



ГАЗИНФОРМСЕРВИС

198096, г. Санкт-Петербург, ул. Кронштадтская, д.10, лит. А, тел.: (812) 677-20-50, факс: (812) 677-20-51
Почтовый адрес: 198096, г. Санкт-Петербург, а/я 59, e-mail: resp@gaz-is.ru, www.gaz-is.ru
р/с 40702810800000001703 Ф-л Банка ГПБ (АО) в г. Санкт-Петербурге БИК 044030827,
к/с 30101810200000000827, ОКПО 72410666, ОГРН 1047833006099, ИНН/КПП 7838017968/783450001

Средство защиты информации от несанкционированного доступа «Блокхост-сеть 2.0»

Руководство по инсталляции (сетевой вариант)



Санкт-Петербург, 2017



Содержание

1.	Установка СЗИ «Блокхост-сеть 2.0»	3
1.1.	Требования к аппаратной конфигурации	3
1.2.	Требования к составу установленного программного обеспечения	3
1.3.	Порядок установки серверной части СЗИ «Блокхост-сеть 2.0»	7
1.4.	Установка клиентской части СЗИ.....	13
2.	Деинсталляция СЗИ «Блокхост-сеть 2.0».....	35
2.1.	Деинсталляция сервера СЗИ «Блокхост-сеть 2.0»	35
2.2.	Деинсталляция клиентской части СЗИ «Блокхост-сеть 2.0»	37
3.	Обновление СЗИ «Блокхост-сеть 2.0»	39
3.1.	Обновление серверной части СЗИ.....	39
3.2.	Обновление клиентской части СЗИ.....	39

1. Установка СЗИ «Блокхост-сеть 2.0»

1.1. Требования к аппаратной конфигурации

СЗИ «Блокхост-сеть 2.0» (сетевой вариант) поставляется в виде файлов Microsoft Windows Installer *BlockHost-Net-2.0 x32.msi*, *BlockHost-Net-2.0 x64.msi* для установки серверной части СЗИ на 32- и 64-битные ОС Windows соответственно и *BlockHost-Net-2.0-Client x32.msi*, *BlockHost-Net-2.0-Client x64.msi* для установки клиентской части СЗИ на 32- и 64-битные ОС Windows соответственно. Также в состав дистрибутива сетевого варианта СЗИ «Блокхост-сеть 2.0» входит файл *BhNet.Installer.exe*, который содержит в себе дистрибутивы клиентской части СЗИ для ОС Windows 32- и 64-бит.

Серверная часть СЗИ «Блокхост-сеть 2.0» функционирует под управлением серверных ОС Windows. Клиентская часть СЗИ может быть установлена на ОС Windows, перечисленные в п. 1.2.1 настоящего руководства. При помощи инсталлятора серверной части СЗИ можно установить на рабочие места и только клиентскую часть СЗИ.

СЗИ «Блокхост-сеть 2.0» (сетевой вариант) устанавливается на компьютеры с процессорами, имеющими архитектуру x86 и AMD64. Для корректной работы СЗИ «Блокхост-сеть 2.0» предъявляются следующие требования к аппаратной конфигурации:

Тактовая частота процессора	Объем оперативной памяти	Объем свободного места на жестком диске	Сетевая карта	Режим видео, не менее
Определяются требованиями операционной системы			Ethernet	800x600, 256 цветов

Для функционирования аппаратных персональных идентификаторов рабочая станция должна иметь:

- USB-порт – при использовании идентификаторов eToken, SafeNet eToken, ruToken, JaCarta, eSmart Token (USB-ключ и смарт-карта), Avest Token и USB-носителей.
- дисковод гибких дисков – при использовании идентификаторов на дискетах.

1.2. Требования к составу установленного программного обеспечения

1.2.1. Общие требования к составу установленного программного обеспечения

Допускается установка СЗИ «Блокхост-сеть 2.0» на компьютеры, функционирующие под управлением операционных систем:

1) серверная часть СЗИ:

- Windows Server 2008R2 Foundation Edition SP1 (64-разрядная);
- Windows Server 2008R2 Standard Edition SP1 (64-разрядная);
- Windows Server 2008R2 Enterprise Edition SP1 (64-разрядная);
- Windows Server 2008R2 Datacenter Edition SP1 (64-разрядная);
- Windows Server 2012/2012R2 Foundation (64-разрядная);
- Windows Server 2012/2012R2 Essentials (64-разрядная);

- Windows Server 2012/2012R2 Standard (64-разрядная);
- Windows Server 2012/2012R2 Datacenter (64-разрядная);
- Windows Server 2016 Standard (64-разрядная);
- Windows Server 2016 Datacenter (64-разрядная);
- Windows Server 2016 Essentials (64-разрядная).

2) клиентская часть СЗИ:

- Windows Server 2008R2 Foundation Edition SP1 (64-разрядная);
- Windows Server 2008R2 Standard Edition SP1 (64-разрядная);
- Windows Server 2008R2 Enterprise Edition SP1 (64-разрядная);
- Windows Server 2008R2 Datacenter Edition SP1 (64-разрядная);
- Windows Vista Business SP2 (32-разрядная);
- Windows Vista Business SP2 (64-разрядная);
- Windows 7 Home Basic SP1 (32-разрядная);
- Windows 7 Home Basic SP1 (64-разрядная);
- Windows 7 Home Premium SP1 (32-разрядная);
- Windows 7 Home Premium SP1 (64-разрядная);
- Windows 7 Professional SP1 (32-разрядная);
- Windows 7 Professional SP1 (64-разрядная);
- Windows 7 Enterprise SP1 (32-разрядная);
- Windows 7 Enterprise SP1 (64-разрядная);
- Windows 7 Ultimate SP1 (32-разрядная);
- Windows 7 Ultimate SP1 (64-разрядная);
- Windows 8/8.1 Core (32-разрядная);
- Windows 8/8.1 Core (64-разрядная);
- Windows 8/8.1 Professional (32-разрядная);
- Windows 8/8.1 Professional (64-разрядная);
- Windows 8/8.1 Enterprise (32-разрядная);
- Windows 8/8.1 Enterprise (64-разрядная);
- Windows Server 2012/2012R2 Foundation (64-разрядная);
- Windows Server 2012/2012R2 Essentials (64-разрядная);
- Windows Server 2012/2012R2 Standard (64-разрядная);
- Windows Server 2012/2012R2 Datacenter (64-разрядная);
- Windows 10 Home/Home N (32-разрядная);
- Windows 10 Home/Home N (64-разрядная);
- Windows 10 Pro/Pro N (32-разрядная);
- Windows 10 Pro/Pro N (64-разрядная);
- Windows 10 Enterprise/Enterprise N (32-разрядная);
- Windows 10 Enterprise/Enterprise N (64-разрядная);
- Windows Server 2016 Standard (64-разрядная);
- Windows Server 2016 Datacenter (64-разрядная);
- Windows Server 2016 Essentials (64-разрядная).

В составе программного установленного обеспечения необходимы следующие компоненты:

- .NET Framework 3.5 (для работы модуля контроля целостности реестра);

- .NET Framework 4.0 (с обновлением NDP40-KB2468871) или выше (для работы консоли администрирования СЗИ);
- Обновление системы безопасности KB3033929 (для ОС Windows Server 2008/2008R2);
- драйверы для устройств eToken и SafeNet eToken (любой из вариантов):
1 SafeNet Authentication Client 8.2. Подходит для всех поддерживаемых ОС, в комплект поставки СЗИ не входит.
2 eToken PKI Client 5.1 SP1 или eToken RTE 3.66 – при использовании персональных идентификаторов eToken PRO, eToken NG-FLASH, eToken NG-ОТР;
3 eToken PKI Client 5.1 SP1 – при использовании персональных идентификаторов eToken NG-FLASH (Java), eToken NG-ОТР (Java), eToken PRO (Java), eToken GT (Java), eToken PRO (Java) SC, eToken PRO SC;
- драйверы для устройств ruToken (версия 4.2.4.0 и выше) – при использовании персональных идентификаторов ruToken;
- драйверы «Единый клиент JaCarta» для устройств JaCarta PRO, JaCarta ГОСТ, JaCarta PKI – при использовании персональных идентификаторов JaCarta;
- драйверы «ESMART PKI Client» для устройств eSmart Token (при использовании персональных идентификаторов eSmart Token USB 64K и eSmart Token SC 64K);
- драйверы AvBignDriver, устанавливаемые в составе пакета Avest CSP Bign, для поддержки персональных идентификаторов AvBign;
- СКЗИ «КриптоПро CSP» версии 3.6 и выше или СКЗИ «ViPNET CSP» версии 3.2 – при организации входа пользователей в ОС с помощью сертификатов.

Для корректного отображения символов русского алфавита перед инсталляцией СЗИ на англоязычных ОС следует установить **Русский язык** в качестве **Языка системы** для программ, не поддерживающих Юникод

Для сетевого взаимодействия серверной и клиентских частей СЗИ на сервере безопасности должен быть открыт 999 TCP-порт, а на контролируемых рабочих станциях – 5555 UDP-порт.



|| Установка СЗИ «Блокхост-сеть 2.0» должна выполняться на диск C:\.

СЗИ «Блокхост-сеть 2.0» имеет следующие ограничения:

- На жестком диске не должно быть других установленных операционных систем.
- На компьютере не должно быть динамических дисков, работу с ними «Блокхост-Сеть 2.0» не поддерживает. Также не поддерживается работа с твердотельными магнитными накопителями (SSD-дисками).
- Для устойчивой работы СЗИ и во избежание конфликта с другими программными средствами перед инсталляцией СЗИ необходимо удалить ранее установленные и не устанавливать новые программы, следящие за работой файловой системы.

К таким программам относятся:

- ☐ средства защиты от несанкционированного доступа;
- ☐ анализаторы файловой системы;

- утилиты мониторинга файловой системы (ProcessMonitor и т.п.).
- Использование антивирусных программ допускается после проверки их совместимости с программным комплексом СЗИ.
- Для корректной работы консолей администрирования СЗИ необходимо отключить параметр безопасности локальной политики ОС Windows **Системная криптография: использовать FIPS совместимые алгоритмы для шифрования, хеширования и подписывания**.
- Эксплуатация СЗИ «Блокхост-сеть 2.0» совместно с ОС семейства Windows допускается только в условиях выполненной активации операционной системы.
- Для эксплуатации и эффективного применения СЗИ «Блокхост-сеть 2.0» необходимо использование лицензионного системного ПО.
- Не рекомендуется ставить на контроль системные папки, так как это приводит к большому числу записей в журналы аудита и может повлиять на работоспособность СЗИ.

В некоторых случаях для корректного функционирования СЗИ необходимо понизить уровень контроля учетных записей (UAC) в ОС Windows (вплоть до полного отключения). Для изменения параметров UAC необходимо войти в ОС под учетной записью встроенного администратора.

