнение задачи любого типа на рабочей станции завершилось ошибкой; • при установке клиента Блокост-Сеть было обнаружено, что на рабочей станции не выполняются требования для установки (см. подраздел 1.2 «Требования к составу установленного ПО» документа «Средство защиты информации от несанкционированного доступа «Блокост-Сеть 3». Руководство по инсталляции (вариант с удаленным управлением)»); • выполнение задачи было остановлено администратором (нажата кнопка Остановить, рисунок 3.63), когда процесс установки программы на рабочей станции уже был запущен.
Недоступны	• не удалось установить связь с клиентом СРиА целевой рабочей станции, чтобы начать выполнение задачи.
Завершено с	• в параметрах перезагрузки задачи выбран параметр «не перезагружать»

предупреждением	компьютер»; после завершения инсталляции/деинсталляции программное обеспечение затребовало перезагрузку; • выполнение задачи было остановлено администратором безопасности (нажата кнопка Остановить, рисунок 3.63) на этапе, когда задача для рабочей станции была завершена со статусом Требуется перезагрузка (установка программы на рабочей станции была успешно завершена, однако, в соответствии с настройками задачи, пользователь, работающий за рабочей станции, должен выполнить перезагрузку, см. пункт «3.3.7 Остановка задачи»); • 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	• параметр перезагрузки рабочей станции при создании задачи на установку (удаление) ПО рабочей станции выбран 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 администратором (была нажата кнопка Остановить, рисунок 3.63) на этапе копирования инсталляционного файла на рабочую станцию (см. пункт «3.3.7 Остановка задачи»).
Останавливается	• была нажата кнопка Остановить (рисунок 3.63); идет процесс остановки задачи.

Для отслеживания состояния задачи в ходе ее выполнения на рабочей станции, необходимо левой кнопкой мыши нажать на одну из имеющихся ссылок *<статус задачи>*, либо на ссылку **Просмотреть все результаты** (рисунок 3.38).

В верхней части открывшегося окна просмотра результатов (рисунок 3.39), выделить интересующую рабочую станцию, после чего в нижней части окна отобразится список операций, выполненных на этой рабочей станции в ходе выполнения задачи. Для обновления списка операций, следует нажать кнопку **Обновить**.

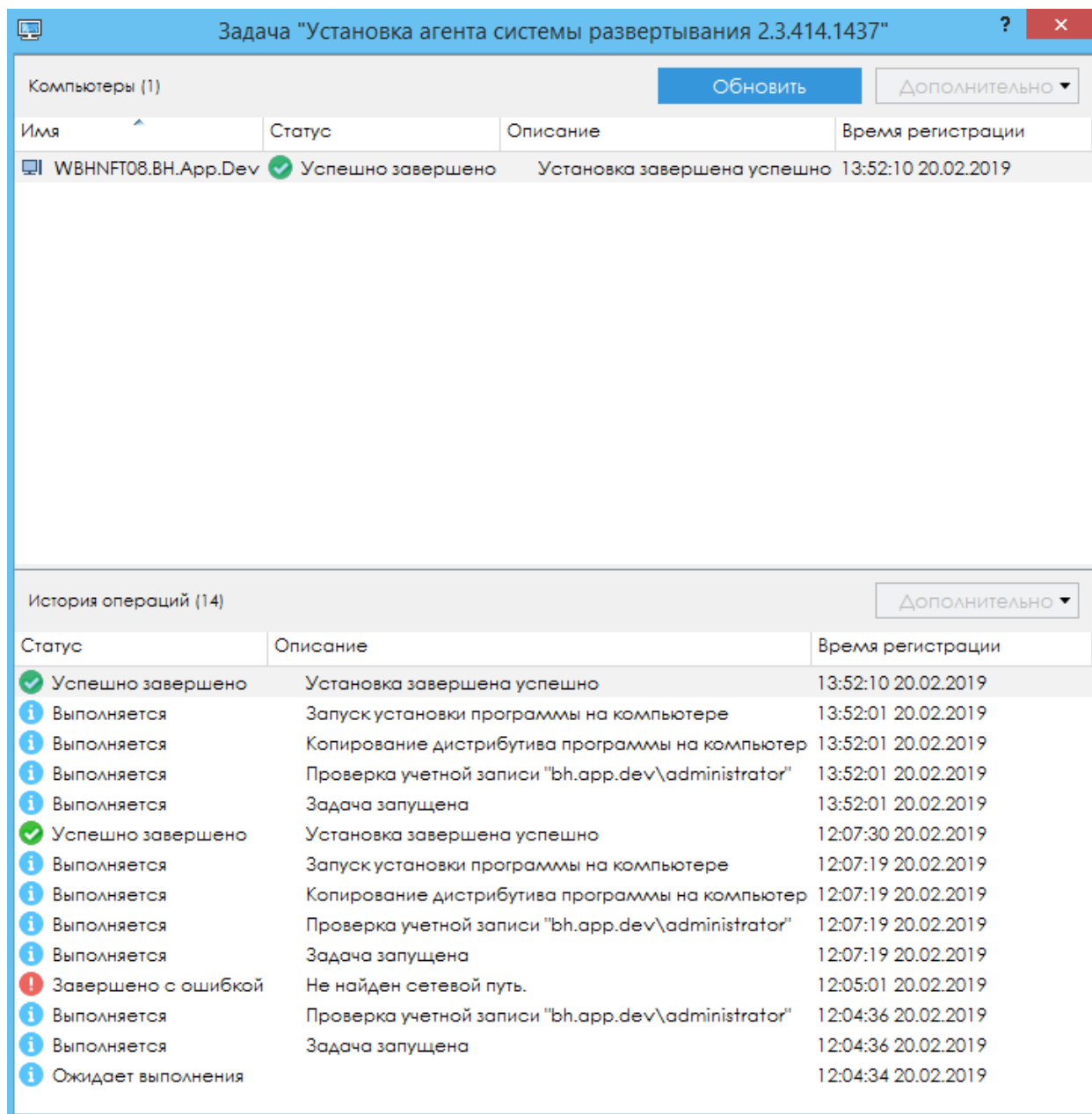


Рисунок 3.39 – Результаты выполнения задачи



Выполнение задач возможно только на компьютерах с установленным агентом развертывания. Подробнее об установке агента развертывания см. пункт 3.1.1 «Установка агента развертывания» данного документа.

3.3.1 Создание задачи на установку ПО

Для создания задачи на установку ПО на рабочие станции администратору безопасности необходимо выполнить следующие действия в консоли СРиА:

- 1) Перейти в раздел **Развертывание** на вкладку **Задачи** и нажав кнопку **Создать задачу** выбрать пункт **Создать задачу на установку программы** (см. пример на рисунке 3.37).

2) В открывшемся окне мастера создания задачи на установку программы (рисунок 3.40) выделить инсталляционный пакет из списка имеющихся в базе данных системы развертывания и нажать кнопку **Далее**.

На этом шаге мастера также существует возможность создания нового инсталляционного пакета. Для этого необходимо нажать кнопку **Создать новый**, после чего последовательно пройти все шаги стандартного мастера создания нового инсталляционного пакета (см. пункт 3.2.1 «Создание инсталляционных пакетов»). По завершению создания нового пакета будет произведен возврат к окну мастера создания задачи, в котором созданный инсталляционный пакет будет доступен для выбора.

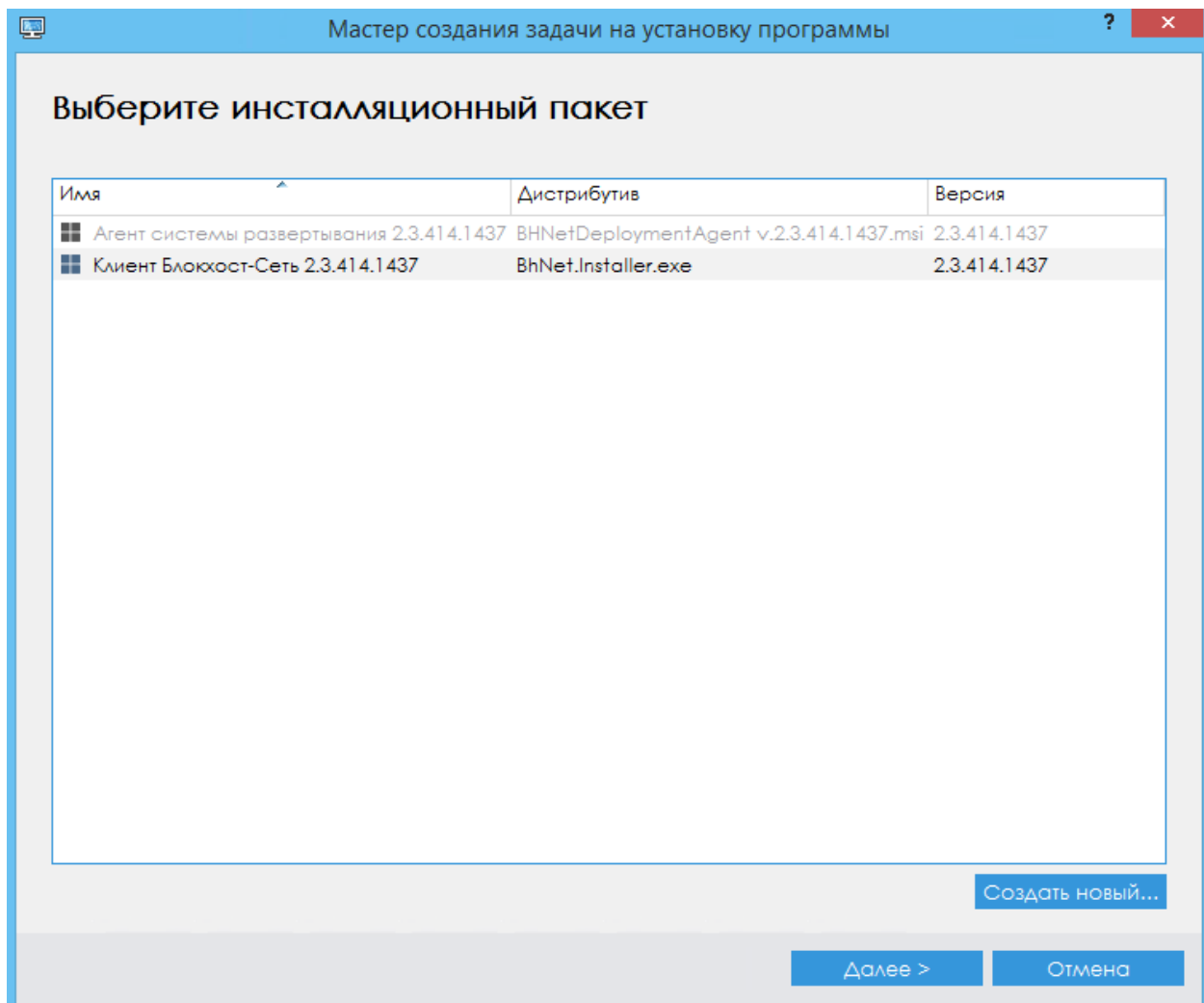


Рисунок 3.40 – Выбор инсталляционного пакета

3) На следующем шаге мастера (рисунок 3.41) необходимо отметить в списке те рабочие станции, на которые необходимо выполнить установку ПО, и нажать кнопку **Далее** (см. пункт 3.3.2 «Добавление в задачу нескольких рабочих станций»).

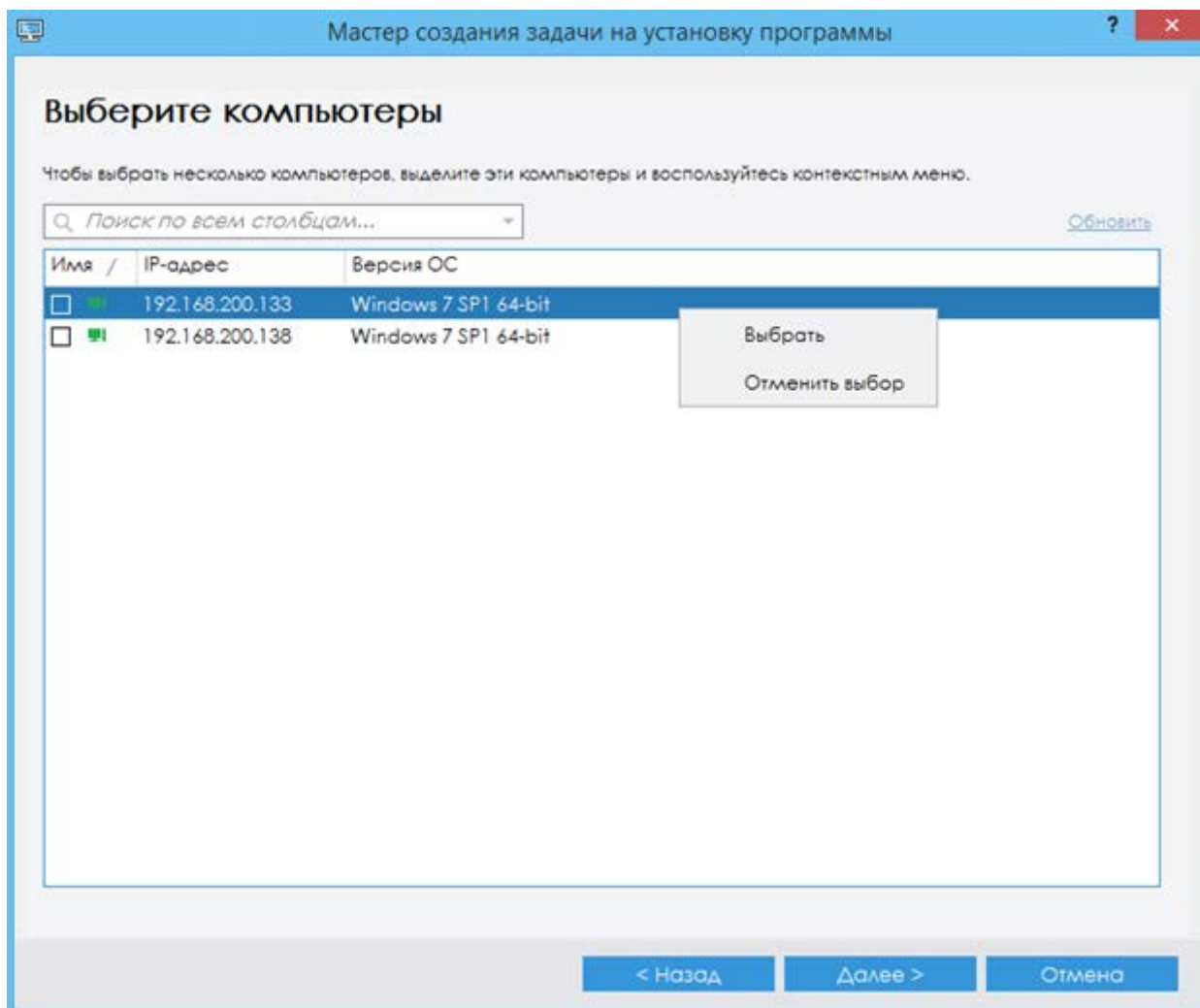


Рисунок 3.41 – Определение списка рабочих станций для установки программы

4) На следующем шаге мастера создания задачи на установку программы (рисунок 3.42) задать параметры планировщика запуска задачи (подробнее см. п.7 подпункта 3.1.1.1 «Установка из консоли СРиА») и определить интервалы времени выполнения задачи. Для продолжения нажать кнопку **Далее**.

Мастер создания задачи на установку программы

Задайте параметры планировщика и интервалы выполнения задачи

Параметры планировщика задач

Тип запуска задачи: Вручную

Временные интервалы выполнения задачи

Прервать установку программы на компьютере, если инсталлятор не активен дольше (мин.): 40

☐ Остановить, если задача выполняется дольше (часы): 2

< Назад Далее > Отмена

Рисунок 3.42 – Определение параметров планировщика и интервалов выполнения задачи

5) В открывшемся окне мастера создания задачи на установку программы (рисунок 3.43) указать параметры перезагрузки рабочей станции после установки на нее программного обеспечения (см. пункт 3.3.3 «Параметры перезагрузки рабочих станций»).

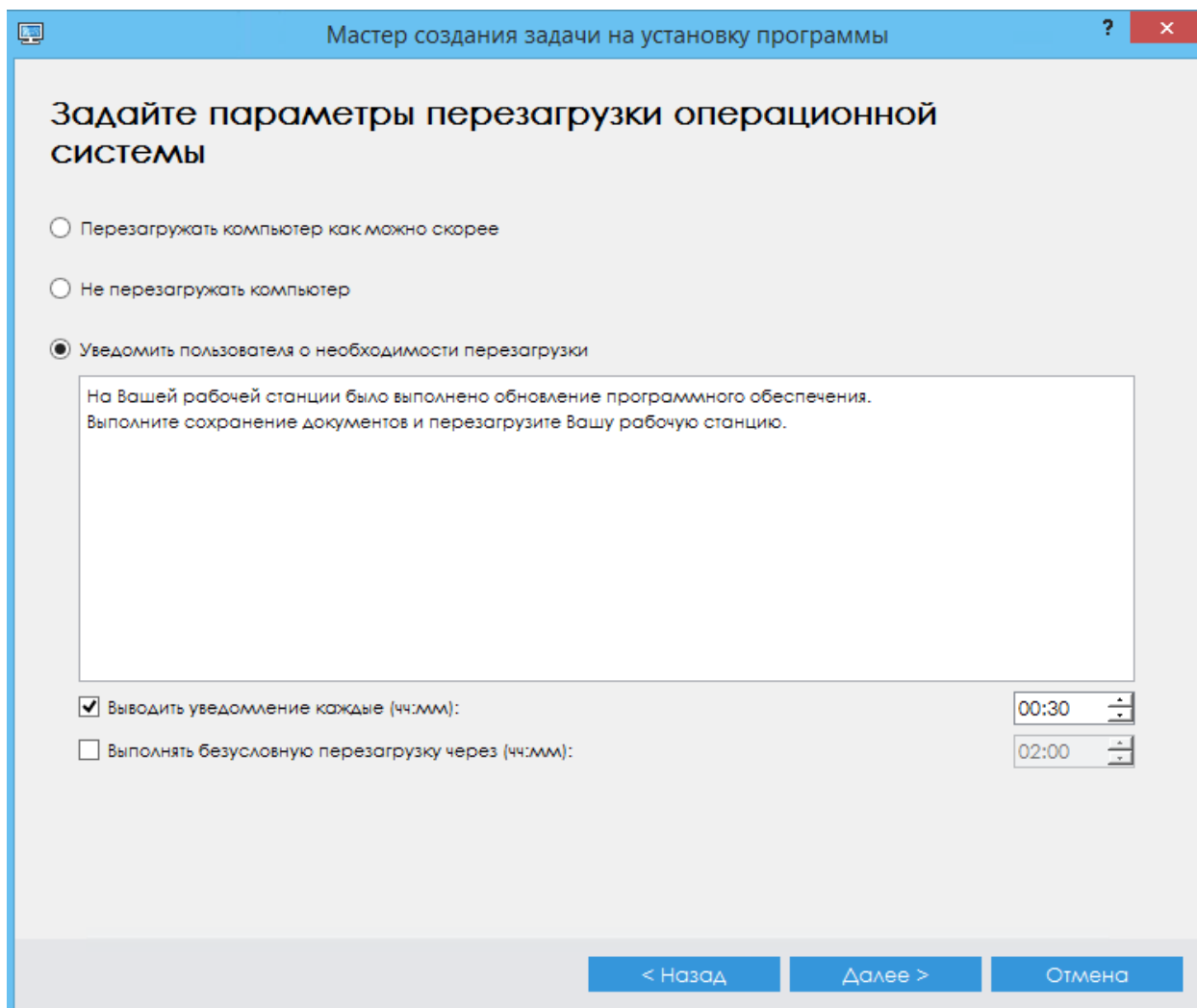


Рисунок 3.43 – Определение параметров перезагрузки ОС

6) На следующем шаге мастера создания задачи на установку программы необходимо ввести имя создаваемой задачи и нажать кнопку **Создать** (рисунок 3.44).

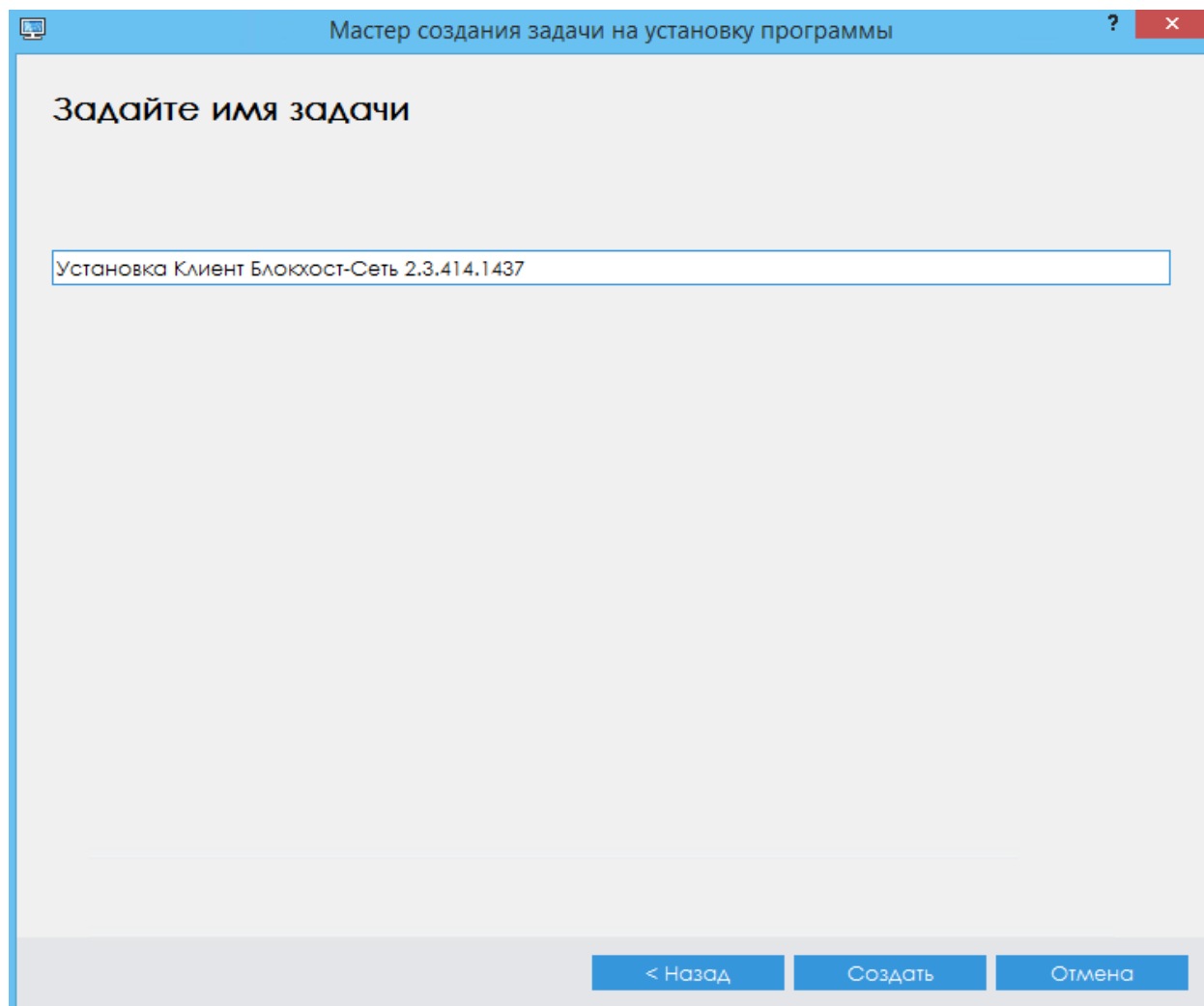


Рисунок 3.44 – Ввод имени создаваемой задачи

- 7) В окне завершения работы мастера создания задачи на установку программы (рисунок 3.45) нажать кнопку **Заккрыть**.

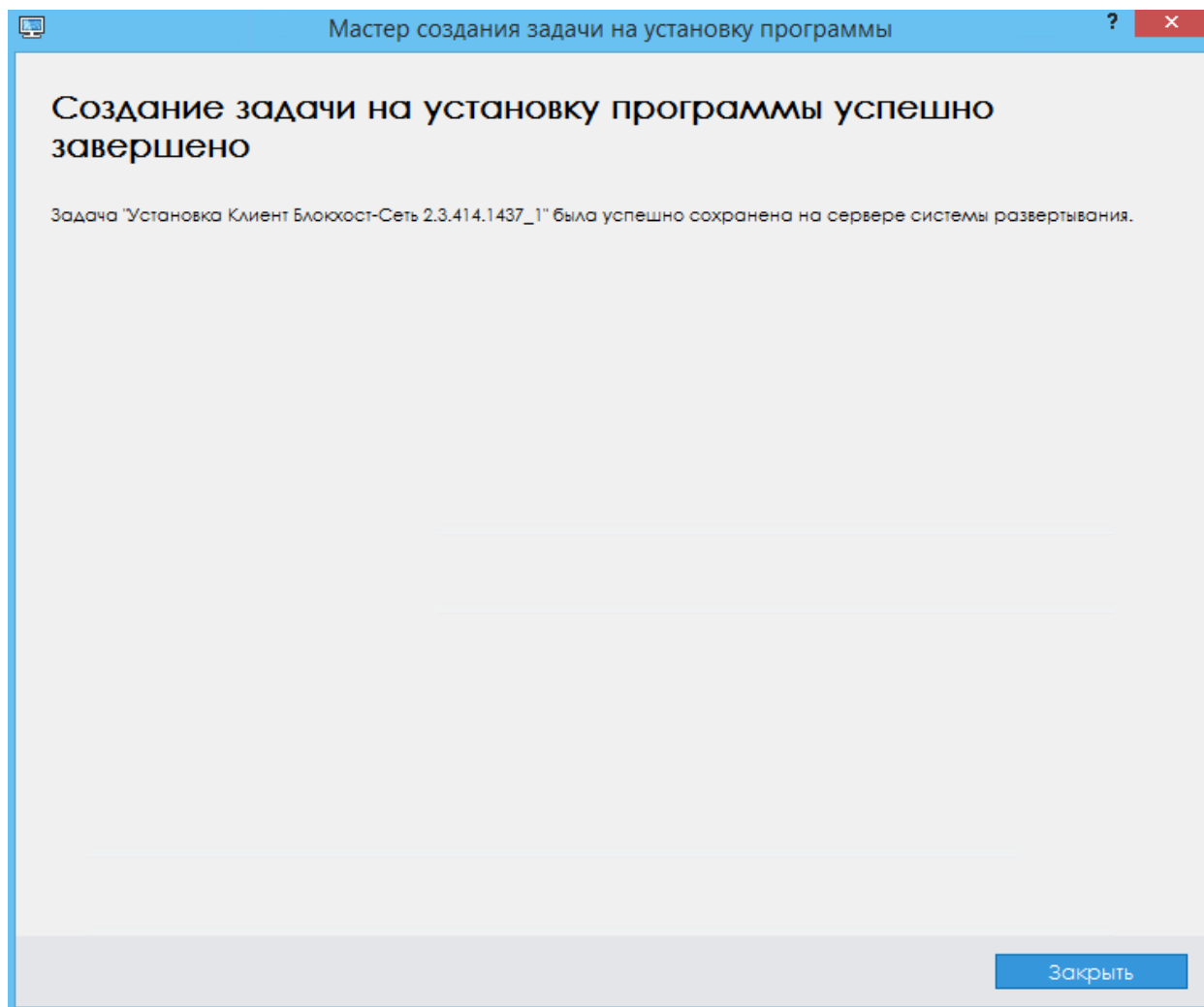


Рисунок 3.45 – Окно завершения работы мастера создания задачи на установку программы

В результате в консоли СРиА будет создана новая задача на установку ПО с заданными в ходе работы мастера параметрами.

3.3.2 Добавление в задачу нескольких рабочих станций

Добавление в задачу нескольких рабочих станций администратору безопасности доступно разными способами:

- для добавления в задачу всех имеющихся в списке рабочих станций, выделите все элементы списка с помощью сочетания клавиш **Ctrl+A**, осуществите вызов контекстного меню щелчком правой кнопки мыши на любой из выделенных рабочих станций, и нажмите **Выбрать** (рисунок 3.46);
- для выбора несколько рабочих станций в списке, удерживая клавишу **Ctrl**, осуществите вызов контекстного меню щелчком правой кнопки мыши на одной из выделенных рабочих станций, и нажмите **Выбрать** (рисунок 3.46);
- для выбора серии рабочих станций, расположенных последовательно друг за

другом, выделите мышью первую рабочую станцию серии и, удерживая клавишу **Shift**, щелкните на последней рабочей станции серии, осуществите вызов контекстного меню, как описано в предыдущих пунктах.

- для изменения набора выделенных рабочих станций удерживая клавишу **Ctrl**, выделите дополнительные рабочие станции без потери первоначально выделенных элементов.

Для отмены выбора одновременно для нескольких рабочих станций, выберите рабочие станции одним из указанных выше способов и нажмите **Отменить выбор** в контекстном меню.

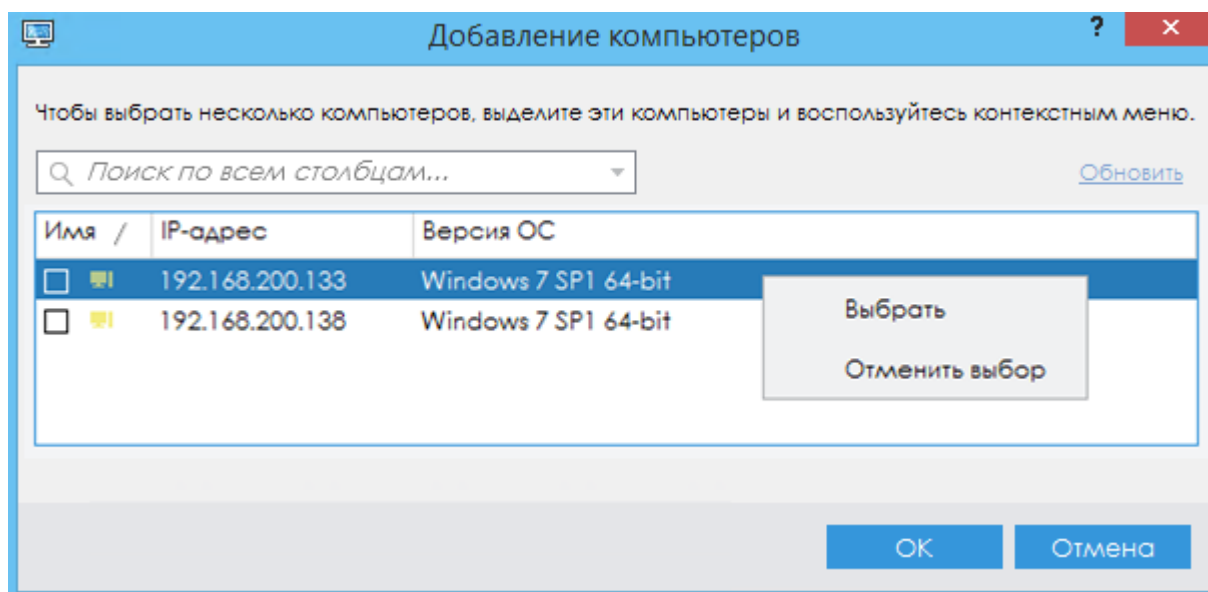


Рисунок 3.46 – Контекстное меню окна добавления компьютеров

3.3.3 Параметры перезагрузки рабочих станций

В процессе создания или редактирования задачи доступны следующие виды перезагрузки рабочей станции:

- 1) **Перезагружать компьютер как можно скорее** – рабочая станция будет перезагружена в течение 5 минут после завершения установки (удаления) ПО. Пользователи не смогут отказаться или отложить перезагрузку. На рабочей станции откроется окно с сообщением о необходимости перезагрузки рабочей станции (рисунок 3.47). В окне расположена кнопка **Перезагрузить сейчас**, нажатие на которую приведет к немедленной перезагрузке рабочей станции. Кнопка **Отложить** при выборе данного варианта перезагрузки не активна.

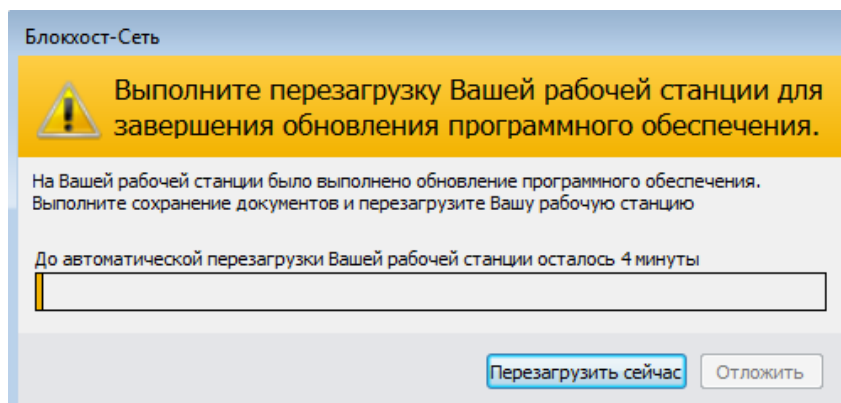


Рисунок 3.47 – Сообщение с предупреждением о перезагрузке рабочей станции

При установке данного параметра и нажатии кнопки **Далее** с выбранным параметром, администратору безопасности будет выведено предупреждение об установке параметра с возможностью сохранения результатов редактирования задачи (рисунок 3.48).

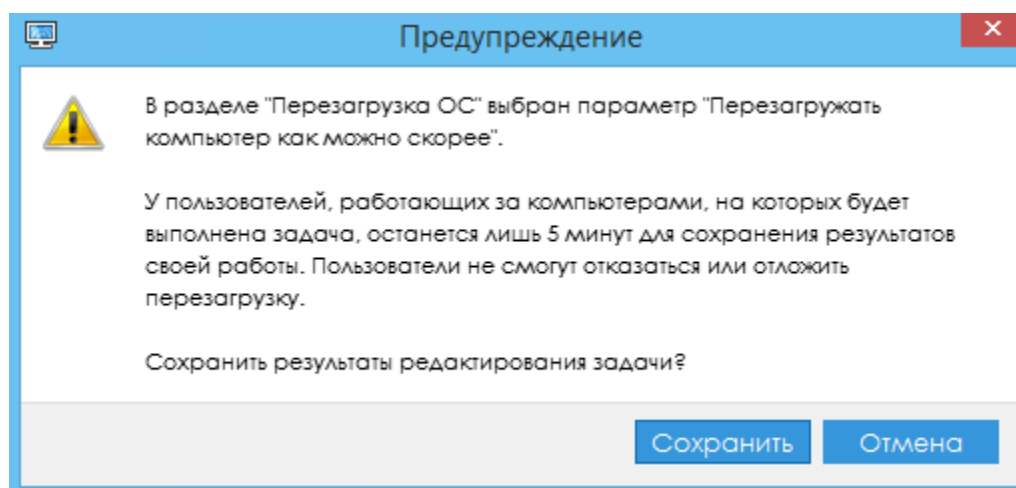


Рисунок 3.48 – Предупреждение об установке параметра и сохранение результатов редактирования задачи

- 2) **Не перезагружать компьютер** – рабочая станция не будет перезагружена после завершения установки на нее ПО.
- 3) **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 3.47). 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 безусловной перезагрузки останется менее 5 минут (кнопка **Отложить** будет не активна).

Отмеченный параметр **Выводить уведомление каждые (чч:мм)** (рисунок 3.43) позволит выводить информационное сообщение через указанный промежуток времени,

если пользователь закрыл его нажав кнопку **Отложить**.

Отмеченный параметр **Выполнять безусловную перезагрузку через (чч:мм)** позволит выполнить перезагрузку рабочей станции через указанный промежуток времени независимо от действий пользователя на рабочей станции. При этом в информационном окне, отображающемся на рабочей станции, указывается оставшееся до автоматической перезагрузки время.

3.3.4 Создание задачи на удаление программы

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

- 1) Перейти в раздел **Развертывание** во вкладку **Задачи** и нажав кнопку **Создать задачу** выбрать пункт **Создать задачу на удаление программы** (см. пример на рисунок 3.37).
- 2) В открывшемся окне мастера создания задачи на удаление программы (рисунок 3.49) выбрать 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 СРиА создан инсталляционный пакет;
 - **Выполнение скрипта для удаления программы** – создание задачи для запуска на удаленной рабочей станции скрипта *PowerShell* или командного (*.bat) файла для удаления программы.

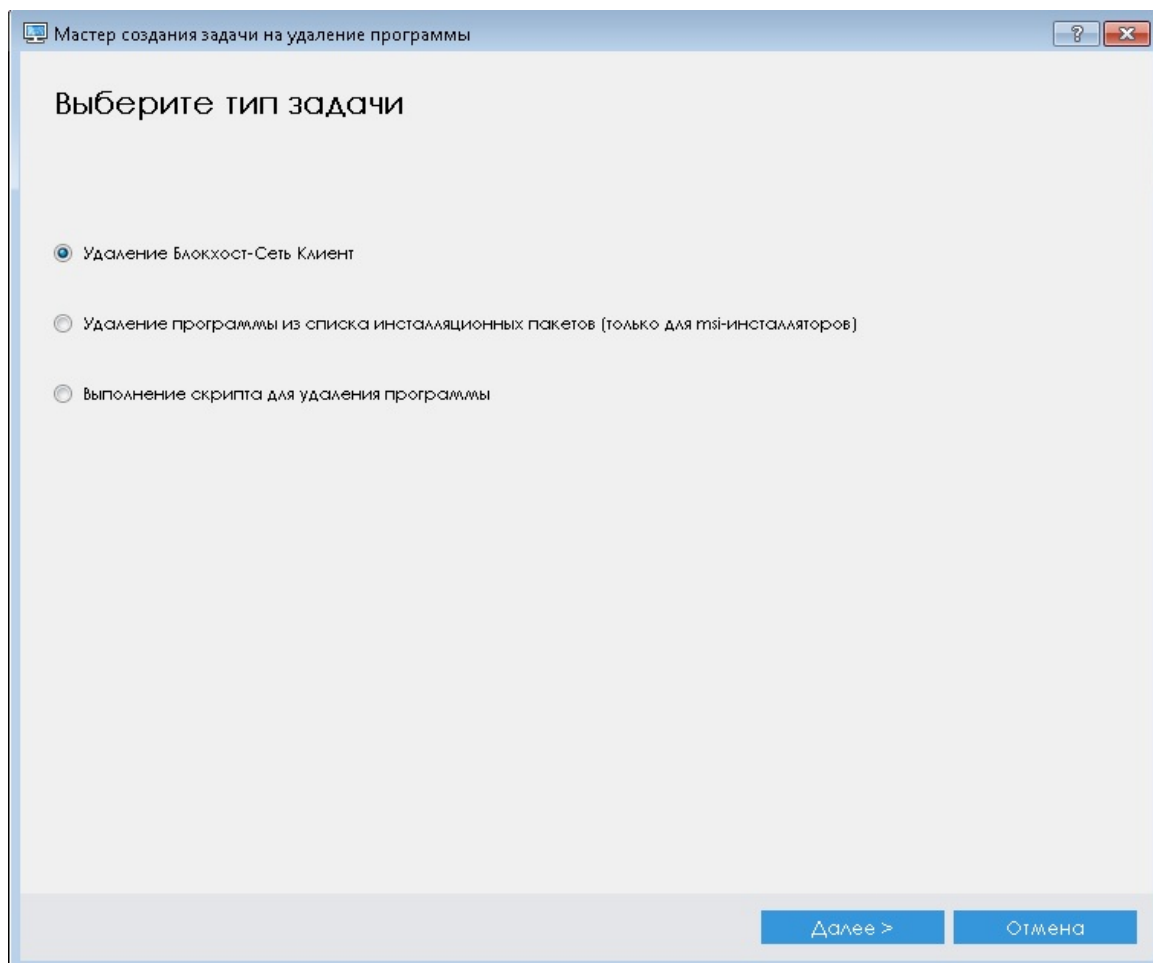


Рисунок 3.49 – Выбор типа задачи на удаление программы

3) После сделанного выбора, нажать кнопку **Далее**.