1.2.3. Особенности установки СЗИ «Блокхост-сеть 2.0» на ПК под управлением ОС Windows 2012/2012R2

Перед началом установки СЗИ «Блокхост-сеть 2.0» необходимо отключить встроенный в ОС Windows 2012/2012R2 стандартный защитник Windows (Windows Defender), для чего следует:

- 1) запустить *Windows Defender* (*Пуск* → *Все приложения* → *Windows Defender*);

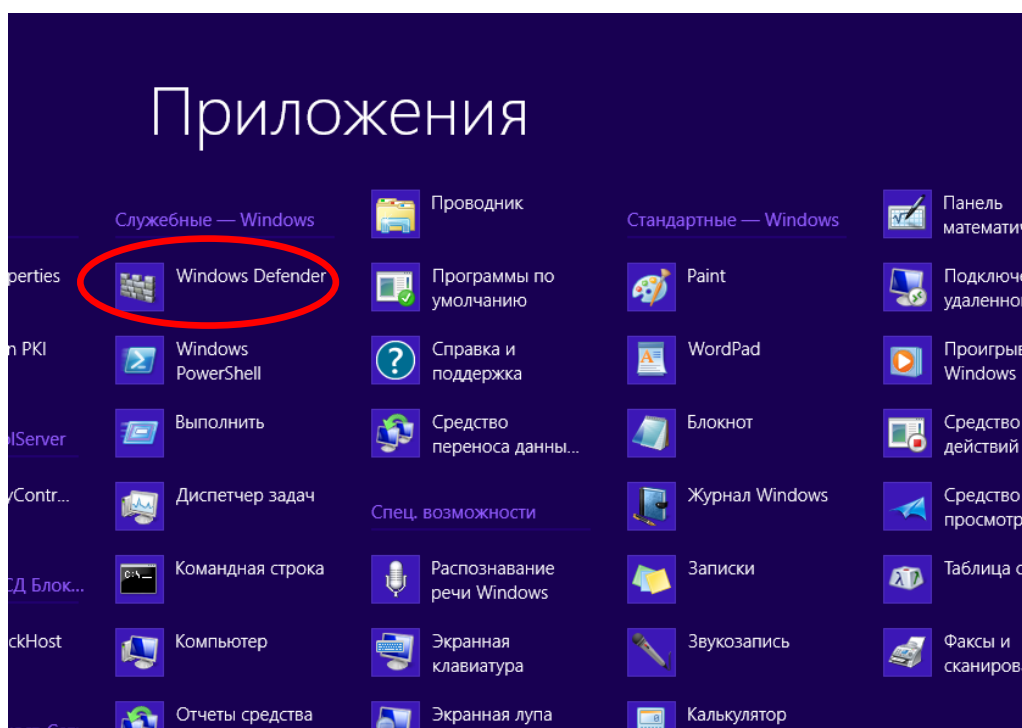


Рисунок 1. Выбор пункта «Windows Defender»

- 2) во вкладке **Параметры** окна «**Windows Defender**» выбрать пункт **Администратор**, снять флажок с пункта **Включить Windows Defender**.

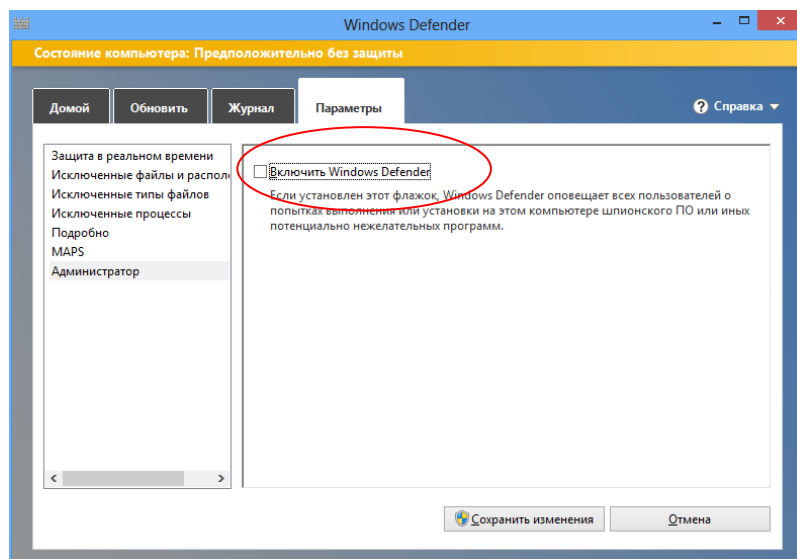


Рисунок 2. Отключение «Windows Defender»

После завершения процесса установки СЗИ «Блокхост-сеть 2.0» стандартный защитник Windows (Windows Defender) можно снова включить.

1.3. Порядок установки серверной части СЗИ «Блокхост-сеть 2.0»

Серверная часть СЗИ устанавливается на рабочее место администратора безопасности, одновременно с установкой серверной части на рабочее место администратора безопасности будет установлена и клиентская часть СЗИ. Инсталляция СЗИ производится с компакт-диска или другого носителя. Программа поставляется в виде файлов Microsoft Windows Installer *BlockHost-Net-2.0 x32.msi* (для 32-bit ОС) и *BlockHost-Net-2.0 x64.msi* (для 64-bit ОС). Мастер установки серверной части СЗИ «Блокхост-сеть 2.0» имеет оконный графический интерфейс.

ПЕРЕД ИНСТАЛЛЯЦИЕЙ СЗИ «БЛОКХОСТ-СЕТЬ 2.0» НЕОБХОДИМО УБЕДИТЬСЯ, ЧТО ДЛЯ ВСТРОЕННОЙ УЧЕТНОЙ ЗАПИСИ АДМИНИСТРАТОРА В ОС (ДОМЕНЕ) ЗАДАН ПАРОЛЬ!

Для инсталляции серверной части СЗИ необходимо войти в операционную систему под учетной записью встроенного администратора ОС Windows (контроллера домена). Запустить на выполнение файл-установщик СЗИ (*BlockHost-Net-2.0 x32.msi* – для 32-bit ОС или *BlockHost-Net-2.0 x64.msi* – для 64-bit ОС). Запустить файл-установщик на выполнение можно дважды щелкнув по нему в окне **Проводника** Windows или выполнив следующие действия:

- нажать на панели задач кнопку **Пуск**, выбрать команду **Выполнить...**;
- в окне «**Выполнить**» с помощью кнопки **Обзор...** выбрать на соответствующем диске необходимый файл-установщик СЗИ и нажать кнопку **Открыть**;
- в диалоговом окне «**Выполнить**» кнопкой **ОК** запустить выбранный файл на выполнение:

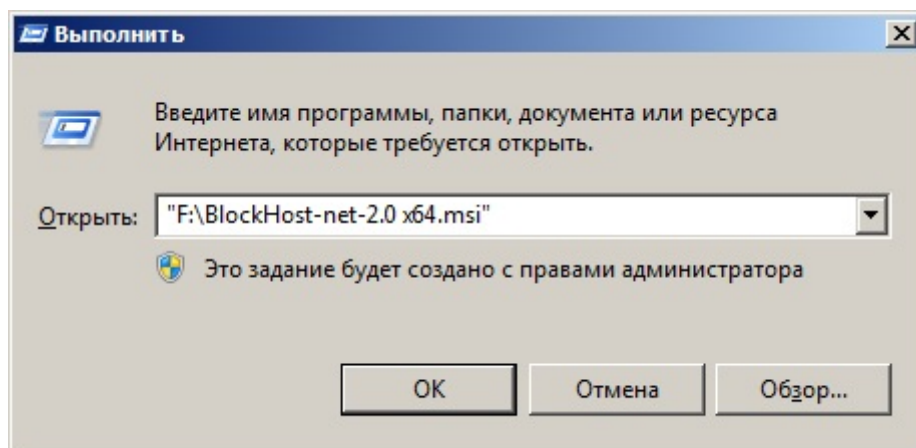


Рисунок 3. Запуск файла-установщика

В результате запуска файла-установщика на экране монитора появится окно приветствия мастера установки серверной части СЗИ «Блокхост-сеть 2.0» (рис. 4).

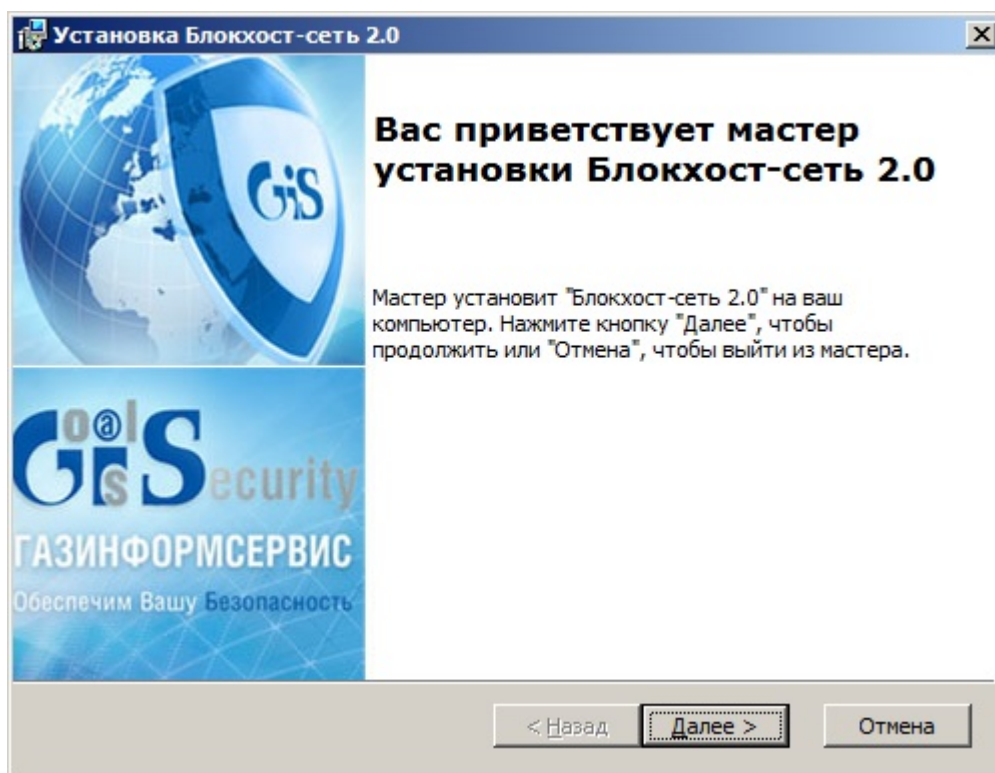


Рисунок 4. Окно мастера установки сервера СЗИ «Блокхост-сеть 2.0»

На любом этапе работы мастера установки серверной части СЗИ можно нажать кнопку **Отмена**. На экране появится окно, показанное на рисунке 5. При нажатии кнопки **Да** установка будет прервана. При нажатии кнопки **Нет** установка будет продолжена.

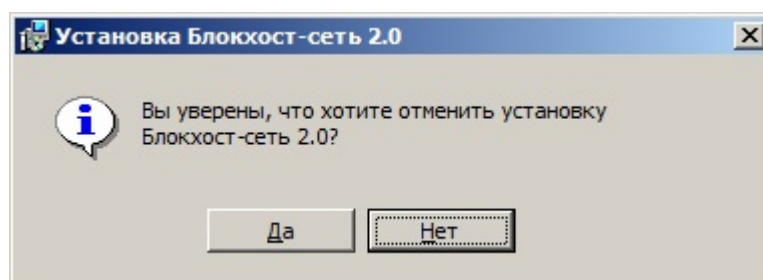


Рисунок 5. Окно прекращения установки

После нажатия в окне приветствия мастера установки СЗИ кнопки *Далее* (см. рис. 4) на экране монитора появится окно с текстом условий лицензионного соглашения (рис. 6).