Дальнейший этап работы мастера создания задачи на удаление программы зависит от выбранной подзадачи. Подробнее каждый вариант описан ниже.

3.3.4.1 Удаление клиента Блокхост-Сеть

При выборе пункта **Удаление Блокхост-Сеть Клиент** выполняется запуск мастера по созданию задачи на удаление программы. Администратору безопасности необходимо выполнить следующие действия:

1) На этапе выбора рабочей станции в окне мастера создания задачи на удаление программы (рисунок 3.50) отметить в списке те рабочие станции, с которых будет удаляться клиент Блокхост-Сеть (см. пункт «3.3.2 Добавление в задачу нескольких рабочих станций»), и нажать кнопку **Далее**.

Для отображения только тех рабочих станций, на которых установлен клиент Блокхост-Сеть, необходимо активировать параметр **Показывать компьютеры только с установленными клиентами Блокхост-Сеть** в нижней части окна.

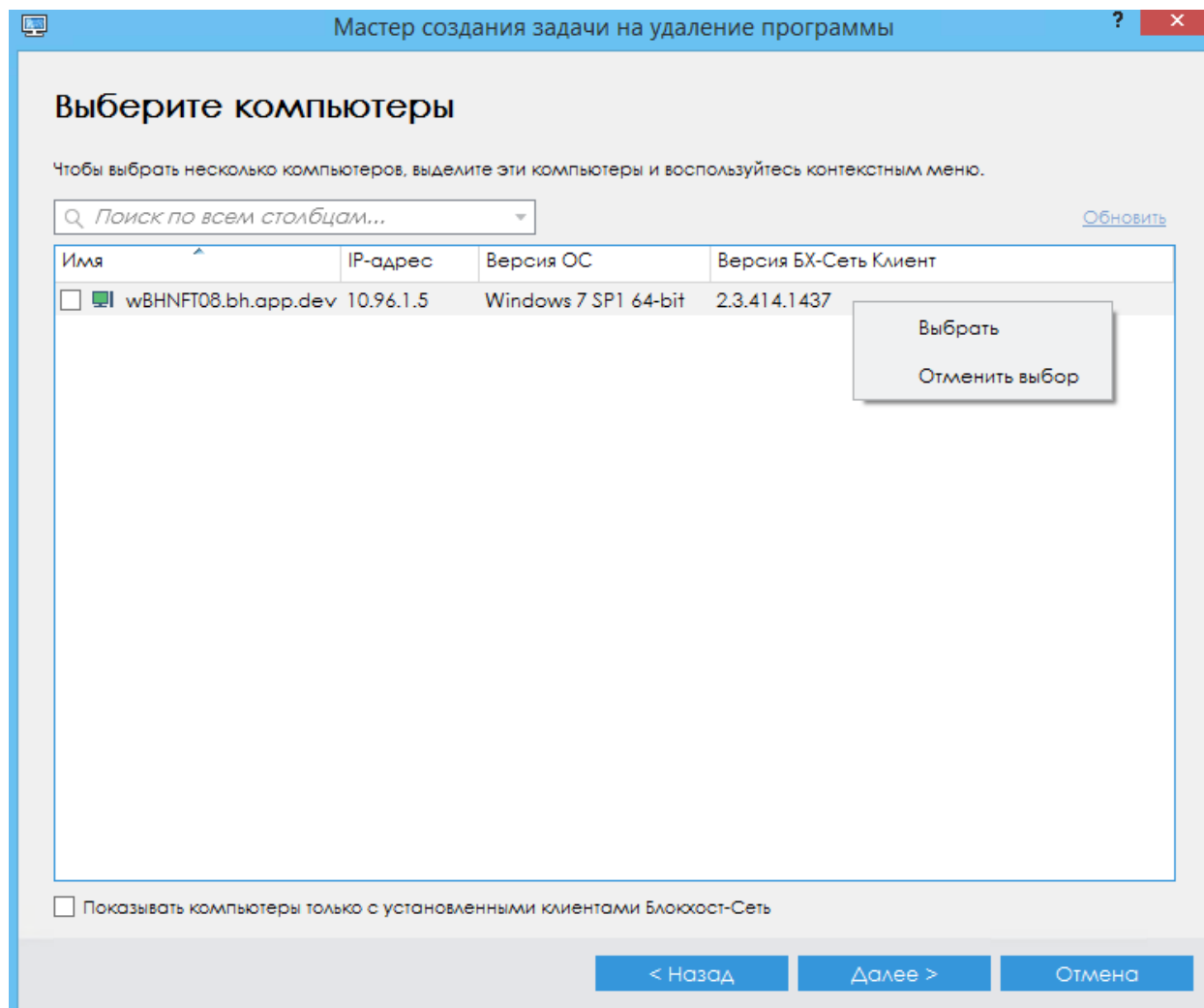


Рисунок 3.50 – Выбор списка рабочих станций для удаления клиента Блокхост-Сеть

- 2) На следующем шаге мастера создания задачи на удаление программы (рисунок 3.42) необходимо задать параметры планировщика запуска задачи (подробнее см. п. 7 подпункта «3.1.1.1 Установка из консоли СРиА») и определить интервалы времени выполнения задачи. Для продолжения нажать кнопку **Далее**.
- 3) В следующем окне мастера создания задачи на удаление программы (рисунок 3.43) указать параметры перезагрузки рабочей станции после удаления с нее ПО (см. пункт «3.3.3 Параметры перезагрузки рабочих станций») и нажать кнопку **Далее**.
- 4) На следующем шаге мастера создания задачи на удаление программы (рисунок 3.51) необходимо ввести имя создаваемой задачи и нажать кнопку **Создать**.

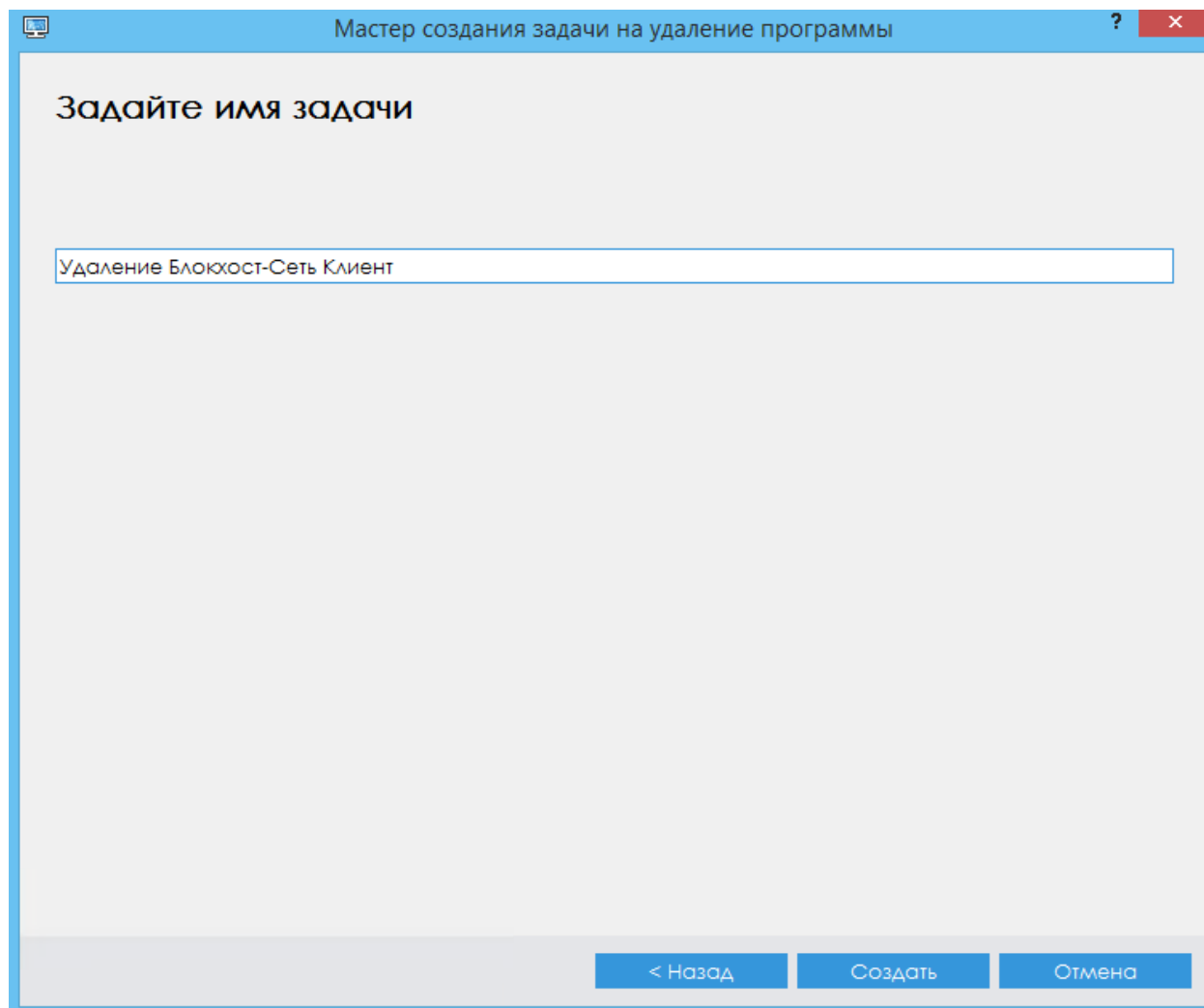


Рисунок 3.51 – Ввод имени создаваемой задачи на удаление программы

- 5) В окне завершения работы мастера создания задачи на удаление программы (рисунок 3.52) нажать кнопку **Заккрыть**.

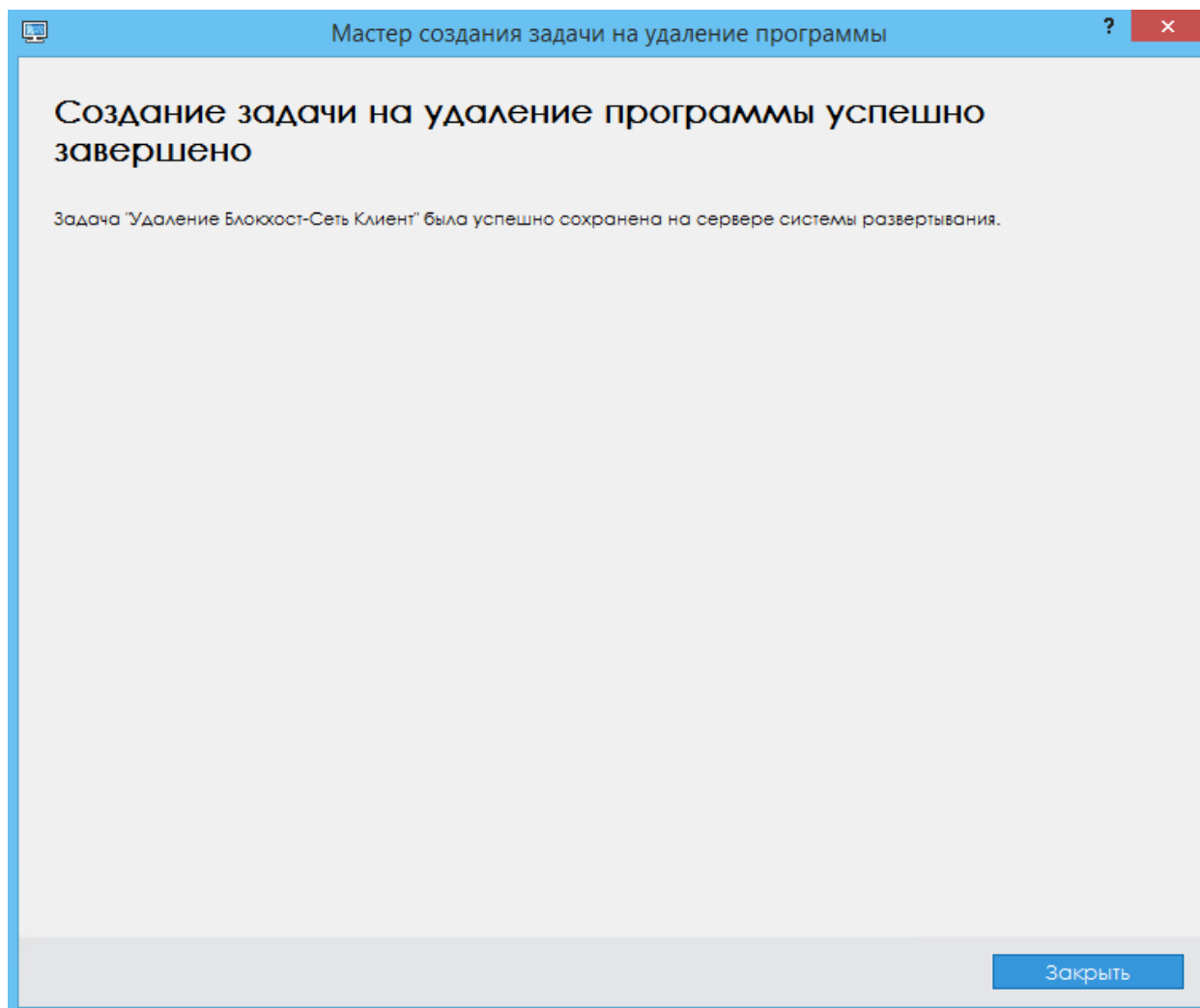


Рисунок 3.52 – Окно завершения работы мастера создания задачи на удаление программы

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

3.3.4.2 Удаление программы из списка инсталляционных пакетов

При выборе пункта **Удаление программы из списка инсталляционных пакетов (только для msi-инсталляторов)** (рисунок 3.49) выполняется запуск мастера по созданию задачи на удаление программы. Администратору безопасности необходимо выполнить следующие действия:

1) На этапе выбора пакета в окне мастера создания задачи на удаление программы (рисунок 3.53) выбрать инсталляционный пакет из списка имеющихся. Для ввода имени инсталляционного пакета необходимо:

- в окне мастера создания задачи на удаление программы нажать кнопку **Выбрать**;
- в открывшемся окне выбора инсталляционного пакета (рисунок 3.54) выделить имя инсталляционного пакета удаляемой программы и нажать кнопку **Выбрать**.

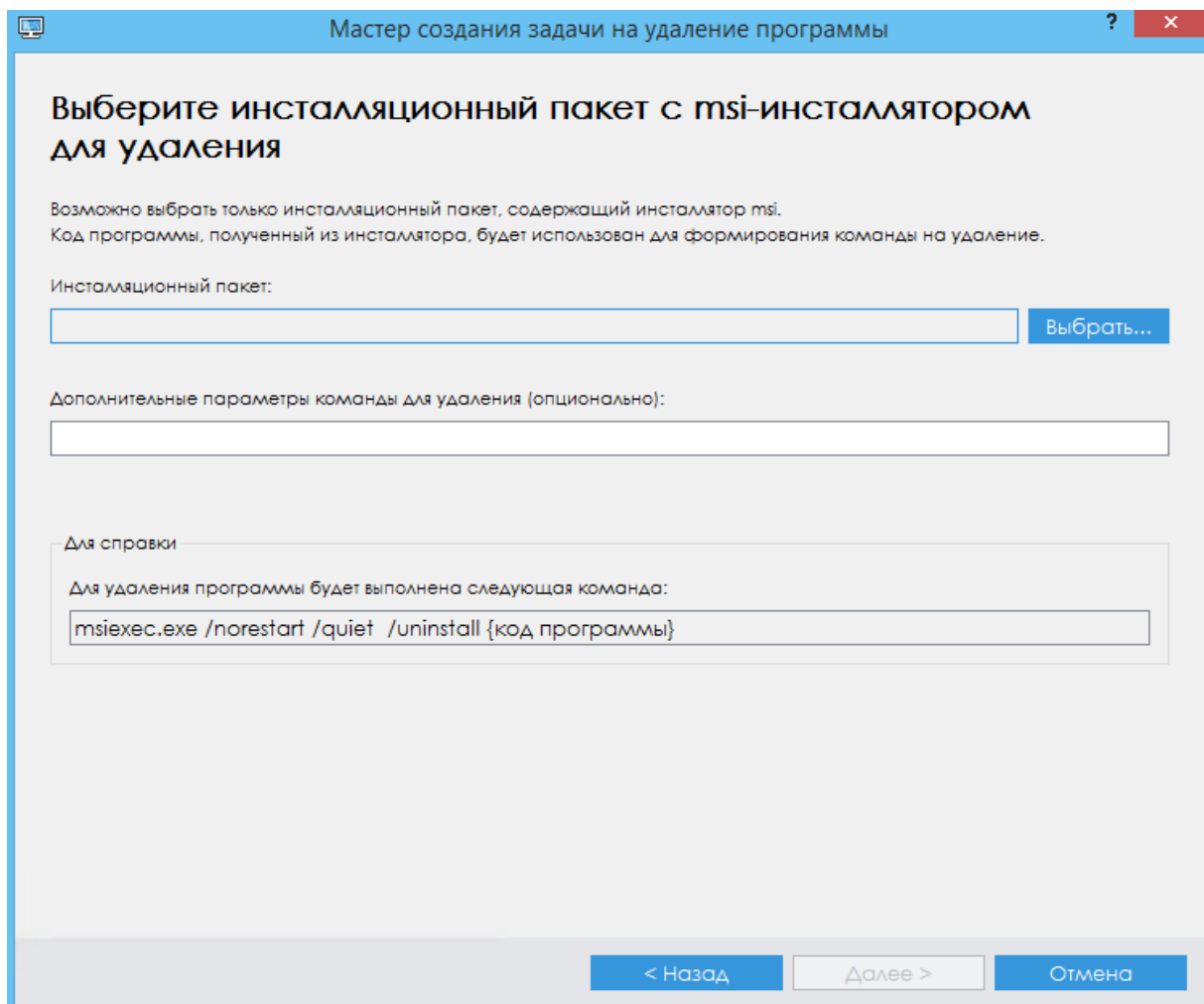


Рисунок 3.53 – Окно ввода параметров инсталляционного пакета с программой для удаления

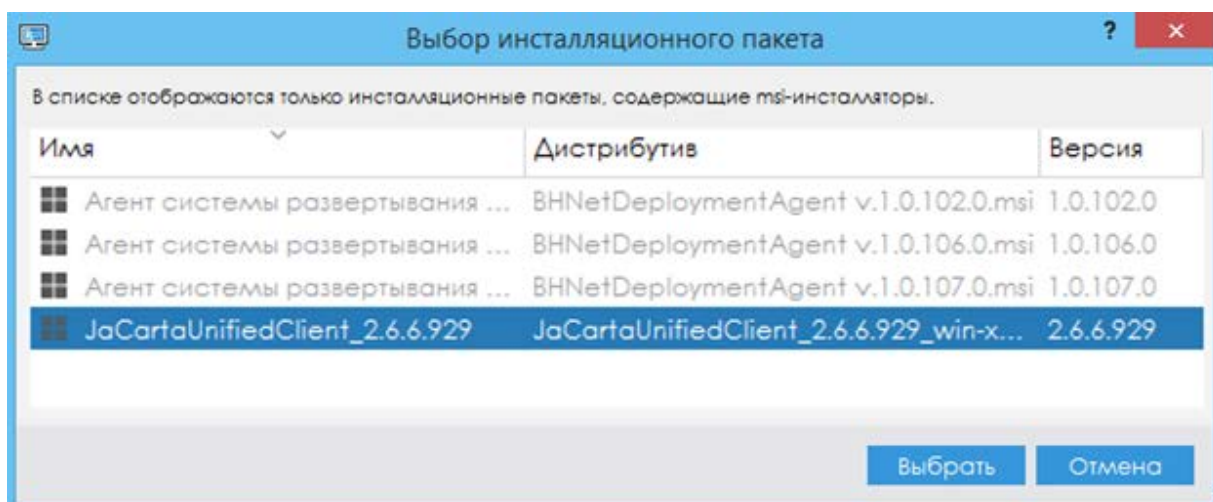


Рисунок 3.54 – Окно выбора инсталляционного пакета

- 2) При необходимости в поле **Дополнительные параметры команды для удаления (опционально)** (рисунок 3.53) ввести дополнительные параметры выполнения команды по удалению выбранной программы и нажать кнопку **Далее**, для

продолжения создания задачи на удаление программы.

3) На следующем шаге мастера создания задачи на удаление программы отметить рабочие станции, с которых будет удаляться выбранная программа (см. пункт «3.3.2 Добавление в задачу нескольких рабочих станций») и нажать кнопку **Далее**.

4) Последующие шаги мастера создания задачи на удаление программы аналогичны пп. 2-5 подпункта «3.3.4.1 Удаление клиента Блокхост-Сеть».

В результате в консоли СРиА будет создана новая задача на удаление программы из списка инсталляционных пакетов с заданными в ходе работы мастера параметрами.

3.3.4.3 Удаление программы с использованием скрипта PowerShell или командного файла Windows

При выборе пункта **Выполнение скрипта для удаления программы** выполняется запуск мастера по созданию задачи на удаление программы. Администратору безопасности необходимо выполнить следующие действия:

1) На этапе выбора файла скрипта в окне мастера создания задачи на удаление программы (рисунок 3.55) необходимо выбрать файла скрипта (*.ps1) или командного файла (*.bat) по удалению программы с рабочей станции. Для выбора файла необходимо:

- в окне мастера создания задачи на удаление программы нажать кнопку **Выбрать** (рисунок 3.55);
- в открывшемся окне выбора файла скрипта (рисунок 3.56) выделить необходимый файл и нажать кнопку **Открыть**.

Мастер создания задачи на удаление программы

Выберите файл скрипта

Выберите файл скрипта, содержащий команды для удаления программы.
Поддерживаются bat и ps1 скрипты.

Файл скрипта:

Выбрать...

Параметры командной строки файла скрипта (опционально):

< Назад Далее > Отмена

Рисунок 3.55 – Окно ввода параметров файла скрипта по удалению программы

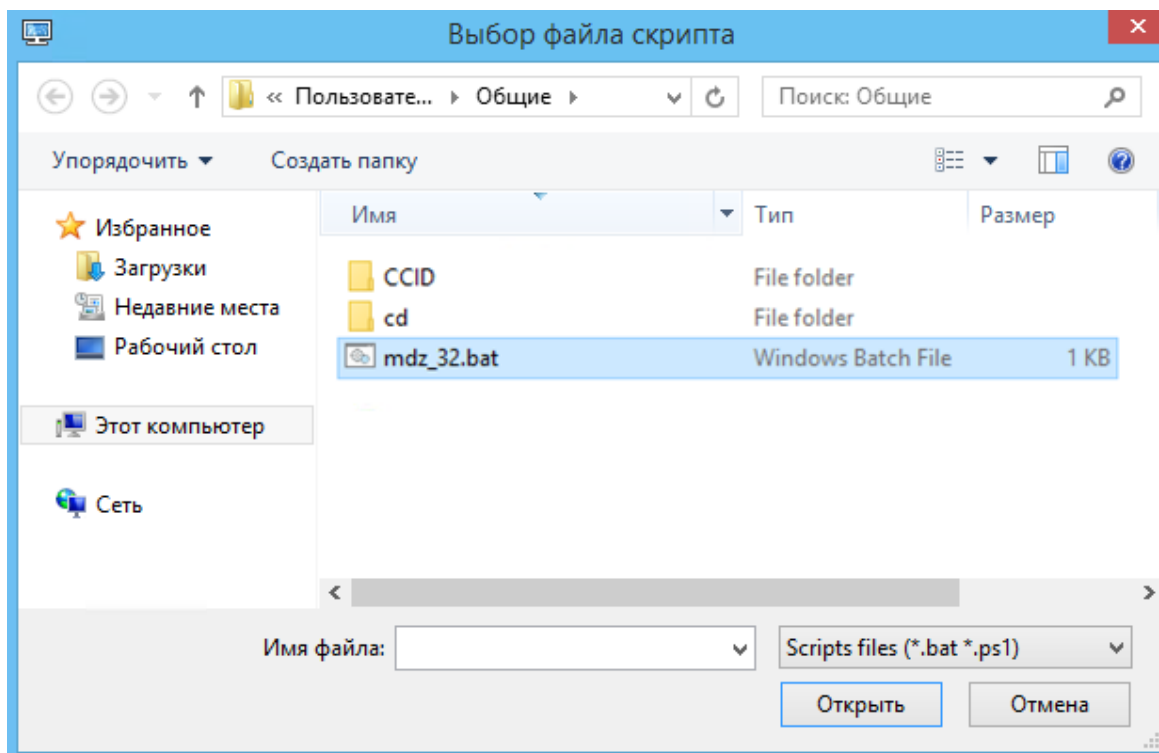


Рисунок 3.56 – Окно выбора файла скрипта по удалению программы

2) При необходимости в поле **Параметры командной строки файла скрипта (опционально)** (рисунок 3.55) ввести параметры выполнения скрипта по удалению программного обеспечения и 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 (см. пункт «3.3.2 Добавление в задачу нескольких рабочих станций») и нажать кнопку **Далее**.

4) Последующие шаги мастера создания задачи на удаление программы аналогичны пп. 2-5 подпункта «3.3.4.1 Удаление клиента Блокхост-Сеть».

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.

3.3.5 Создание задачи на перезагрузку компьютеров

Для запуска мастера по созданию задачи на перезагрузку рабочих станций администратору безопасности необходимо в консоли СРиА выполнить следующие действия:

1) Перейти в раздел **Развертывание** во вкладку **Задачи** и нажав кнопку **Создать задачу** выбрать пункт **Создать задачу на перезагрузку компьютеров** (см. пример на рисунке 3.37).

2) В открывшемся окне мастера создания задачи на перезагрузку компьютеров (рисунок 3.57) отметить требуемые к перезагрузке рабочие станции (см. пункт «3.3.2 Добавление в задачу нескольких рабочих станций») и нажать кнопку **Далее**.

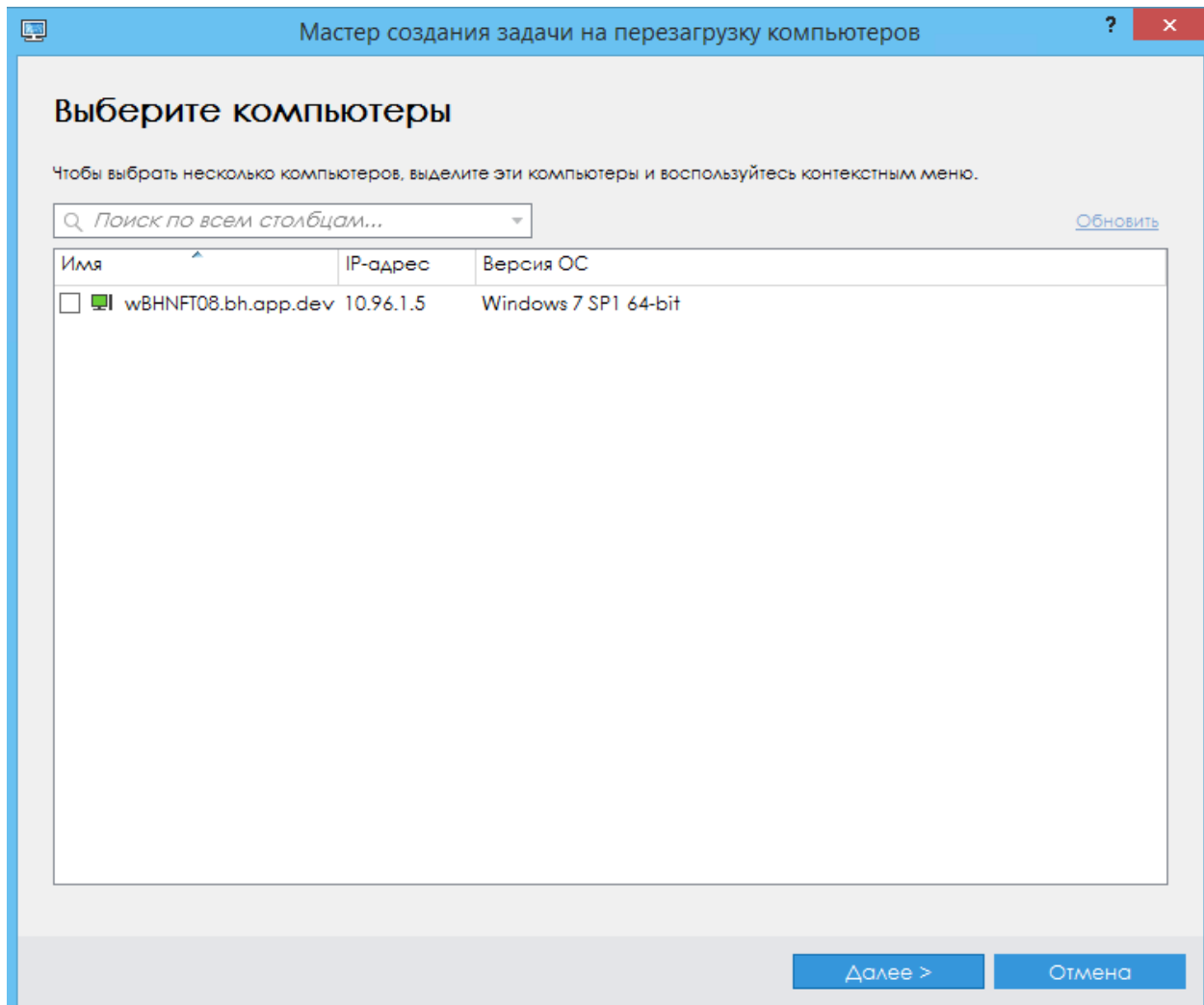


Рисунок 3.57 – Окно выбора рабочих станций для выполнения задачи перезагрузки

3) Последующие шаги мастера создания задачи на перезагрузку компьютеров аналогичны шагам мастера на удаление программы и соответствуют пп. 2-5 подпункта «3.3.4.1 Удаление клиента Блокхост-Сеть».

В результате в консоли СРиА будет создана новая задача на перезагрузку компьютеров с заданными в ходе работы мастера параметрами.

3.3.6 Запуск задачи на установку/удаление ПО

В зависимости от установленных параметров планировщика запуск задачи на установку/удаление программ с рабочих станций может быть осуществлен автоматически или вручную. При этом любую задачу, имеющую статус *Ожидает выполнения* или *Завершено*, независимо от установленных параметров планировщика, можно запустить вручную.

Для запуска задачи необходимо выделить ее в списке и в открывшейся панели нажать кнопку **Запустить** (рисунок 3.58).

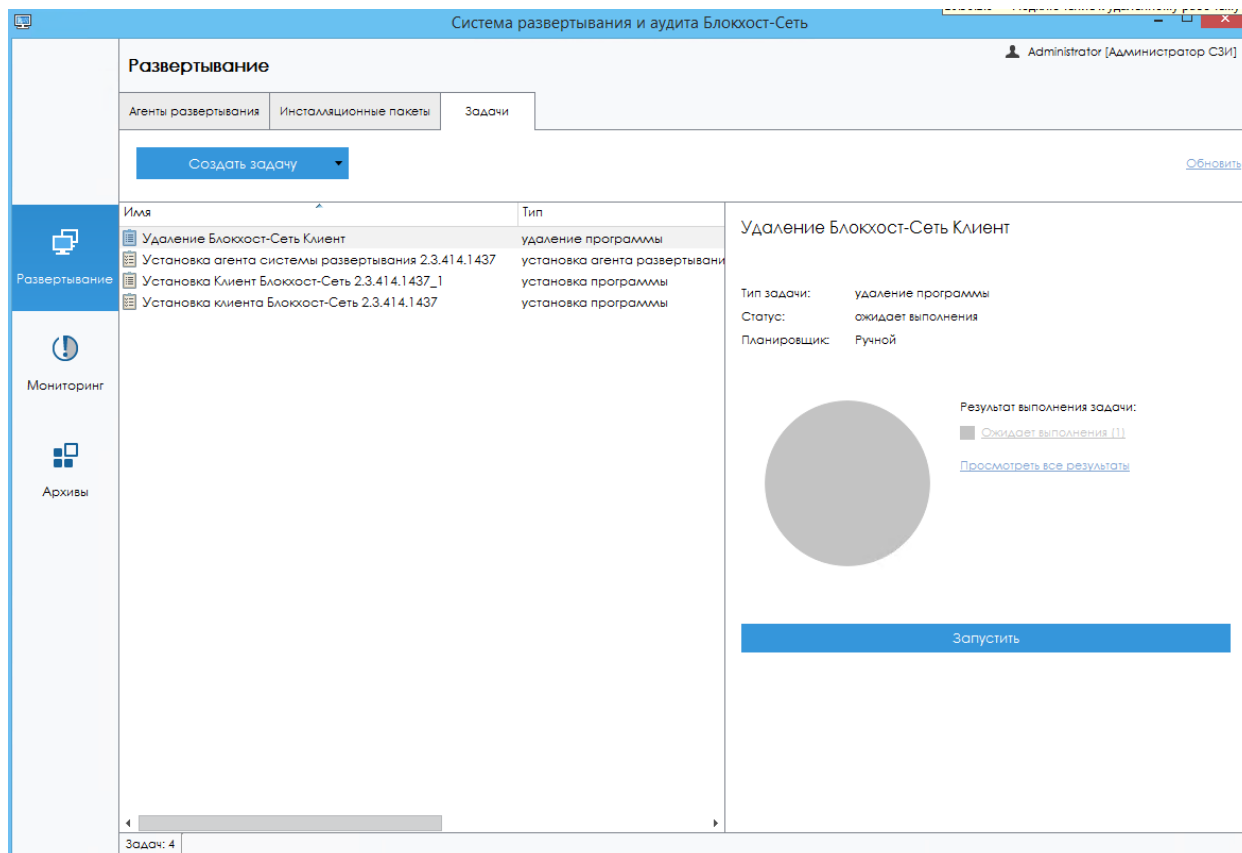


Рисунок 3.58 – Запуск задачи на установку программы

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

- фрагмента журнала Windows, относящегося к выполняемой задаче;
- журнала файла-установщика программного обеспечения.

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

Просмотр журналов доступен в окне просмотра результатов выполнения задачи по ссылке **Просмотреть все результаты** (рисунок 3.59), если в списке имеется описание статуса, содержащее иконку «» (иконка дублируется как в верхней части окна, так и в нижней). При выделении такой строки кнопка **Дополнительно** становится активна (рис 3.59).

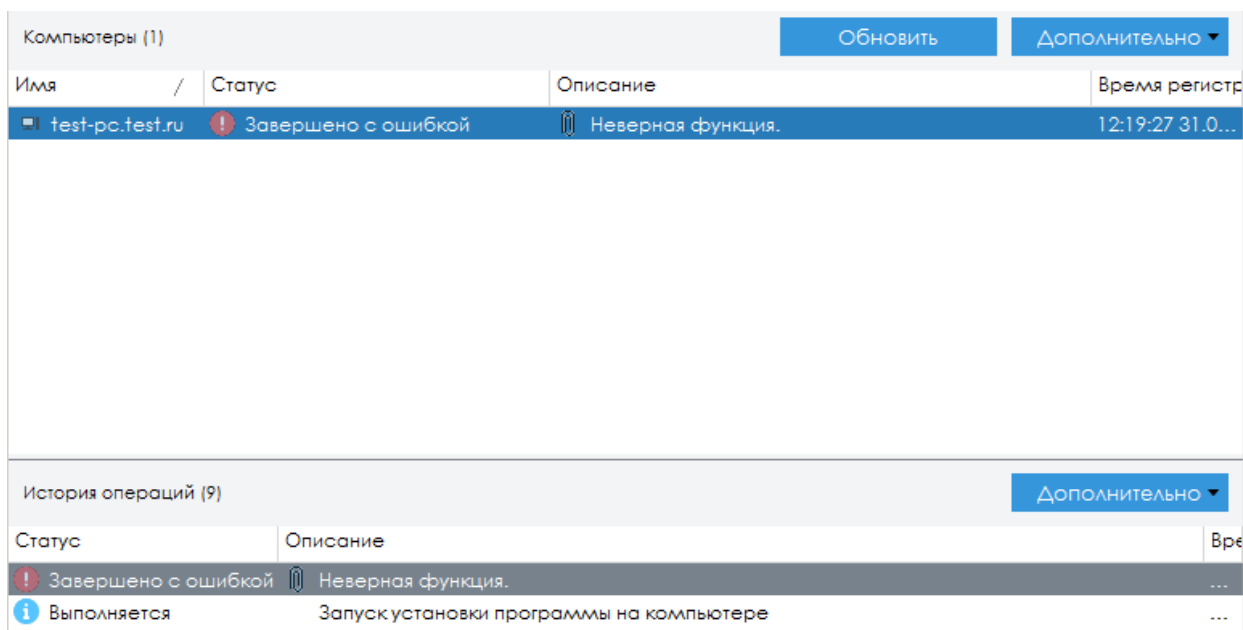
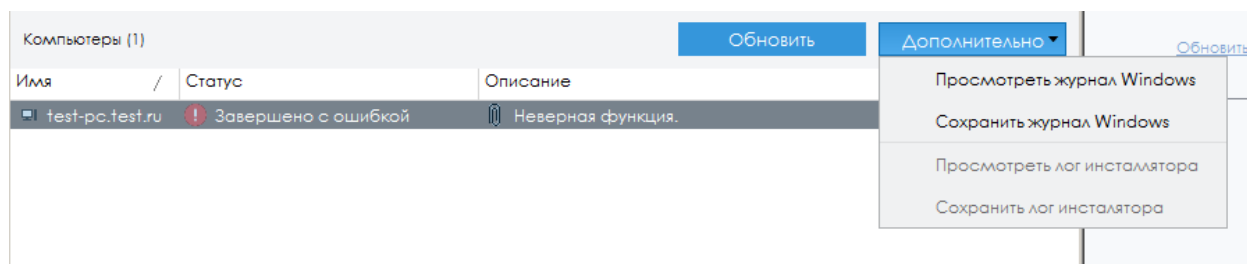


Рисунок 3.59 – Сообщение об ошибке установки в истории операций

Щелчок по кнопке **Дополнительно** открывает контекстное меню (рисунок 3.60), которое позволяет либо сразу просмотреть указанные журналы, либо выполнить их сохранение на жесткий диск в виде текстовых файлов. Доступность журналов зависит от типа ошибочной ситуации.

Рисунок 3.60 – Контекстное меню кнопки **Дополнительно**

При выборе пунктов меню «**Просмотреть журнал Windows**»/ «**Просмотреть лог инсталлятора**», открываются соответственно сообщения журнала Windows, относящиеся к процессу установки/удаления ПО (рисунок 3.61) или сообщения лога установки инсталляционного пакета (рисунок 3.62).