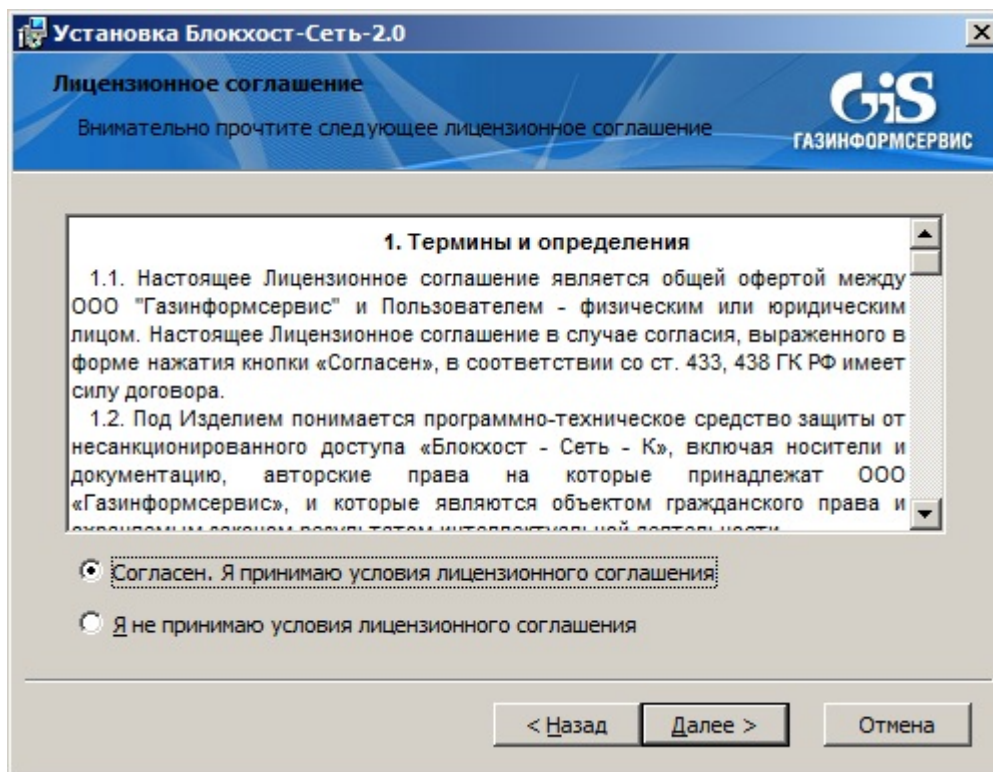


Рисунок 6. Окно мастера установки СЗИ «Блокхост-сеть 2.0» с лицензионным соглашением

Необходимо внимательно прочитать условия лицензионного соглашения. В случае несогласия с условиями лицензионного соглашения (выбран пункт ***Я не принимаю условиями лицензионного соглашения***) дальнейшая установка СЗИ становится невозможна (кнопка *Далее* – неактивна). Для выхода из программы установки СЗИ необходимо нажать кнопку *Отмена*.

В случае принятия условий лицензионного соглашения необходимо выбрать пункт ***Я принимаю условия лицензионного соглашения*** и нажать кнопку *Далее*. После этого появится окно (рис. 7), в котором необходимо ввести в соответствующие поля коды лицензий и коды активации клиентской части, сетевой и серверной лицензий СЗИ, которые прописаны в выданной лицензии.



Нельзя оставить незаполненными поля ввода кодов лицензий и кодов их активации – в этом случае на экране откроется окно с сообщением о необходимости ввода данных лицензий. Работа мастера установки СЗИ будет продолжена только в случае заполнения всех полей ввода данных лицензий.

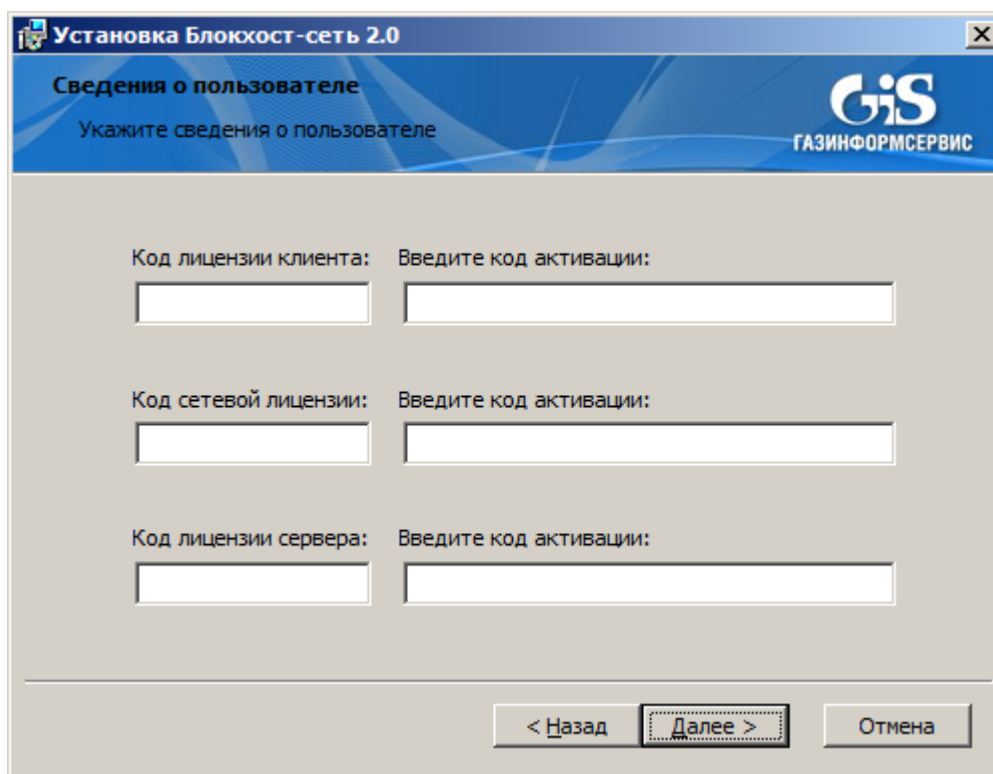


Рисунок 7. Окно ввода кода лицензии и кода активации СЗИ «Блокхост-сеть 2.0»

После заполнения полей ввода кода всех лицензий и кода их активации нажмите кнопку *Далее*. Если код лицензии или код активации был введен неверно, то на экране появится окно с сообщением об ошибке ввода кода активации лицензии (на рис. 8 показано окно с сообщением о неверном вводе кода активации лицензии клиентской части).

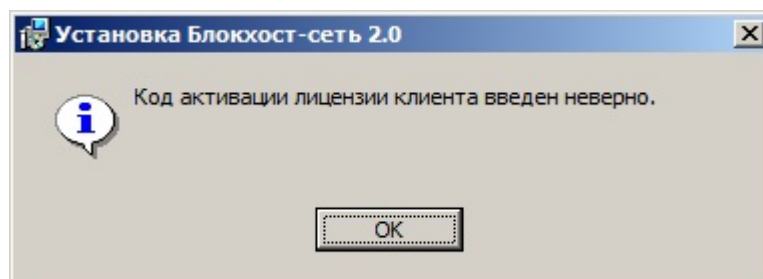


Рисунок 8. Окно с сообщением о неверно введенном коде

Если код лицензии и код активации были введены верно, установка будет продолжена и на экране появится окно формирования ключевого носителя администратора безопасности СЗИ (рис. 9).

Необходимо подключить к рабочей станции, на которую производится установка СЗИ, ключевой носитель, из выпадающего списка поля **Тип ключевого носителя** выбрать тип носителя (eToken, SafeNet eToken, ruToken, eSmart Token, Avest Token, USB-носитель, дискета или персональный идентификатор в реестре Windows. Электронный идентификатор JaCarta определится в списке, как eToken), ввести PIN-код доступа к ключевому носителю и его подтверждение в соответствующие поля. PIN-код доступа к ключевому носителю задается с помощью специального программного обеспечения, поставляемого вместе с носителем (ПО для SafeNet eToken, драйверы JaCarta для ОС Windows 8/8.1/2012/2012R2/10/2016, драйверы eSmart Token и Avest Token не входят в комплект поставки СЗИ). По умолчанию PIN-код eToken и SafeNet eToken – «1234567890», ruToken –

«12345678», JaCarta – «1234567890», AvBign – «12345678». Для USB-накопителя, дискеты и персонального идентификатора в реестре PIN-код задается средствами СЗИ «Блокхост-сеть 2.0» (если USB-накопитель или дискета использовались ранее в качестве персонального идентификатора администратора в СЗИ «Блокхост-сеть 2.0», то необходимо ввести PIN-код доступа к ним, установленный ранее). Если при установке СЗИ в поле **Тип ключевого носителя** выбрать пункт **Registry Add Device**, в защищенном хранилище реестра Windows будет создан ключ, содержащий информацию, идентичную информации для других типов ключевых носителей. Для продолжения установки нажмите кнопку **Далее**.



Следует учесть, что, если при установке серверной части СЗИ в качестве ключевого носителя используется персональный идентификатор в реестре Windows, то для генерации списка рабочих станций (через вкладку **Ручная генерация** серверной консоли администрирования СЗИ) и дальнейшего подключения их к серверу безопасности необходимо использовать другой вид носителя, например, eToken (подробнее см. документ «СЗИ «Блокхост-сеть 2.0». Руководство администратора безопасности»).

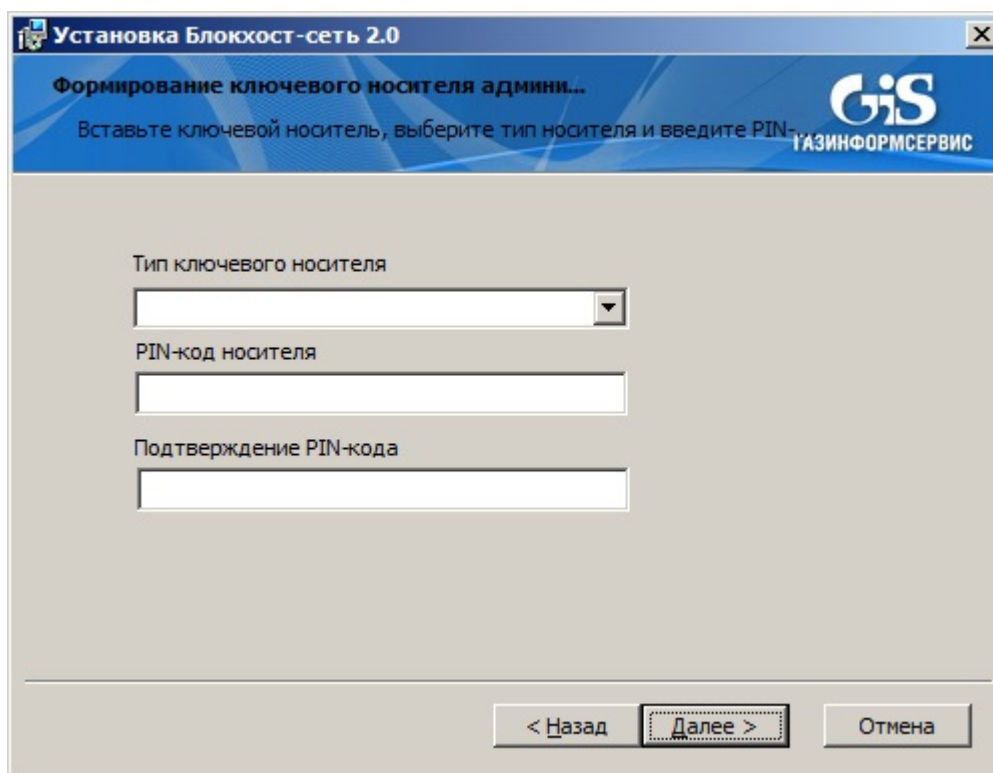


Рисунок 9. Окно формирования ключевого носителя администратора

Если введен неверный PIN-код доступа к ключевому носителю, то на экране появится сообщение, показанное на рис. 10. После нажатия на кнопку **ОК** происходит возврат в окно формирования ключевого носителя (рис. 9), в котором необходимо заново ввести PIN-код доступа к ключевому носителю.