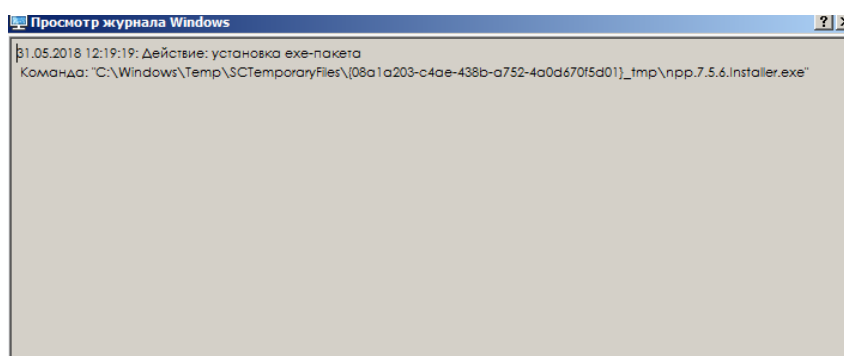


Рисунок 3.61 – Просмотр журнала Windows

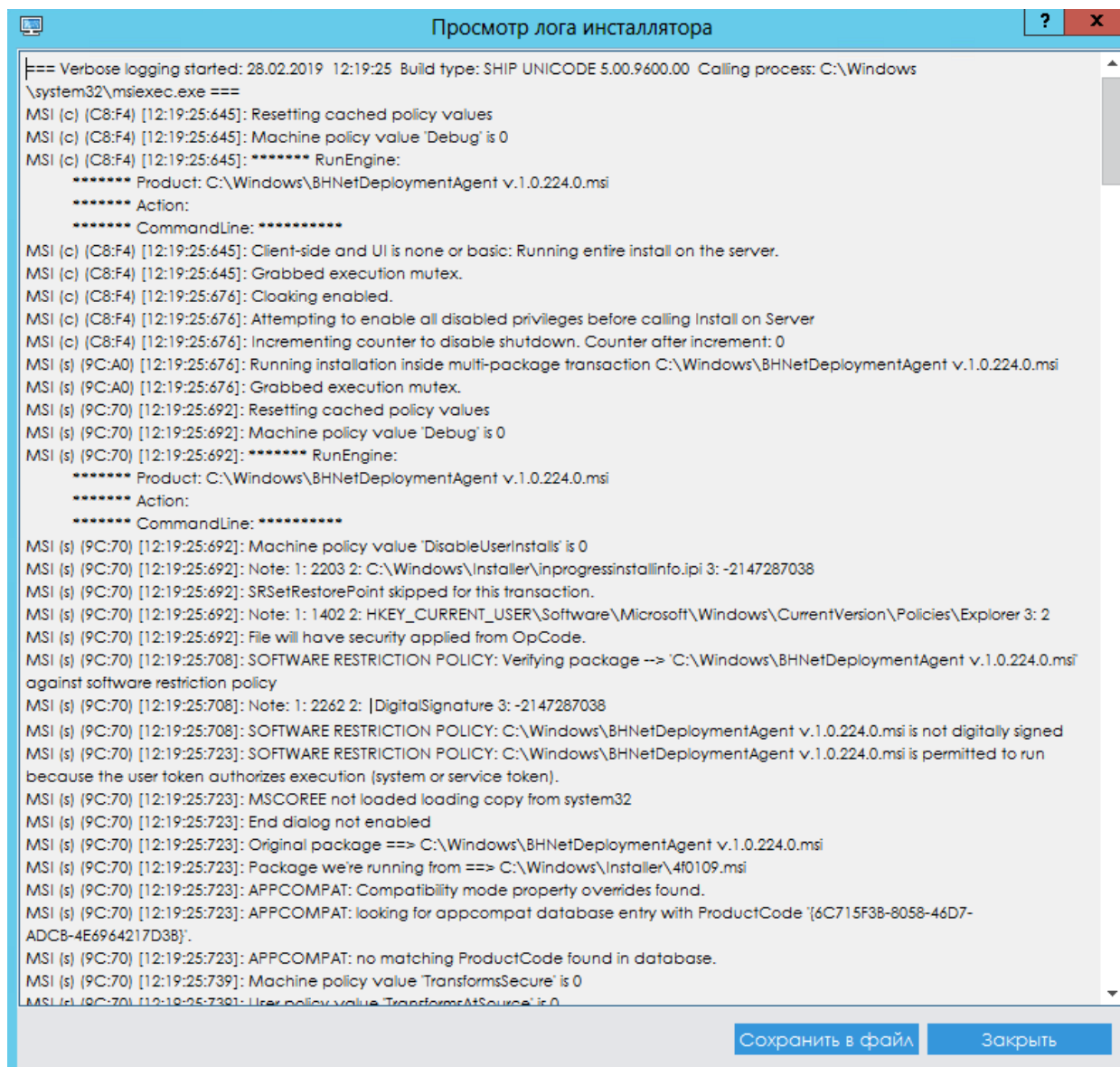


Рисунок 3.62 – Просмотр лога инсталлятора

Пункты контекстного меню **«Сохранить журнал Windows»/«Сохранить лог инсталлятора»** позволяют сохранить сообщения журнала Windows/сообщения лога установки инсталляционного пакета в текстовом файле в указанном каталоге.



При несовместимости версий сервера СРиА и агента развертывания задача на установку/удаление ПО будет завершена с ошибкой. В историю операций заносится запись о несовместимости сервера СРиА и агента развертывания. В этом случае необходимо обновить версию агента развёртывания.

3.3.7 Остановка задачи

Задача на установку/удаление ПО может быть прервана на любом этапе своего выполнения. Для остановки задачи необходимо в панели выполнения задачи нажать кнопку **Остановить** (рисунок 3.63).

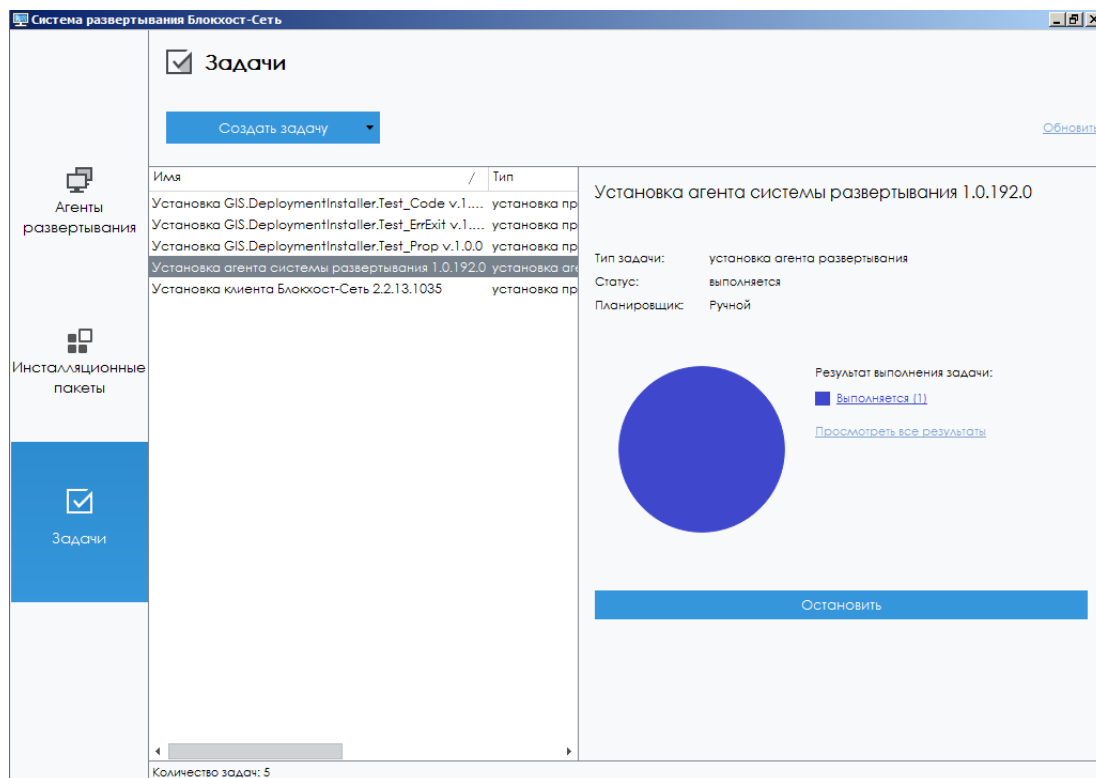


Рисунок 3.63 – Остановка задачи на установку/удаление программного обеспечения

В зависимости от этапа выполнения, реакция на прерывание будет различной. Описание возможных вариантов приведено в таблице 3.3.

Таблица 3.3 – 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 рабочей станции: <i>ожидает выполнения</i>	На рабочей станции не происходит каких-либо изменений. Статус рабочей станции: <i>ожидает выполнения</i>
На рабочую станцию была начата загрузка файла-установщика программы. Статус рабочей станции: <i>выполняется</i>	На рабочей станции не происходит каких-либо изменений. Процесс установки программы еще не был запущен. Статус рабочей станции: <i>ожидает выполнения</i>
На рабочей станции запущен процесс установки (удаления) программы. Статус рабочей станции: <i>выполняется</i>	Остановка задачи не приводит к прерыванию процесса установки программы на рабочей станции. Установка программы либо завершается естественным путем, либо прекращается в случае превышения временного интервала, заданного параметром задачи Прервать установку программы на рабочей станции, если инсталлятор не активен дольше (рисунок 3.42). Статус рабочей станции: <i>завершено с ошибкой</i>
Выполняется ожидание перезагрузки клиентской рабочей станции (в соответствии с параметрами перезагрузки, заданными в задаче, см. пункт «3.2.1 Создание инсталляционных пакетов»). Статус рабочей станции: <i>требуется перезагрузка</i>	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 рабочей станции: <i>завершено с предупреждением</i>
Установка (удаление) программы завершено. Перезагрузка, в случае необходимости ее выполнения, была выполнена. Статус рабочей станции: <i>успешно завершено, завершено с ошибкой, завершено с предупреждением, недоступен</i>	На рабочей станции не происходит каких-либо изменений. Статус рабочей станции остается без изменений.

3.3.8 Установка клиента Блокхост-Сеть

Для установки клиента Блокхост-Сеть на рабочие станции администратору необходимо выполнить следующие действия в консоли СРиА:

- 1) Отредактировать параметры автоматически созданной задачи на установку клиента Блокхост-Сеть (либо создать новую задачу, см. пункт «3.3.1 Создание задачи на установку ПО» данного документа):

- сформировать список рабочих станций, на которые будет устанавливаться клиент Блокхост-Сеть;
- указать параметры расписания установки агента Блокхост-Сеть на рабочие станции;
- указать параметры перезагрузки рабочей станции после окончания установки на нее клиента Блокхост-Сеть (см. пункт «3.3.3 Параметры перезагрузки рабочих станций»).

2) Запустить задачу по установке клиента Блокхост-Сеть.

Для редактирования параметров автоматически созданной задачи по установке клиента Блокхост-Сеть администратору безопасности необходимо:

- 1) Запустить консоль СРиА, перейти в раздел **Развертывание** во вкладку **Задачи** (см. пример на рисунке 3.37).
- 2) Щелкнуть правой кнопкой мыши на строке с именем **Установка клиента Блокхост-Сеть <номер_версии>** и выбрать в открывшемся контекстном меню пункт **Редактировать**.
- 3) Далее выполнить шаги, описанные в подпункте «3.1.1.1 Установка из консоли СРиА» данного документа в части касающейся редактирования задач.
- 4) Если выбран вариант запуска задачи **Вручную**, запустить задачу по установке клиента Блокхост-Сеть на выполнение, нажав кнопку **Запустить**, расположенную в нижней части области дополнительной информации выделенной задачи (рисунок 3.38).

В результате выполнения задачи по установке клиента Блокхост-Сеть на рабочие станции 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.

Клиент Блокхост-Сеть сразу после установки функционирует в **Мягком режиме** (подробнее о **Мягком режиме СЗИ** см. п. 6.2.5 «Механизм мягкого режима» документа «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Руководство администратора безопасности»).

3.3.9 Удаление агента Блокхост-Сеть с защищаемых рабочих станций

Клиент Блокхост-Сеть можно удалить с защищаемой рабочей станции через консоль СРиА – подробно процесс удаления клиента Блокхост-Сеть с рабочих станций описан в подпункте «3.3.4.1 Удаление клиента Блокхост-Сеть».

Окончательное удаление компонентов клиентской части СЗИ с рабочей станции произойдет после перезагрузки. В зависимости от выбранных при редактировании задачи по удалению клиентской части СЗИ параметров, перезагрузка будет выполнена сразу после завершения работы задачи, либо через некоторое время, либо по команде пользователя рабочей станции.

4 Раздел «Мониторинг»

Подсистема сбора событий аудита (рисунок 4.1) обладает следующим набором функций:

- отображение иерархии серверов СЗИ;
- отображение иерархии групп и компьютеров с установленными клиентами СЗИ;
- формирование сводного отчета с информацией о состоянии клиентов, подключенных к серверам иерархии;
- сбор событий аудита с клиентов на сервер СЗИ;
- просмотр и фильтрация событий аудита, собранных с клиентских компьютеров на сервер;
- просмотр и фильтрация событий аудита напрямую из журнала клиентского компьютера;
- передача событий аудита вверх по иерархии серверов вплоть до головного сервера с последующей передачей в SIEM-систему (рисунок 4.2).

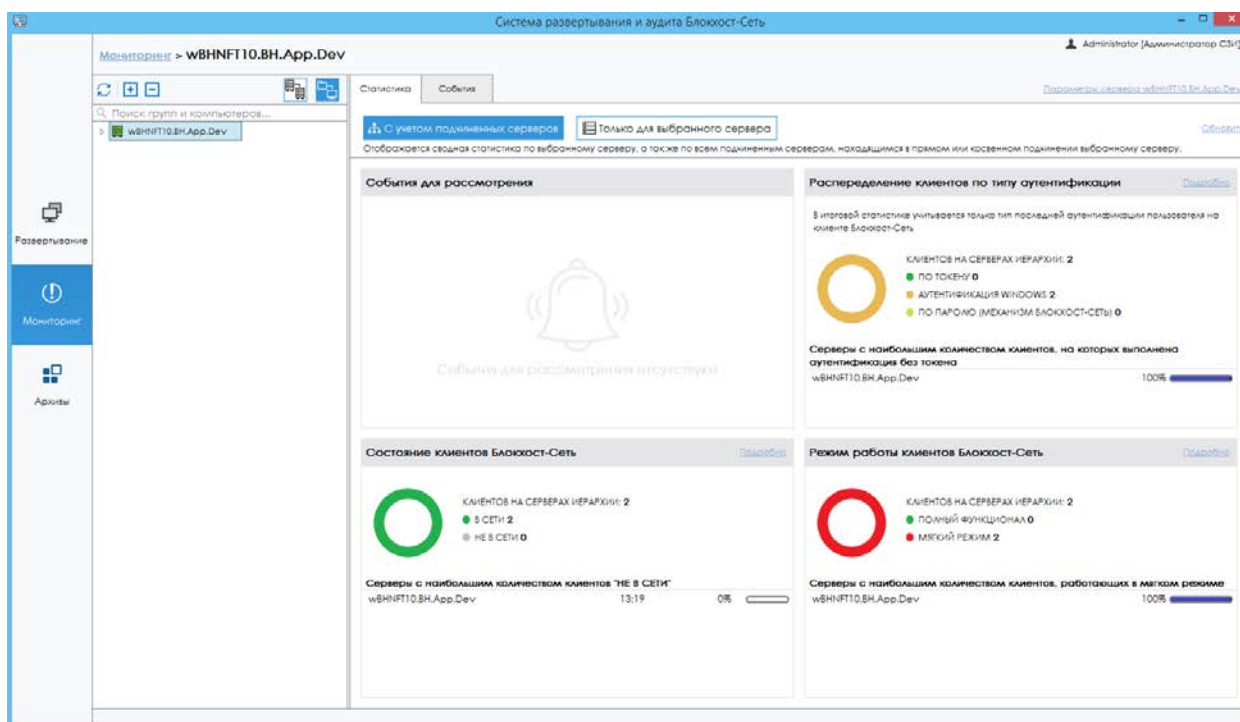


Рисунок 4.1 – Раздел **Мониторинг**

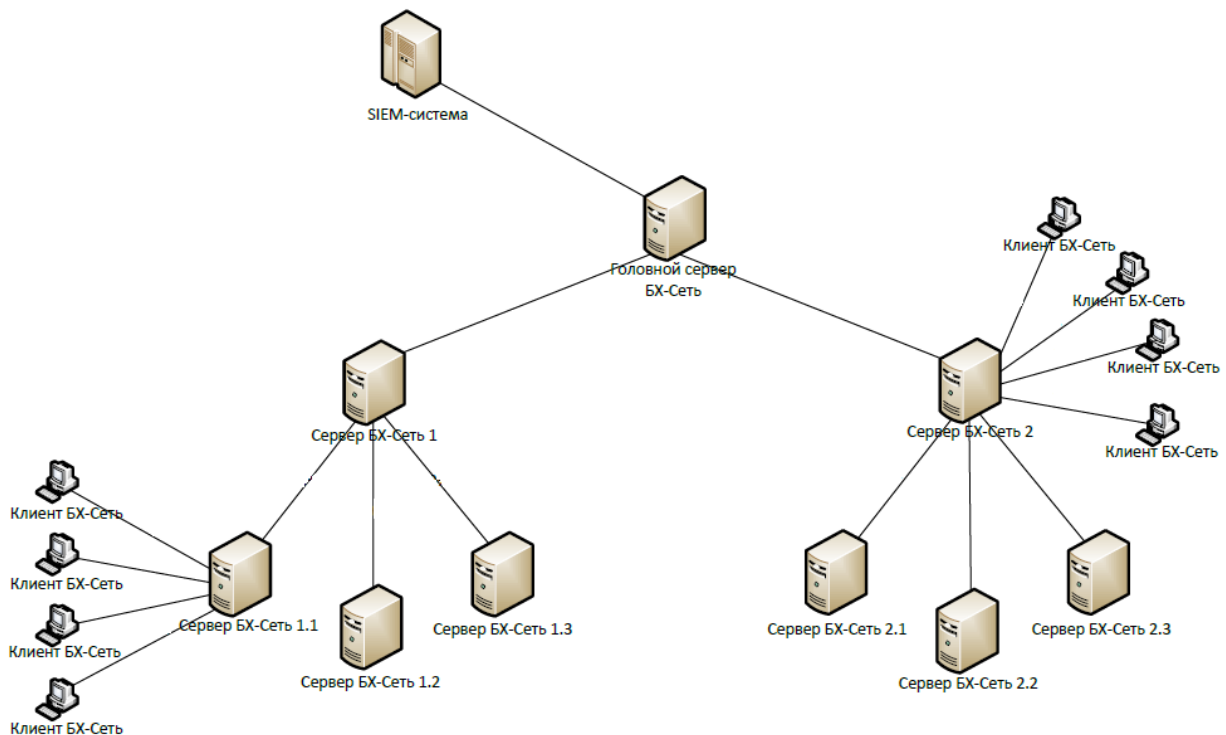


Рисунок 4.2 – Иерархия серверов Блокхост-Сеть

4.1 Дерево иерархии

В разделе отображения дерева иерархии серверов по умолчанию содержится список всех подчиненных серверов, контролируемых на сервере Блокхост-Сеть (рисунок 4.3).

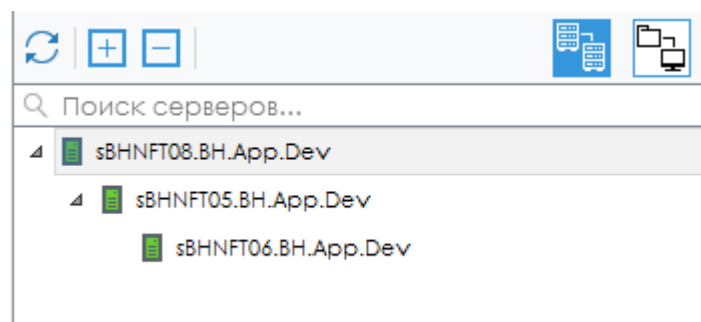


Рисунок 4.3 – Отображение дерева иерархии серверов

В верхней части раздела отображения дерева иерархии серверов расположены следующие элементы управления:

- кнопка **Группы и компьютеры сервера**  позволяет осуществить переход к группам и компьютерам выбранного сервера (аналогичный переход можно осуществить по двойному щелчку левой кнопки мыши на нужном сервере в списке серверов) (рисунок 4.4);
- кнопка **Иерархия серверов**  позволяет осуществить обратный переход от

групп и компьютеров выбранного сервера к списку подчиненных серверов;

- кнопки **Развернуть на один уровень**  / **Свернуть на один уровень**  предназначены, соответственно, для развертывания/свертывания каждого последующего уровня дерева иерархии;
- кнопка **Обновить**  позволяет обновить дерево иерархии серверов и увидеть текущее состояние подчиненных серверов, групп и компьютеров серверов.

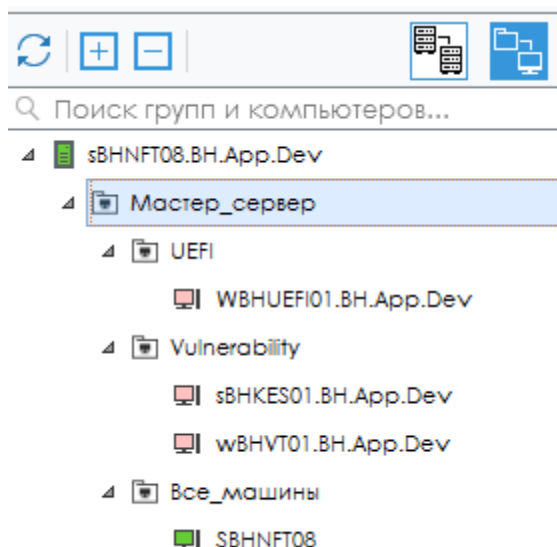


Рисунок 4.4 – Отображение списка всех групп и компьютеров выбранного сервера



Если выбранный подчиненный сервер в состоянии online изменил свое состояние нахождения в сети на offline, при нажатии кнопки **Обновить**, администратору будет выведено информационное сообщение о невозможности установки соединения с сервером (рисунок 4.5).

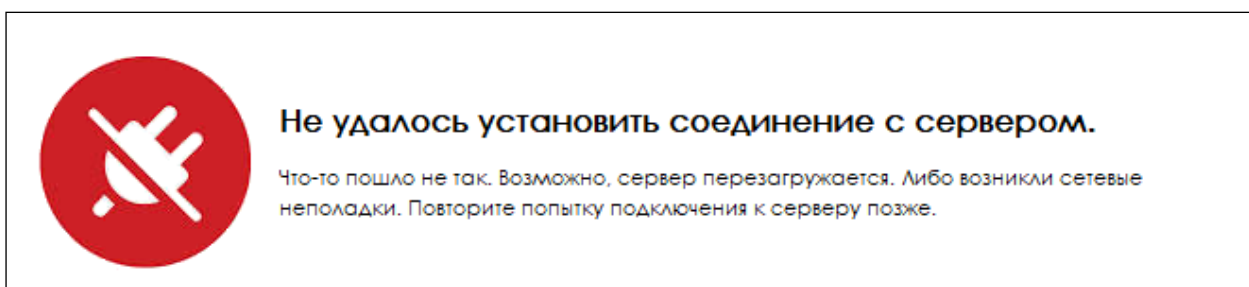


Рисунок 4.5 – Информационное сообщение об отсутствии соединения с сервером



При обновлении настроек подчиненных серверов и клиентских компьютеров возможна временная задержка (до 1,5 минут), связанная с передачей данных по иерархии серверов.

Также в верхней части раздела отображения дерева иерархии серверов расположена строка поиска, предназначенная для отбора серверов, групп или компьютеров сервера в дереве иерархии в соответствии со значением, введенным в строку поиска. Фильтрация по вводимому в строку значению осуществляется в списке иерархии автоматически, сразу после начала введения символов (рисунок 4.6), при этом регистр вводимых символов не учитывается.

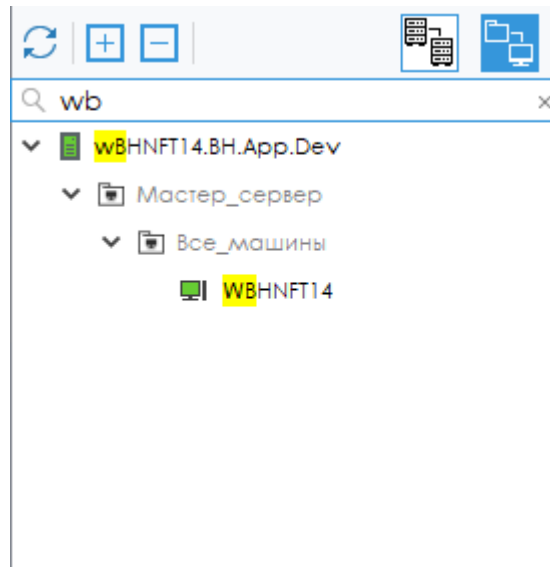


Рисунок 4.6 – Поиск в дереве иерархии

При поиске подчиненного сервера, в дереве иерархии отобразятся все уровни иерархии серверов до искомого сервера (все родительские серверы). Серверы, подчиненные искомому, не отобразятся.



При поиске группы/компьютера сервера, в списке отобразятся все уровни иерархии групп до искомой группы/компьютера (все родительские группы). При поиске группы, группы и компьютеры, находящиеся внутри искомой группы, не отобразятся.

В зависимости от состояния контролируемых подчиненных серверов, групп и компьютеров сервера отображение пиктограмм будет различаться:

-  /  – сервер/компьютеры сервера включены;
-  /  – сервер/компьютеры сервера выключены;
-  - пиктограмма группы компьютеров сервера.



При переходе в древе иерархии или в списке групп/компьютеров сервера к подчиненному серверу или клиентскому компьютеру с установленной устаревшей версией Блокхост-Сеть будет выведено уведомление о невозможности использования функционала Блокхост-Сеть выбранного подчиненного сервера/клиентского компьютера до момента обновления версии (рисунок 4.7).



После обновления устаревшей версии Блокхост-Сеть, с подчиненных серверов или клиентских компьютеров на родительский сервер будут собираться только те события, которые были сгенерированы системой после обновления.

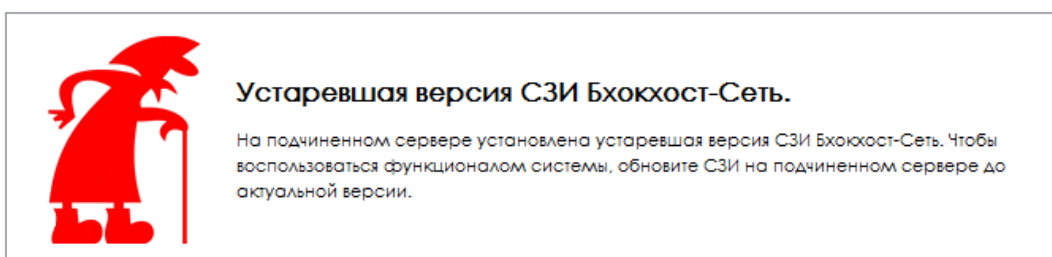


Рисунок 4.7 – Уведомление об устаревшей версии Блокхост-Сеть

Для каждого элемента древа иерархии доступно контекстное меню по щелчку правой кнопки мыши на выбранном элементе. Содержание контекстного меню сервера, группы сервера или клиентского компьютера различается и приведено в подразделах, описывающих порядок работы администратора в отношении каждого элемента древа иерархии (подразделы 4.3-4.5).

В зависимости от выбранного элемента в древе иерархии, информация в правой части окна **Мониторинг** будет различной. Подробное описание информации по выбранному элементу (сервер, группа сервера или компьютер сервера) приведено в подразделах 4.3-4.5.

4.2 Строка навигации

В верхней части окна раздела **Мониторинг** отображается строка навигации, в которой содержатся все уровни иерархии до элемента, выбранного в древе иерархии (рисунок 4.8).

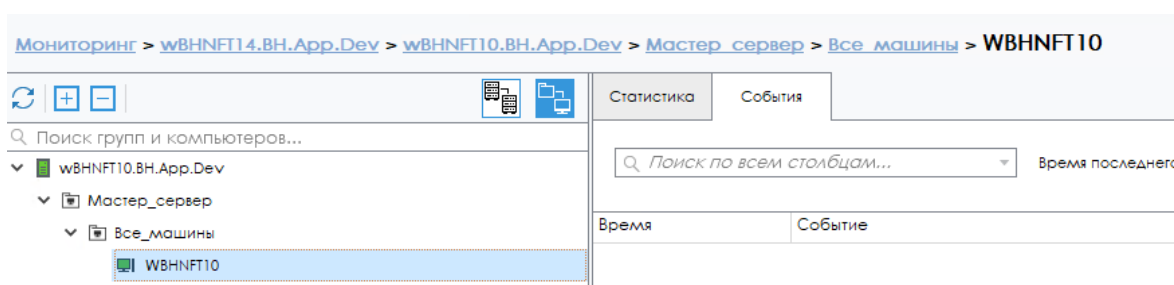


Рисунок 4.8 – Отображение строки навигации

Строка навигации предназначена для быстрого перехода на любой из вышестоящих уровней иерархии по щелчку мыши на нем.

4.3 Настройка сбора событий в консоли управления политиками сервера

Настройка сбора событий, собираемых с клиентских компьютеров и подчиненных серверов на родительский сервер, и отображаемых в консоли СРиА, осуществляется в консоли управления политиками сервера при выделении в окне **Список машин** рабочей станции на которой будет производиться сбор, и выборе в окне **Настройки машины** пункта **Сбор аудита** (рисунок 4.9).

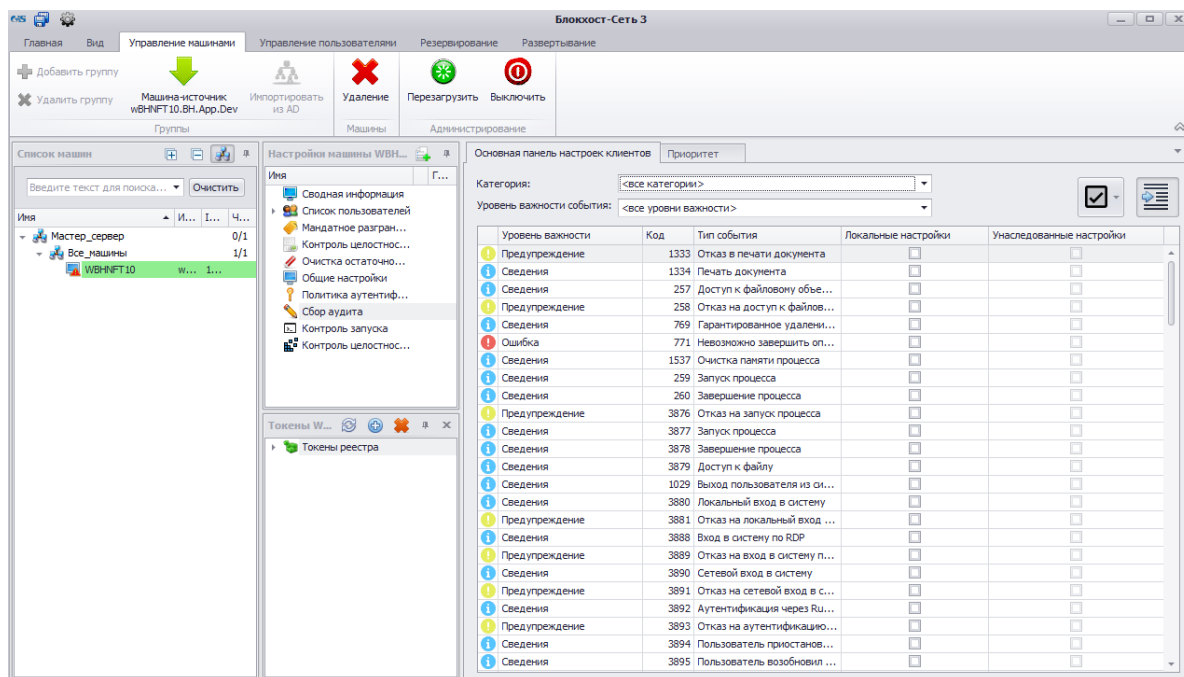


Рисунок 4.9 – Настройка сбора аудита в консоли управления политиками сервера

Вкладка **Основная панель настроек клиентов** содержит полный список событий, регистрируемых на клиентах Блокхост-Сеть.

Для каждого события в списке отображается информация:

- «Уровень важности» - уровень важности события (возможны три варианта важности: Сведения, Предупреждение или Ошибка);
- «Код» - код типа события;
- «Тип события» - краткое описание типа события;
- «Локальные настройки» - события, отобранные для сбора локально на выбранном сервере;
- «Унаследованные настройки» - события, отобранные для сбора на головном/родительском сервере и наследуемые для всех подчиненных серверов иерархии.

В верхней части вкладки **Основная панель настроек клиентов** расположены кнопки:

-  - кнопка, позволяющая выделить все/сбросить все/сбросить к рекомендованным событиям в списке;
-  - кнопка, позволяющая объединять/разделять отображение в списке (в зависимости от вида) **Локальных** и **Унаследованных настроек** в **Результирующие настройки**.
- кнопки выбора категории и уровня важности события, позволяющие отфильтровать список событий по заданному значению:
 - о **Категория** - выборка событий, относящихся только к заданной категории (значение <все категории>, установленное по умолчанию, отфильтрует список событий по всем категориям).
 - о **Уровень важности события** - выборка событий только с заданным уровнем важности (значение <все уровни важности>, установленное по умолчанию, отфильтрует список событий по всем уровням важности).

Для выбора собираемых на сервере событий необходимо для каждого, требуемого к сбору, события установить флаг **Локальные настройки**. При этом все события с серверов и клиентских компьютеров, подчиненных текущему серверу для которых установлен параметр **Локальные настройки**, будут собираться локально на выбранном сервере.

В параметре **Унаследованные настройки** отображаются все события, отобранные для сбора на головном/родительском сервере и наследуемые для выбранного сервера и всех подчиненных ему серверов. Параметр недоступен для редактирования.

Логика настройки сбора событий сервера описана в таблице 4.1.

Таблица 4.1. – Сбор событий в зависимости от локальных и унаследованных настроек сервера

Параметр «Локальные настройки»	Параметр «Унаследованные настройки»	Параметр «Результирующие настройки»	Описание сбора событий
Да	Нет	Да	События заданного типа собираются на выбранном сервере со всех подчиненных серверов. Передача на родительский сервер не осуществляется.
Да	Да	Да	События заданного типа собираются на выбранном сервере со всех подчиненных серверов. Передача на родительский сервер осуществляется.

Нет	Да	Да	События заданного типа собираются на выбранном сервере со всех подчиненных серверов. Передача на родительский сервер осуществляется. При отмене сбора события заданного типа на родительском сервере, сбор на выбранном сервере осуществляться не будет.
Нет	Нет	Нет	События заданного типа не собираются и не передаются.



В SIEM-систему экспортируются только события, заданные в настройках **Сбора аудита** головного сервера, наследуемые всеми подчиненными серверами.



При установке в параметрах сервера флага **Выполнять экспорт событий аудита в SIEM-систему** на подчиненном сервере, экспортируются только события, заданные на головном сервере, вне зависимости от уровня иерархии и наследовании настроек родительских серверов.

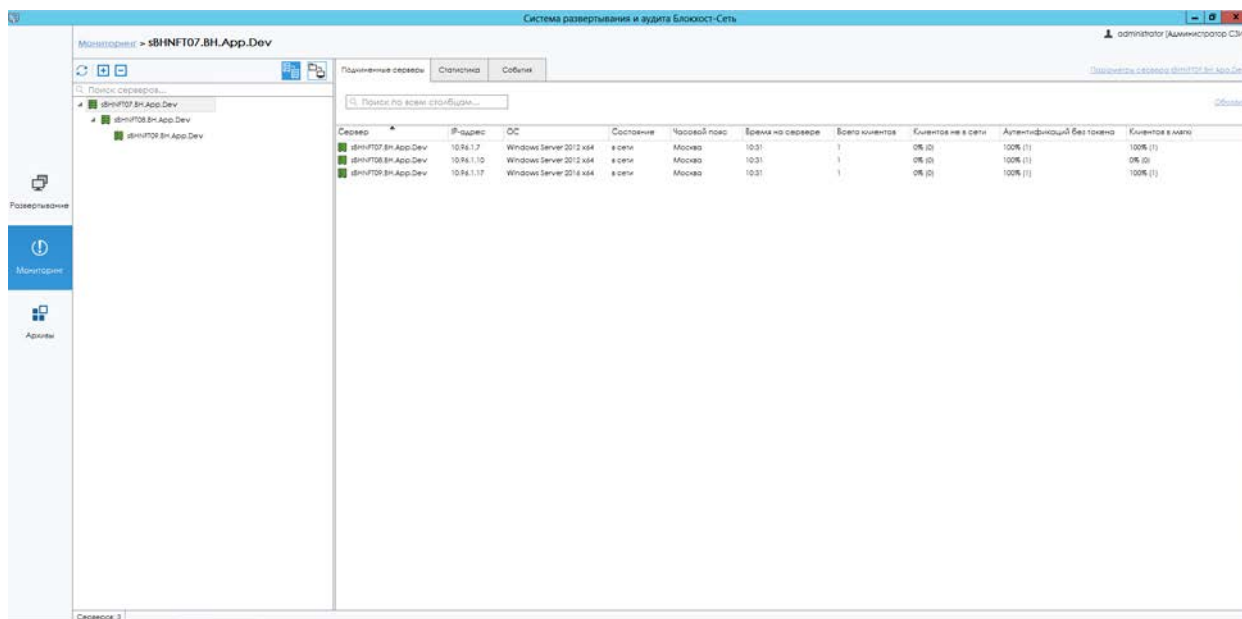
4.4 Аудит серверов

При выборе в дереве иерархии сервера, правая часть окна будет содержать информацию о выбранном сервере: список подчиненных серверов, сводную статистику по клиентам сервера, список событий, зафиксированный на клиентах, и настройку архивации собранных данных. При этом для удобства просмотра вся информация разделена на вкладки:

- **Подчиненные серверы;**
- **Статистика;**
- **События.**

4.4.1 Вкладка «Подчиненные серверы»

Вкладка **Подчиненные серверы** содержит список всех подчиненных серверов, находящихся в прямом или косвенном подчинении выбранному серверу, а также сам выделенный сервер (рисунок 4.10).

Рисунок 4.10 – Вкладка **Подчиненные серверы**

Для каждого сервера в списке отображается информация:

- «Сервер» - DNS имя сервера;
- «IP-адрес» - IP-адрес сервера;
- «ОС» - информация о версии и разрядности ОС;
- «Состояние» - сетевой статус соответствующего сервера (в сети/не в сети);
- «Часовой пояс» - часовой пояс выбранного сервера, а также разница между часовым поясом сервера, на котором работает администратор и часовым поясом выбранного сервера (если серверы находятся в одном часовом поясе, разница во времени не отображается);
- «Время на сервере» - время на выбранном сервере с учетом разницы часовых поясов;
- «Всего клиентов» - количество клиентов Блокхост-Сеть, зарегистрированных на соответствующем сервере;
- «Клиентов не в сети» - процентное соотношение клиентов, находящихся в состоянии «не в сети» к общему количеству клиентов, и соответствующее количество таких клиентов;
- «Аутентификаций без токена» - процентное соотношение клиентов, с типами аутентификации «Аутентификация Windows» и «По паролю (механизм Блокхост-Сеть)» к общему количеству клиентов, и соответствующее количество таких клиентов;
- «Клиентов в мягком режиме» - процентное соотношение клиентов, работающих в режиме «мягкий режим» к общему количеству клиентов, и соответствующее количество таких клиентов.

Для удобства просмотра информации администратор безопасности может сортировать список объектов в каждом столбце. Объекты выбранного столбца сортируются по возрастанию/убыванию при щелчке левой кнопкой мыши на заголовке столбца. Сортировка по выбранному столбцу выделяется пиктограммами «^»/«v» в заголовке столбца. По умолчанию список подчиненных серверов сортируется по DNS имени сервера (рисунок 4.11).

Подчиненные серверы

Статистика

Запросы

Настройки архивации

Поиск по всем столбцам...

Сервер	/	IP-адрес	ОС	Состояние	Часовой пояс	Время на сервере	Всего клиентов
 s8HNFT06.BH.App.Dev		10.96.1.8	Windows Server 2008 R2 x64	в сети	Москва	12:41	2
 s8HNFT07.BH.App.Dev		10.96.1.9	Windows Server 2012 x64	в сети	Москва	12:41	2
 s8HNFT08.BH.App.Dev		10.96.1.10	Windows Server 2012 x64	в сети	Москва	12:41	1
 s8HNFT10.BH.App.Dev		10.96.1.19	Windows Server 2016 Technical Preview x64	в сети	Москва	12:41	72

Рисунок 4.11 – Сортировка в списке подчиненных серверов

Для каждого подчиненного сервера в списке доступно контекстное меню (рисунок 4.12) содержащее пункты:

- **Перейти к серверу** – осуществляет переход к выбранному серверу в дереве иерархии;
- **Открыть консоль управления политиками сервера** – осуществляет переход в консоль управления политиками выбранного сервера;
- **Запустить внеплановую загрузку событий аудита** – запуск внепланового сбора событий аудита. Содержит подпункты:
 - **С подчиненных серверов** – для внепланового сбора событий аудита с подчиненных серверов;
 - **С клиентских компьютеров** – для внепланового сбора событий аудита с клиентских компьютеров выбранного сервера.
- **Параметры сервера** – переход к окну, содержащему общую информацию о сервере и настройку сбора событий с подчиненных серверов и клиентских компьютеров сервера (подробнее см. пункт «4.4.5 Параметры сервера»).

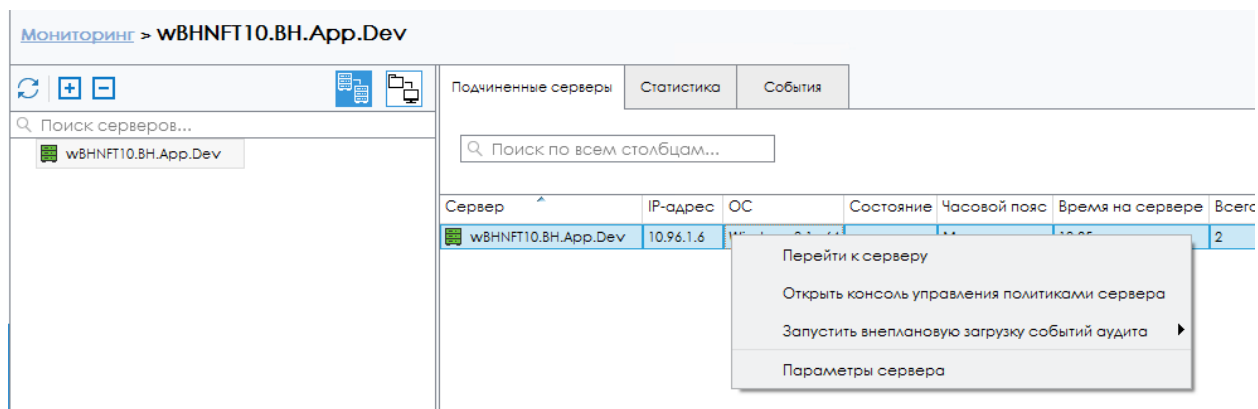


Рисунок 4.12 – Контекстное меню выбранного сервера

В верхней части окна, над именами колонок располагается поле ввода критериев отбора объектов из списка **Поиск по всем столбцам...**. Проверка соответствия заданного в поле ввода значения осуществляется по значениям сразу всех колонок (рисунок 4.13).

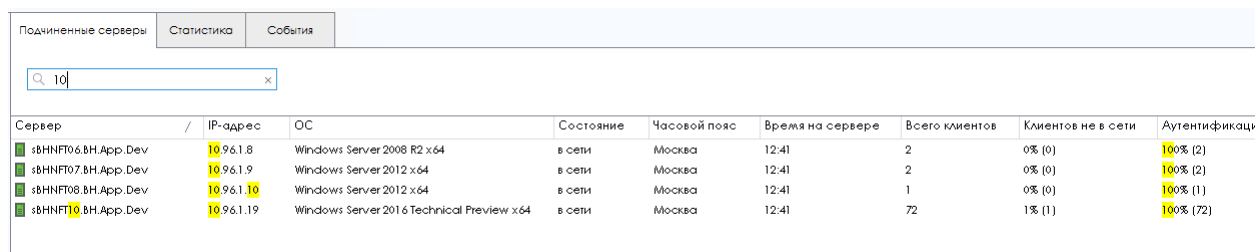


Рисунок 4.13 – Поиск по всем столбцам списка подчиненных серверов

4.4.2 Вкладка «Статистика»

Во вкладке **Статистика** отображается сводная статистика только по выбранному серверу или с учетом всех подчиненных серверов, находящимся в прямом или косвенном подчинении выбранному серверу (рисунок 4.14).

Сводная статистика только по выбранному серверу предполагает отображение событий аудита, в соответствии с заданными в консоли управления политиками сервера настройками, собранных только с клиентских компьютеров выбранного сервера, подчиненных ему напрямую.

Сводная статистика с учетом всех подчиненных серверов предполагает отображение событий аудита, в соответствии с заданными в консоли управления политиками сервера настройками, собранных и с клиентских компьютеров выбранного сервера и со всех подчиненных серверов, находящихся на любом нижестоящем уровне иерархии выбранного сервера.



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



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

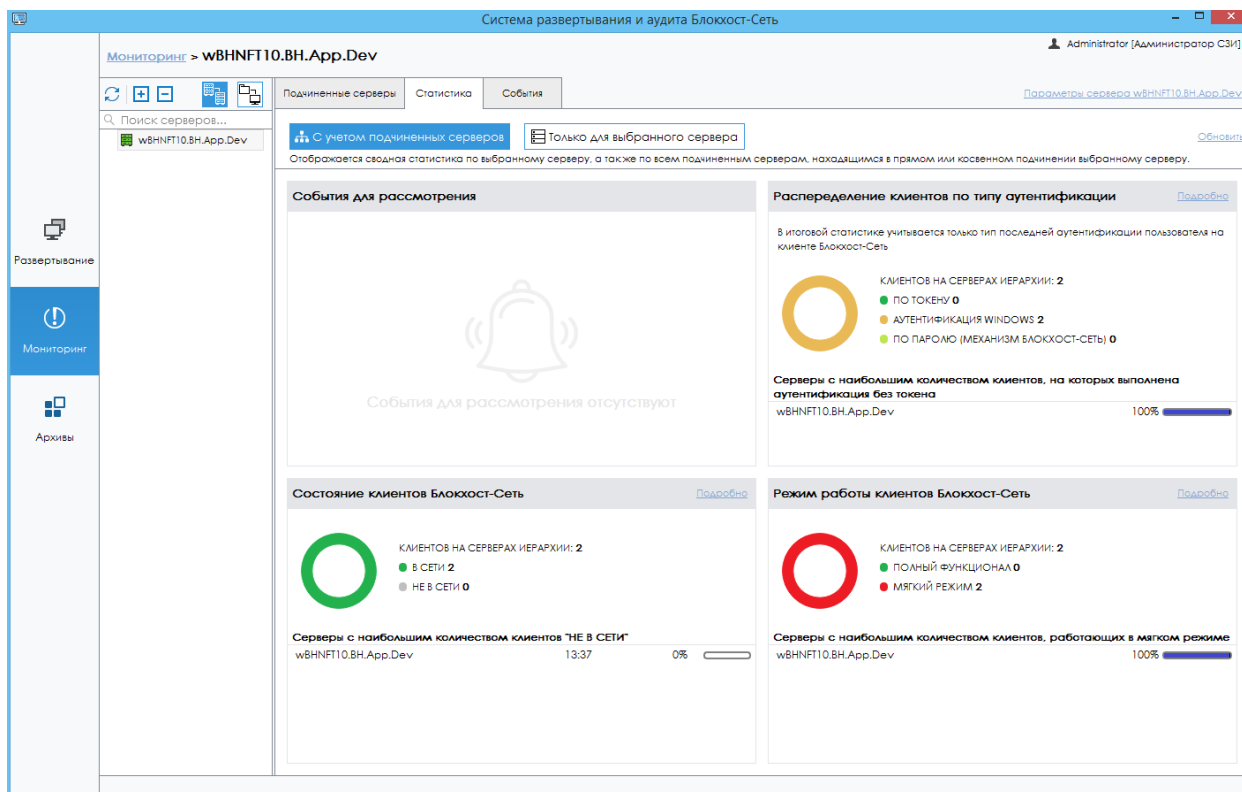


Рисунок 4.14 – Вкладка **Статистика**

По умолчанию, во вкладке **Статистика** отображается сводная статистика с учетом всех подчиненных серверов. Для просмотра сводной статистики только по выбранному в дереве иерархии серверу, необходимо нажать кнопку **Только для выбранного сервера**, расположенную в верхней части вкладки (рисунок 4.14).

События, информация о которых отражена во вкладке **Статистика**, поделены на четыре раздела:

- **События для рассмотрения** (наличие неактивных шаблонов клиентов и ошибок при синхронизации политик);
- **Распределение клиентов по типу аутентификации;**
- **Состояние клиентов Блокхост-Сеть;**
- **Режим работы клиентов Блокхост-Сеть.**

Разделы **Распределение клиентов по типу аутентификации**, **Состояние клиентов Блокхост-Сеть** и **Режим работы клиентов Блокхост-Сеть** имеют схожую структуру и содержат общие элементы (рисунок 4.15):

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

компьютерах серверов.

- 2) Общее количество клиентов на серверах иерархии.
- 3) Возможные значения, которые может принимать контролируемый параметр аудита и количество клиентов, с тем или иным значением параметра.
- 4) Перечень из 5-и серверов, имеющих худшие показатели контролируемого параметра и, соответственно, требующих наиболее пристального внимания администратора.
- 5) Кнопку **Подробнее**, открывающую окно, содержащее полный список клиентов Блокхост-Сеть и детальную информацию по каждому контролируемому параметру.

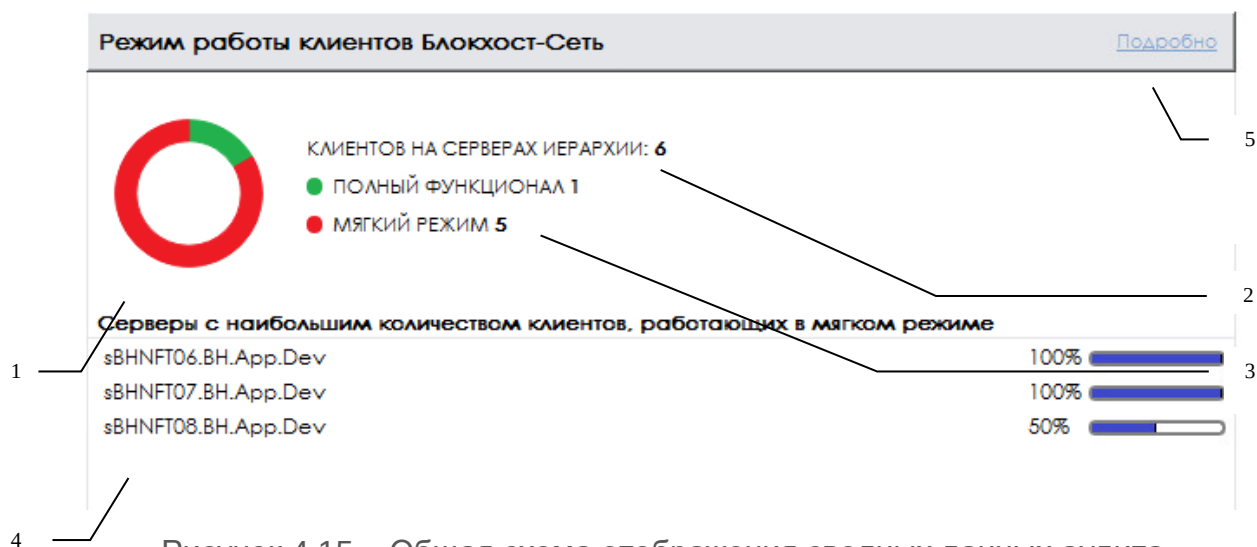


Рисунок 4.15 – Общая схема отображения сводных данных аудита

4.4.2.1 Распределение клиентов по типу аутентификации

В разделе **Распределение клиентов по типу аутентификации** отображается информация о типе аутентификации пользователя на клиенте (рисунок 4.16). Для пользователей на клиенте Блокхост-Сеть возможны следующие варианты аутентификации:

- аутентификация по токenu (с применением аппаратного идентификатора, (двухфакторная аутентификация);
- аутентификация по паролю (использование механизма Блокхост-Сеть, без использования аппаратного идентификатора);
- аутентификация ОС Windows (аутентификация стандартными средствами ОС).

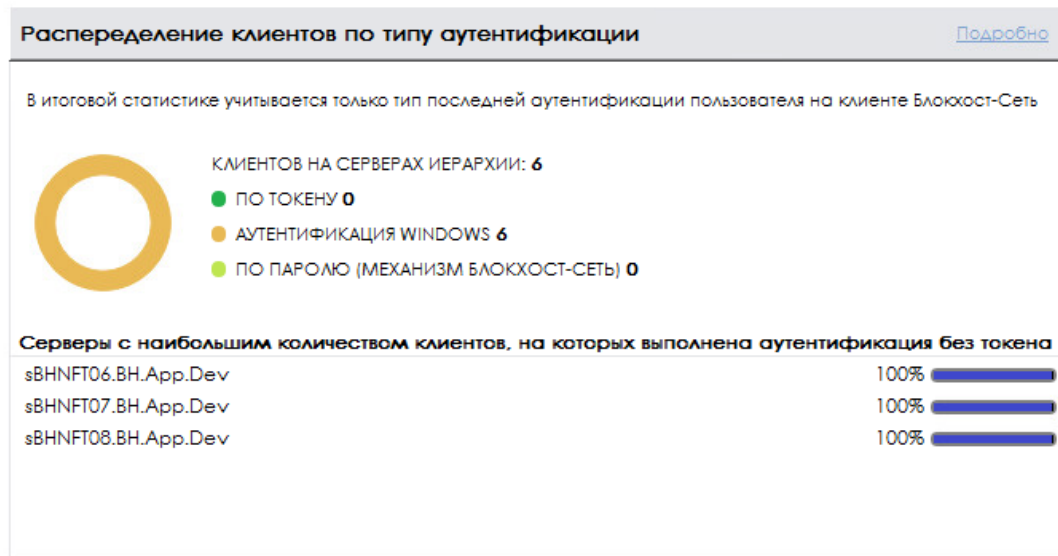


Рисунок 4.16 – Распределение клиентов по типу аутентификации



Необходимо учитывать, что в итоговой статистике учитывается только последний тип аутентификации пользователя на клиенте Блокхост-Сеть.

В нижней части окна отображается список из пяти серверов с наибольшим количеством клиентов, на которых была выполнена аутентификация пользователя без токена.

Для просмотра всего списка серверов, необходимо перейти в окно **Распределение клиентов по типу аутентификации пользователей** по кнопке **Подробнее** (рисунок 4.17).

Распределение клиентов по типу аутентификации пользователей

Поиск по имени сервера

Действие

Сервер	Процент аутентификаций без токена	Всего клиентов	По токену	Аутентификация WINDOWS
wBHNFT10.BH.App.Dev	100%	2	0	2

Заккрыть

Рисунок 4.17 – Полный список распределения клиентов по типу аутентификации

Для каждого сервера в списке в окне **Распределение клиентов по типу аутентификации пользователей** отображается информация:

- «Сервер» - DNS имя сервера;
- «Процент аутентификаций без токена» - процентное соотношение количества

аутентификаций пользователей без токена (совокупность типов «Аутентификация Windows» и «По паролю (механизм Блокхост-Сеть)») к общему числу клиентов;

- «Всего клиентов» – общее количество клиентов Блокхост-Сеть, зарегистрированных на соответствующем сервере;
- «По токену» – значение, определяющее количество аутентификаций пользователей на клиентах с применением аппаратного идентификатора;
- «Аутентификация Windows» – значение, определяющее количество аутентификаций пользователей на клиентах, использующих для аутентификации стандартные средства ОС;
- «По паролю (механизм Блокхост-Сеть)» - значение, определяющее количество аутентификаций пользователя с использованием механизма Блокхост-Сеть, без применения аппаратного идентификатора.

Для удобства просмотра информации администратор безопасности может сортировать список объектов в каждом столбце по возрастанию или убыванию. Объекты выбранного столбца сортируются по возрастанию/убыванию при щелчке левой кнопкой мыши на заголовке столбца. Сортировка по выбранному столбцу выделяется пиктограммами «^»/«v» в заголовке столбца. По умолчанию, список серверов сортируется по DNS имени сервера.

Для каждого сервера в списке доступно контекстное меню содержащее пункты:

- **Перейти к серверу** – осуществляет переход к выбранному серверу в дереве иерархии;
- **Открыть консоль управления политиками сервера** – осуществляет переход в консоль управления политиками выбранного сервера.

Действия, аналогичные содержащимся в контекстном меню, можно выполнить нажав на кнопку **Действие**, расположенную над списком серверов (рисунок 4.18). При нажатии на кнопку раскрывается список, состоящий из пунктов **Перейти к серверу** и **Открыть консоль управления политиками сервера**, описание которых приведено выше.

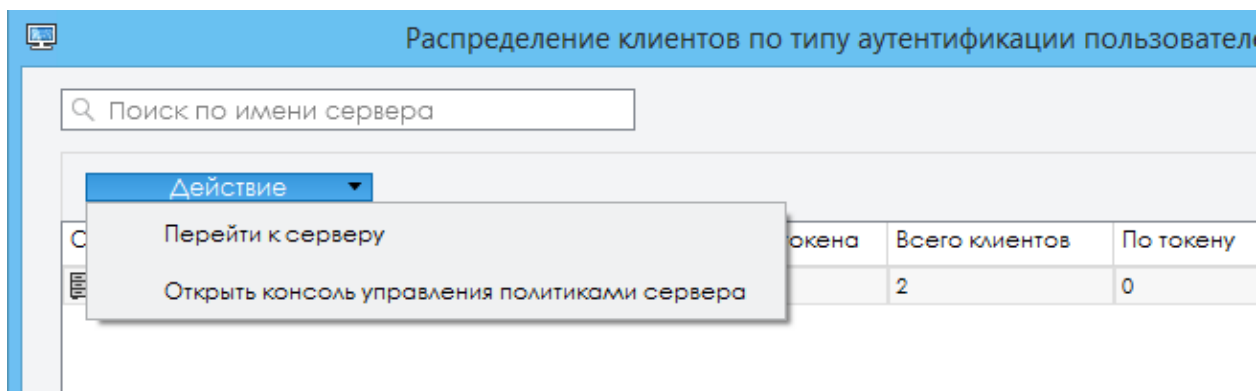


Рисунок 4.18 – Действия, доступные для серверов из списка

В верхней части окна, над списком серверов, располагается поле ввода критериев отбора объектов из списка **Поиск по имени сервера**. Проверка соответствия введенного в поле ввода значения осуществляется по значениям сразу всех колонок.

4.4.2.2 Состояние клиентов Блокхост-Сеть

В разделе **Состояние клиентов Блокхост-Сеть** отображается информация о нахождении в сети клиентов (рисунок 4.19). Клиенты Блокхост-Сеть могут находиться в состояниях:

- в сети (клиенты Блокхост-Сеть в состоянии online);
- не в сети (клиенты Блокхост-Сеть в состоянии offline).

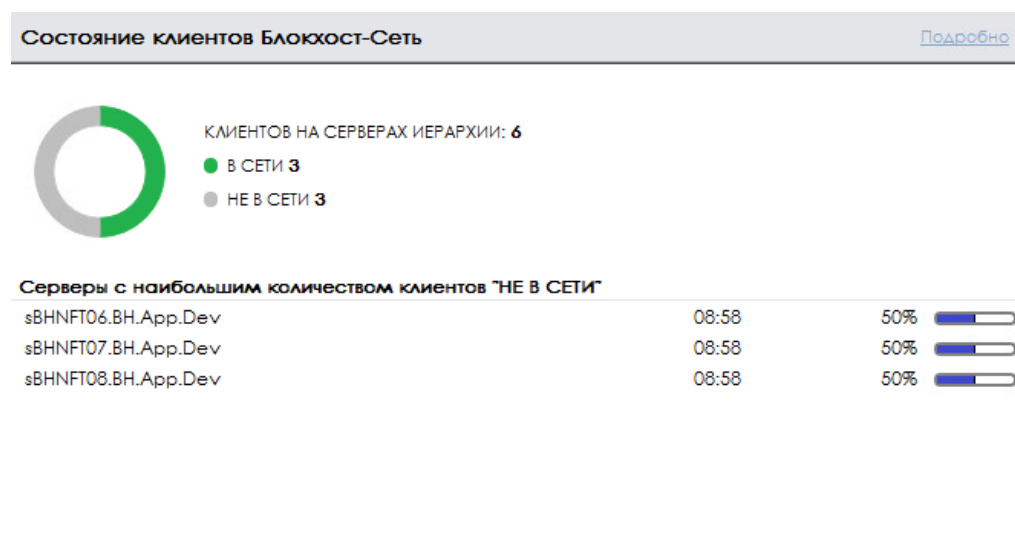


Рисунок 4.19 – Состояние клиентов в сети

В нижней части окна отображается список из пяти серверов с наибольшим количеством клиентов, находящихся offline. Для просмотра всего списка серверов, необходимо перейти в окно **Состояние клиентов Блокхост-Сеть** по кнопке **Подробнее** (рисунок 4.20).

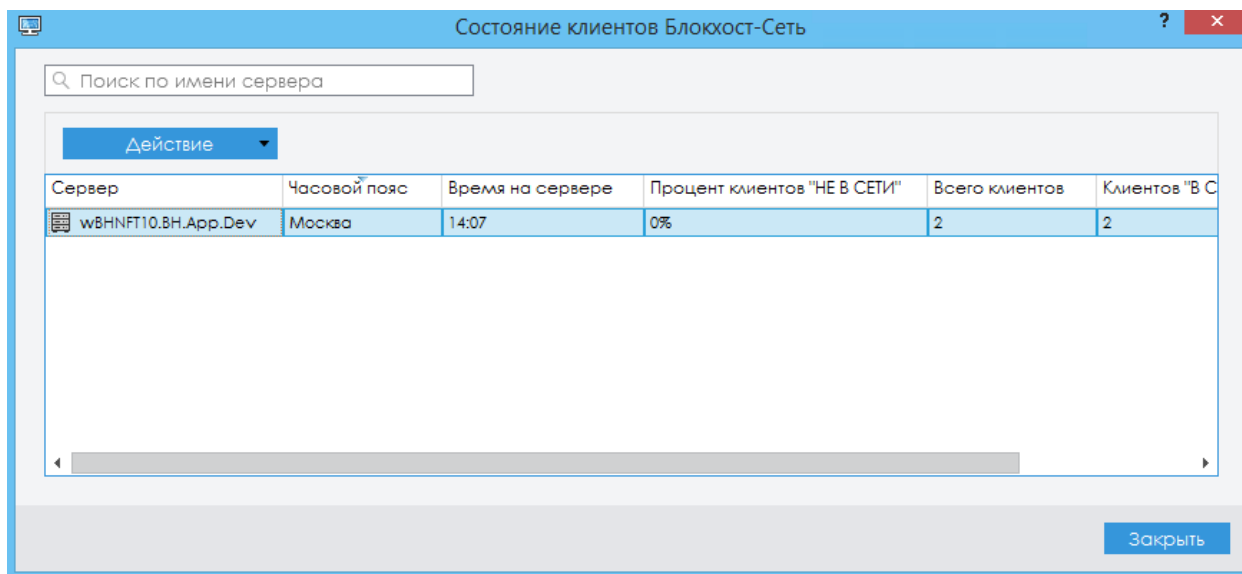


Рисунок 4.20 – Полный список клиентов и их состояние в сети

Для каждого сервера в списке в окне **Состояние клиентов Блокхост-Сеть** отображается информация:

- «Сервер» - DNS имя сервера;
- «Часовой пояс» - часовой пояс выбранного сервера, а также разница между часовым поясом сервера, на котором работает администратор и часовым поясом выбранного сервера (если серверы находятся в одном часовом поясе, разница во времени не отображается);
- «Время на сервере» - время на соответствующем сервере с учетом разницы часовых поясов;
- «Процент клиентов "НЕ В СЕТИ"» - процентное соотношение количества клиентов, находящихся в состоянии «не в сети», к общему количеству клиентов (округление производится в меньшую сторону при $\geq 50\%$, в большую сторону при $< 50\%$);
- «Всего клиентов» – общее количество клиентов Блокхост-Сеть, зарегистрированных на соответствующем сервере;
- «Клиентов "В СЕТИ"» – количество клиентов, находящихся в состоянии online;
- «Клиентов "НЕ В СЕТИ"» – количество клиентов, находящихся в состоянии offline.

Сортировка объектов в списке, элементы контекстного меню, кнопка **Действие** и поиск по столбцам списка осуществляется аналогично для всех сводных областей вкладки **Статистика**. Подробное описание работы с ними описано в подпункте «4.4.2.1 Распределение клиентов по типу аутентификации».

4.4.2.3 Режим работы клиентов Блокхост-Сеть

В разделе **Режим работы клиентов Блокхост-Сеть** отображается информация о режиме работы клиентов Блокхост-Сеть (рисунок 4.21). Возможные режимы работы клиентов:

- полный функционал - все механизмы разграничения доступа и защиты информации, настроенные в СЗИ, функционируют в полном объеме;
- мягкий режим – доступ пользователей к ресурсам, запрещенным настройками СЗИ, разрешен; осуществляется только регистрация событий, связанных с попытками доступа к запрещенной информации.

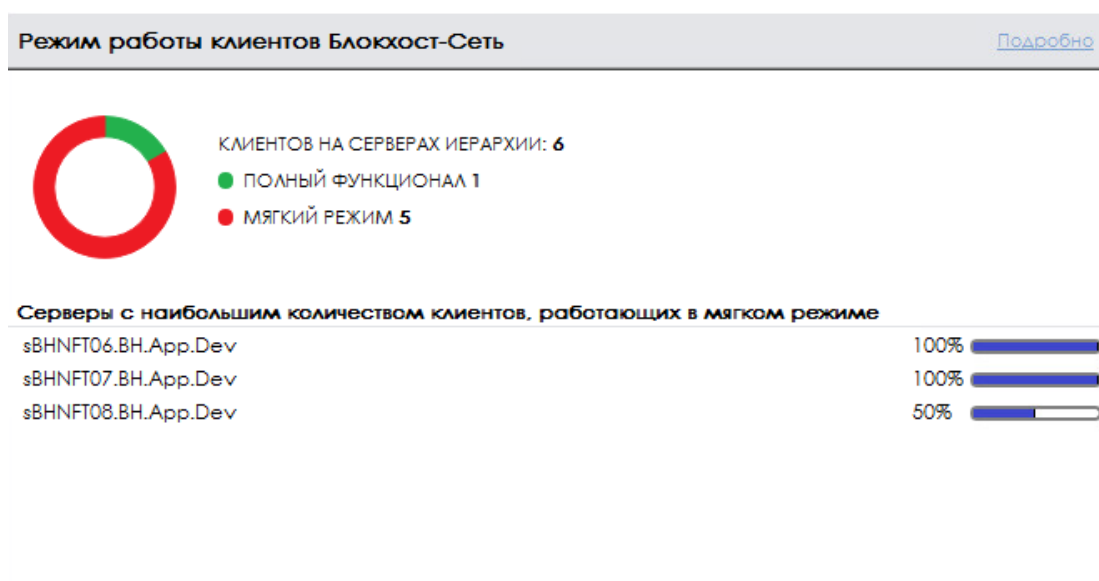


Рисунок 4.21 – Режим работы клиентов Блокхост-Сеть

В нижней части окна отображается список из пяти серверов с наибольшим количеством клиентов, работающих в мягком режиме. Для просмотра всего списка серверов, необходимо перейти в окно **Режим работы клиентов Блокхост-Сеть** по кнопке **Подробнее** (рисунок 4.22).

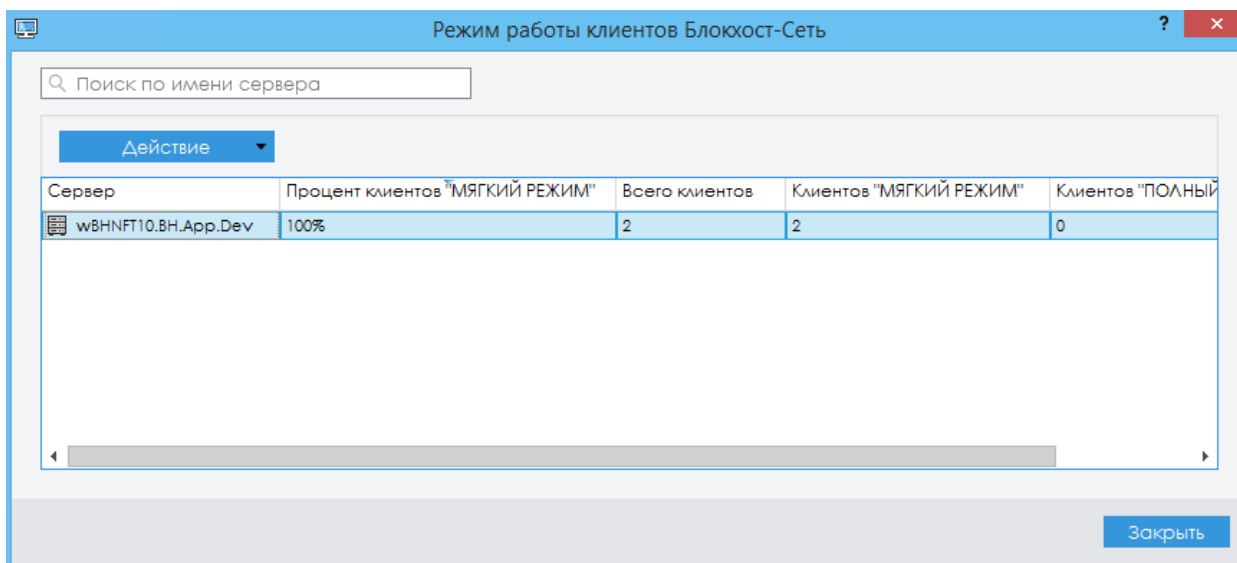


Рисунок 4.22 – Полный список клиентов и их режим работы

Для каждого сервера в списке в окне **Режим работы клиентов Блокхост-Сеть** отображается информация:

- «Сервер» - DNS имя сервера;
- «Процент клиентов "МЯГКИЙ РЕЖИМ"» - процентное соотношение количества клиентов, работающих в режиме "МЯГКИЙ РЕЖИМ", к общему количеству клиентов сервера;
- «Всего клиентов» — общее количество клиентов Блокхост-Сеть, зарегистрированных на соответствующем сервере;
- «Клиентов "МЯГКИЙ РЕЖИМ"» — значение, определяющее количество клиентов, работающих в режиме "МЯГКИЙ РЕЖИМ";
- «Клиентов "ПОЛНЫЙ ФУНКЦИОНАЛ"» — значение, определяющее количество клиентов, работающих в режиме "ПОЛНЫЙ ФУНКЦИОНАЛ".

Сортировка объектов в списке, элементы контекстного меню, кнопка **Действие** и поиск по столбцам списка осуществляется аналогично для всех сводных областей вкладки **Статистика**. Подробное описание работы с ними описано в подпункте «4.4.2.1 Распределение клиентов по типу аутентификации».

4.4.2.4 События для рассмотрения

В разделе **События для рассмотрения** (рисунок 4.23) отображается информация:

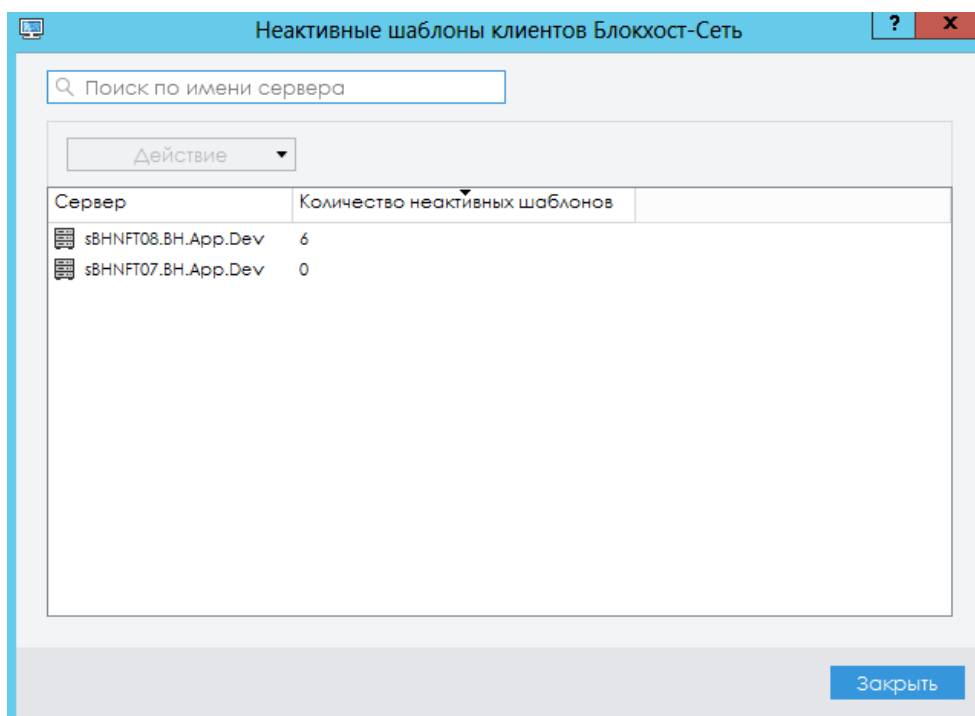
- о наличии неактивных шаблонов клиентов Блокхост-Сеть;
- о наличии ошибок при синхронизации политик.

Информация представлена в виде списка, содержащего наименование события и количество серверов, на которых данное событие зарегистрировано.

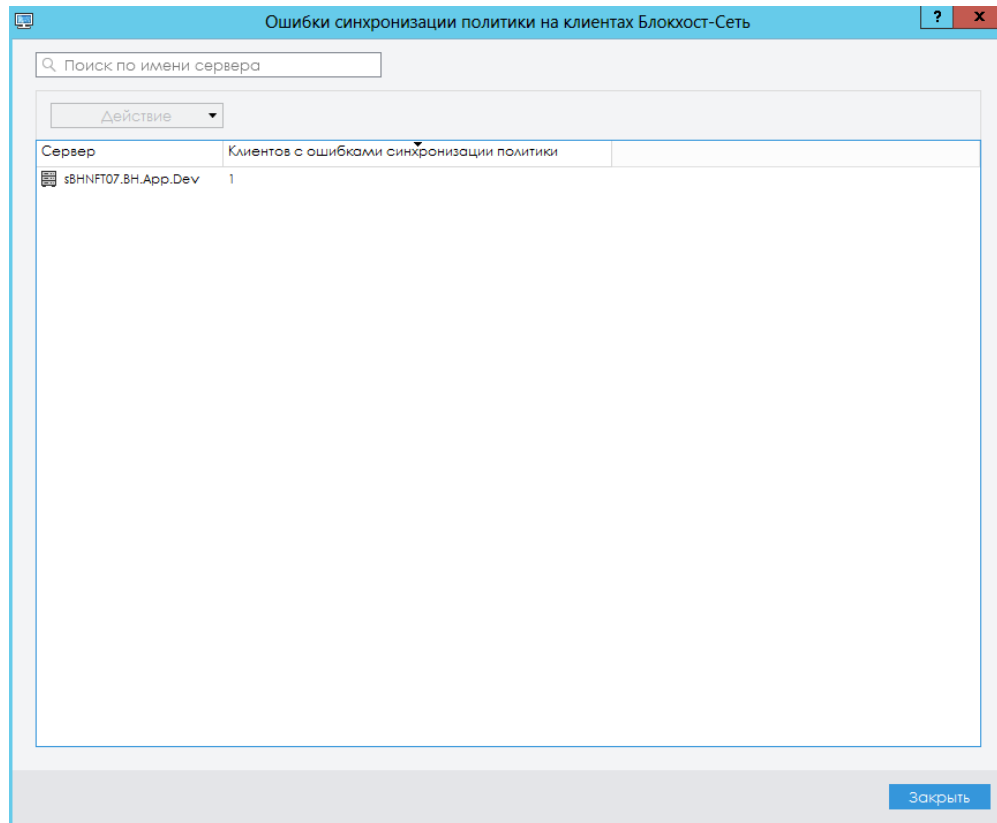
События для рассмотрения		
Неактивные шаблоны клиентов	1 сервер	Подробнее
Ошибки синхронизации политики	1 сервер	Подробнее

Рисунок 4.23 – События для рассмотрения

Для просмотра всего списка серверов, на которых зарегистрированы данные события, необходимо перейти в окна **Неактивные шаблоны клиентов Блокхост-Сеть** или **Ошибки синхронизации политики на клиентах Блокхост-Сеть** по кнопке **Подробнее**, расположенной в строке с событием (рисунок 4.24 а, б).



а)



б)

Рисунок 4.24 – Полный список клиентов с ошибками синхронизации политик/с неактивными шаблонами

Для каждого сервера в списке в окнах **Неактивные шаблоны клиентов Блокхост-Сеть** / **Ошибки синхронизации политики на клиентах Блокхост-Сеть**, в зависимости от выбранного события в разделе **События для рассмотрения**, отображается информация:

- «Сервер» - DNS имя сервера;
- «Количество неактивных шаблонов клиентов» / «Клиентов с ошибками синхронизации политики» - значения, определяющие количество неактивных шаблонов клиентов или количество клиентов с ошибками синхронизации политик, в зависимости от выбранного события в разделе **События для рассмотрения**.

Сортировка объектов в списке, элементы контекстного меню, кнопка **Действие** и поиск по столбцам списка осуществляется аналогично для всех сводных областей вкладки **Статистика**. Подробное описание работы с ними описано в подпункте «4.4.2.1 Распределение клиентов по типу аутентификации».

4.4.3 Вкладка «События»

Вкладка **События** предназначена для отслеживания событий, заданных в консоли управления политиками сервера настройками, 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 4.25).