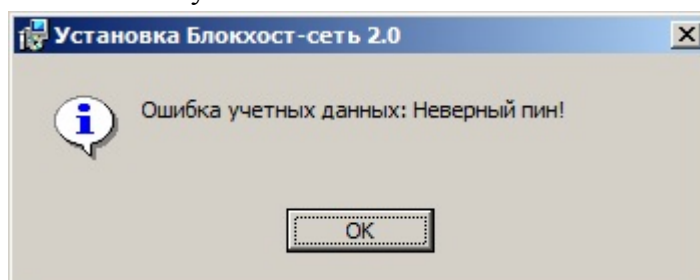


Рисунок 10. Окно сообщения о неверном PIN-коде

Если операция проверки PIN-кода доступа к ключевому носителю прошла успешно, то появится окно начала установки СЗИ (рис. 11), в котором необходимо нажать кнопку **Установить**, после чего начнется процесс установки серверной части СЗИ «Блокхост-сеть 2.0».

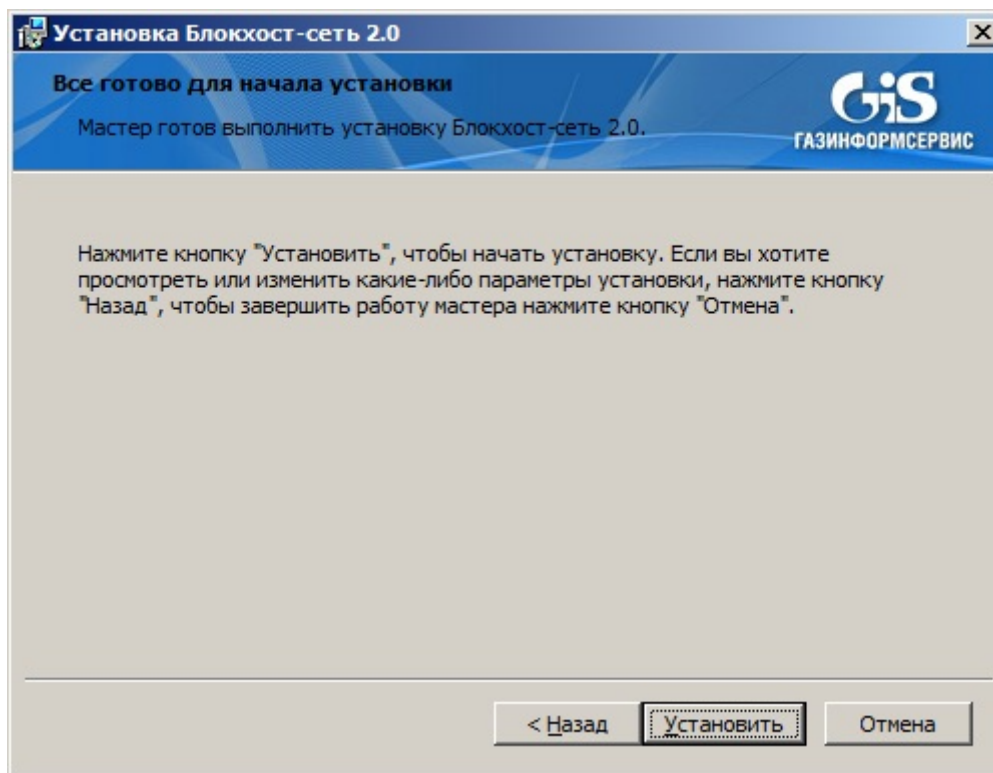


Рисунок 11. Окно готовности к установке СЗИ «Блокхост-сеть 2.0»

Ход установки будет отображаться в окне мастера установки (рис. 12), программный продукт будет установлен на локальный компьютер в папку **C:\BlockHost**.

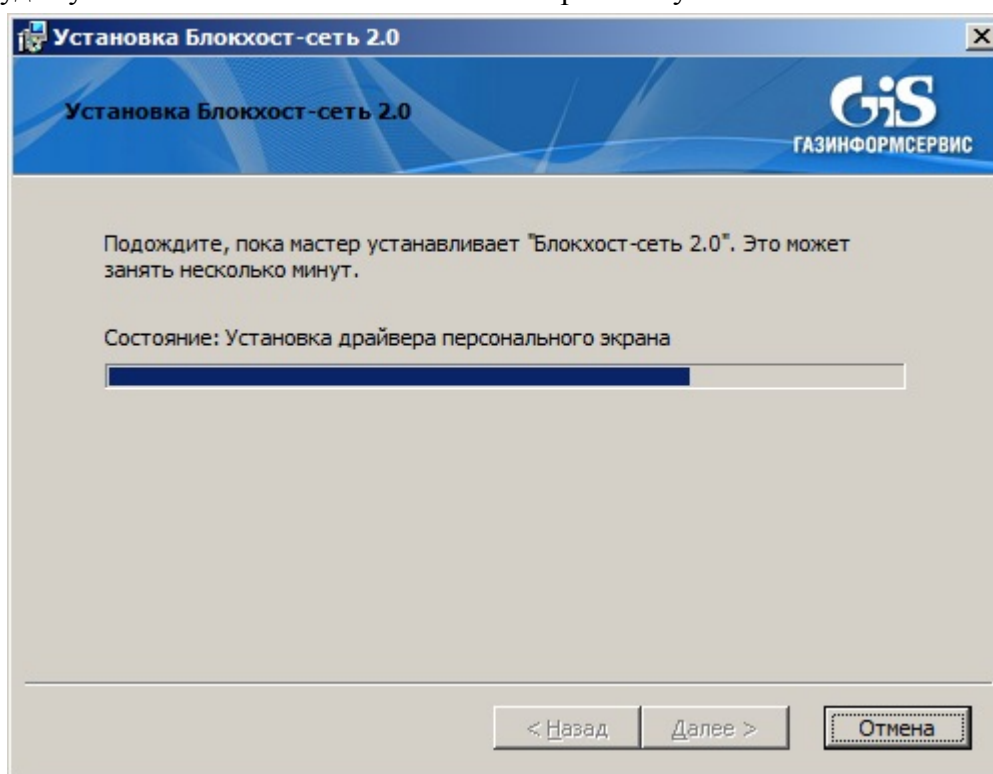


Рисунок 12. Ход установки СЗИ «Блокхост-сеть 2.0»

Если установка закончена успешно, то на экране появится окно окончания установки (рис. 13). Для окончания работы мастера установки СЗИ необходимо нажать кнопку **Готово**:

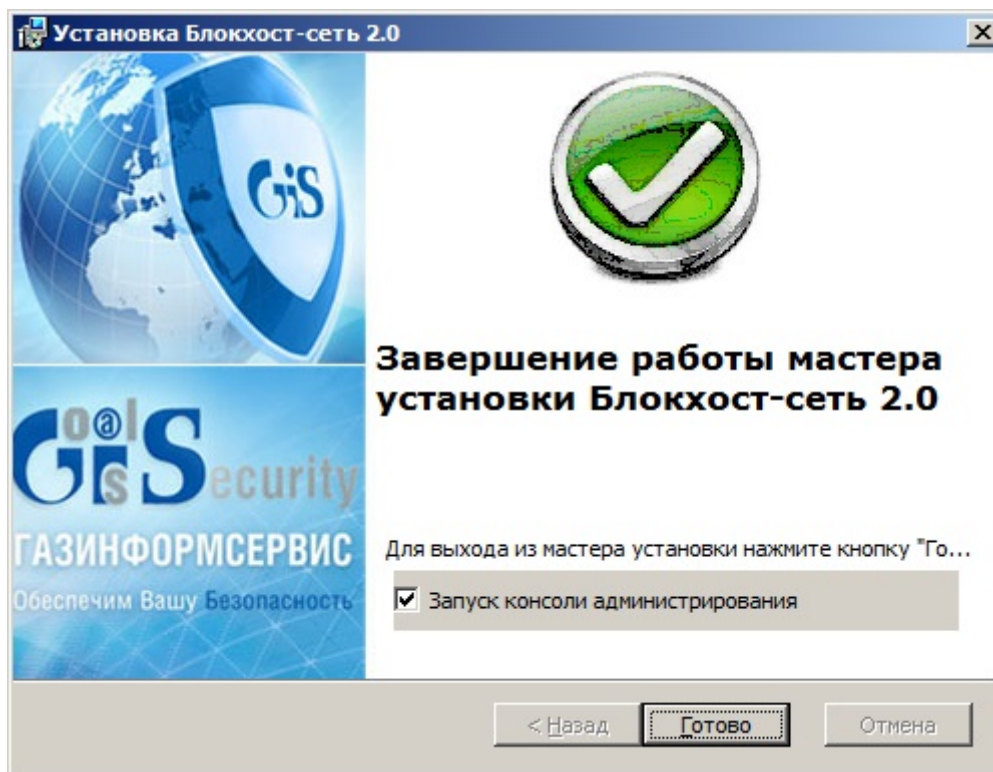


Рисунок 13. Окно окончания установки серверной части СЗИ «Блокхост-сеть 2.0»

В окне завершения работы мастера установки есть дополнительный параметр – **Запуск консоли администрирования** (см. рис. 22). При необходимости работы в серверной консоли администрирования СЗИ «Блокхост-сеть 2.0» сразу после окончания установки следует оставить отмеченным пункт **Запуск консоли администрирования** – в результате, после закрытия окна работы мастера установки СЗИ (нажата кнопка **Готово**), произойдет запуск серверной консоли администрирования СЗИ. Описание работы в серверной консоли СЗИ приведено в документе «Средство защиты информации от несанкционированного доступа «Блокхост-сеть 2.0». Руководство администратора безопасности (серверная консоль)».

1.4. Установка клиентской части СЗИ

1.4.1. Установка клиентской части СЗИ из серверной консоли администрирования СЗИ

Установка клиентской части СЗИ из серверной консоли администрирования заключается в последовательном выполнении следующих шагов:

- запустить серверную консоль администрирования СЗИ;
- перейти во вкладку **Развертывание MSI пакетов**;
- сформировать список рабочих станций сети, на которые будет осуществляться установка клиентской части СЗИ;
- ввести идентификационные данные пользователя (члена группы **Администраторы** удаленной рабочей станции), от имени которого будет

производиться установка;

- указать размещение файла-дистрибутива клиентской части СЗИ и ввести параметры подключения клиентской части к серверу СЗИ в соответствующее поле ввода;
- загрузить файл-установщик клиентской части СЗИ на удаленную рабочую станцию, выполнив соответствующую команду в серверной консоли администрирования СЗИ.