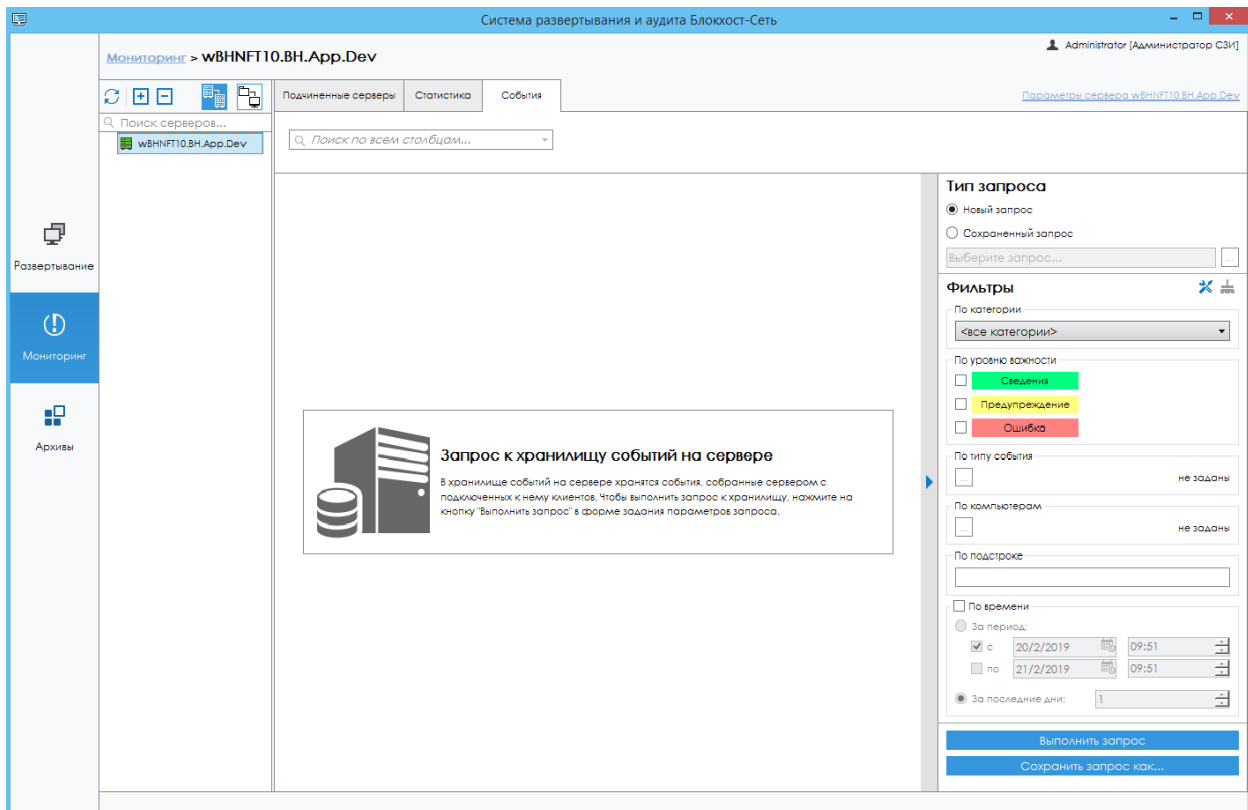


Рисунок 4.25 – Вкладка **События**

Обновление списка событий происходит при выполнении запроса и содержит информацию (рисунок 4.26):

- «Время» - дата и время момента фиксации произошедшего события;
- «Компьютер» - DNS имя компьютера;
- «Событие» - краткое описание зафиксированного события (полный перечень событий, фиксируемых в консоли СРиА приведен в Приложении 5 к документу «Средство защиты информации от несанкционированного доступа «Блокост-Сеть 3». Руководство администратора безопасности»);
- «Категория» - категория, которой принадлежит зафиксированное событие;
- «Уровень важности» - уровень важности зафиксированного события (сведения, предупреждения или ошибка).

Подчиненные серверы Статистика События [Параметры сервера w8NFT10.8H App Dev](#)

Поиск по всем столбцам... Результат запроса: 20 сообщений

Время	Компьютер	Событие	Категория	Уровень важности
09:30:08 17.12.2018	WBNNFT10	Открытие сессии управления по иерархии	События сервера СЗИ	Сведения
09:18:50 17.12.2018	WBNNFT10	Подключение клиента к серверу	События сервера СЗИ	Сведения
09:18:50 17.12.2018	WBNNFT10	Подключение к серверу	События клиента СЗИ	Сведения
09:18:50 17.12.2018	WBNNFT10	Подключение к головному серверу	События сервера СЗИ	Сведения
18:58:43 14.12.2018	WBNNFT10	Выход пользователя из системы	Аутентификация	Сведения
17:35:01 14.12.2018	WBNNFT10	Подключение к головному серверу	События сервера СЗИ	Сведения
17:34:35 14.12.2018	WBNNFT10	Отключение от головного сервера	События сервера СЗИ	Сведения
13:02:57 14.12.2018	WBNNFT10	Подключение к головному серверу	События сервера СЗИ	Сведения
13:02:55 14.12.2018	WBNNFT10	Отключение от головного сервера	События сервера СЗИ	Сведения
13:02:55 14.12.2018	WBNNFT10	Подключение к головному серверу	События сервера СЗИ	Сведения
13:02:54 14.12.2018	WBNNFT10	Изменение параметров работы СЗИ	Действия администратора СЗИ	Сведения
13:00:53 14.12.2018	WBNNFT10	Запуск консоли СЗИ	Действия администратора СЗИ	Сведения
13:00:47 14.12.2018	WBNNFT10	Создание задачи на установку произвольной программы	Система развертывания	Сведения
13:00:47 14.12.2018	WBNNFT10	Создание задачи на установку агента системы развертывания	Система развертывания	Сведения
13:00:00 14.12.2018	WBNNFT10	Подключение клиента к серверу	События сервера СЗИ	Сведения
13:00:00 14.12.2018	WBNNFT10	Подключение к серверу	События клиента СЗИ	Сведения
09:18:49 17.12.2018	WBNNFT10	Отказ в подключении к серверу	События клиента СЗИ	Ошибка
17:34:59 14.12.2018	WBNNFT10	Отказ в установке соединения	События сервера СЗИ	Ошибка
17:34:51 14.12.2018	WBNNFT10	Отказ в установке соединения	События сервера СЗИ	Ошибка
17:34:49 14.12.2018	WBNNFT10	Отказ в установке соединения	События сервера СЗИ	Ошибка

Тип запроса

☐ Новый запрос

☒ Сохраненный запрос

Стандартные\За 30 дней

Фильтры

По категории: <все категории>

По уровню важности:

☐ Сведения

☐ Предупреждение

☐ Ошибка

По типу события: не заданы

По компьютерам: не заданы

По подстроке:

По времени:

☒ За период:

☒ с 20/2/2019 09:51

☐ по 21/2/2019 09:51

☒ За последние дни: 30

Выполнить запрос

Сохранить изменения

Сохранить запрос как...

Рисунок 4.26 – Список событий после выполнения запроса

В верхней части окна, над списком событий, располагается поле ввода критериев отбора объектов из списка **Поиск по всем столбцам...**. Проверка соответствия введенного в поле ввода значения осуществляется по значениям сразу всех колонок (рисунок 4.13).

При двойном щелчке мыши на выбранном событии в списке, внизу списка отобразится подробная информация о событии (рисунок 4.27).

Время	Компьютер	Событие	Категория	Уровень важности
09:30:08 17.12.2018	WBHNFT10	Открытие сессии управления по иерархии	События сервера СЗИ	Сведения
09:18:50 17.12.2018	WBHNFT10	Подключение клиента к серверу	События сервера СЗИ	Сведения
09:18:50 17.12.2018	WBHNFT10	Подключение к серверу	События клиента СЗИ	Сведения
09:18:50 17.12.2018	WBHNFT10	Подключение к головному серверу	События сервера СЗИ	Сведения
18:58:43 14.12.2018	WBHNFT10	Выход пользователя из системы	Аутентификация	Сведения
17:35:01 14.12.2018	WBHNFT10	Подключение к головному серверу	События сервера СЗИ	Сведения
17:34:35 14.12.2018	WBHNFT10	Отключение от головного сервера	События сервера СЗИ	Сведения
13:02:57 14.12.2018	WBHNFT10	Подключение к головному серверу	События сервера СЗИ	Сведения
13:02:55 14.12.2018	WBHNFT10	Отключение от головного сервера	События сервера СЗИ	Сведения
13:02:55 14.12.2018	WBHNFT10	Подключение к головному серверу	События сервера СЗИ	Сведения
13:02:54 14.12.2018	WBHNFT10	Изменение параметров работы СЗИ	Действия администратора СЗИ	Сведения
13:00:53 14.12.2018	WBHNFT10	Запуск консоли СЗИ	Действия администратора СЗИ	Сведения
13:00:47 14.12.2018	WBHNFT10	Создание задачи на установку произвольной программы	Система развертывания	Сведения
13:00:47 14.12.2018	WBHNFT10	Создание задачи на установку агента системы развертывания	Система развертывания	Сведения
13:00:00 14.12.2018	WBHNFT10	Подключение клиента к серверу	События сервера СЗИ	Сведения
13:00:00 14.12.2018	WBHNFT10	Подключение к серверу	События клиента СЗИ	Сведения
09:18:49 17.12.2018	WBHNFT10	Отказ в подключении к серверу	События клиента СЗИ	Ошибка
17:34:59 14.12.2018	WBHNFT10	Отказ в установке соединения	События сервера СЗИ	Ошибка
17:34:51 14.12.2018	WBHNFT10	Отказ в установке соединения	События сервера СЗИ	Ошибка
17:34:49 14.12.2018	WBHNFT10	Отказ в установке соединения	События сервера СЗИ	Ошибка

Подробная информация
Событие: изменение параметров работы СЗИ
Источник: BH\administrator
Изменения внес: серверная консоль
Изменения: Список изменений:
Настройки подключения к Мастер-серверу
Пароль подключения подчиненных серверов
Машины:
WBHNFT10
Группы машин:
Мастер_сервер (Изменение)
Механизмы:
Мандатное разграничение
Контроль целостности файлов
Очистка остаточной информации
Общие настройки
Политика аутентификации
Сбор аудита
Контроль запуска программ
Контроль целостности среды

Рисунок 4.27 – 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.

4.4.3.1 Выбор типа запроса

В области **Тип запроса** доступен выбор типа запроса:

- «Новый запрос» - при выборе типа запроса «Новый запрос», выполняется новая выборка по событиям серверов, при этом доступна настройка всех параметров запроса и запрос доступен к сохранению.
- «Сохраненный запрос» - позволяет выполнить запрос, сохраненный ранее.

Для выбора сохраненного запроса, необходимо установить переключатель в позицию **Сохраненный запрос** и выбрать запрос, сохраненный ранее. При нажатии на кнопку выбора сохраненного запроса, откроется окно, содержащее список сохраненных запросов (рисунок 4.28). При этом сохраненные запросы могут относиться к одному из типов:

- «Стандартные запросы» - запросы, предустановленные в консоли СРиА по умолчанию, не подлежащие редактированию.
- «Запросы, общие для всех серверов» - запросы, которые могут выполнены на любом сервере иерархии (в запросах этого типа не задан фильтр «по компьютерам»);

- «Запросы сервера <наименование сервера>» - запросы, которые могут быть выполнены только на том сервере, для которого они были созданы (в запросах этого типа задан фильтр «по компьютерам»).

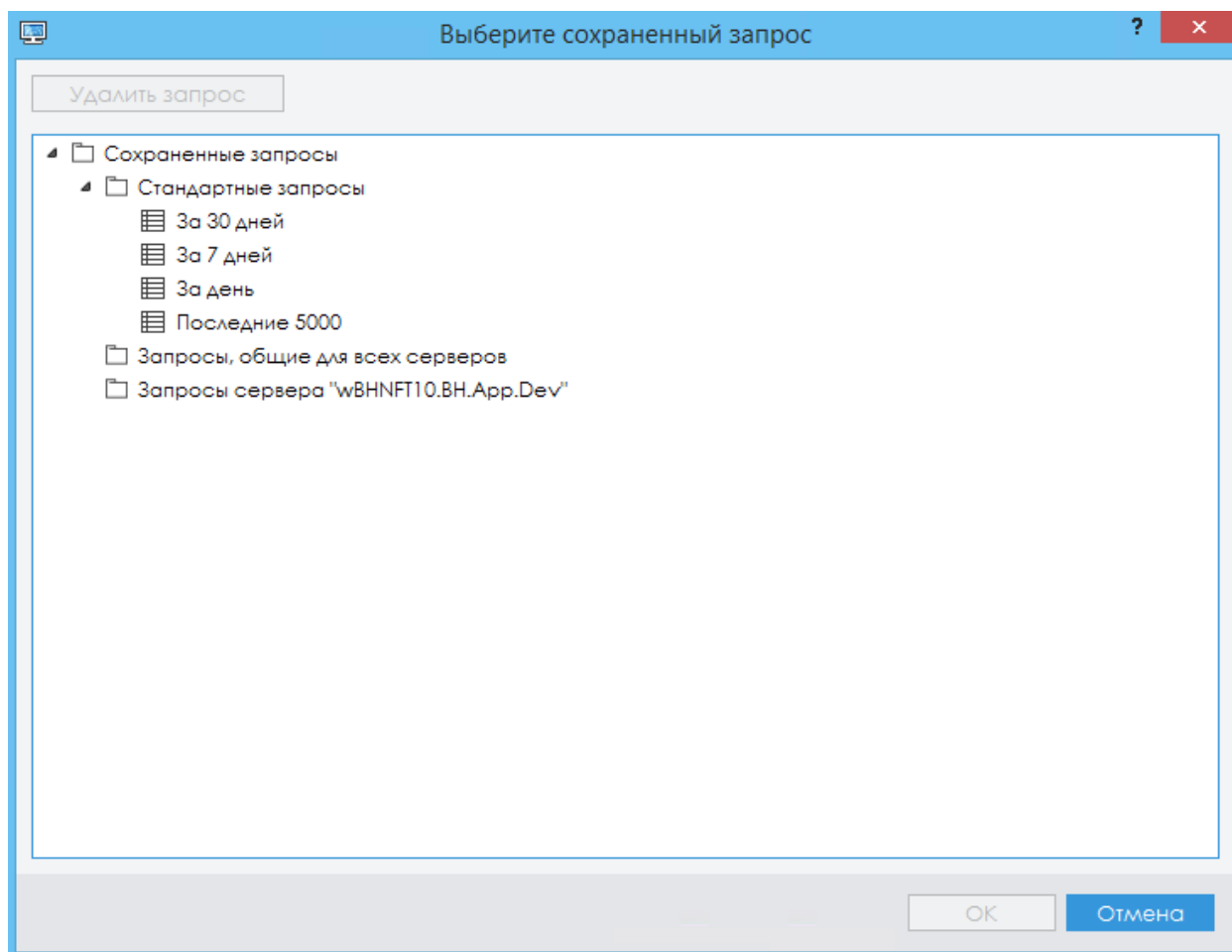


Рисунок 4.28 – Окно выбора сохраненного запроса

В верхней части окна расположена кнопка **Удалить запрос**, позволяющая удалить сохраненный запрос.



|| Операция удаления запроса типа «Стандартные запросы» недоступна.

Для выбора запроса необходимо перейти в нужный тип запроса, найти наименование запроса, который нужно выполнить и нажать кнопку **OK**. При этом в области фильтрации списка событий отобразятся все параметры выбранного запроса (рисунок 4.29).

Тип запроса

- ☐ Новый запрос
- ☒ Сохраненный запрос

Стандартные\Последние 5000

Фильтры



По категории

<все категории>

По уровню важности

- ☐ Сведения
- ☐ Предупреждение
- ☐ Ошибка

По типу события

...

не заданы

По компьютерам

...

не заданы

По подстроке

☐ По времени

☐ За период:

☒ с 20/2/2019 09:51

☐ по 21/2/2019 09:51

☒ За последние дни: 30

Выполнить запрос

Сохранить изменения

Сохранить запрос как...

Рисунок 4.29 – Отображение параметров сохраненного запроса

4.4.3.2 Настройка параметров запроса

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

- 1) «По категории» - выборка событий, относящихся только к заданной категории (значение <все источники>, установленное по умолчанию, отфильтрует список событий по всем категориям).
- 2) «По уровню важности» - выборка событий только с заданным уровнем важности.

3) «По типу событий» - выборка событий только указанных типов.

Для фильтрации по типу события, необходимо нажать на кнопку выбора типа события и в открывшемся окне выбрать в списке события, по которым нужно осуществить выборку (рисунок 4.30). В окне содержится информация:

- «Уровень важности» - уровень важности события (возможны три варианта важности: Сведения, Предупреждение или Ошибка);
- «Имя» - краткое описание типа события;
- «Код» - код типа события.

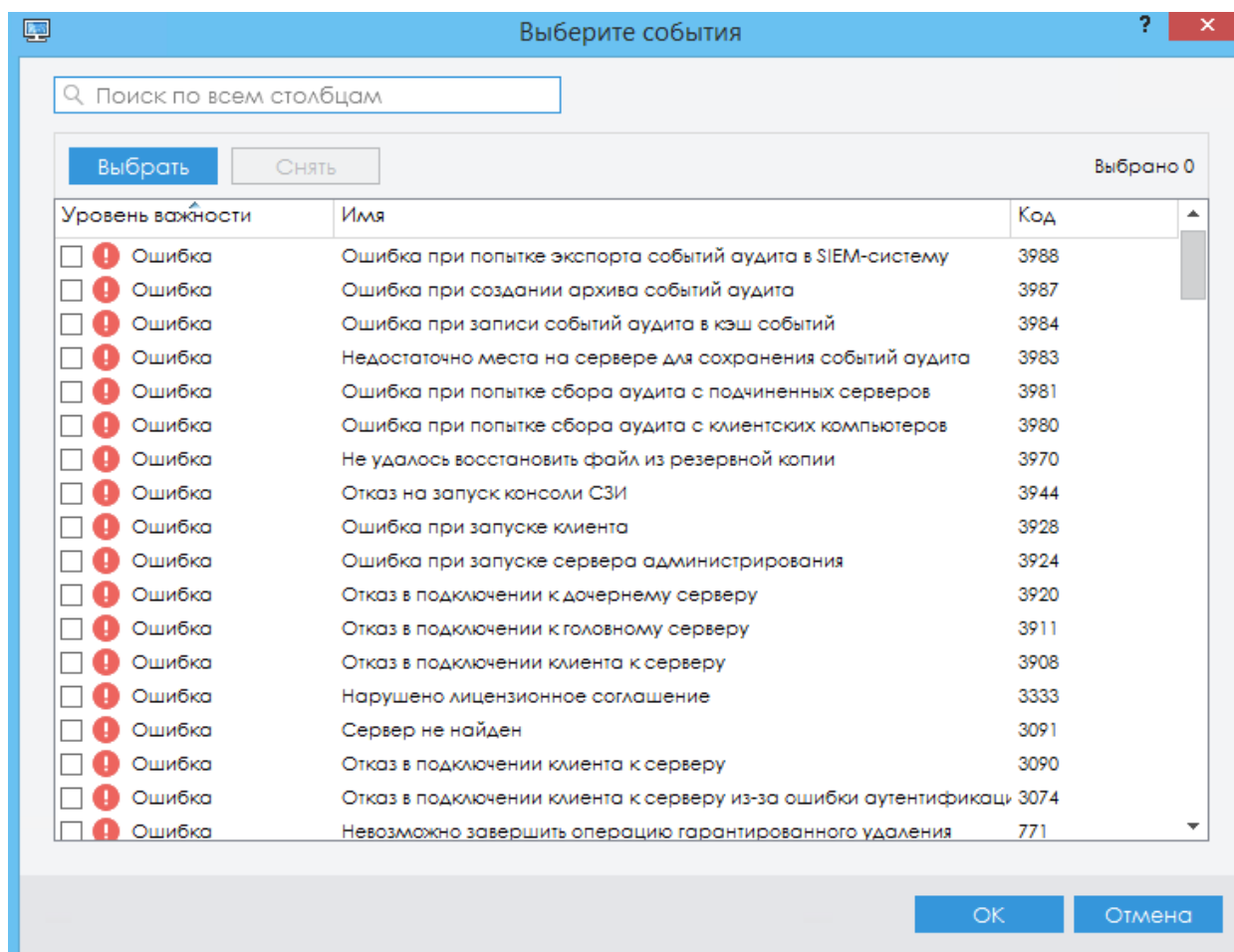


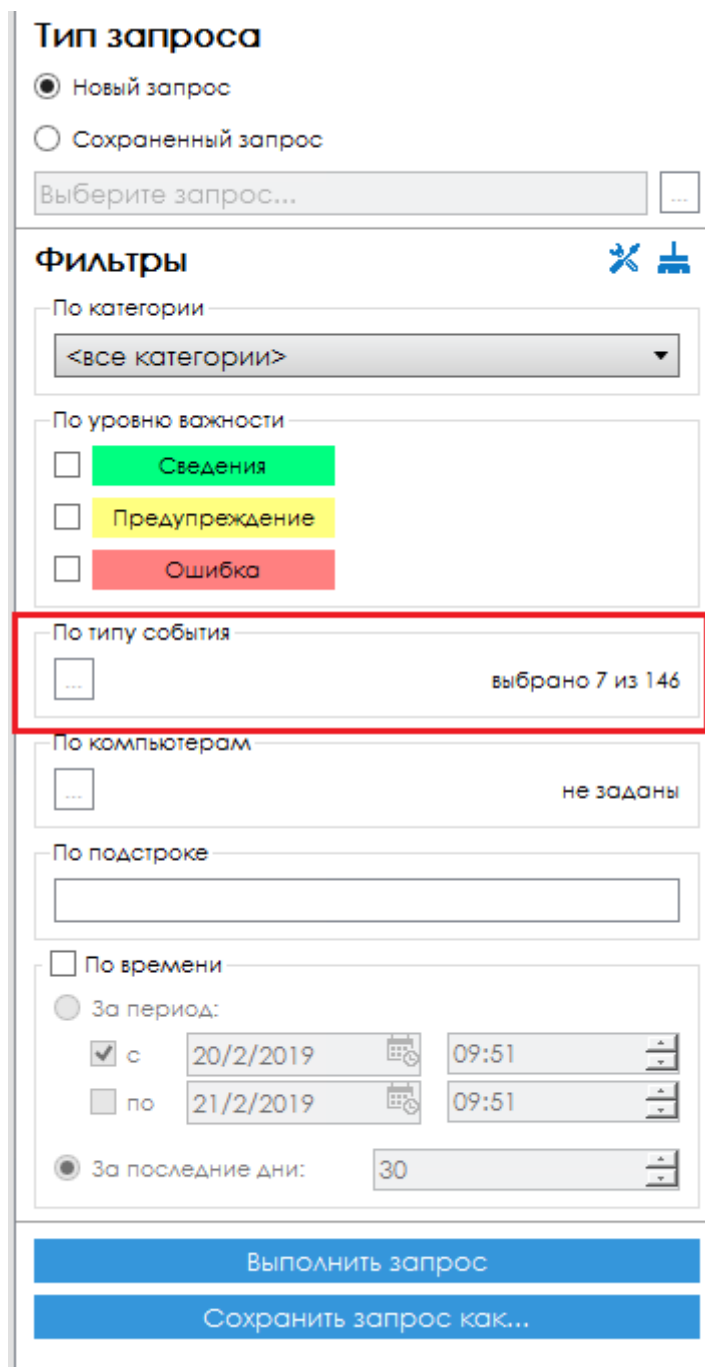
Рисунок 4.30 – Список типов событий



Полный перечень фиксируемых событий приведен в Приложении 5 к документу «Средство защиты информации от несанкционированного доступа «Блокост-Сеть 3». Руководство администратора безопасности».

В верхней части окна, над списком типов событий, располагается поле ввода критериев отбора объектов из списка **Поиск по всем столбцам** (проверка соответствия введенного в поле ввода значения осуществляется по значениям сразу всех колонок), и кнопки **Выбрать/Снять**, позволяющие установить или снять отметки со всего списка событий сразу.

Для выбора типа события, необходимо установить флаг в нужной строке и нажать кнопку **ОК**. При этом в параметре **По типу события** отобразится количество событий, выбранных для сортировки из всего возможного перечня событий (рисунок 4.31).



Тип запроса

☒ Новый запрос
☐ Сохраненный запрос

Выберите запрос...

Фильтры

По категории
<все категории>

По уровню важности
☐ Сведения
☐ Предупреждение
☐ Ошибка

По типу события
выбрано 7 из 146

По компьютерам
не заданы

По подстроке

☐ По времени
☒ За период:
с 20/2/2019 09:51 по 21/2/2019 09:51
☒ За последние дни: 30

Выполнить запрос
Сохранить запрос как...

Рисунок 4.31 – Отображение количества выбранных типов событий

4) «По компьютерам» - фильтрация событий по компьютерам с установленными клиентами Блокхост-Сеть.

Для выборки событий, зарегистрированных на выбранных компьютерах, необходимо нажать на кнопку выбора компьютеров из списка, и в открывшемся окне выбрать те, по которым нужно осуществить выборку (рисунок 4.32). В окне содержится информация:

- «Имя» - имя компьютера;
- «IP-адрес» - адрес компьютера.

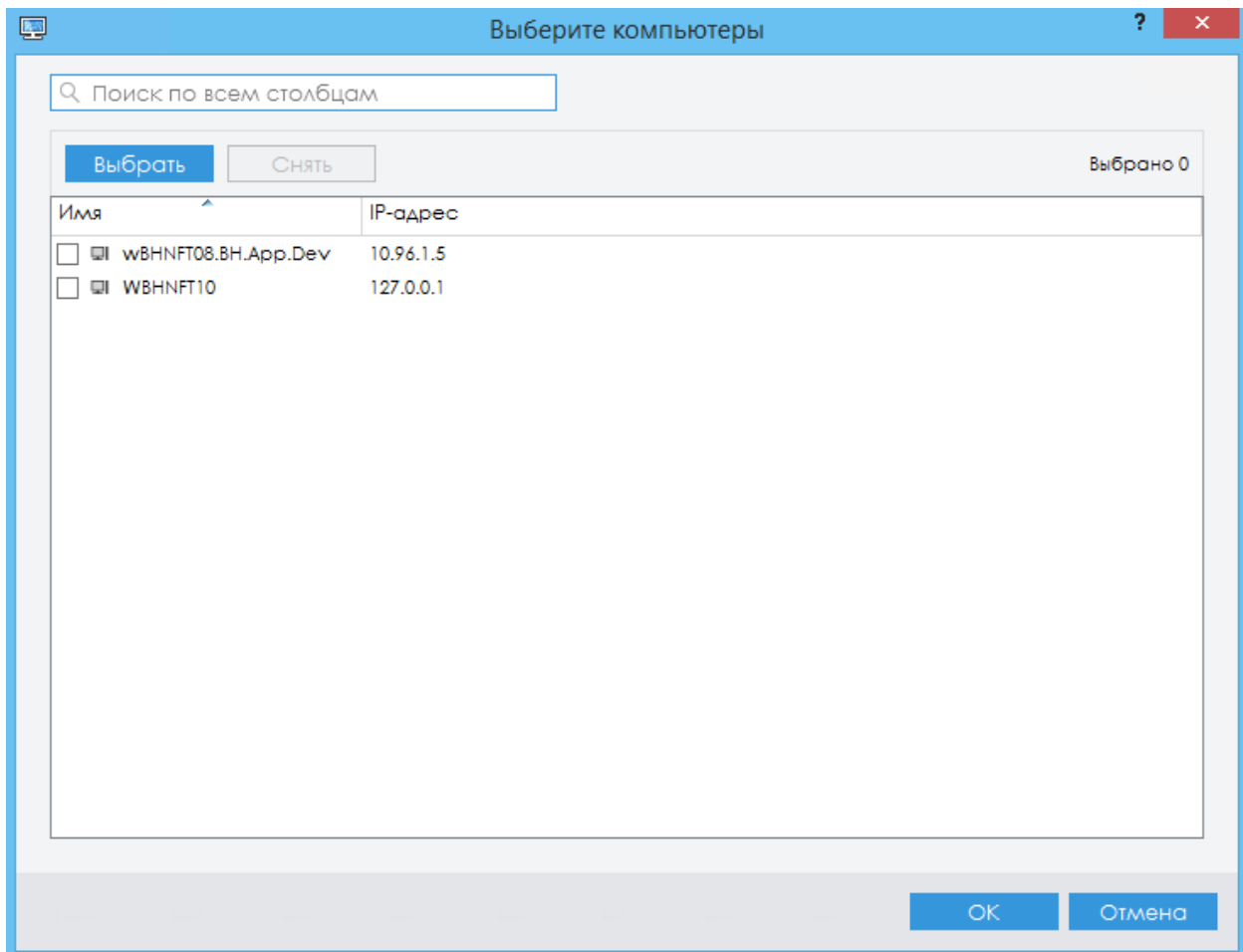


Рисунок 4.32 – Отображение списка компьютеров сервера

В верхней части окна, над списком типов событий, располагается поле ввода критериев отбора объектов из списка **Поиск по всем столбцам** (проверка соответствия введенного в поле ввода значения осуществляется по значениям сразу всех колонок), и кнопки **Выбрать/Снять**, позволяющие установить или снять отметки со всего списка компьютеров сразу.

Для выбора компьютера из списка, необходимо установить флаг в нужной строке и нажать кнопку **ОК**. При этом в параметре **По компьютерам** отобразится количество компьютеров, выбранных из перечня доступных компьютеров с установленными клиентами Блокост-Сеть.

- 5) «По подстроке» - выборка по подробной информации о событии.



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

- 6) «По времени» - выборка событий за определенный период времени:

- **За период** - ввод даты начала и даты окончания выборки в поля с и по:
 - о при введенном значении в поле **с**, будут выбраны все события, начиная с указанной даты. При отсутствии значения в поле **с**, выборка будет осуществлена с самого первого события, имеющегося в системе.
 - о при введенном значении в поле **по**, будут выбраны все события, имеющиеся в системе до указанной даты. При отсутствии значения в поле **по**, выборка будет осуществлена по текущее время.
- **За последние дни** - выбор событий за один или несколько дней, предшествующих текущему.



При выборе фильтра **За последние дни** 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.

После выбора всех необходимых параметров запроса или после ввода сохраненного запроса, для выборки событий необходимо нажать кнопку **Выполнить запрос**. 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:

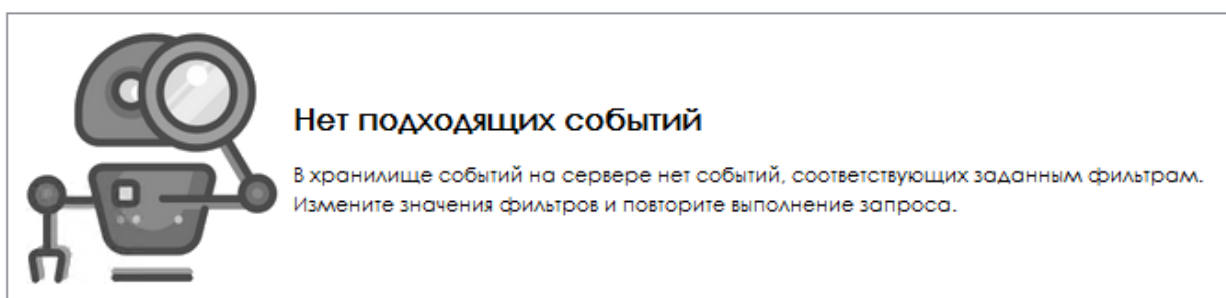


Рисунок 4.33 – Сообщение об отсутствии событий, соответствующих фильтрам

Кнопка **Сохранить изменения** доступна только при выборе типа запроса **Сохраненный запрос**, после внесения изменений в значение какого-либо параметра в выбранном запросе. Изменения возможно сохранить только для запросов, входящих в группу «Запросы, общие для всех серверов» или «Запросы сервера». При этом изменения вносятся в имеющийся запрос.

Кнопка **Сохранить запрос как...** доступна при выборе типа запроса **Новый запрос** или **Сохраненный запрос**. При нажатии кнопки, открывается окно, в котором необходимо ввести имя создаваемого запроса в поле **Имя запроса**, и задать тип запроса (рисунок 4.34):

- **Общие запросы** – запросы, которые могут выполнены на любом сервере иерархии (в запросах этого типа не задан фильтр «по компьютерам»).
- **Запросы сервера <имя сервера>** - запросы, которые могут быть выполнены только на том сервере, для которого они были созданы (в запросах этого типа задан фильтр «по компьютерам»).

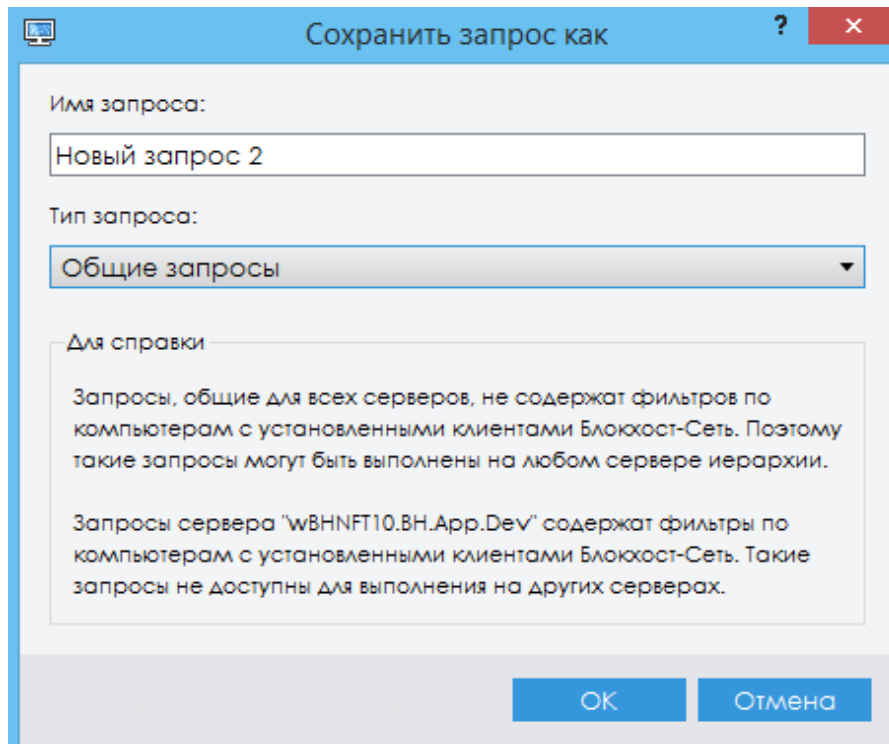


Рисунок 4.34 – Окно сохранения нового запроса



Сохранение запроса с типом «Стандартные запросы» не доступно.



Если при сохранении запроса в выбранном разделе уже имеется запрос с заданным наименованием, появится предупреждение (рисунок 4.35). Для сохранения созданного запроса необходимо использовать другое наименование или удалить запрос, созданный ранее в выбранном разделе.

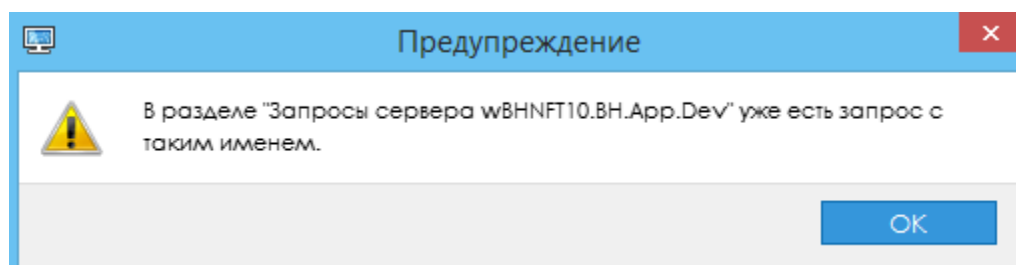


Рисунок 4.35 – Предупреждение о совпадении имен запросов

Для сброса параметров фильтрации администратору безопасности необходимо нажать кнопку **Сбросить фильтры** «», расположенную в правом верхнем углу области **Фильтры** (рисунок 4.31).

Кнопка **Дополнительные параметры** «✖» позволяет настроить максимальное количество событий, собранных по запросу и отображаемых в консоли СРиА. При нажатии на кнопку появится окно для ввода максимального количества событий (рисунок 4.36).

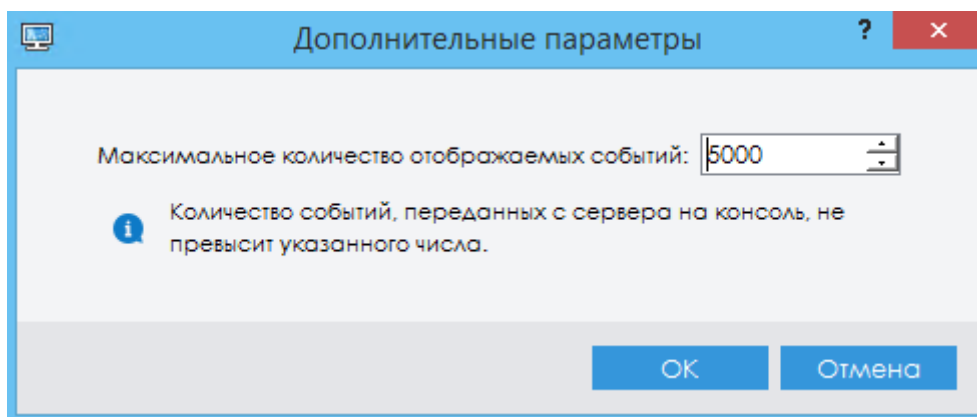


Рисунок 4.36 – Настройка максимального количества отображаемых событий

4.4.4 Контекстное меню сервера

Для каждого сервера в дереве иерархии, по щелчку правой кнопки мыши на нем, доступно контекстное меню (рисунок 4.37) содержащее пункты:

- **Просмотреть группы и компьютеры сервера** – пункт доступен при нахождении в иерархии серверов и предназначен для перехода к группам и компьютерам выбранного сервера;
- **Открыть консоль управления политиками сервера** – осуществляет переход в консоль управления политиками выбранного сервера;
- **Запустить внеплановую загрузку событий аудита** – запуск внепланового сбора событий аудита. Содержит подпункты:
 - **С подчиненных серверов** – для внепланового сбора событий аудита с подчиненных серверов;
 - **С клиентских компьютеров** – для внепланового сбора событий аудита с клиентских компьютеров выбранного сервера.
- **Параметры сервера** – конфигурирование параметров сервера в области сбора событий с подчиненных серверов/клиентов, автоархивации и экспорта событий в SIEM-систему (подробнее см. пункт «4.4.5 Параметры сервера»).

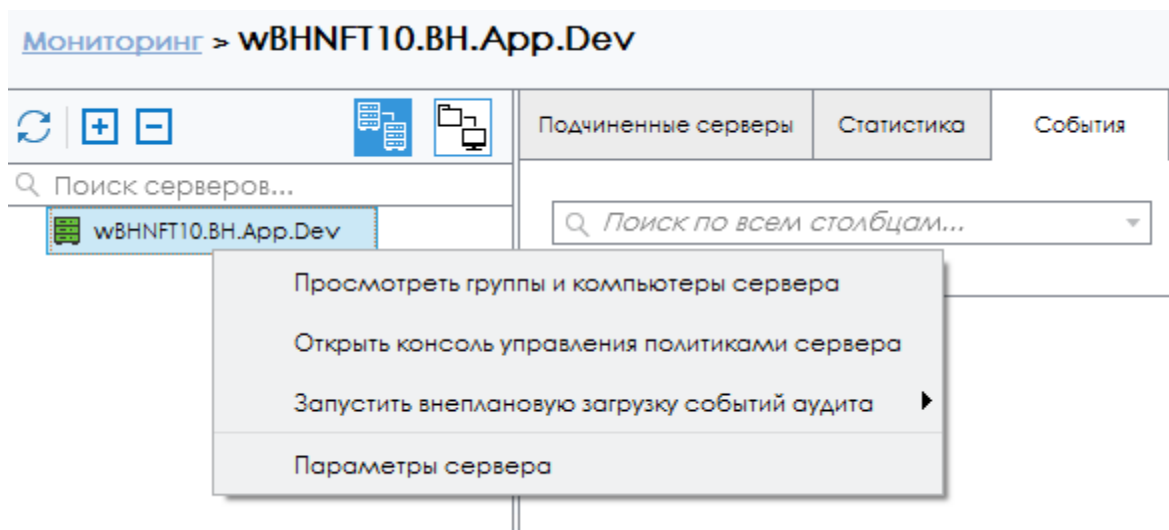


Рисунок 4.37 – Контекстное меню сервера

4.4.5 Параметры сервера

В верхней части окна раздела **Мониторинг**, при выборе сервера в дереве иерархии, отображается ссылка дублирующая пункт контекстного меню сервера **Параметры сервера** вида **Параметры сервера <имя сервера>** (рисунок 4.38).

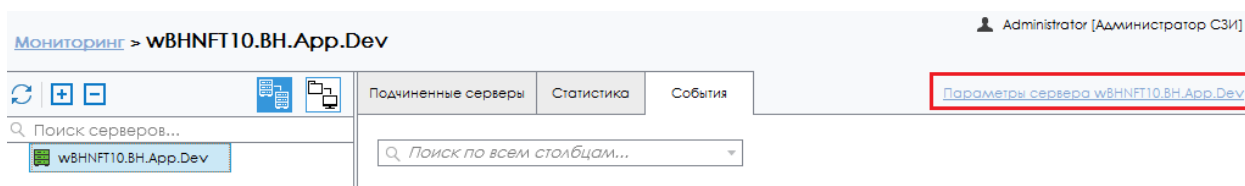


Рисунок 4.38 – Контекстное меню сервера

При переходе по ссылке открывается окно «Параметры сервера <имя сервера>» (рисунок 4.39), в котором доступны вкладки настройки параметров выбранного сервера:

- **Общая информация** – просмотр системной информации о выбранном сервере и информации о последнем цикле опроса подчиненных серверов/клиентских компьютеров;
- **Сбор событий с подсерверов** – настройка параметров сбора событий аудита с подчиненных серверов;
- **Сбор событий с клиентов** – настройка параметров сбора событий аудита с клиентских компьютеров;
- **Автоархивация событий** – настройка параметров автоархивации собранных событий;
- **Экспорт событий в SIEM** – настройка параметров экспорта событий в SIEM-систему;
- **Кэш событий** – настройка параметров кэша событий для временного хранения событий подчиненных серверов/клиентских компьютеров.

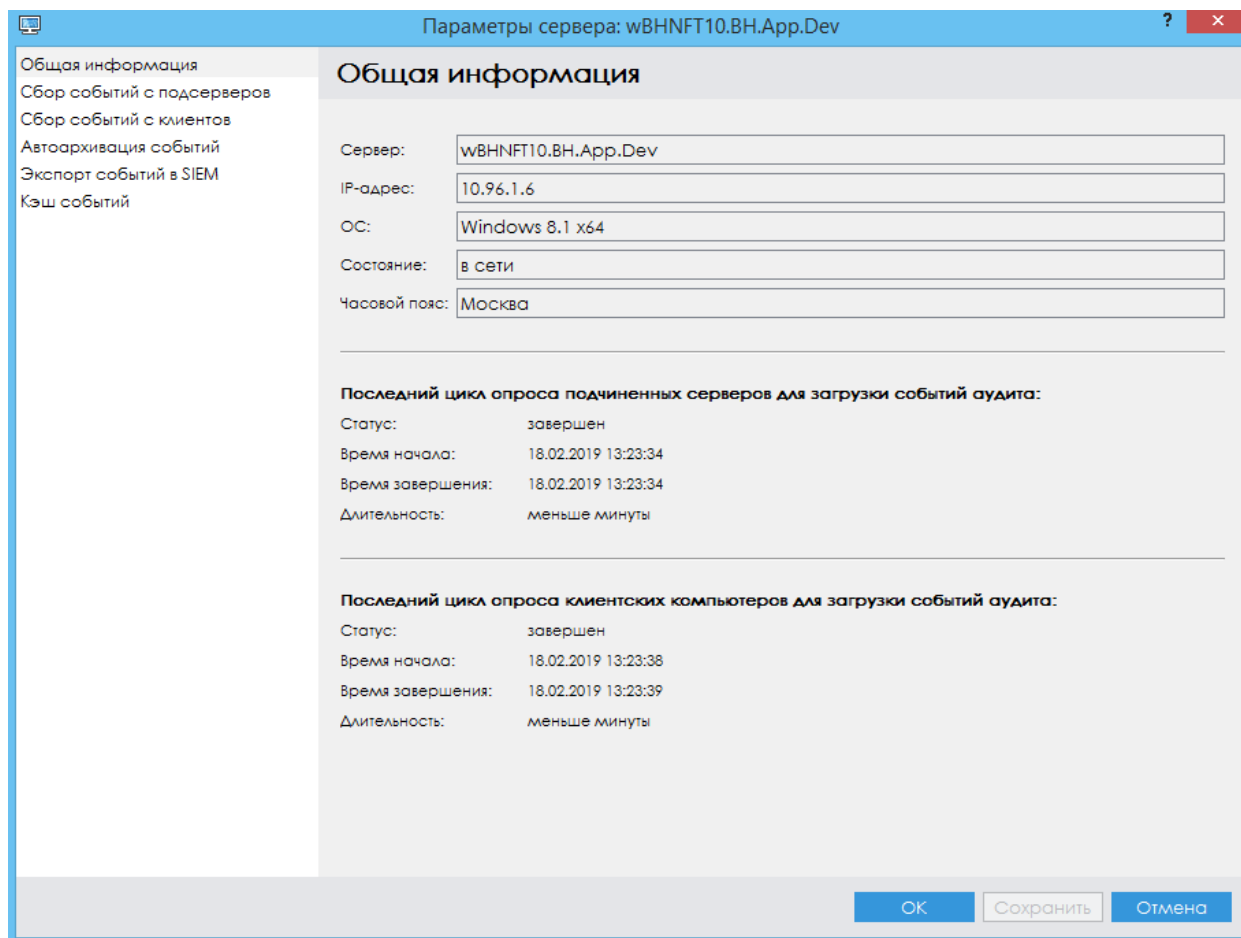


Рисунок 4.39 – Окно параметров сервера

4.4.5.1 Общая информация

Вкладка **Общая информация** (рисунок 4.39) предназначена для просмотра системной информации о выбранном сервере и информации о последнем цикле опроса подчиненных серверов/клиентских компьютеров.

Область информации о сервере, содержит данные:

- «Сервер» - DNS имя сервера;
- «IP-адрес» - IP-адрес сервера;
- «ОС» - информация о версии и разрядности ОС;
- «Состояние» - сетевой статус соответствующего сервера (в сети/не в сети);
- «Часовой пояс» - часовой пояс выбранного сервера, а также разница между часовым поясом сервера, на котором работает администратор и часовым поясом выбранного сервера (если серверы находятся в одном часовом поясе, разница во времени не отображается).

Области информации о последнем цикле опроса подчиненных серверов/клиентских компьютеров, содержат данные:

- «Статус» - статус последнего цикла опроса подчиненных серверов/клиентских компьютеров (завершен, выполняется, не выполнялся);
- «Время начала» - дата и время начала последнего цикла опроса подчиненных серверов/клиентских компьютеров;
- «Время завершения» - дата и время завершения последнего цикла опроса подчиненных серверов/клиентских компьютеров;
- «Длительность» - продолжительность последнего цикла опроса подчиненных серверов/клиентских компьютеров.



Для серверов в дереве иерархии, находящихся в состоянии offline, в контекстном меню доступен только просмотр **Общей информации** о сервере в пункте **Параметры сервера**, пункты **Просмотреть группы и компьютеры сервера**, **Открыть консоль управления политиками сервера** и **Запустить внеплановую загрузку событий аудита** не активны.

4.4.5.2 Сбор событий с подчиненных серверов

Вкладка **Сбор событий с подсерверов** (рисунок 4.40) предназначена для настройки параметров загрузки событий аудита со всех подчиненных серверов на выбранный в дереве иерархии сервер.

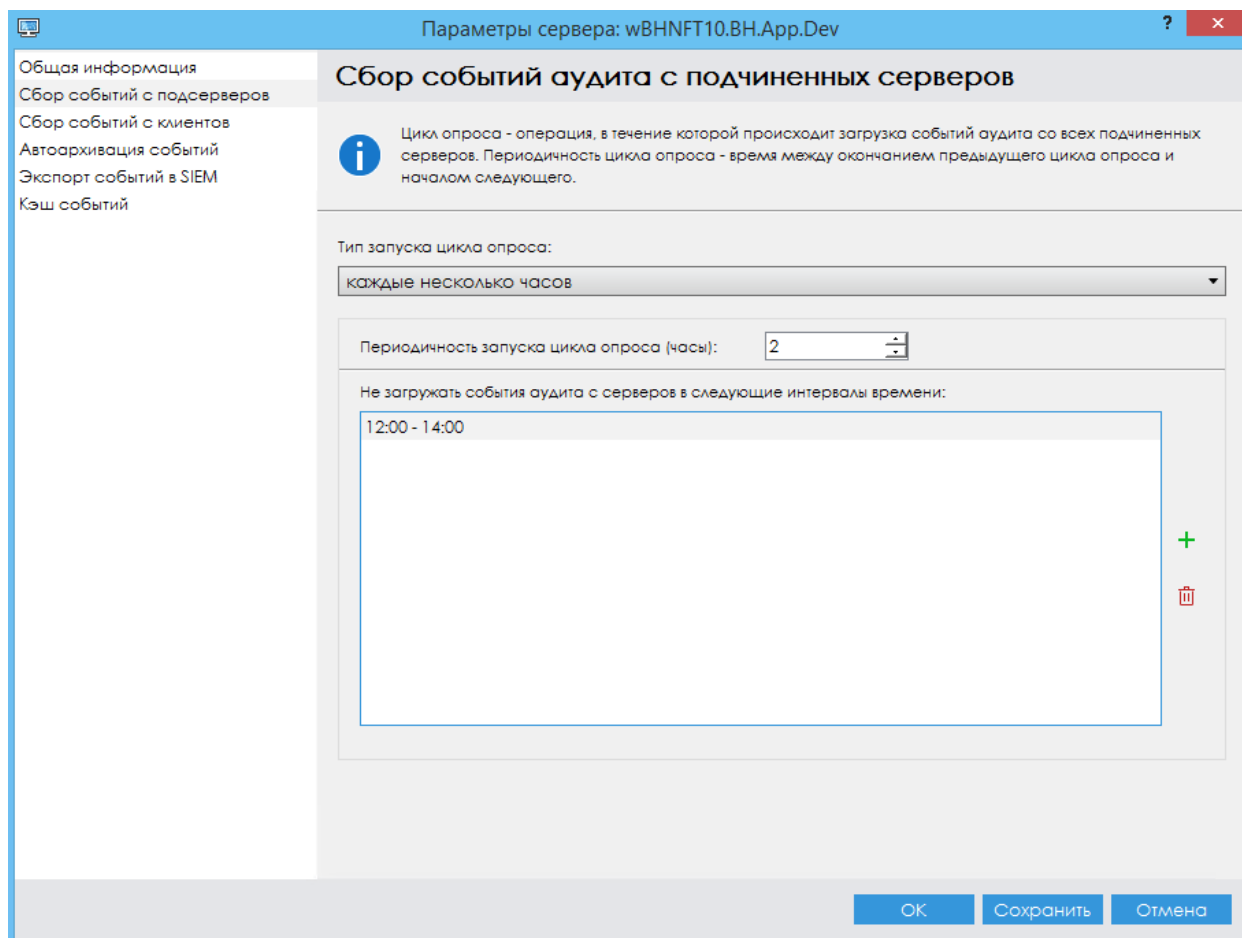


Рисунок 4.40 – Настройка загрузки событий аудита с подчиненных серверов

В зависимости от выбранного значения параметра **Тип запуска цикла опроса**, регулирующего частоту запуска опроса подчиненных серверов, доступные к настройке параметры будут различаться:

Сбор событий аудита каждые несколько часов

При выборе значения параметра **Тип запуска цикла опроса** «*каждые несколько часов*» (рисунок 4.40), к настройке доступны параметры:

- **Периодичность запуска цикла опроса (часы)** – период, заданный в часах, между окончанием предыдущей загрузки событий аудита с подчиненных серверов и началом следующей загрузки (допустимые значения 1-10);
- **Не загружать события аудита с серверов в следующие интервалы времени** – ввод одного или нескольких промежутков времени (в часах), в которые загрузка событий аудита произведена не будет.



Цикл опроса – это операция, в течение которой происходит загрузка событий аудита со всех подчиненных серверов.

Периодичность цикла опроса – время между окончанием предыдущего цикла опроса и началом следующего.

Для ввода интервалов времени прерывания загрузки событий с серверов необходимо в области **Не загружать события аудита с серверов в следующие интервалы времени** нажать на кнопку , и в появившемся окне (рисунок 4.41) ввести время начала и время окончания периода, в который сбор событий с подчиненных серверов производиться не будет.

Для удаления созданного интервала времени необходимо перейти курсором в нужную строку в списке и нажать на кнопку .

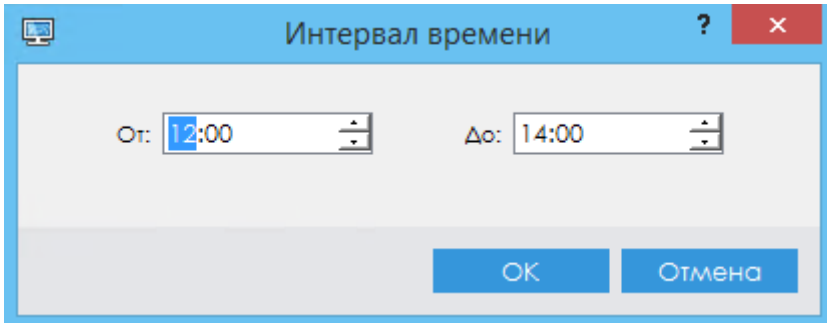


Рисунок 4.41 – Ввод интервала времени прерывания загрузки событий с серверов

Время запуска цикла опроса в соответствии с заданной периодичностью и промежутков времени, в который загрузка событий аудита осуществляться не должна, могут пересекаться. При этом в зависимости от точки пересечения этих параметров, цикл опроса может быть запущен и прерван, либо не начаться вообще. Возможные варианты пересечения и итоговый результат приведены в таблице 4.2.

Таблица 4.2 – Пересечение времени запуска цикла опроса с промежутком прерывания загрузки

Описание пересечения	Пример пересечения
Время запуска следующего цикла опроса попадает в интервал времени, в который загрузка не должна осуществляться	Время завершения предыдущего цикла опроса: Последний цикл опроса подчиненных серверов для загрузки событий аудита: Статус: завершен Время начала: 18.02.2019 13:23:34 Время завершения: 18.02.2019 13:23:34 Длительность: меньше минуты Заданная периодичность: 2 часа Промежуток прерывания: 15:00 – 16:00 Тип запуска цикла опроса: каждые несколько часов Периодичность запуска цикла опроса (часы): 2 Не загружать события аудита с серверов в следующие интервалы времени: 15:00 - 16:00 Результат: Цикл опроса не будет запущен

Цикл следующего опроса начинается раньше интервала времени, в который загрузка не должна осуществляться, но в процессе выполнения пересекается с ним	Время завершения предыдущего цикла опроса:
	Последний цикл опроса подчиненных серверов для загрузки событий аудита:
	Статус: завершен
	Время начала: 18.02.2019 13:23:34
	Время завершения: 18.02.2019 13:23:34
	Длительность: меньше минуты
	Заданная периодичность: 1 час
	Промежуток прерывания: 14:33 – 15:33
	Тип запуска цикла опроса: каждые несколько часов
	Периодичность запуска цикла опроса (часы): 1
	Не загружать события аудита с серверов в следующие интервалы времени: 14:33 - 15:33
	Результат:
	Цикл опроса будет запущен в 14.23 и продлится 10 минут. В 14.33 цикл будет прерван. Последующий запуск цикла будет осуществлен в соответствии с заданной периодичностью в полном объеме.

Запуск загрузки событий аудита с подчиненных серверов будет осуществляться в соответствии с настроенными во вкладке параметрами после подтверждения введенных данных по кнопке **Сохранить**.

Успешная загрузка событий аудита с подчиненных серверов или выполнение операции с ошибкой фиксируется в событиях сервера (рисунок 4.42).

Время	Событие	Категория	Уровень важности
04/03/2019 13:57:15	Запуск цикла опроса клиентских компьютеров (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 13:57:11	Завершение цикла опроса подчиненных серверов (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 13:57:11	Запуск цикла опроса подчиненных серверов (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 13:28:31	Вход в систему по RDP	Аутентификация	Сведения
04/03/2019 12:57:15	Завершение цикла опроса клиентских компьютеров (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 12:57:15	Запуск цикла опроса клиентских компьютеров (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 11:57:14	Завершение цикла опроса клиентских компьютеров (по расписанию)	События сервера СЗИ	Сведения

Подробная информация

Событие: завершение цикла опроса подчиненных серверов (по расписанию)

Рисунок 4.42 – Просмотр события на сервере

Сбор событий аудита один или несколько раз в неделю

При выборе значения параметра **Тип запуска цикла опроса** «один или несколько раз в неделю» (рисунок 4.43), к настройке доступны параметры:

- **Время запуска цикла опроса** – ввод времени запуска загрузки событий аудита с подчиненных серверов (при этом операция будет запущена по локальному времени выбранного в дереве иерархии сервера);
- **Дни недели** – выбор дней недели, в которые будет запущена загрузка событий аудита с подчиненных серверов.

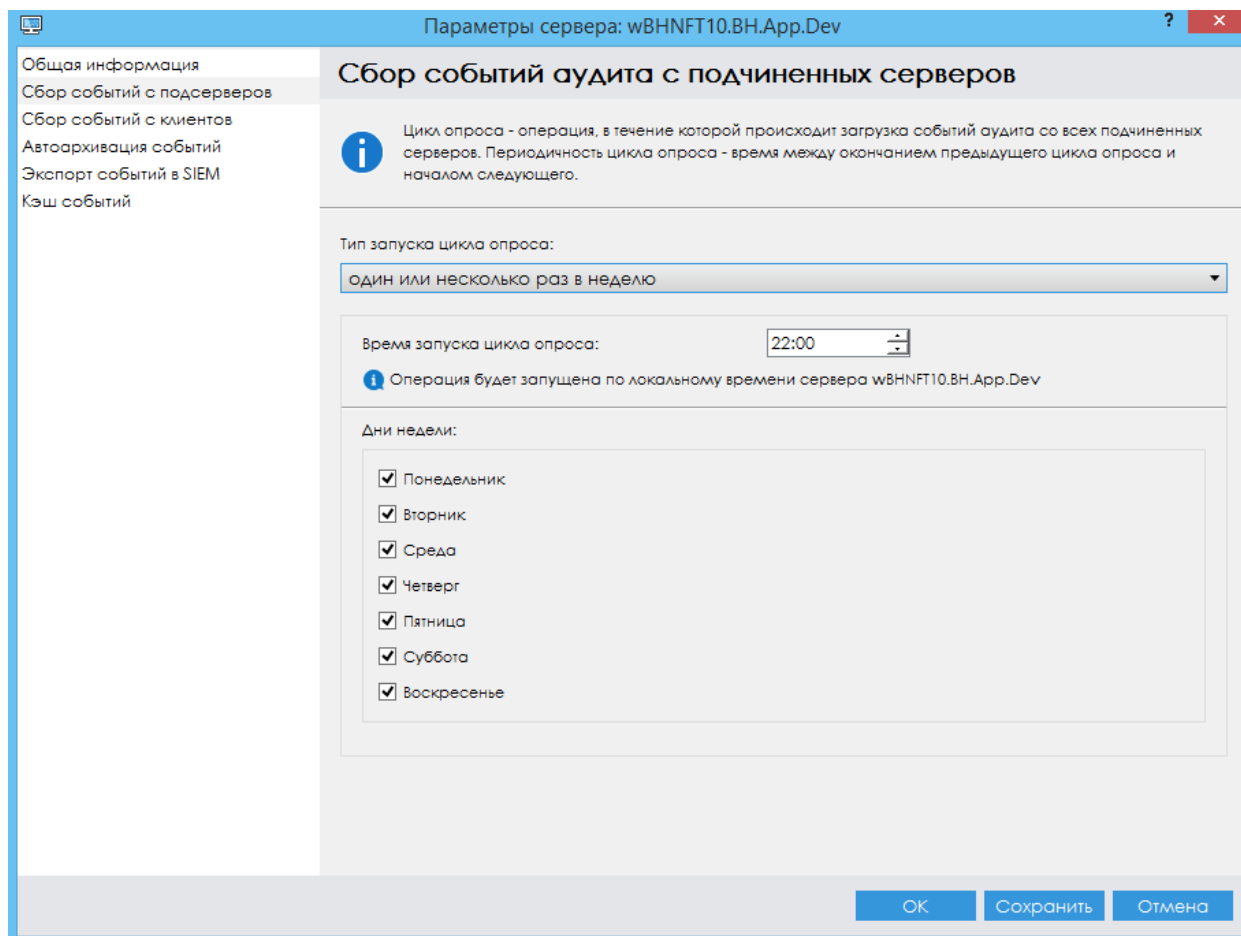


Рисунок 4.43 – Настройка загрузки событий с серверов один или несколько раз в неделю

Запуск загрузки событий аудита с подчиненных серверов будет осуществляться в соответствии с настроенными во вкладке параметрами после подтверждения введенных данных по кнопке **Сохранить**.

Успешная загрузка событий аудита с подчиненных серверов или выполнение операции с ошибкой фиксируется в событиях сервера (рисунок 4.42).

4.4.5.3 Сбор событий с клиентов

Вкладка **Сбор событий с клиентов** (рисунок 4.44) предназначена для настройки параметров загрузки событий аудита с клиентских компьютеров сервера, выбранного в дереве иерархии.

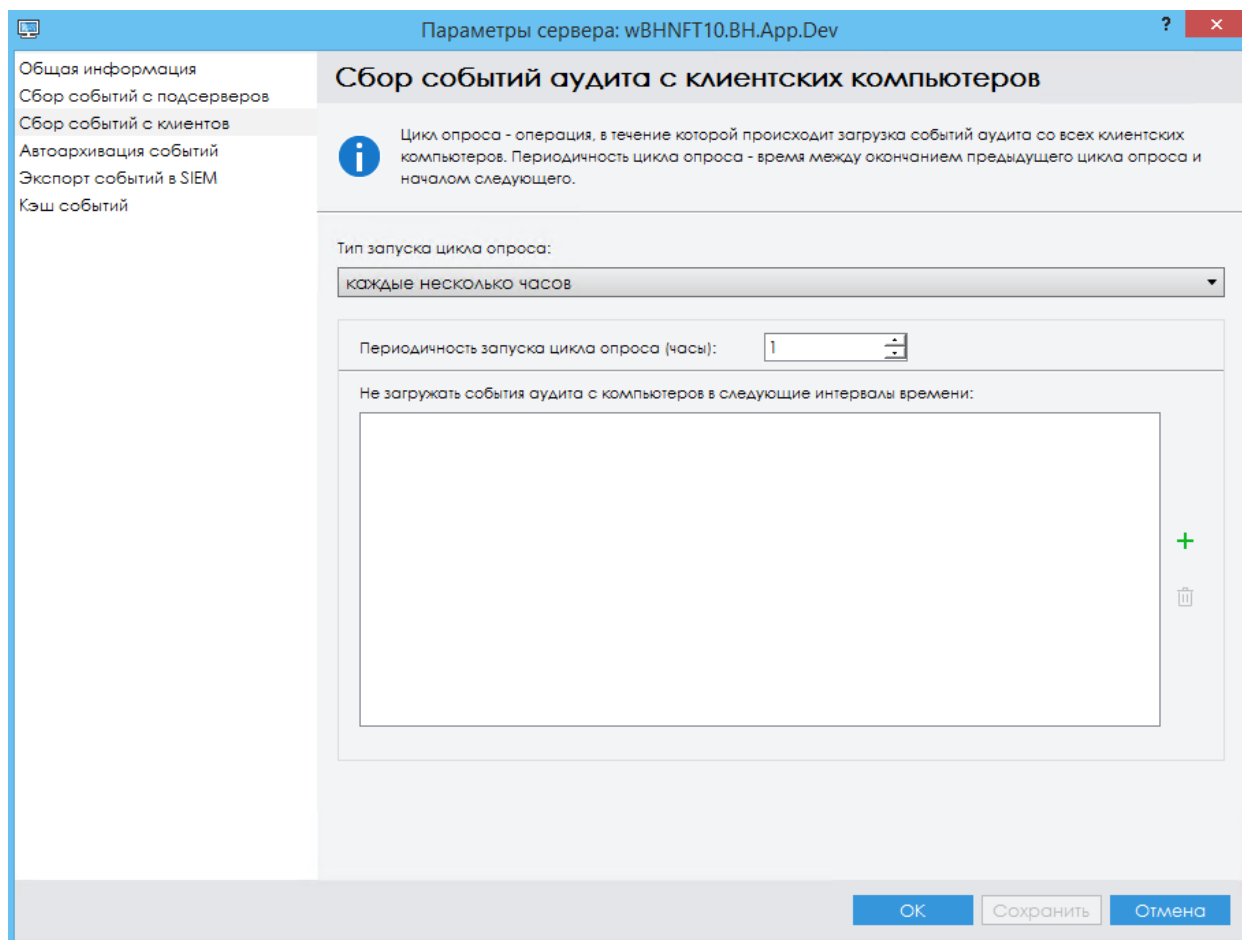


Рисунок 4.44 – Настройка загрузки событий аудита с клиентских компьютеров сервера

Логика настройки сбора событий аудита с клиентов аналогична настройке событий аудита с подчиненных серверов:

- 1) Необходимо выбрать **Тип запуска цикла опроса**, регулирующий частоту запуска опроса клиентских компьютеров.
- 2) В зависимости от выбранного значения параметра **Тип запуска цикла опроса**, заполнить:
 - **Периодичность запуска цикла опроса** и ввести промежутки времени, в которые загрузка событий не должна производиться;
 - **Время запуска цикла опроса и Дни недели**, по которым будет производиться сбор событий.

Подробное описание параметров настройки сбора событий приведено в подпункте «4.4.5.2 Сбор событий с подчиненных серверов».

Запуск загрузки событий аудита с клиентских компьютеров будет осуществляться в соответствии с настроенными во вкладке параметрами после подтверждения введенных данных по кнопке **Сохранить**.

Успешная загрузка событий аудита с клиентских компьютеров или выполнение операции

с ошибкой фиксируется в событиях сервера (рисунок 4.45).

Время	Событие	Категория	Уровень важности
04/03/2019 13:57:11	запуск цикла опроса подчиненных серверов (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 13:28:31	Вход в систему по RDP	Аутентификация	Сведения
04/03/2019 12:57:15	Завершение цикла опроса клиентских компьютеров (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 12:57:15	Запуск цикла опроса клиентских компьютеров (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 11:57:14	Завершение цикла опроса клиентских компьютеров (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 11:57:14	Запуск цикла опроса клиентских компьютеров (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 11:57:10	Завершение цикла опроса подчиненных серверов (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 11:57:10	Запуск цикла опроса подчиненных серверов (по расписанию)	События сервера СЗИ	Сведения

Подробная информация

Событие: завершение цикла опроса клиентских компьютеров (по расписанию)

Рисунок 4.45 – Просмотр события сервера

4.4.5.4 Автоархивация событий аудита

Вкладка **Автоархивация событий** (рисунок 4.46), предназначена для настройки параметров архивации событий, собранных на выбранном в дереве иерархии сервере.

Параметры сервера: w8HNFT10.BH.App.Dev

Общая информация
Сбор событий с подсерверов
Сбор событий с клиентов
Автоархивация событий
Экспорт событий в SIEM
Кэш событий

Автоархивация событий

☒ Выполнять автоархивацию хранилища событий на сервере

Время первого запуска: 19.02.2019 00:00

Интервал запуска (дни): 1

Операция будет запущена по локальному времени сервера w8HNFT10.BH.App.Dev

Перемещать в архив:

☒ все события в хранилище

☐ только события, старше (дни): 1

☒ Создавать архивы событий в каталоге:

Проверить возможность создания архивов Обзор

Путь к сетевому ресурсу необходимо указывать вручную в UNC формате.
Например: \\Server\Share\ArchiveFolder

☐ Удалять события навсегда

ОК Сохранить Отмена

Рисунок 4.46 – Настройка автоархивации хранилища событий на сервере

Для выполнения архивации необходимо установить флаг **Выполнять автоархивацию хранилища событий на сервере** и выполнить настройку доступных параметров:

- **Время первого запуска** – ввод даты и времени первоначального запуска архивации хранилища событий на сервере (по локальному времени сервера,

выбранного в деревне иерархии);

- **Интервал запуска (дни)** – период, заданный в днях, между окончанием предыдущей архивации событий на сервере и началом следующей (допустимые значения 1-365);
- **Перемещать в архив** – возможность выбора событий для перемещения в архив:
 - о *все события в хранилище* – для перемещения в архив всех событий, находящихся в хранилище;
 - о *только события, старше (дни)* – для перемещения в архив только тех событий, которые хранятся на сервере начиная с даты, предшествующей текущей дате на введенное в поле количество дней, и по текущее время (допустимые значения 1-365);
- Выбор действий над событиями хранилища, отмеченными для архивации:
 - о *Создавать архивы событий в каталоге* – создание архива событий, хранящихся на сервере, и выбор директории создаваемого архива;
 - о *Удалять события навсегда* – удаление событий, хранящихся на сервере (подробно удаление событий описано в подпункте «4.4.5.5 Удаление событий аудита»).

При создании архива событий возможно проверить введенную директорию в поле *Создавать архивы событий в каталоге* по кнопке **Проверить возможность создания архивов**. Если искомая директория не найдена, при проверке появится сообщение об ошибке (рисунок 4.47) и архив в указанном каталоге не будет создан.



Для архивации событий в новом каталоге, необходимо заранее, в нужной директории создать каталог. Создание нового каталога при вводе директории архива невозможно.

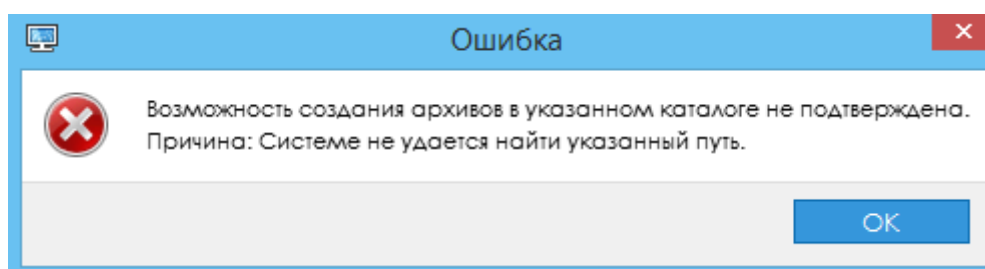


Рисунок 4.47 – Настройка автоархивации хранилища событий на сервере



При создании архива событий не на текущем сервере, путь к сетевому ресурсу необходимо прописать вручную в UNC формате. Например: \\Server\Share\ArchiveFolder

Запуск автоархивации хранилища событий на сервере будет осуществляться в соответствии с настроенными во вкладке параметрами после подтверждения введенных

данных по кнопке **Сохранить**.

Успешное создание архива событий аудита или выполнение операции с ошибкой фиксируется в событиях сервера (рисунок 4.48).

Время	Событие	Категория	Уровень важно
04/03/2019 14:31:00	Успешное создание архива событий аудита	События сервера СЗИ	Сведения
04/03/2019 14:31:00	Запуск создания архива событий аудита по расписанию	События сервера СЗИ	Сведения
04/03/2019 13:57:15	Завершение цикла опроса клиентских компьютеров (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 13:57:15	Запуск цикла опроса клиентских компьютеров (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 13:57:11	Завершение цикла опроса подчиненных серверов (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 13:57:11	Запуск цикла опроса подчиненных серверов (по расписанию)	События сервера СЗИ	Сведения

Подробная информация

Событие: успешное создание архива событий аудита

Рисунок 4.48 – Просмотр события на сервере

4.4.5.5 Удаление событий аудита

Вкладка **Автоархивация событий** (рисунок 4.46), предназначена также для удаления собранных на выбранном в дереве иерархии сервере событий аудита.

Для удаления событий аудита необходимо установить флаг **Выполнять автоархивацию хранилища событий на сервере** и выполнить настройку параметров, описанных выше в подпункте «4.4.5.4 Автоархивация событий аудита»: время запуска удаления событий, интервал запуска и выбор событий для удаления.

После настройки необходимых параметров удаления, необходимо установить переключатель в позицию **Удалять события навсегда** и нажать кнопку **Сохранить**.

Успешное удаление событий аудита или выполнение операции с ошибкой фиксируется в событиях сервера (рисунок 4.49).

Время	Событие	Категория	Уровень важно
04/03/2019 14:31:00	Успешное создание архива событий аудита	События сервера СЗИ	Сведения
04/03/2019 14:31:00	Запуск создания архива событий аудита по расписанию	События сервера СЗИ	Сведения
04/03/2019 13:57:15	Завершение цикла опроса клиентских компьютеров (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 13:57:15	Запуск цикла опроса клиентских компьютеров (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 13:57:11	Завершение цикла опроса подчиненных серверов (по расписанию)	События сервера СЗИ	Сведения
04/03/2019 13:57:11	Запуск цикла опроса подчиненных серверов (по расписанию)	События сервера СЗИ	Сведения

Подробная информация

Событие: успешное создание архива событий аудита

Рисунок 4.49 – Просмотр события на сервере



При выполнении удаления событий аудита происходит очищение базы данных событий. Восстановление удаленных событий невозможно!

4.4.5.6 Экспорт событий в SIEM-систему

Вкладка **Экспорт событий в SIEM** (рисунок 4.50) предназначена для настройки параметров экспорта событий аудита в SIEM-систему.



Включение/выключение механизма экспорта событий аудита в SIEM-систему осуществляется только на головном сервере иерархии (рисунок 4.50). Изменение параметров работы механизма на подчиненных серверах не доступно (рисунок 4.51).



Экспорт событий аудита предполагает передачу в SIEM-систему только тех событий, которые заданы к сбору на головном сервере, вне зависимости наследования настроек родительских серверов и локальных настроек выбранного сервера.

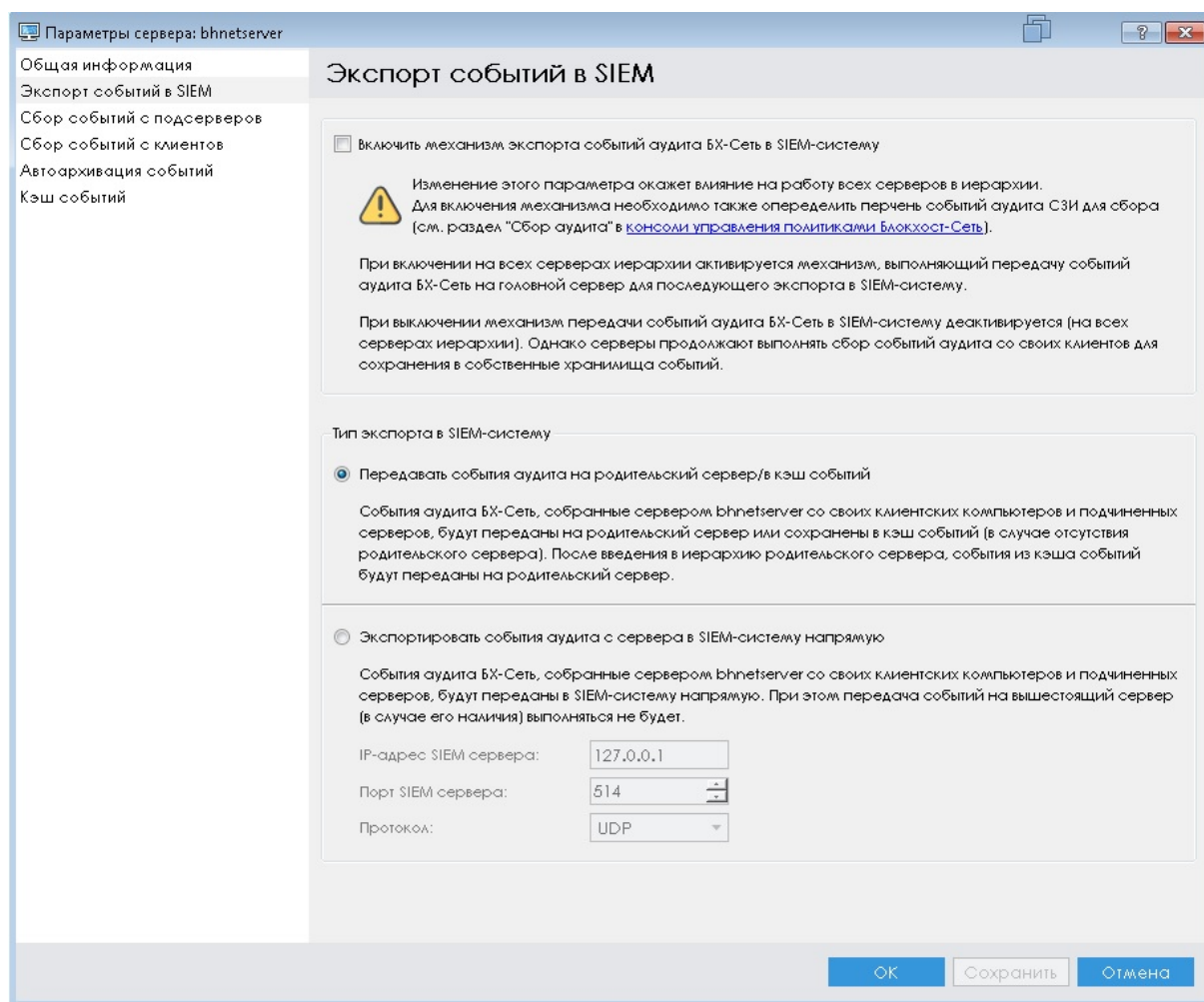


Рисунок 4.50 – Настройка экспорта событий в SIEM-систему головного сервера

При включении механизма экспорта событий аудита в SIEM-систему на головном сервере, на всех серверах иерархии активируется механизм, выполняющий передачу событий аудита на головной сервер для последующего экспорта в SIEM-систему.

Для включения механизма необходимо также определить перечень событий аудита в консоли управления политиками. Описание настройки перечня событий приведено в подразделе 4.3. «Настройка сбора событий в консоли управления политиками сервера».

При выключенном механизме передачи событий в SIEM-систему серверы продолжают выполнять сбор событий аудита со своих клиентов для сохранения в собственные

хранилища событий.