Для установки клиентской части СЗИ «Блокхост-сеть 2.0» на удаленные рабочие станции из серверной консоли администрирования СЗИ администратору безопасности необходимо:

1. Запустить серверную консоль администрирования СЗИ выбрав пункт меню **Пуск** → **Все программы** → **Блокхост-сеть 2.0** → **ConsoleServerBlockHost (Start → All Programs → Blockhost-net 2.0 → ConsoleServerBlockHost)**
2. В окне «Список машин» выделить пункт **Все машины**;
3. Выбрать пункт главного меню **Развертывание** → **Развертывание MSI пакетов** – откроется вкладка **Развертывание MSI пакетов**:

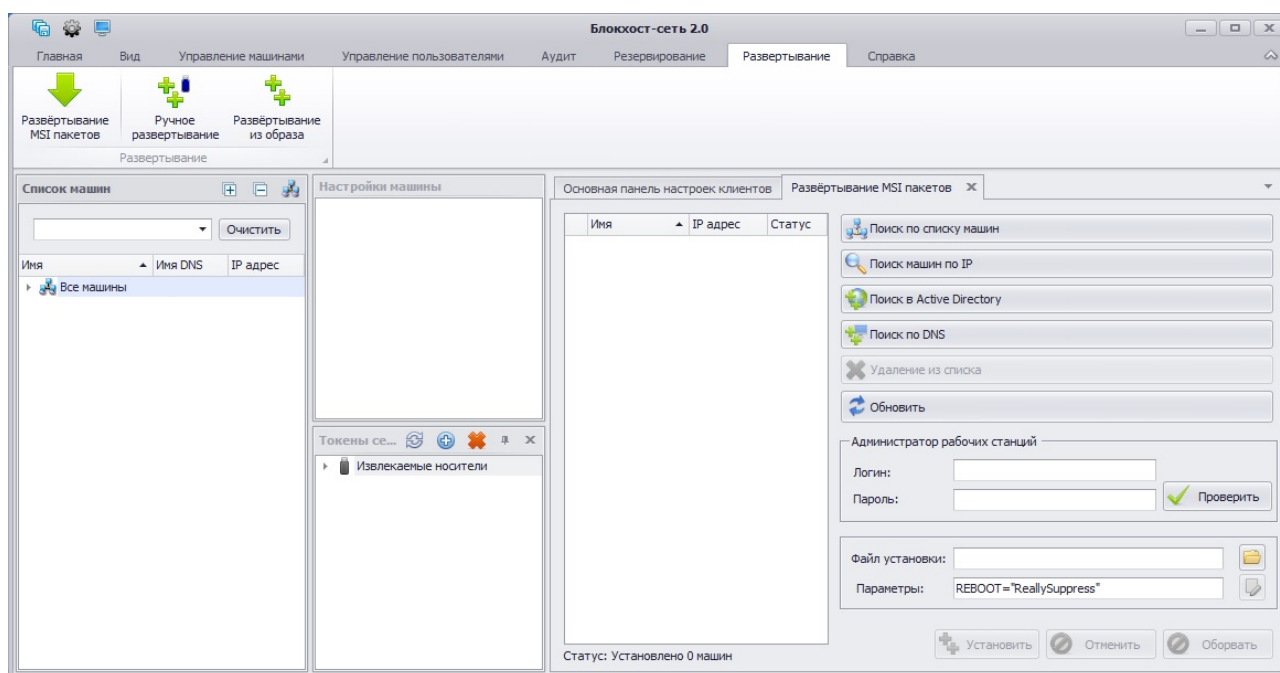


Рисунок 14. Вкладка «Развертывание MSI пакетов»

4. Сформировать список рабочих станций для установки клиентской части СЗИ одним из перечисленных ниже способов:

а. *Добавление рабочих станций из списка объектов Active Directory:*

Для формирования списка рабочих станций для установки клиентской части СЗИ на основе списка объектов Active Directory необходимо нажать кнопку **Пуск в Active Directory** (см. рис. 14), в результате откроется окно «Добавление клиентов из Active Directory» (рис. 15). В окне «Добавление клиентов из Active Directory» выбрать требуемый домен, щелкнув по его имени левой кнопкой мыши, и авторизоваться в нем, для чего ввести логин и пароль пользователя домена в соответствующие поля открывшегося окна (рис. 16), затем нажать кнопку **Подключить**.

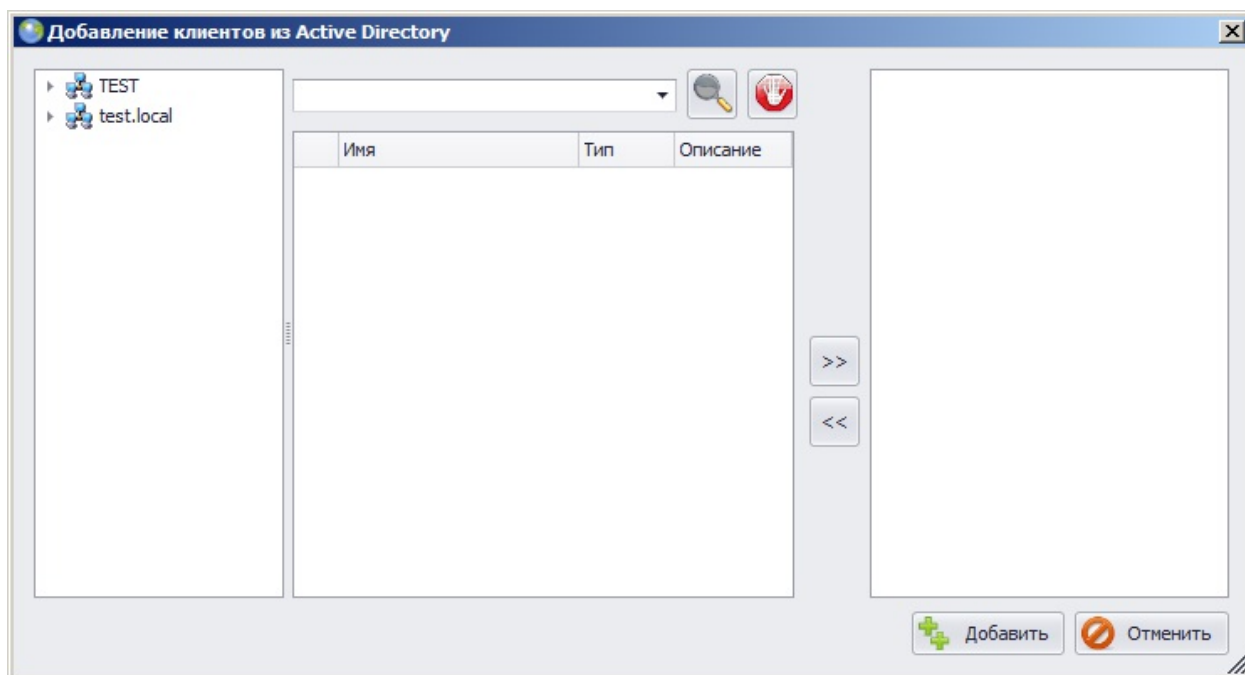


Рисунок 15. Окно поиска рабочих станций в структуре Active Directory

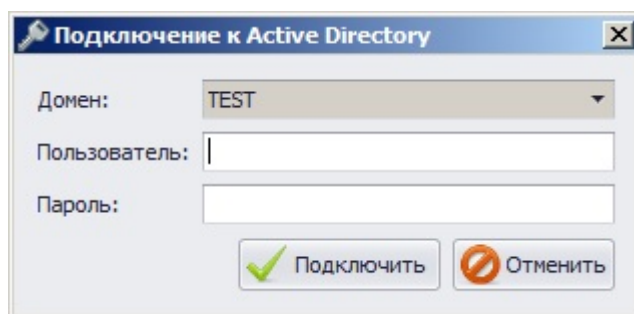


Рисунок 16. Окно «Подключение к Active Directory»

В отобразившейся в окне «**Добавление клиентов из Active Directory**» структуре объектов Active Directory выделить контейнер, содержащий добавляемые рабочие станции (в примере на рис. 17 – это контейнер **Computers**), в средней части окна выделить необходимые рабочие станции (для выделения нескольких рабочих станций можно воспользоваться клавишами <Ctrl> или <Shift>) и с помощью кнопки  переместить их в правую часть окна, затем нажать кнопку **Добавить**.

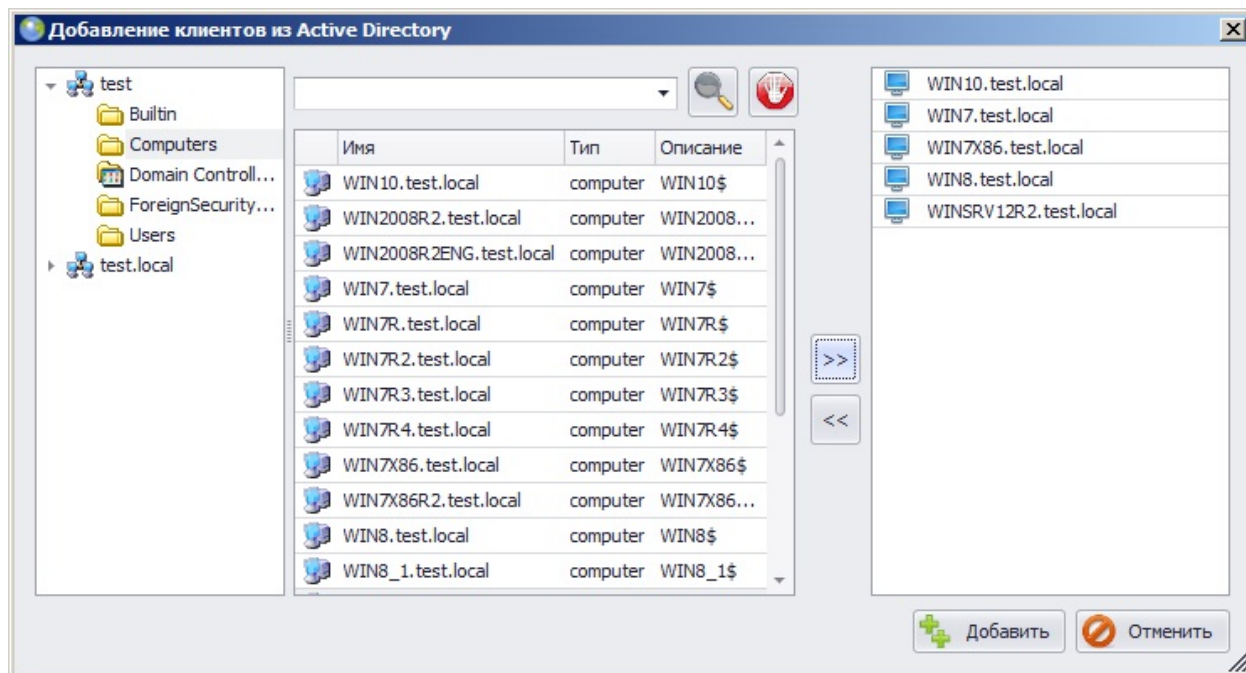


Рисунок 17. Сформированный список рабочих станций в окне выбора из AD

В результате выбранные рабочие станции появятся во вкладке **Развертывание MSI пакетов**.

b. Поиск рабочих станций на основе данных сервера DNS:

Для выбора рабочих станций на основе данных сервера DNS необходимо нажать кнопку **Поиск по DNS** (см. рис. 14), в результате откроется окно «Добавление клиентов на основе DNS-имен» (рис. 18), в котором отображаются все включавшиеся за время работы сервера DNS рабочие станции сети. В списке доступных для выбора следует выбрать необходимые рабочие станции (для выделения нескольких рабочих станций можно воспользоваться клавишами <Ctrl> или <Shift>) и при помощи кнопок управления (>> и <<) сформировать список для добавления на сервер СЗИ, затем нажать кнопку **Добавить**.



Использование параметра **Поиск по DNS** подразумевает наличие не более 100 рабочих станций в домене.

Значение, введенное в поле ввода окна «Добавление клиентов на основе DNS-имен», позволяет осуществить фильтрацию списка найденных рабочих станций.

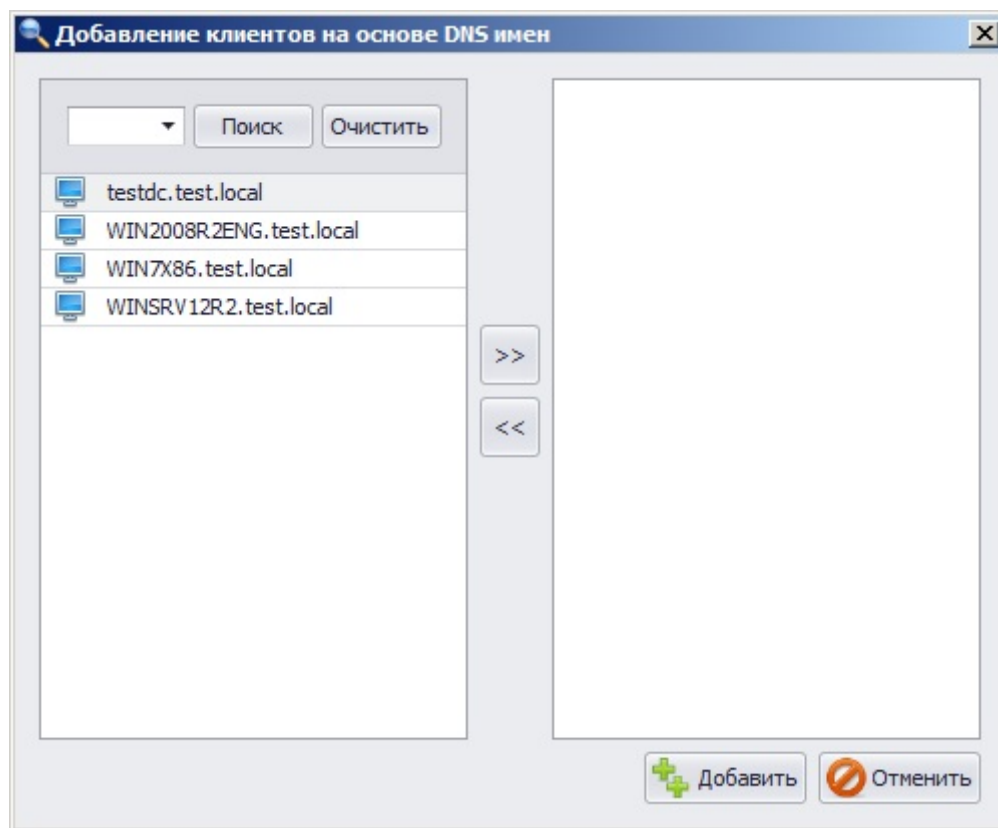


Рисунок. 18 Окно «Добавление клиентов на основе DNS имен»

В результате выбранные рабочие станции появятся во вкладке **Развертывание MSI пакетов**.

с. *Поиск рабочих станций по IP-адресу:*

Для поиска компьютеров в подсети администратору безопасности необходимо нажать кнопку **Поиск машин по IP**, в результате откроется окно «Поиск машин в сети» (рис. 19) в поле **Адрес подсети** ввести IP-адрес (либо диапазон IP-адресов в формате 192.168.0.* или 192.168.0.1-50) и нажать кнопку **Поиск**.



В случае ввода неверного IP-адреса (диапазона IP-адресов) рядом с полем ввода появится пиктограмма ошибки , а в окне «Лог» появится сообщение **Неверный формат адреса рассылки**.

После успешного завершения поиска выделить необходимые рабочие станции в списке и нажать кнопку **Добавить**.

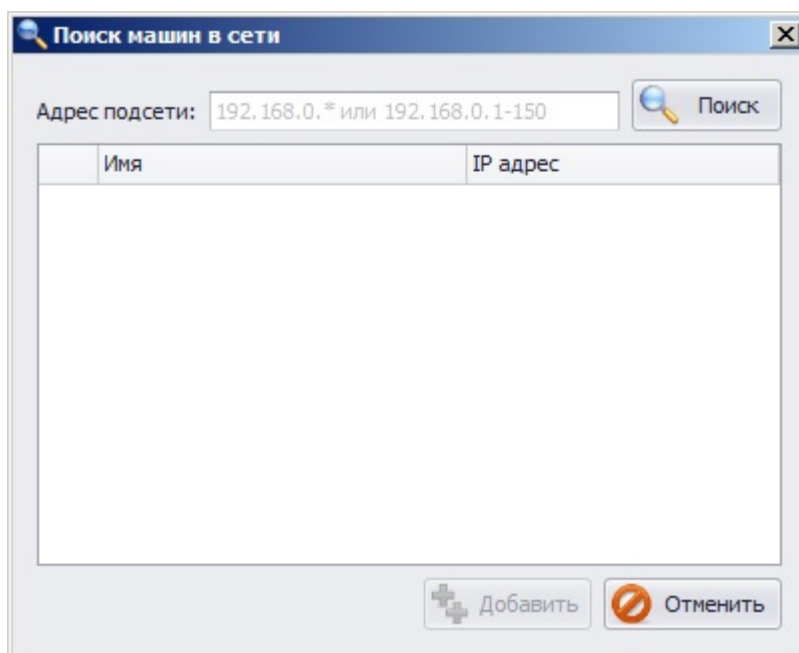


Рисунок 19. Окно поиска рабочих станций в сети

В результате выбранные рабочие станции появятся во вкладке **Развертывание MSI пакетов**.

5. Рабочие станции, добавленные в список для установки клиентской части СЗИ вкладки **Развертывание MSI пакетов**, могут иметь различный статус: рабочие станции, недоступные в настоящий момент для установки, будут иметь статус *Не в сети* и подсвечены красным цветом:

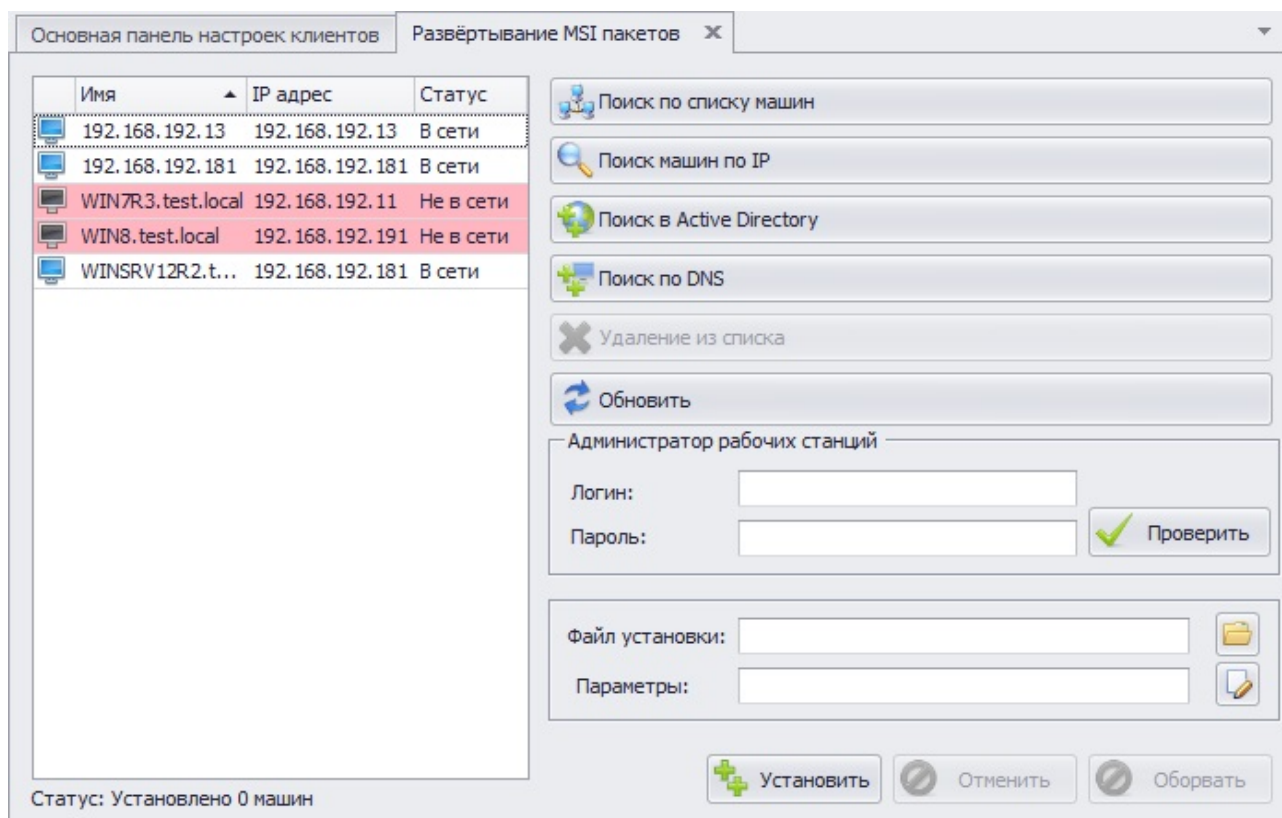


Рисунок 20. Список рабочих станций во вкладке «Развертывание MSI пакетов»

6. Ввести в поля **Логин** и **Пароль** данные учетной записи пользователя, входящего в группу **Администраторы** удаленной рабочей станции, от имени которого будет происходить установка.



Учетная запись пользователя может быть как локальной, так и доменной. В случае использования учетной записи пользователя домена, логин такого пользователя следует вводить с указанием имени домена, например: *Domain_name\user_name*.



При авторизации в ОС Windows на удаленной рабочей станции от имени учетной записи **локального** пользователя, входящего в группу администраторов (за исключением учетной записи встроенного администратора), на удаленной рабочей станции должен быть отключен параметр локальной политики безопасности **Контроль учетных записей: все администраторы работают в режиме одобрения администратором**. В противном случае попытка доступа к рабочей станции из консоли администрирования СЗИ закончится ошибкой, а в поле **Статус** рабочей станции появится запись *Отсутствует доступ* (при операции проверки введенных данных авторизации администратора рабочей станции) или *Проблема при копировании файла установщика* (при попытке установки СЗИ на рабочую станцию).