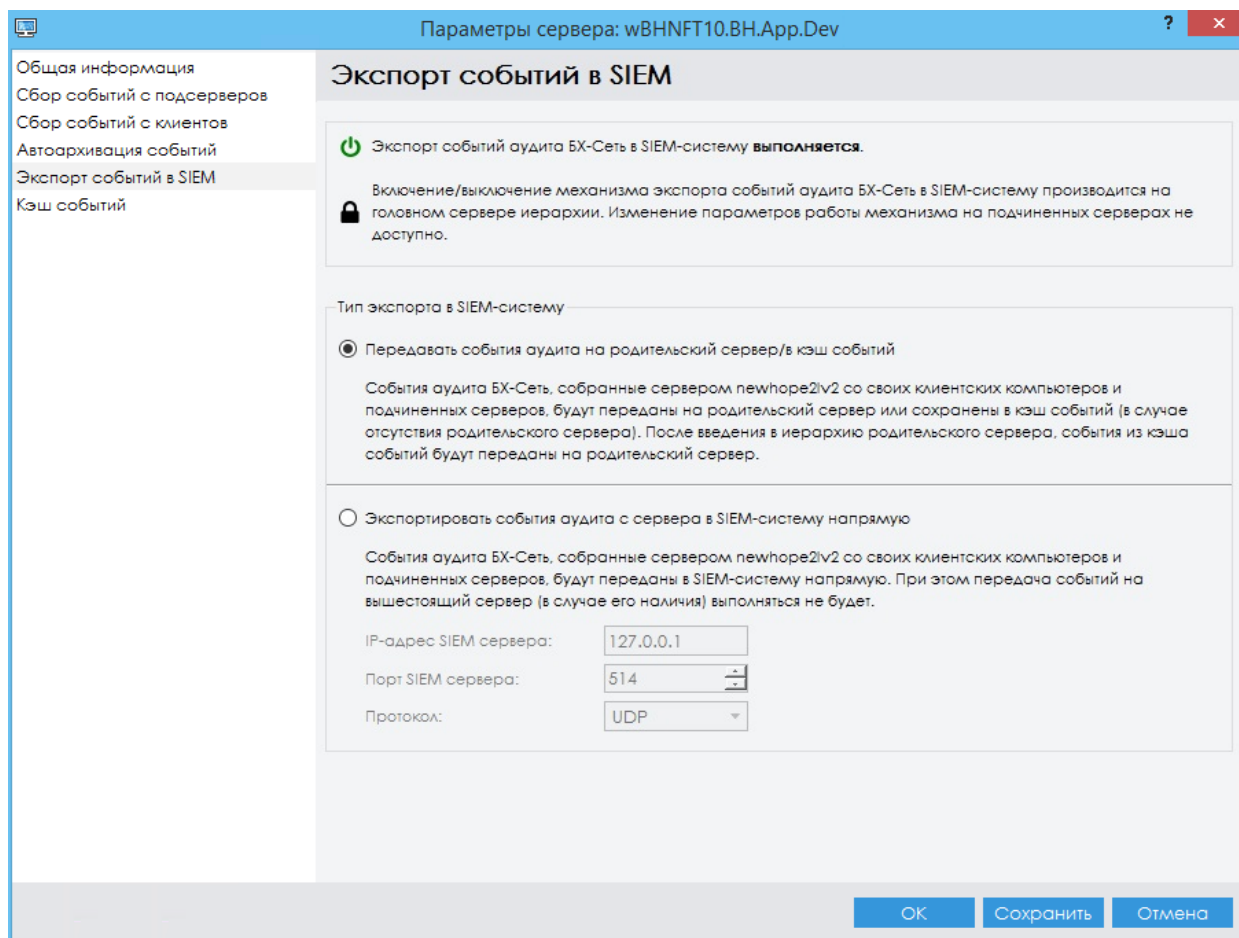


Рисунок 4.51 – Вкладка экспорта событий в SIEM-систему подчиненного сервера

По умолчанию экспорт событий в SIEM-систему осуществляется через родительский сервер (установлен флаг **Передавать события аудита на родительский сервер/в кэш событий**). При этом события аудита, собранные текущим сервером со своих клиентских компьютеров и подчиненных серверов, будут переданы на родительский сервер или сохранены в кэш событий (в случае отсутствия родительского сервера).

При включенном на головном сервере механизме экспорта событий в SIEM-систему, на подчиненном сервере возможна установка экспорта в SIEM-систему напрямую. Для выполнения экспорта необходимо установить флаг **Экспортировать события аудита с сервера в SIEM-систему напрямую** и выполнить настройку доступных параметров:

- **IP-адрес SIEM сервера** – ввод IP-адреса сервера, на котором установлена SIEM-система;
- **Порт SIEM сервера** – ввод значения порта, по которому осуществляется работа сервера, с установленной SIEM-системой (допустимые значения 1-65535);
- **Протокол** – выбор протокола для передачи данных в SIEM-систему (TCP/IP или UDP).

Запуск экспорта событий аудита в SIEM-систему будет осуществляться в соответствии с настроенными во вкладке параметрами после подтверждения введенных данных по кнопке **Сохранить**.



При установке флага **Экспортировать события аудита с сервера в SIEM-систему напрямую** сбор данных на родительский сервер (при его наличии) не будет осуществляться, события будут передаваться напрямую в SIEM-систему.

4.4.5.7 Кэш событий

Вкладка **Кэш событий** (рисунок 4.52), предназначена для настройки размера кэша событий, используемого для временного хранения событий, полученных с клиентских компьютеров и со всех подчиненных серверов. События хранятся в кэше событий до момента передачи на вышестоящий сервер. После передачи событий, хранящихся в кэше событий, на вышестоящий сервер, кэш событий очищается.

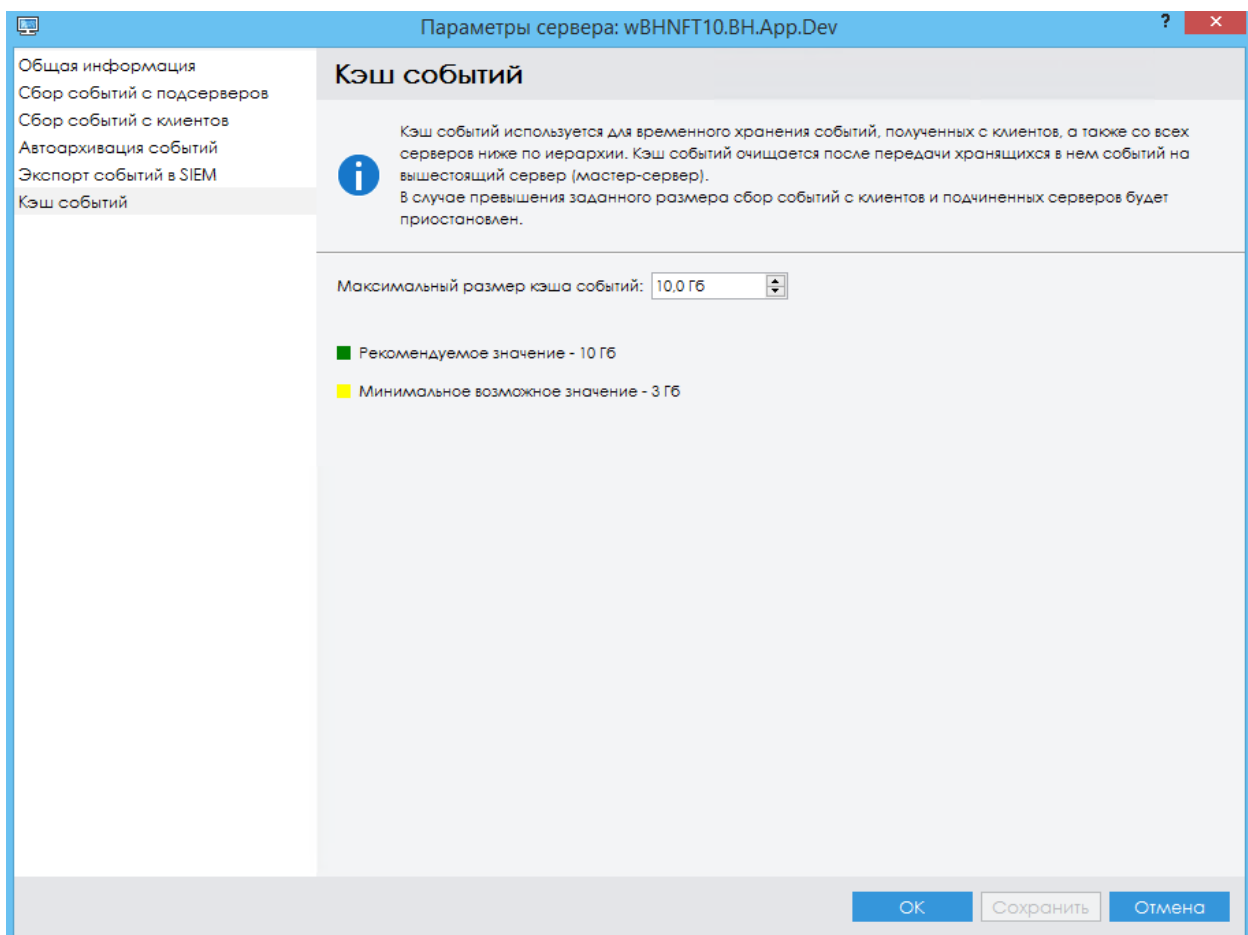


Рисунок 4.52 – Настройка размера кэша событий

Для установки максимального размера кэша событий необходимо в параметре **Максимальный размер кэша событий** установить требуемое значение (минимально допустимый размер кэша событий – 3 Гб).



В случае превышения установленного максимального размера кэша событий сбор событий с клиентских компьютеров и подчиненных серверов будет приостановлен. Сбор событий возобновится в случае, когда актуальный размер кэша событий станет меньше установленного максимального значения.

Измененное значение размера кэша событий необходимо подтвердить по кнопке **Сохранить**.

Превышение максимально допустимого размера кэша событий фиксируется в событиях сервера (рисунок 4.53).

Время	Событие	Категория	Уровень важности
01/03/2019 13:23:32	Сервер администрирования запущен	События сервера СЗИ	Сведения
01/03/2019 13:26:57	Завершение цикла опроса клиентских компьютеров (по требованию)	События сервера СЗИ	Сведения
01/03/2019 13:26:57	Запуск цикла опроса клиентских компьютеров (по требованию)	События сервера СЗИ	Сведения
01/03/2019 13:25:37	Локальный вход в систему	Аутентификация	Сведения
01/03/2019 13:26:57	Ошибка при записи событий аудита в кэш событий	События сервера СЗИ	Ошибка
01/03/2019 13:23:33	Подключение к головному серверу	События сервера СЗИ	Сведения
01/03/2019 13:23:32	Подключение клиента к серверу	События клиента СЗИ	Сведения
01/03/2019 13:23:32	Подключение клиента к серверу	События сервера СЗИ	Сведения

Рисунок 4.53 – Просмотр события на сервере

4.4.6 Запуск внеплановой загрузки событий аудита

Пункт контекстного меню сервера **Запустить внеплановую загрузку событий аудита** (рисунок 4.54) предназначен для запуска внепланового сбора событий аудита на выбранный в дереве иерархии сервер и содержит пункты:

- **С подчиненных серверов** – для внепланового сбора событий аудита с подчиненных серверов;
- **С клиентских компьютеров** – для внепланового сбора событий аудита с клиентских компьютеров выбранного сервера.

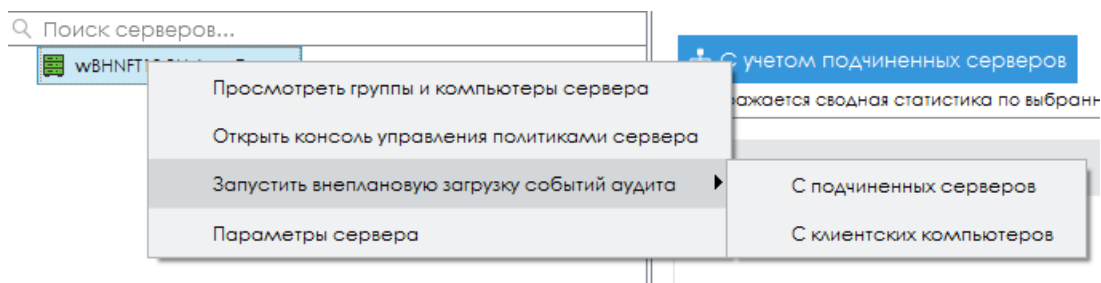


Рисунок 4.54 – Контекстное меню **Запустить внеплановую загрузку событий аудита**

Если запуск внепланового цикла опроса может быть выполнен, пользователю выдается уведомление об успешности запуска (рисунок 4.55).

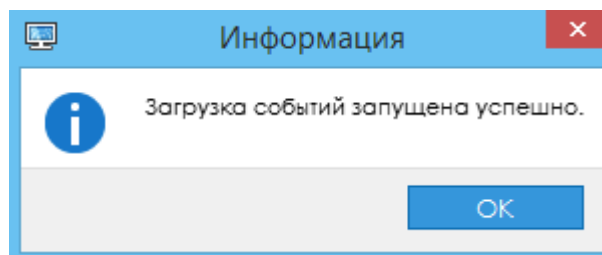


Рисунок 4.55 – Уведомление об успешности запуска внеплановой загрузки событий



Запуск внепланового цикла опроса не будет произведен при:

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

При этом на экране появится сообщение о невозможности запуска внеплановой загрузки событий (рисунок 4.56).

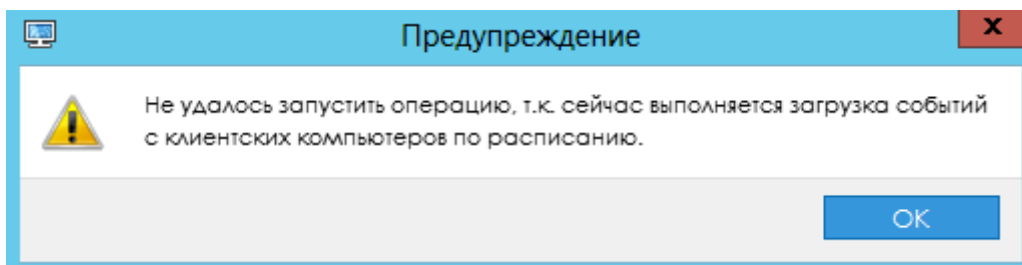


Рисунок 4.56 – Сообщение о невозможности запуска внеплановой загрузки событий

Логика выполнения запуска внепланового цикла опроса в зависимости от включения/отключения передачи данных аудита в SIEM-систему на выбранном сервере описана в таблице 4.3.

Таблица 4.3 – Запуск внепланового цикла опроса в зависимости от включения/отключения передачи данных аудита в SIEM-систему

Действие	Экспорт в SIEM-систему включен	Ожидаемое поведение
Внеплановая загрузка событий с подчиненных серверов/клиентских компьютеров	Да	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.
	Нет	Выполняется загрузка событий с подчиненных серверов/клиентских компьютеров текущего сервера. Выполняется передача собранных данных на родительский сервер. Загруженные события не экспортируются в SIEM.

4.5 Аудит групп серверов

При выборе группы сервера в дереве иерархии, правая часть окна будет содержать информацию по всем компьютерам, входящим в выбранную группу и во все группы, подчиненные выбранной (рисунок 4.57).

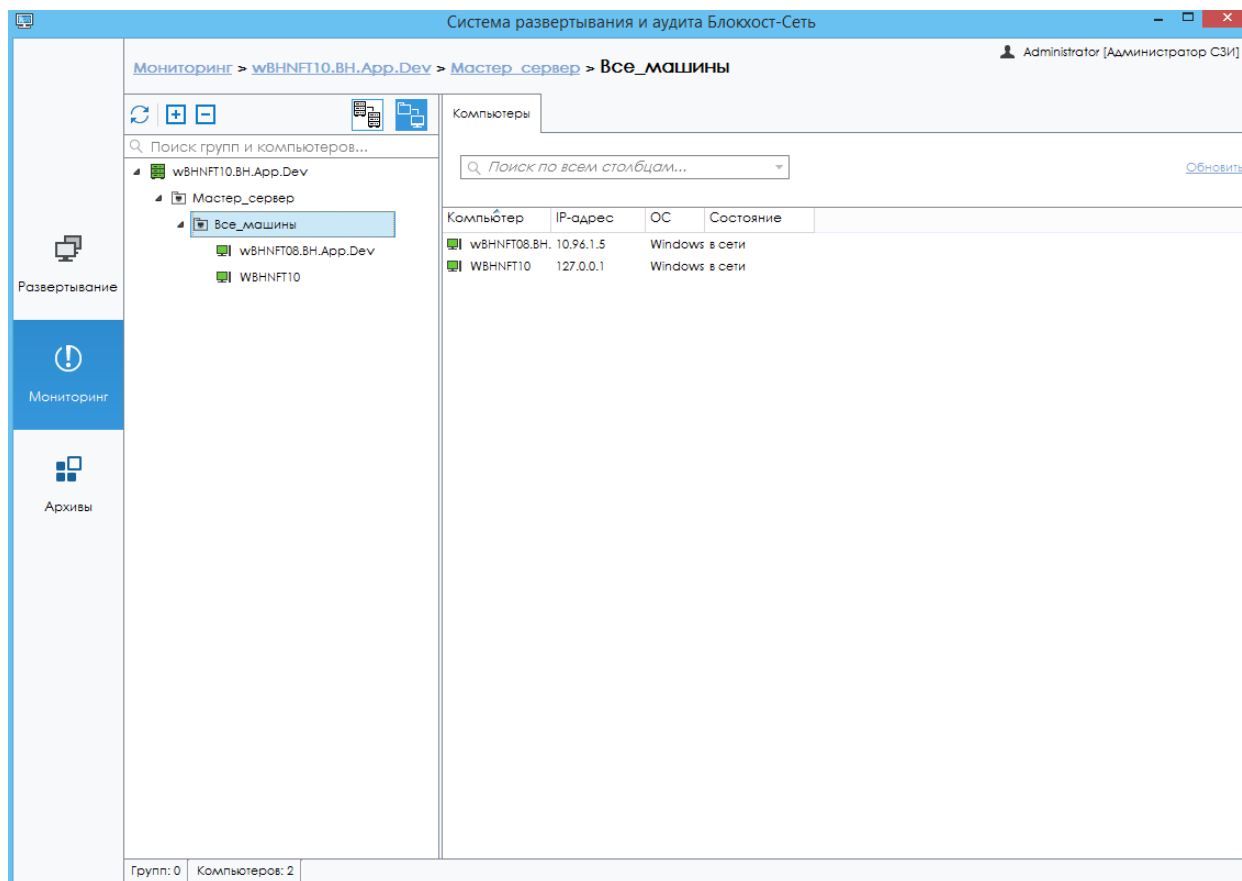


Рисунок 4.57 – Список компьютеров выбранной группы

Для каждого компьютера в списке отображается информация:

- «Компьютер» - DNS имя клиентского компьютера;
- «IP-адрес» - IP-адрес клиентского компьютера;
- «ОС» - информация о версии и разрядности ОС;
- «Состояние» - сетевой статус выбранного клиентского компьютера (в сети/не в сети).

Для удобства просмотра информации администратор безопасности может сортировать список объектов в каждом столбце. Объекты выбранного столбца сортируются по возрастанию/убыванию при щелчке левой кнопкой мыши на заголовке столбца (рисунок 4.57). Сортировка по выбранному столбцу выделяется пиктограммами «^»/«v» в заголовке столбца. По умолчанию, список компьютеров выбранной группы сортируется по DNS имени компьютера.

Для каждого компьютера в списке доступно контекстное меню (рисунок 4.58)

содержащее пункты:

- **Перейти к компьютеру** – осуществляет переход к выбранному компьютеру в списке иерархии;
- **Информация о компьютере** – вывод окна, содержащего информацию о выбранном компьютере (рисунок 4.62).

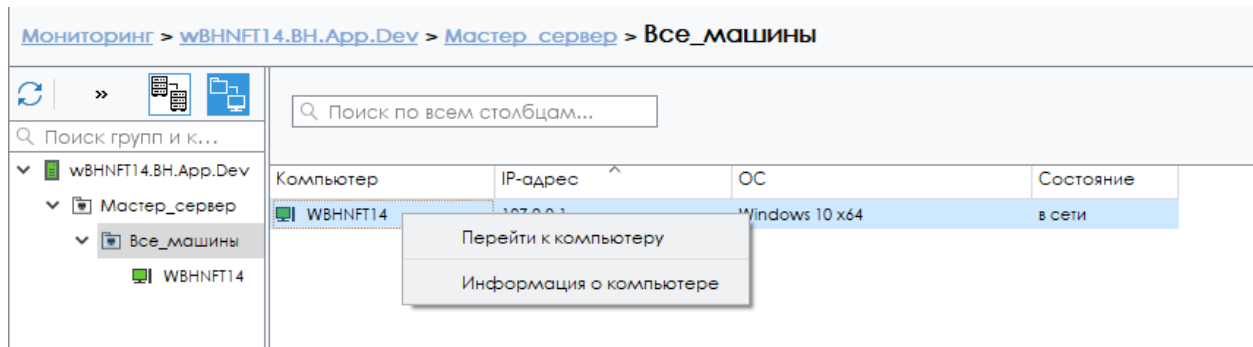


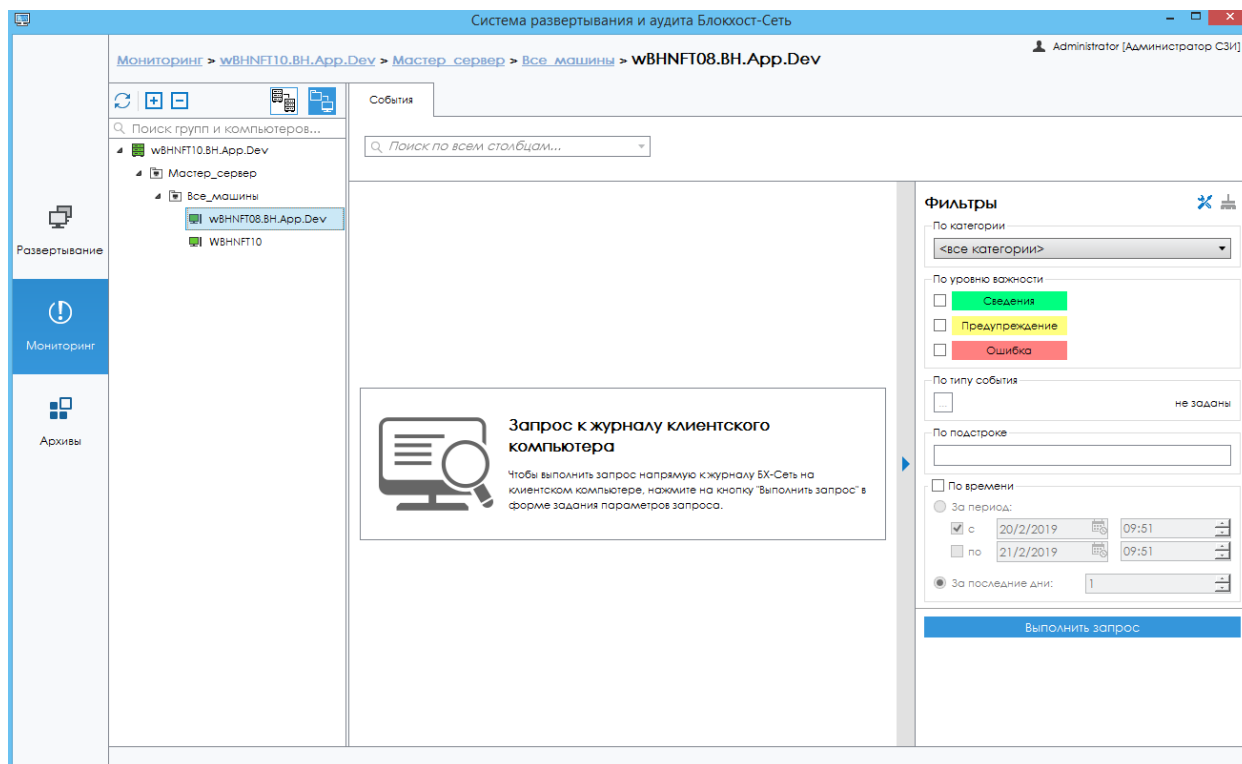
Рисунок 4.58 – Контекстное меню выбранного в списке компьютера

В верхней части окна, над именами колонок, располагается поле ввода критериев отбора объектов из списка **Поиск по всем столбцам...**. Проверка соответствия введенного в поле ввода значения осуществляется по значениям сразу всех колонок (рисунок 4.13).

Кнопка **Обновить** (рисунок 4.57) позволяет обновить текущую информацию о состоянии компьютеров, входящих в выбранную группу.

4.6 Аудит клиентов сервера

При выборе клиентского компьютера в дереве иерархии, правая часть окна будет предназначена для выполнения запросов и отслеживания событий на выбранном клиентском компьютере (рисунок 4.59). До выполнения запроса в основной части вкладки выводится сообщение с пояснением дальнейших действий.

Рисунок 4.59 – Вкладка **События** клиентского компьютера

4.6.1 Вкладка «События»

Вкладка **События** в правой части окна **Мониторинг** при выборе в дереве иерархии клиентского компьютера предназначена для выполнения запросов и отслеживания всех событий, зафиксированных на выбранном компьютере.

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 доступна форма для задания параметров выполняемого запроса (рисунок 4.59).

Обновление списка событий происходит при выполнении запроса и содержит информацию:

- «Время» - дата и время момента фиксации произошедшего события;
- «Событие» - краткое описание зафиксированного события (полный перечень событий, фиксируемых в консоли СРиА приведен в Приложении 5 к документу «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Руководство администратора безопасности»);
- «Категория» - категория, которой принадлежит зафиксированное событие;
- «Уровень важности» - уровень важности зафиксированного события (сведения, предупреждения или ошибка).

Статистика		События	
Поиск по всем столбцам...		Время последнего сбора аудита: 15:33:51 17.12.2018 Результат запроса: 24 сообщения	
Время	Событие	Категория	Уровень важности
13:00:00 14.12.2018	Изменение параметров работы СЗИ	События клиента СЗИ	Предупреждение
13:00:00 14.12.2018	Сервер администрирования запущен	События сервера СЗИ	Сведения
13:00:00 14.12.2018	Подключение к серверу	События клиента СЗИ	Сведения
13:00:00 14.12.2018	Подключение клиента к серверу	События сервера СЗИ	Сведения
13:00:47 14.12.2018	Создание задачи на установку агента системы развертывания	Система развертывания	Сведения
13:00:47 14.12.2018	Создание задачи на установку произвольной программы	Система развертывания	Сведения
13:00:53 14.12.2018	Запуск консоли СЗИ	Действия администратора СЗИ	Сведения
13:02:54 14.12.2018	Изменение параметров работы СЗИ	Действия администратора СЗИ	Сведения
13:02:55 14.12.2018	Подключение к головному серверу	События сервера СЗИ	Сведения
13:02:55 14.12.2018	Отключение от головного сервера	События сервера СЗИ	Сведения
13:02:57 14.12.2018	Подключение к головному серверу	События сервера СЗИ	Сведения
17:34:35 14.12.2018	Отключение от головного сервера	События сервера СЗИ	Сведения
17:35:01 14.12.2018	Подключение к головному серверу	События сервера СЗИ	Сведения
18:58:43 14.12.2018	Выход пользователя из системы	Аутентификация	Сведения
18:58:43 14.12.2018	Сервер администрирования остановлен	События сервера СЗИ	Сведения
09:18:50 17.12.2018	Подключение к головному серверу	События сервера СЗИ	Сведения
09:18:50 17.12.2018	Подключение к серверу	События клиента СЗИ	Сведения
09:18:50 17.12.2018	Подключение клиента к серверу	События сервера СЗИ	Сведения
09:18:51 17.12.2018	Сервер администрирования запущен	События сервера СЗИ	Сведения
09:30:08 17.12.2018	Открытие сессии управления по иерархии	События сервера СЗИ	Сведения
17:34:49 14.12.2018	Отказ в установке соединения	События сервера СЗИ	Ошибка
17:34:51 14.12.2018	Отказ в установке соединения	События сервера СЗИ	Ошибка
17:34:59 14.12.2018	Отказ в установке соединения	События сервера СЗИ	Ошибка
09:18:49 17.12.2018	Отказ в подключении к серверу	События клиента СЗИ	Ошибка

Фильтры
По категории
<все источники>
По уровню важности
☐ Сведения
☐ Предупреждение
☐ Ошибка
По типу события
☐ не заданы
По подстроке
☐ По времени
☐ За период:
☒ с 16/12/2018 09:29
☐ по 17/12/2018 09:29
☒ За последние дни: 1
Выполнить запрос

Рисунок 4.60 – Список событий после выполнения запроса

В верхней части окна, над списком событий, располагается поле ввода критериев отбора объектов из списка **Поиск по всем столбцам...**. Проверка соответствия введенного в поле ввода значения осуществляется по значениям сразу всех колонок (рисунок 4.13).

При двойном щелчке мыши на выбранном событии в списке, внизу списка отобразится подробная информация о событии (рисунок 4.27).

В правой части вкладки доступна форма настройки параметров для выборки событий с клиентского компьютера. Для выполнения запроса необходимо ввести данные о параметрах запроса (по каким параметрам будет осуществляться выборка событий: по категориям, по уровню важности, по типу события, по подстроке, по времени).

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

- 1) «По категории» - выборка событий, относящихся только к заданной категории (значение <все источники>, установленное по умолчанию, отфильтрует список событий по всем категориям).
- 2) «По уровню важности» - выборка событий только с заданным уровнем важности.
- 3) «По типу событий» - выборка событий только указанных типов (подробнее, параметр «По типу событий» описан в п. 3 подпункта «4.4.3.2 Настройка параметров запроса»).
- 4) «По подстроке» - выборка осуществляется по подробной информации события.



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

- 5) «По времени» - выборка событий за определенный период времени (подробнее, параметр «По времени» описан в п. 5 подпункта «4.4.3.2 Настройка параметров запроса»).

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

4.6.2 Контекстное меню клиентского компьютера

Для каждого клиентского компьютера в дереве иерархии, по щелчку правой кнопки мыши на нем, доступно контекстное меню (рисунок 4.61) содержащее пункт:

- **Информация о компьютере** – вывод системной информации о выбранном клиентском компьютере.

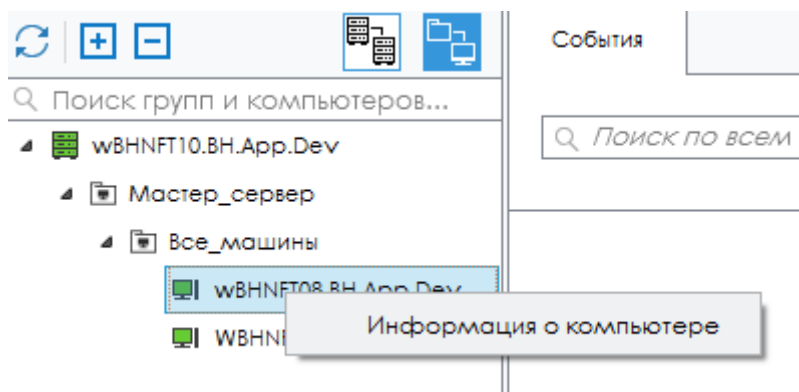


Рисунок 4.61 – Контекстное меню клиентского компьютера

При выборе пункта контекстного меню **Информация о компьютере** осуществляется переход к окну «Информация о компьютере: <имя компьютера>», содержащему системную информацию о выбранном компьютере (рисунок 4.62):

- «Имя» - имя выбранного компьютера;
- «IP-адрес» - IP-адрес выбранного компьютера;
- «ОС» - информация об установленной версии и разрядности ОС;
- «Состояние» - сетевой статус соответствующего компьютера сервера (в сети/не в сети).

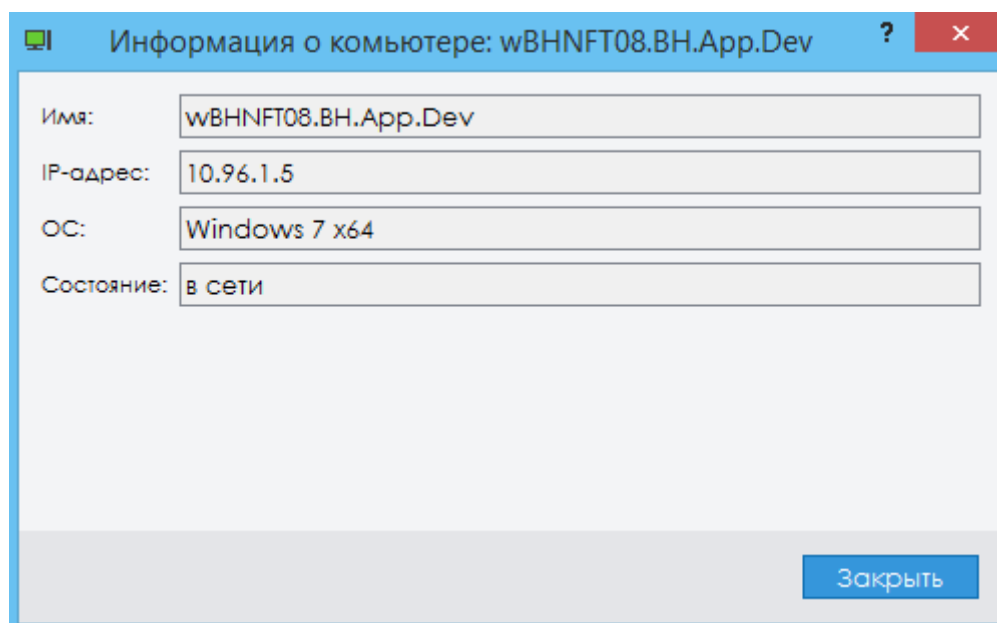


Рисунок 4.62 – Информация о выбранном клиентском компьютере

5 Раздел «Архивы»

В разделе **Архивы** консоли СРиА осуществляется работа с созданными ранее архивами событий аудита с возможностью выбора событий при помощи фильтрации (рисунок 5.1).

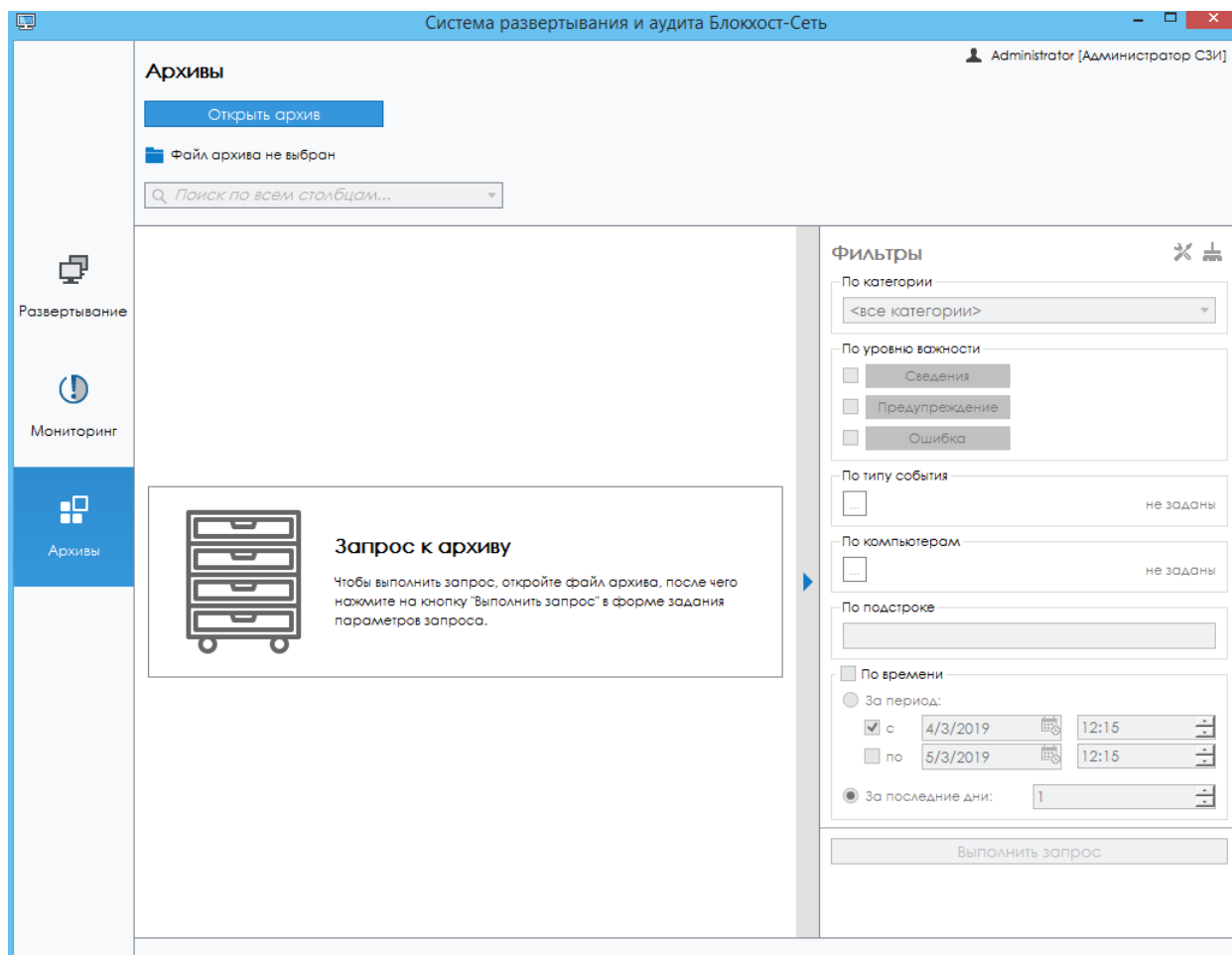


Рисунок 5.1 – Раздел **Архивы**

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 5.1).

Для начала работы с архивом событий аудита необходимо выбрать файл архива (рисунок 5.2), содержащий требуемую информацию, по кнопке **Открыть архив**, расположенной в верхней части раздела **Архивы**.

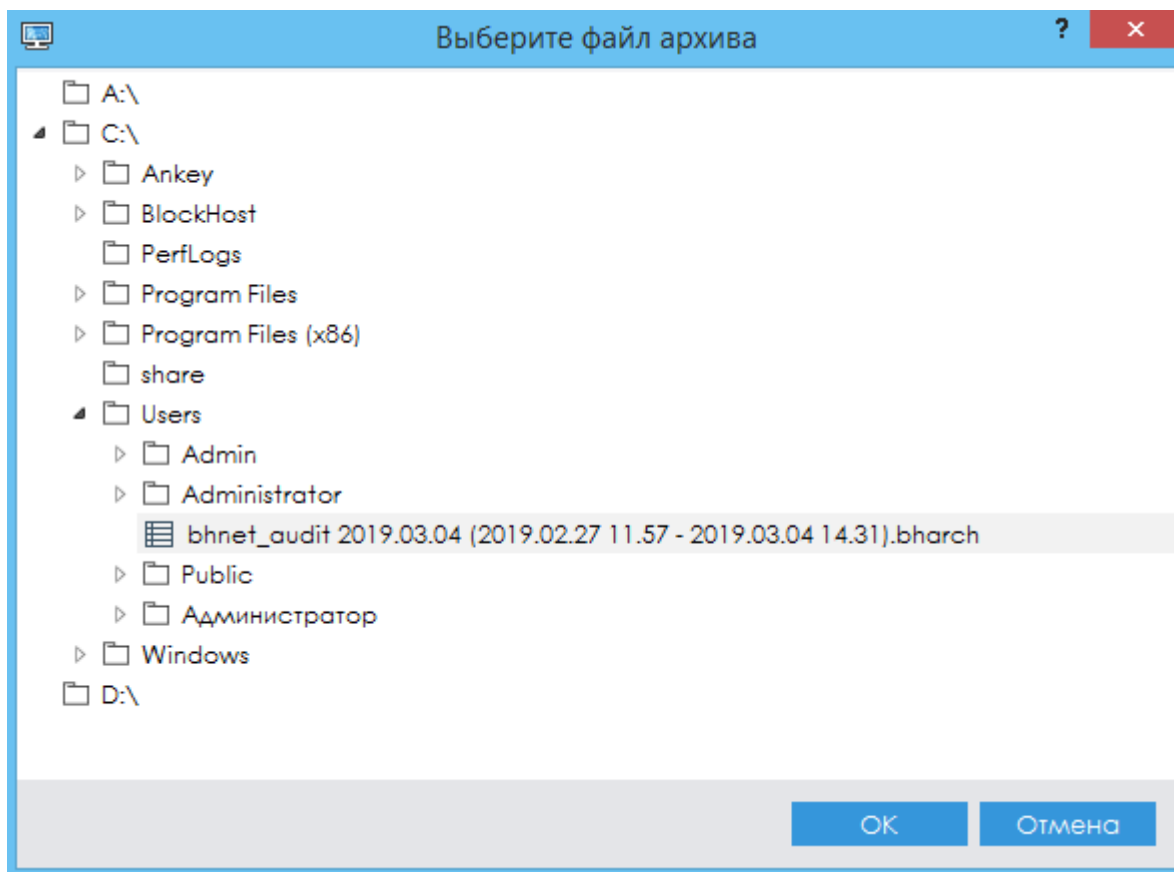


Рисунок 5.2 – Выбор файла архива

После выбора файла архива правая часть раздела, содержащая параметры выполняемого запроса, становится доступной для выполнения фильтрации по выбранному архиву. В верхней части раздела указан путь к выбранному файлу архива (рисунок 5.3).