7. В поле **Файл установки** ввести полный путь к файлу-установщику клиентской части СЗИ *BlockHost-Net-2.0-Client x32.msi*, *BlockHost-Net-2.0-Client x64.msi* или *BhNet.Installer.exe*. Указать размещение файла дистрибутива клиентской части СЗИ можно с использованием стандартного окна Windows **«Открыть»**, которое открывается после нажатия на кнопку **Выбрать файл** . Также указать размещение файла дистрибутива клиентской части СЗИ можно введя полный путь к файлу в данное поле вручную.



При использовании для установки клиентской части СЗИ файла *BhNet.Installer.exe* будет автоматически проведена проверка разрядности ОС рабочей станции, на которую предполагается установка, и на рабочую станцию будет скопирован файл-установщик необходимой разрядности.

8. Для проверки корректности введенных идентификационных данных администратора удаленной рабочей станции следует нажать кнопку **Проверить**. В случае успешной проверки запись в поле **Статус** рабочей станции изменится на *Успешная аутентификация*, а в случае ошибки введенных данных – запись в поле **Статус** изменится на *Отсутствует доступ*. Для устранения ошибки необходимо ввести верные данные идентификации и повторно нажать кнопку **Проверить**.



По умолчанию процесс повторной проверки проходит только для тех рабочих станций из списка, которые не прошли проверку.

При необходимости проверки корректности введенных идентификационных данных администратора на всех рабочих станциях из списка следует нажать кнопку **Обновить** перед повторной проверкой.

9. В поле **Параметры** ввести необходимые для установки клиентской части СЗИ параметры: лицензию на использование СЗИ на удаленных рабочих станциях, идентификатор сервера СЗИ и пароль для подключения к нему удаленной рабочей станции, параметры подключения клиента СЗИ к серверу и др. Ввести необходимые параметры можно двумя способами:

а) вручную – список параметров, их описание, возможные значения и значения по умолчанию приведены в табл. 1. Ввод параметров осуществляется через пробел. Например: `SERVER_ADDRESS=192.168.119.90:999`
`PIN=12345 LOC=код_лицензии LOCKEY=ключ_активации`
`NET=код_лицензии NETKEY = ключ_активации`
`MACHINE_ID=11111111111111111111111111111111`
`NET_KEY=12345 SOFTMODE=1 REBOOT=ReallySuppress /L *V`
`"C:\<имя_файла_установщика>.log"`. В случае отсутствия параметров конфигурации клиента в поле **Параметры**, они принимают значения по умолчанию (см. табл. 1).

б) воспользоваться механизмом генерации параметров – нажать кнопку **Параметры по умолчанию** , расположенную справа от поля **Параметры**. В открывшемся окне «Генерация командной строки инсталлятора» (рис. 21) администратору безопасности доступны для изменения следующие параметры (для возможности изменения необходимо установить флажок слева от имени редактируемого параметра):

- **PIN токена** – PIN-код доступа к создаваемому в процессе установки клиентской части СЗИ персональному идентификатору в реестре Windows удаленной рабочей станции. Если параметр не отмечен (по умолчанию), то на рабочей станции при установке СЗИ не будет создан ключевой носитель в реестре Windows;



|| При установке PIN-кода ключевого носителя запрещено использовать символы русского алфавита и спецсимволы: ~ / \ | ; ? \$ & % @ ^ = * ' + " [] ` { } () < > .

- **Syslog сервер** – IP-адрес и номер UDP-порта Syslog-сервера, на который будут передаваться сообщения о работе СЗИ на контролируемой PC;
- **Перезагрузка после установки** – параметр отвечает за перезагрузку рабочей станции сразу после установки клиентской части СЗИ. При его активации, рабочая станция будет перезагружена в процессе установки клиентской части СЗИ. Снятый параметр позволит избежать перезагрузки после установки СЗИ;
- **Дополнительные пользователи** – при помощи кнопок **Добавление дополнительных пользователей** и **Удаление дополнительных пользователей** можно сформировать список пользователей домена, которые автоматически будут включены в список пользователей рабочей станции по окончании процесса установки на нее клиентской части СЗИ.



|| По умолчанию в окне «Генерация командной строки инсталлятора» активирован недоступный для редактирования параметр **Мягкий режим работы клиента** (параметр `SOFTMODE=1` в командной строке). В результате на контролируемой рабочей станции сразу после установки, СЗИ будет работать в **Мягком режиме** (подробнее о **Мягком режиме** работы СЗИ см. п. 6.2.4 «Руководства администратора безопасности СЗИ «Блокхост-сеть 2.0» (серверная консоль)»).

Для генерации командной строки, с указанными в окне «Генерация командной строки инсталлятора» параметрами, нажать кнопку **Сгенерировать**. В результате в поле **Параметры** вкладки **Развертывание MSI пакетов**, помимо указанных в окне «Генерация командной строки инсталлятора» параметров, будут добавлены значения используемых на сервере СЗИ локальной и сетевой лицензий, параметры сервера и клиента СЗИ, используемые по умолчанию, и необходимые клиенту СЗИ для первичного подключения к серверу, а также параметр командной строки с именем файла-журнала для аудита процесса инсталляции клиентской части СЗИ.

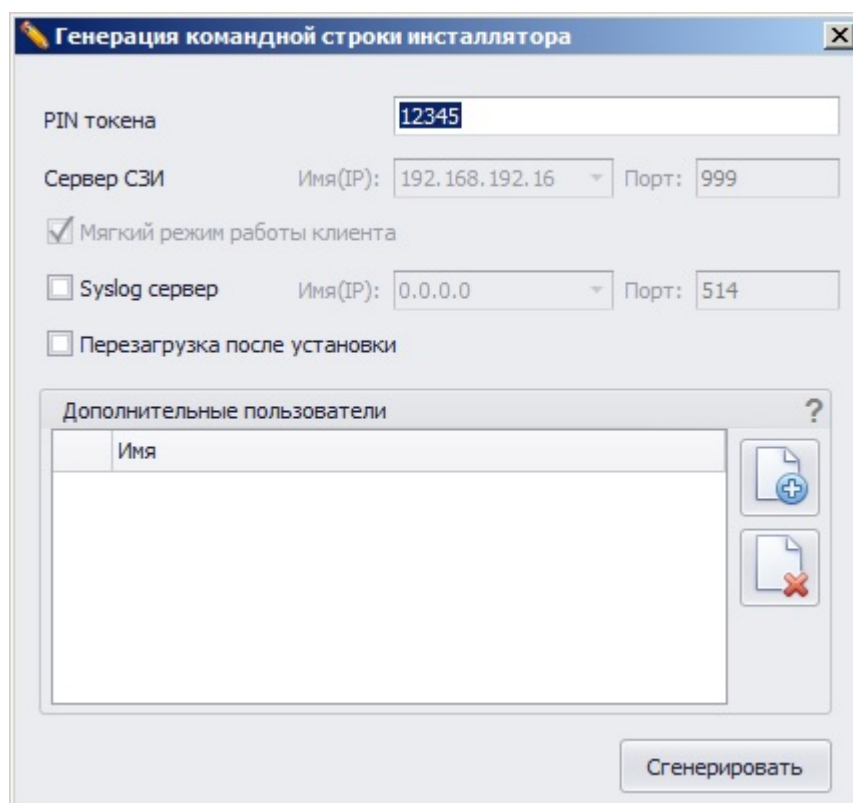


Рисунок 21. Окно задания параметров командной строки инсталлятора

10. Нажать кнопку **Установить** для запуска процесса установки клиентской части СЗИ. Во время процесса установки во вкладке **Развертывание MSI пакетов** доступна только кнопка **Отменить**. Процесс установки клиентской части СЗИ на удаленную рабочую станцию отображается в поле **Статус**. В случае положительного результата установки клиентской части СЗИ статус рабочей станции примет значение *Установка успешно завершена* (рис. 22).

В случае необходимости отмены установки клиентской части СЗИ в процессе ее установки из консоли администрирования СЗИ следует нажать кнопку **Отменить**. Значение в поле **Статус** изменится на *Отмена установки пользователем*, а на удаленной рабочей станции произойдет корректный возврат к состоянию ОС до начала процесса установки клиентской части СЗИ.



В случае установки клиентской части СЗИ на несколько рабочих станций (список которых сформирован во вкладке **Развертывание MSI пакетов**) нажатие на кнопку **Отменить** приведет к отмене установки СЗИ на всех находящихся в списке рабочих станциях.

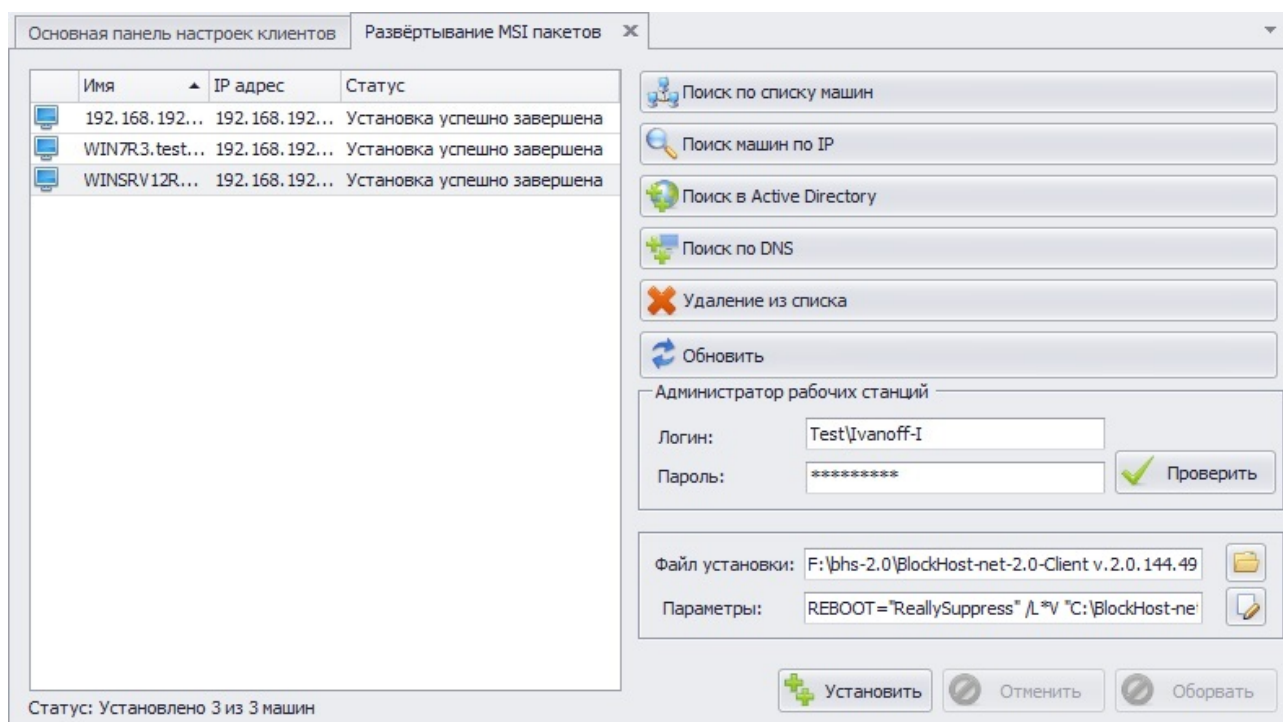


Рисунок 22. Отображение результата установки клиентской части СЗИ на удаленные PC



Копирование файла-установщика с сервера СЗИ осуществляется в общий каталог *admin\$* удаленной рабочей станции. Затем из этой папки система разворачивания СЗИ средствами ОС Windows осуществляет запуск интерпретатора командной строки с командой вида:

msiexec /i [путь до файла] /quiet [параметры],

где:

[путь до файла] – локальный путь до файла-установщика на удаленной машине, то есть туда куда система его скопировала.