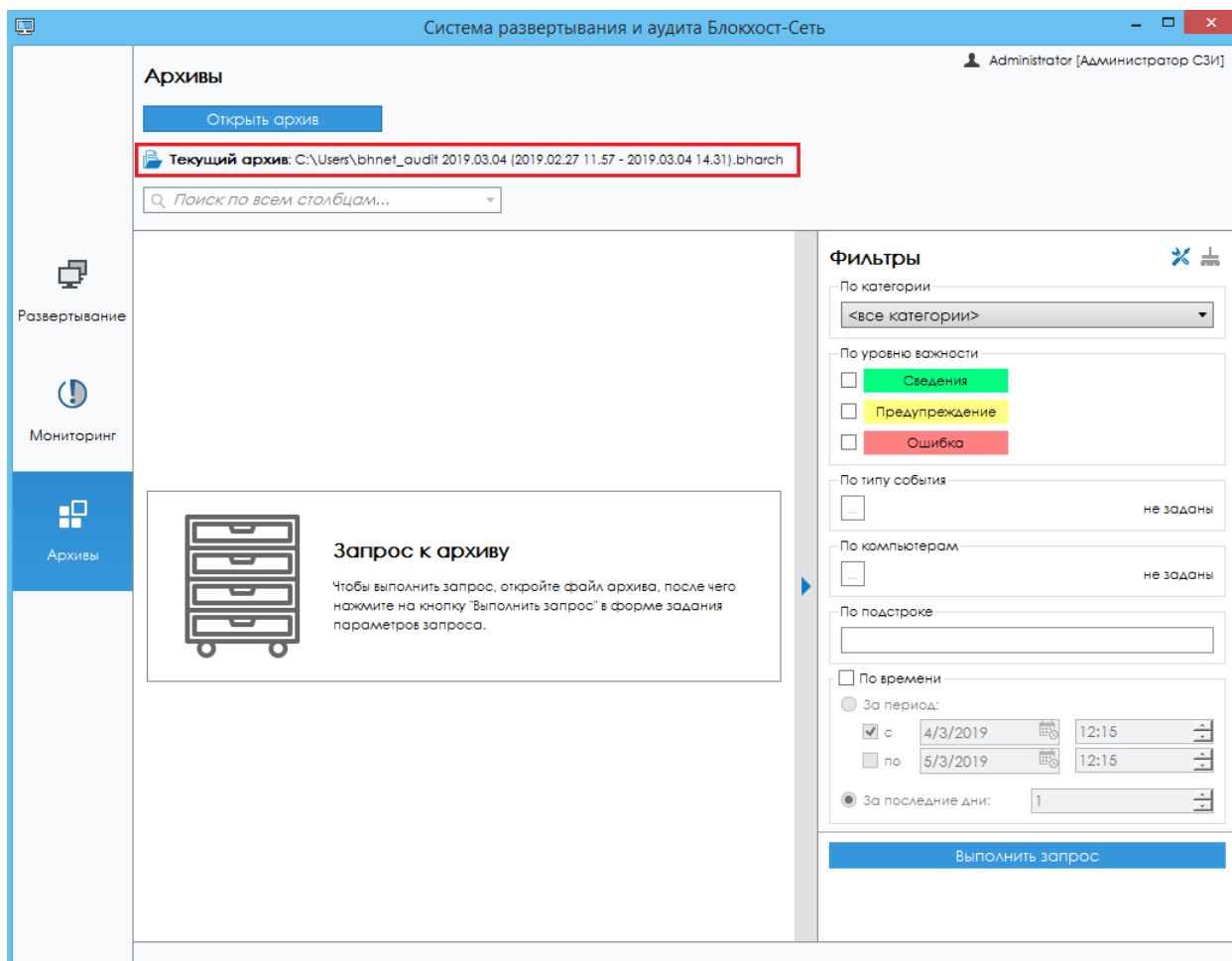


Рисунок 5.3 – Отображение директории выбранного архива

Обновление списка событий выбранного архива происходит при выполнении запроса и содержит информацию:

- «Время» - дата и время момента фиксации произошедшего события;
- «Событие» - краткое описание зафиксированного события (полный перечень событий, фиксируемых в консоли СРиА, приведен в Приложении 5 к документу «Средство защиты информации от несанкционированного доступа «Блокост-Сеть 3». Руководство администратора безопасности»);
- «Категория» - категория, которой принадлежит зафиксированное событие;
- «Уровень важности» - уровень важности зафиксированного события (сведения, предупреждения или ошибка).

Время	Событие	Категория	Уровень важности
13:00:00 14.12.2018	Изменение параметров работы СЗИ	События клиента СЗИ	Предупреждение
13:00:00 14.12.2018	Сервер администрирования запущен	События сервера СЗИ	Сведения
13:00:00 14.12.2018	Подключение к серверу	События клиента СЗИ	Сведения
13:00:00 14.12.2018	Подключение клиента к серверу	События сервера СЗИ	Сведения
13:00:47 14.12.2018	Создание задачи на установку агента системы развертывания	Система развертывания	Сведения
13:00:47 14.12.2018	Создание задачи на установку произвольной программы	Система развертывания	Сведения
13:00:53 14.12.2018	Запуск консоли СЗИ	Действия администратора СЗИ	Сведения
13:02:54 14.12.2018	Изменение параметров работы СЗИ	Действия администратора СЗИ	Сведения
13:02:55 14.12.2018	Подключение к головному серверу	События сервера СЗИ	Сведения
13:02:55 14.12.2018	Отключение от головного сервера	События сервера СЗИ	Сведения
13:02:57 14.12.2018	Подключение к головному серверу	События сервера СЗИ	Сведения
13:02:57 14.12.2018	Отключение от головного сервера	События сервера СЗИ	Сведения
17:34:35 14.12.2018	Подключение к головному серверу	События сервера СЗИ	Сведения
17:35:01 14.12.2018	Подключение к головному серверу	События сервера СЗИ	Сведения
18:58:43 14.12.2018	Выход пользователя из системы	Аутентификация	Сведения
18:58:43 14.12.2018	Сервер администрирования остановлен	События сервера СЗИ	Сведения
09:18:50 17.12.2018	Подключение к головному серверу	События сервера СЗИ	Сведения
09:18:50 17.12.2018	Подключение к серверу	События клиента СЗИ	Сведения
09:18:50 17.12.2018	Подключение клиента к серверу	События сервера СЗИ	Сведения
09:18:51 17.12.2018	Сервер администрирования запущен	События сервера СЗИ	Сведения
09:30:08 17.12.2018	Открытие сессии управления по иерархии	События сервера СЗИ	Сведения
17:34:49 14.12.2018	Отказ в установке соединения	События сервера СЗИ	Ошибка
17:34:51 14.12.2018	Отказ в установке соединения	События сервера СЗИ	Ошибка
17:34:59 14.12.2018	Отказ в установке соединения	События сервера СЗИ	Ошибка
09:18:49 17.12.2018	Отказ в подключении к серверу	События клиента СЗИ	Ошибка

Фильтры
По категории
<все категории>
По уровню важности
☐ Сведения
☐ Предупреждение
☐ Ошибка
По типу события
☐ не заданы
По компьютерам
☐ не заданы
По подстроке

По времени
☐ За период:
☒ с 4/3/2019 12:15
☐ по 5/3/2019 12:15
☐ За последние дни:
1
Выполнить запрос

Рисунок 5.4 – Список событий после выполнения запроса

В верхней части окна, над списком событий, располагается поле ввода критериев отбора объектов из списка **Поиск по всем столбцам...** Проверка соответствия введенного в поле ввода значения осуществляется по значениям сразу всех колонок (рисунок 4.13).

Для выполнения запроса к выбранному архиву необходимо в области **Фильтры** ввести данные о параметрах запроса (по каким параметрам будет осуществляться выборка событий: по категориям, по уровню важности, по типу события, по подстроке, по времени):

- 1) «По категории» - выборка событий, относящихся только к заданной категории (значение <все источники>, установленное по умолчанию, отфильтрует список событий по всем категориям).
- 2) «По уровню важности» - выборка событий только с заданным уровнем важности.
- 3) «По типу событий» - выборка событий только указанных типов (подробнее, параметр «По типу событий» описан в п. 3 подпункта «4.4.3.2 Настройка параметров запроса»).
- 4) «По подстроке» - выборка осуществляется по подробной информации события.



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

- 5) «По времени» - выборка событий за определенный период времени (подробнее, параметр «По времени» описан в п. 5 подпункта «4.4.3.2 Настройка параметров запроса»).

После выбора всех необходимых параметров запроса, для выборки событий необходимо нажать кнопку **Выполнить запрос**. При этом список в основной части раздела **Архивы** обновится в соответствии с введенными параметрами запроса.



|| При отсутствии в архиве событий, соответствующих заданным фильтрам, в основной части раздела появится сообщение вида:

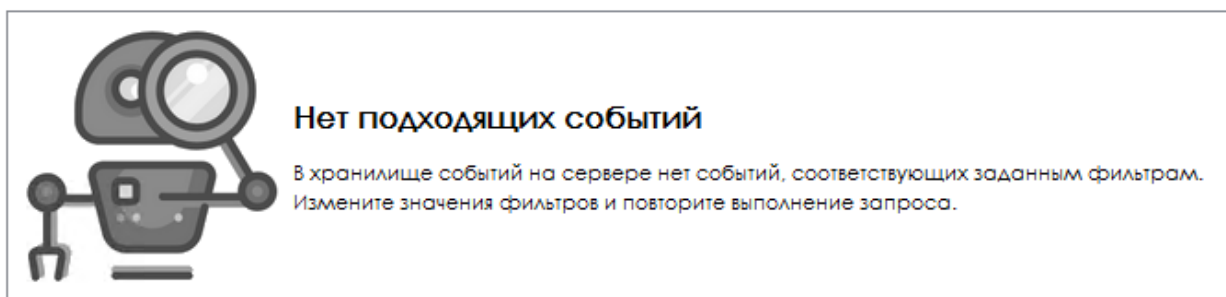


Рисунок 5.5 – Сообщение об отсутствии событий, соответствующих фильтрам

Для сброса параметров фильтрации администратору безопасности необходимо нажать кнопку **Сбросить фильтры** «», расположенную в правом верхнем углу области **Фильтры** (рисунок 4.31).

Кнопка **Дополнительные параметры** «» позволяет настроить максимальное количество событий, собранных по запросу и отображаемых в консоли СРиА. При нажатии на кнопку появится окно для ввода максимального количества событий (рисунок 4.36).

6 Создание и восстановление резервной копии данных сервера СРиА

Регулярное резервирование данных необходимо для сохранения максимума информации при возникновении внезапных сбоев в работе сервера СРиА. Рекомендуется выполнять резервирование данных перед внесением изменений в настройки, обновлением, а также перед переносом данных на другой сервер.

Для обеспечения бесперебойной работы СРиА (быстрого восстановления работы в случае возникновения сбоев) рекомендуется осуществлять резервирование данных на регулярной основе.

Для выполнения операций создания или восстановления резервной копии данных сервера СРиА, необходимо запустить мастер настройки системы развертывания и аудита. Вызов мастера настройки СРиА осуществляется в меню **Пуск** пункт **Все программы** → **Блокхост-Сеть 3** → **Система развертывания и аудита** → **Мастер настройки системы**. (на рисунке 2.1 показан вызов консоли СРиА в ОС Windows 2016).

6.1 Создание резервной копии данных сервера СРиА

Для создания резервной копии данных сервера СРиА администратору безопасности необходимо выполнить следующие действия в мастере настройки системы развертывания:

- 1) В открывшемся окне мастера настройки системы выбрать пункт **Создание резервной копии** и нажать кнопку **Далее** (рисунок 6.1).

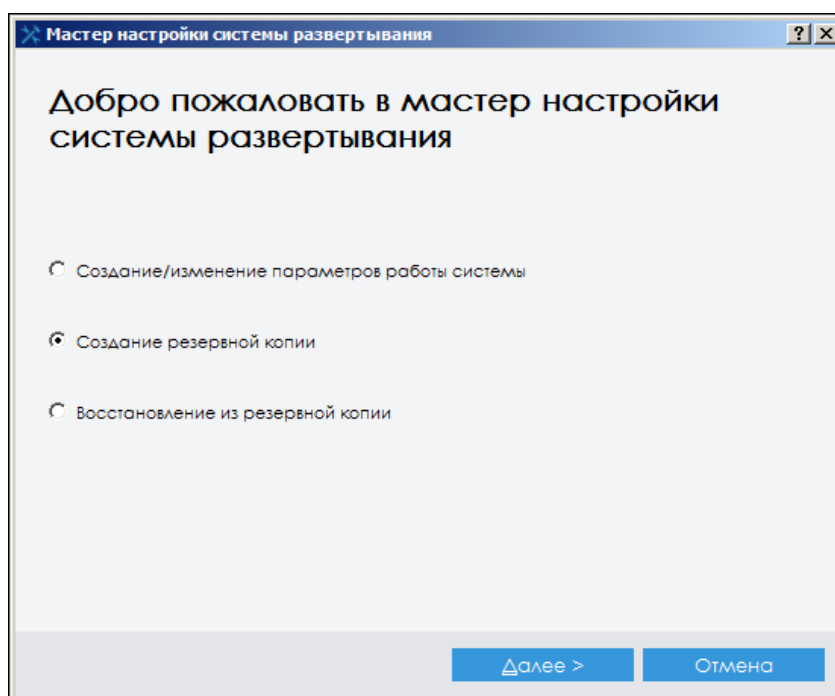


Рисунок 6.1 – Запуск мастера настройки СРиА

2) На следующем шаге мастера настройки системы указать каталог для создания резервной копии по кнопке **Выбрать** (рисунок 6.2) и нажать кнопку **Далее** для продолжения работы мастера.



В резервную копию будут помещены все инсталляционные пакеты ПО. Для уменьшения размера резервной копии рекомендуется удалить неиспользуемые инсталляционные пакеты и задачи.

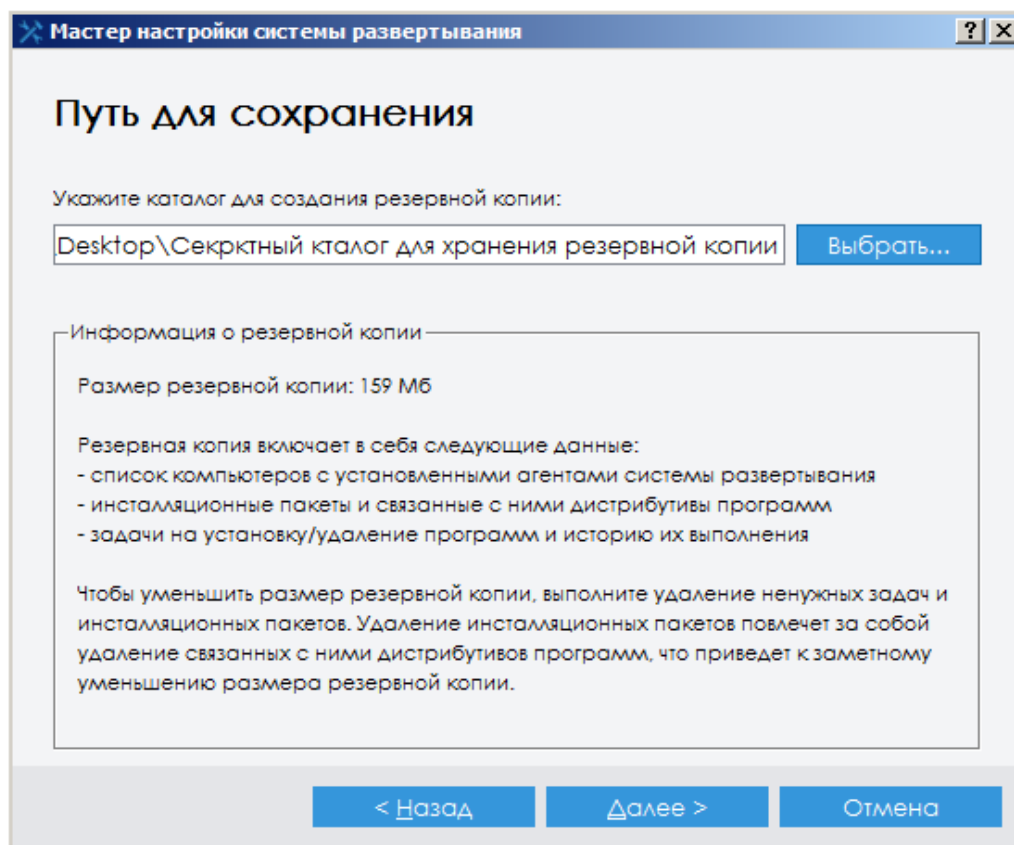


Рисунок 6.2 – Выбор каталога для сохранения резервной копии

3) На следующем шаге необходимо ввести пароль для защиты создаваемой резервной копии и подтвердить введенный пароль в соответствующем поле (рисунок 6.3).

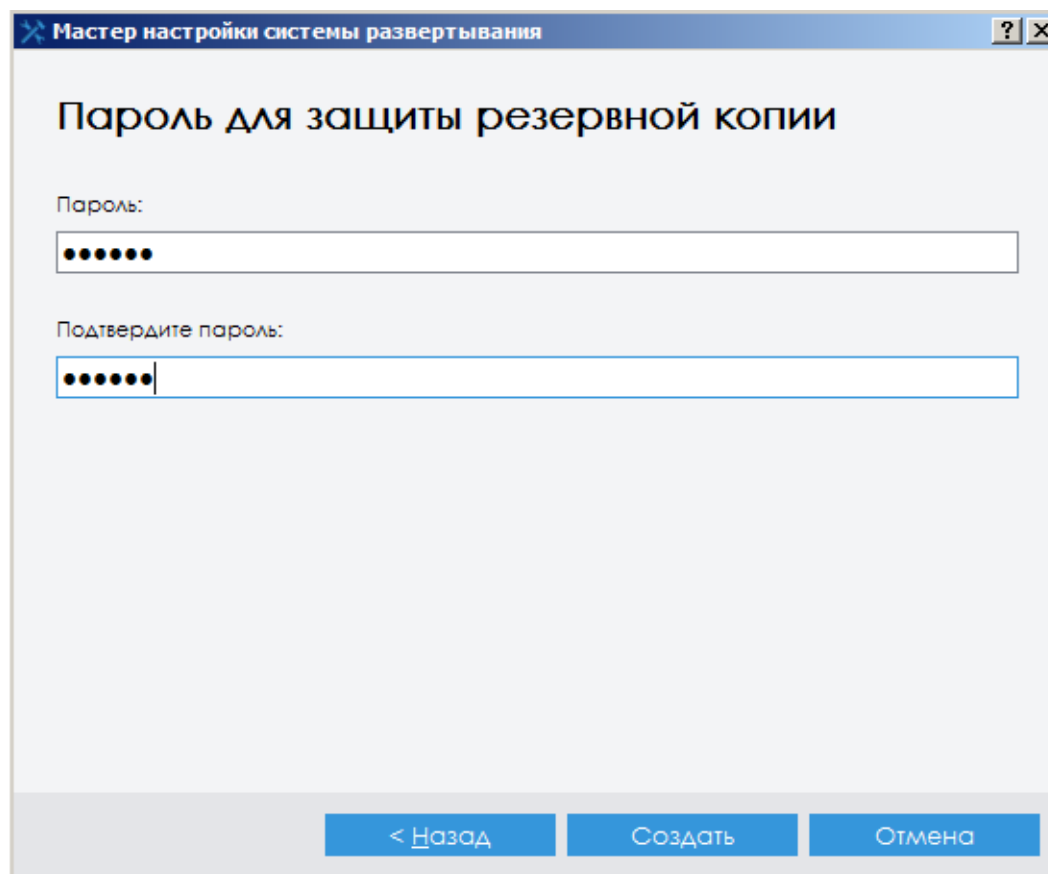


Рисунок 6.3 – Ввод пароля для защиты резервной копии

В результате работы мастера настройки по созданию резервной копии данных сервера СРиА по указанному пути будет создан каталог, в котором будет находиться резервная копия в зашифрованном виде (рисунок 6.4).

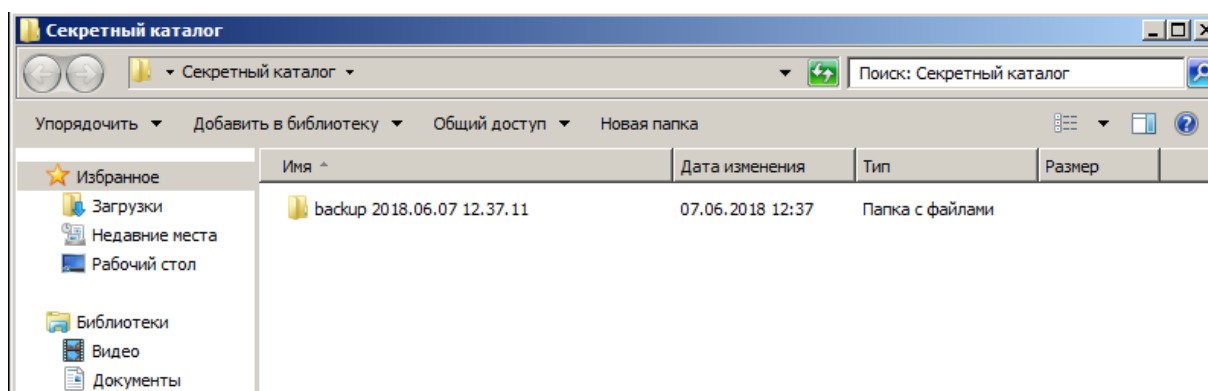


Рисунок 6.4 – Отображение созданной резервной копии в каталоге

6.2 Восстановление резервной копии данных сервера СРиА

Для восстановления данных сервера СРиА из резервной копии администратору безопасности необходимо выполнить следующие действия в мастере настройки системы развертывания:

- 1) В открывшемся окне мастера настройки системы развертывания выбрать пункт

Восстановление из резервной копии и нажать кнопку **Далее**:

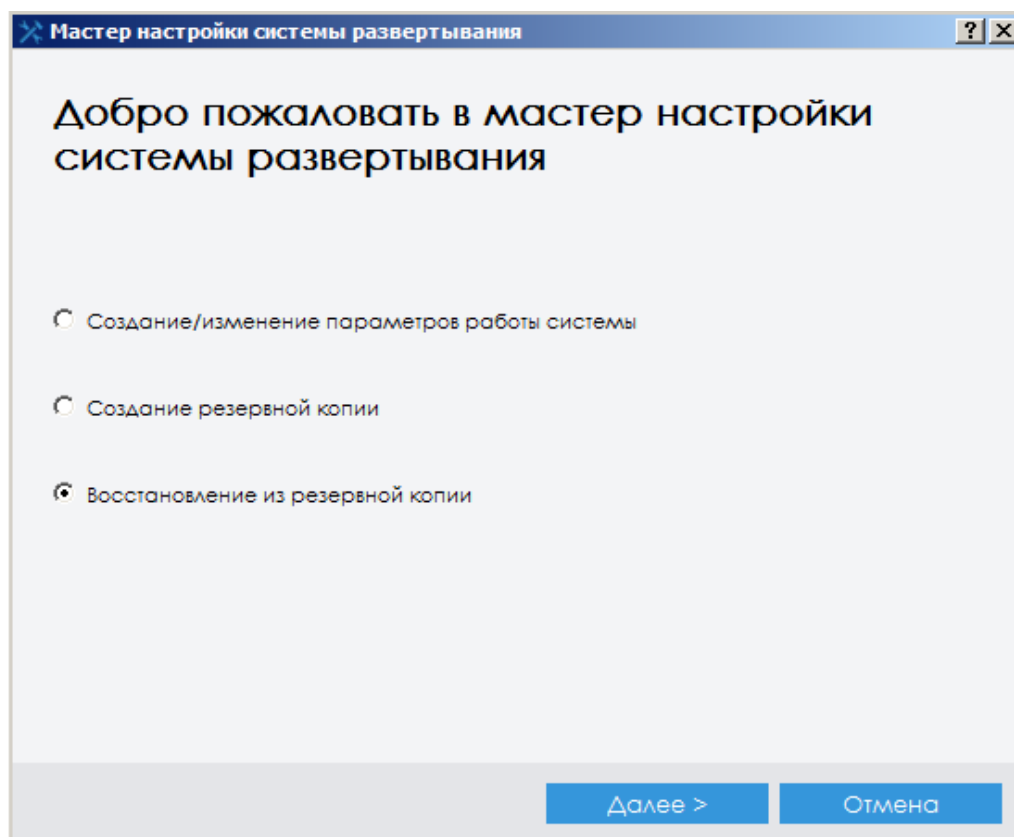


Рисунок 6.5 – Запуск мастера настройки

2) На следующем шаге мастера настройки системы развертывания указать каталог, содержащий резервную копию, по кнопке **Выбрать** (рисунок 6.6), ввести пароль к выбранной резервной копии, и нажать кнопку **Далее** для продолжения работы мастера.

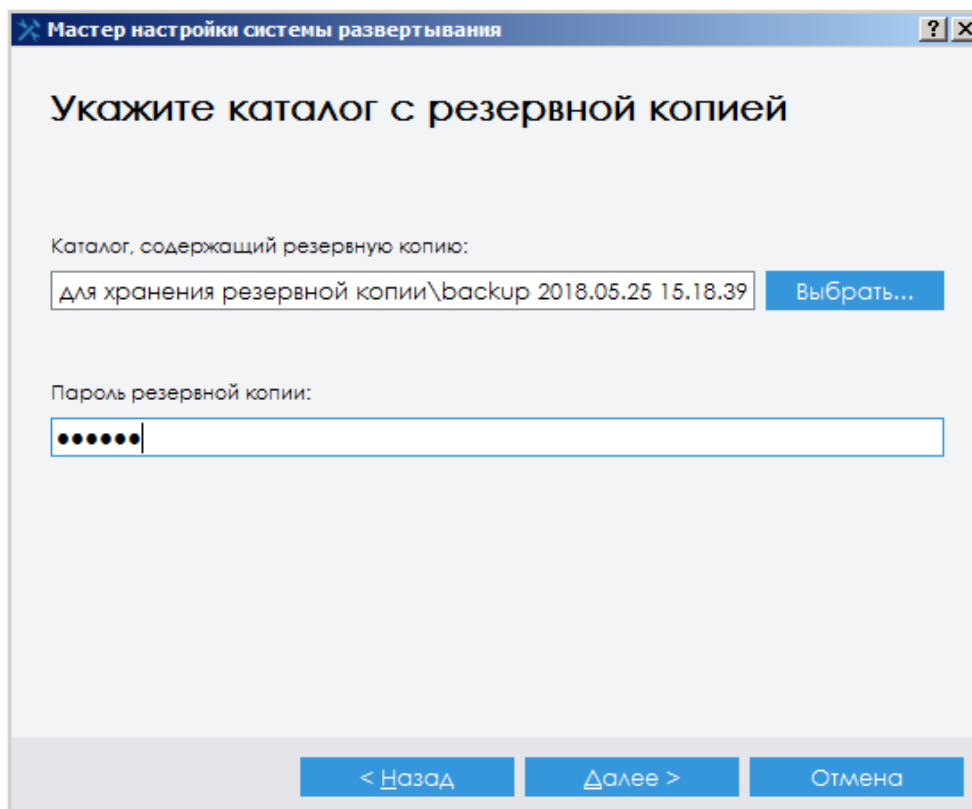


Рисунок 6.6 – Указание пути к каталогу с резервной копией

- 3) На следующем шаге необходимо выбрать из списка активный сетевой интерфейс, который будет выполнять взаимодействие с сетью (рисунок 6.7) и нажать кнопку **Далее**.

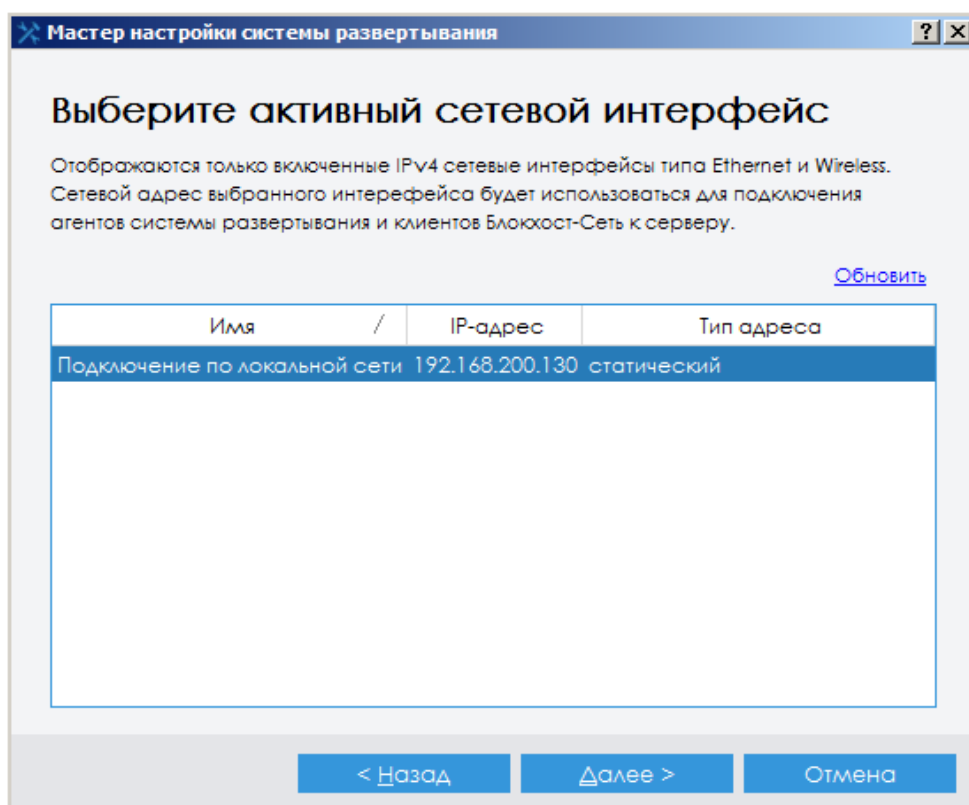


Рисунок 6.7 –Выбор активного сетевого интерфейса

- 4) На следующем шаге необходимо настроить параметры удаленного доступа и логирования (рисунок 6.8) (подробнее см. подраздел «1.2 Настройка консоли СРиА»).

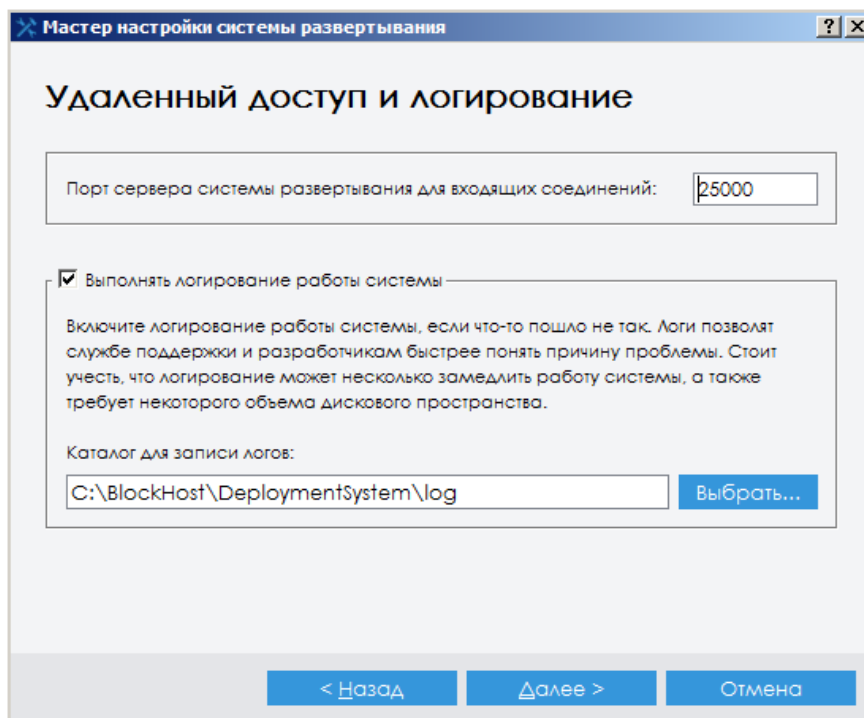


Рисунок 6.8 – Настройка удаленного доступа и логирования

- 5) В появившемся окне для начала процесса восстановления данных нажать кнопку **Готово**:

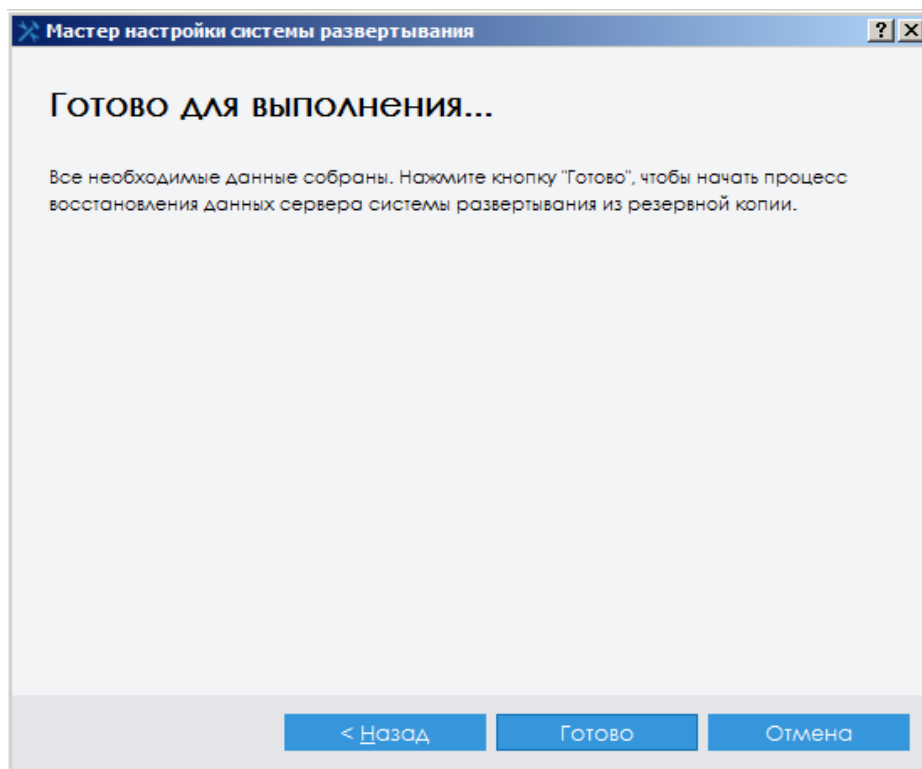


Рисунок 6.9 – Окно подтверждения начала процесса восстановления данных

- 6) В окне завершения работы мастера, после успешного восстановления данных, нажать кнопку **Завершить**:

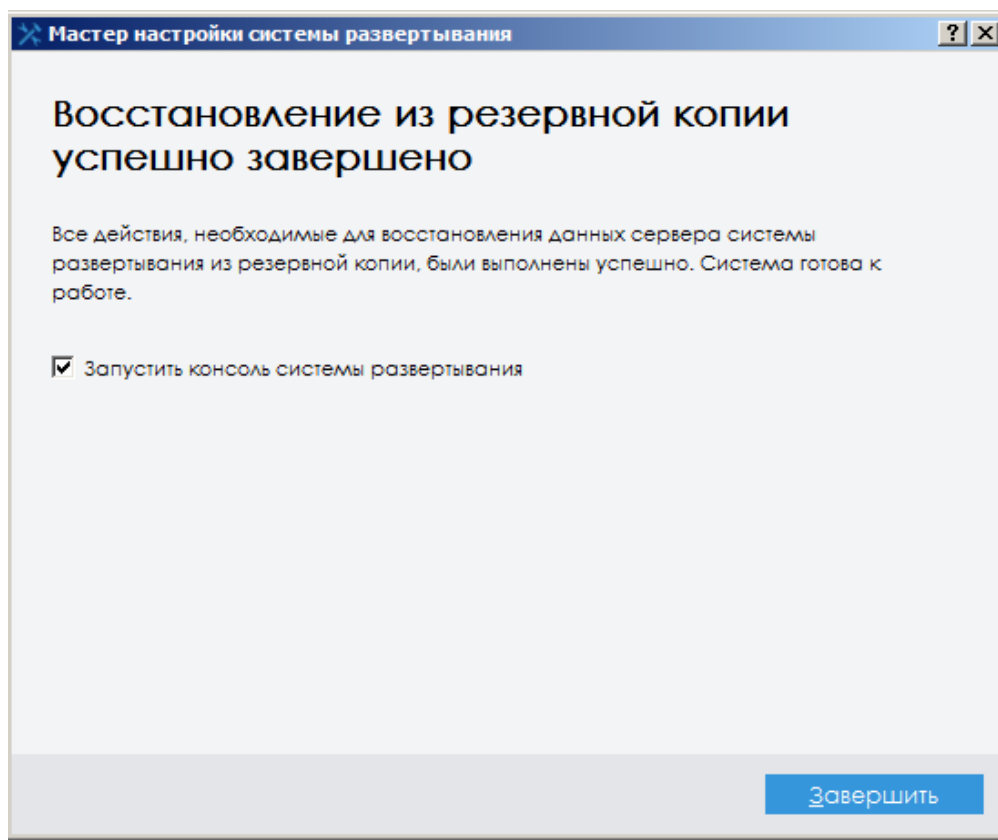


Рисунок 6.10 – Окно успешного выполнения операции восстановления

В результате работы мастера настройки по восстановлению данных из резервной копии, конфигурация данных сервера СРиА будет восстановлена.

Перечень сокращений

АРМ	–	Автоматизированное Рабочее Место
ОС	–	Операционная Система
НСД	–	Несанкционированный Доступ
ПК	–	Программный Комплекс
ПО	–	Программное Обеспечение
СЗИ	–	Средство Защиты Информации
СРиА	–	Система Развертывания и Аудита
СУБД	–	Система Управления Базами Данных
ЭВМ	–	Электронно-Вычислительная Машина