[параметры] – список параметров установки, указанных в виде строки, которые взяты из поля **Параметры** вкладки **Развертывание MSI пакетов** серверной консоли администрирования СЗИ.

Таблица 1. Параметры конфигурации клиента СЗИ

Наименование параметра	Назначение	Возможные значения
SERVER_ADDRESS	IP адрес и порт взаимодействия сервера СЗИ в формате IP-address:Port	Значение устанавливается в серверной консоли администрирования СЗИ во вкладке Параметры сервера . По умолчанию 192.168.1.1:999
PIN	PIN-код доступа к ключевому носителю	Если параметр отсутствует, то при установке СЗИ не будет создан ключевой идентификатор в реестре Windows рабочей станции. При установке PIN-кода ключевому носителю запрещено использовать символы русского алфавита и спецсимволы: ~/\ ; ? \$ & % @ ^ = * ' + " [] ` { } () < >
LOC	Код локальной лицензии	По умолчанию не задан

Наименование параметра	Назначение	Возможные значения
LOCKEY	Ключ активации локальной лицензии	По умолчанию не задан
NET	Код сетевой лицензии	По умолчанию не задан
NETKEY	Ключ активации сетевой лицензии	По умолчанию не задан
MACHINE_ID	Идентификатор рабочей станции, на которую будет устанавливаться СЗИ	Значение устанавливается в серверной консоли администрирования СЗИ во вкладке Параметры сервера . По умолчанию не задан.
NET_KEY	Пароль подключения клиента к серверу СЗИ	Значение устанавливается в серверной консоли администрирования СЗИ во вкладке Параметры сервера .
REBOOT	Параметр перезагрузки	<i>ReallySuppress</i> – перезагрузка подавляется (по умолчанию); <i>Force</i> – по окончании инсталляции СЗИ выполняется перезагрузка рабочей станции
SOFTMODE	Работа СЗИ в мягком режиме	1 – мягкий режим включен (по умолчанию); отсутствие параметра – мягкий режим отключен.
USERS	Список SID-ов пользователей, указанных через запятую.	При отсутствии параметра, в список пользователей будут добавлены все локальные пользователи рабочей станции, а также пользователи домена, профиль которых существует на рабочей станции.
SYSLOG_SERVER	IP адрес и порт взаимодействия с внешним syslog-сервером в формате IP-adress:Port	По умолчанию не задан.
/L*V	Параметр командной строки установщика Windows, указывающий на необходимость вывода подробных сведений процесса инсталляции СЗИ в указанный файл	По умолчанию имя файла-журнала соответствует имени файла-установщика СЗИ с расширением .log.

1.4.2. Локальная установка клиентской части СЗИ с указанием параметров подключения к серверу СЗИ

При локальной установке клиентской части СЗИ «Блокхост-сеть 2.0» можно сразу указать параметры подключения клиента к серверу СЗИ. Такая возможность существует, если указать необходимые параметры подключения к серверу СЗИ в строке вызова файла-установщика, например, при запуске из командной строки или при сетевой установке клиентской части СЗИ при помощи специализированных программных продуктов (в том числе и через групповые политики).



Перед установкой клиентской части необходимо добавить эту рабочую станцию в список контролируемых на сервере СЗИ. Порядок добавления на сервер СЗИ рабочих станций, с установленной и настроенной клиентской частью, описан в п. 3.4.4 «Автоматическое подключение рабочих станций, с настроенным клиентом СЗИ «Блокхост-сеть 2.0» к серверу» документа «СЗИ от НСД «Блокхост-сеть 2.0». Руководство администратора безопасности». На сервере СЗИ после формирования списка контролируемых рабочих станций рекомендуется перезапустить службу *GIS.Server.NetworkServer* или перезагрузить сервер СЗИ.

Для установки клиентской части СЗИ с указанием параметров подключения к серверу СЗИ необходимо войти в ОС от имени учетной записи встроенного администратора ОС Windows (контроллера домена). Вызвать интерпретатор командной строки **cmd.exe**, в котором после указания имени файла дистрибутива СЗИ (*BlockHost-Net-2.0-Client x32.msi*, *BlockHost-Net-2.0-Client x64.msi*, *BhNet.Installer.exe*) ввести необходимые коды и ключи лицензий (локальной и сетевой) и параметры подключения к серверу СЗИ. Кроме параметров, приведенных в табл. 1, при локальной установке клиентской части СЗИ с использованием интерпретатора командной строки доступны параметры, описание которых приведено в табл. 2.

Таблица 2. Параметры конфигурации клиента СЗИ, вводимые в командной строке

Наименование параметра	Назначение	Возможные значения
PIN2	Подтверждение PIN-кода доступа к ключевому носителю	Соответствует значению параметра PIN
DISABLE_SERVICE_AUTOSTART	Отключение автоматического запуска служб СЗИ до входа пользователя в ОС	1- автоматический запуск служб СЗИ отключен; 0 или отсутствие параметра (по умолчанию) – осуществляется автоматический запуск служб СЗИ до входа пользователя в ОС.

Пример командной строки для файлов *BlockHost-Net-2.0-Client x32.msi*, *BlockHost-Net-2.0-Client x64.msi*:

```
msiexec.exe /i BlockHost-Net-2.0-Client x32.msi /qn  
SERVER_ADDRESS=192.168.1.1:999 PIN=12345 PIN2=12345  
LOC=<код локальной лицензии> LOCKEY=<ключ активации  
локальной лицензии> NET=<код сетевой лицензии>  
NETKEY=<ключ активации сетевой лицензии>  
MACHINE_ID=111111111111111111111111111111111111 NET KEY=12345
```

Пример командной строки для файла *BhNet.Installer.exe*:

```
BhNet.Installer.exe /qn SERVER_ADDRESS=192.168.1.1:999
PIN=12345 PIN2=12345 LOC=<код локальной лицензии>
LOCKEY=<ключ активации локальной лицензии> NET=<код
сетевой лицензии> NETKEY=<ключ активации сетевой
лицензии> MACHINE_ID=11111111111111111111111111111111
NET KEY=12345
```

В результате в ходе установки клиентской части СЗИ на рабочей станции будет создан персональный идентификатор пользователя, хранящийся в реестре ОС Windows. PIN-код доступа к этому идентификатору соответствует заданному в параметрах установки. В

список пользователей СЗИ рабочей станции будут добавлены все учетные записи локальных пользователей ОС Windows, учетные записи пользователей домена, профили которых существуют на рабочей станции, а также пользователи, SID-ы которых перечислены среди параметров установки в командной строке. Всем пользователям СЗИ рабочей станции будет присвоен, созданный в ходе установки, персональный идентификатор, хранящийся в реестре ОС Windows, и мандатная метка со значением **1**. Также в результате такой инсталляции всем пользователям СЗИ автоматически устанавливается право только **интерактивного (локального)** входа в ОС.

В дальнейшем, при администрировании механизмов СЗИ рабочей станции из консоли администрирования СЗИ, необходимо скорректировать список пользователей СЗИ и назначить всем пользователям аппаратные персональные идентификаторы. Подробнее о редактировании списка пользователей СЗИ и их параметров см. документ «СЗИ от НСД «Блокхост-сеть 2.0». Руководство администратора безопасности».

1.4.3. Локальная установка клиентской части СЗИ

Для инсталляции клиентской части СЗИ необходимо войти в операционную систему под учетной записью встроенного администратора ОС Windows (контроллера домена). Запустить на выполнение файл-установщик СЗИ (*BlockHost-Net-2.0-Client x32.msi* – для 32-bit ОС, *BlockHost-Net-2.0-Client x64.msi* – для 64-bit ОС или *BhNet.Installer.exe* – для 32- и 64-bit ОС) дважды щелкнув по нему левой кнопкой мыши.

В результате запуска файла-установщика на экране монитора появится окно приветствия мастера установки СЗИ «Блокхост-сеть 2.0» (рис. 23).

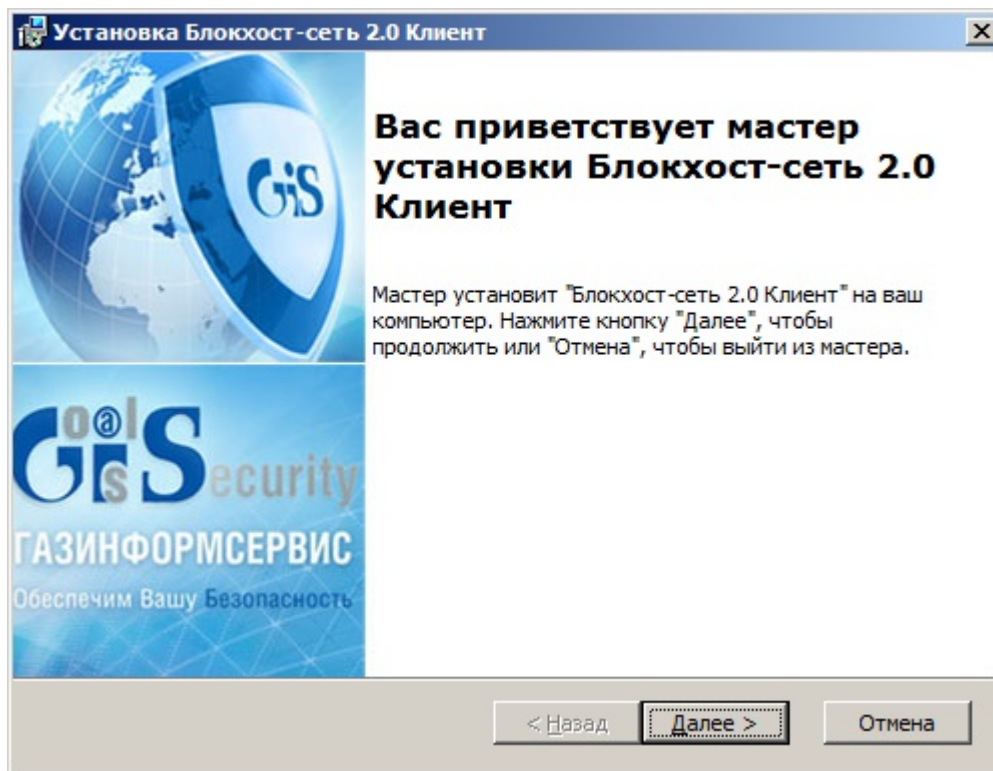


Рисунок 23. Окно установки сервера СЗИ «Блокхост-сеть 2.0»

На любом этапе работы мастера установки СЗИ можно нажать кнопку **Отмена**. На экране появится окно, показанное на рисунке 24. При нажатии кнопки **Да** установка будет прервана. При нажатии кнопки **Нет** установка будет продолжена.

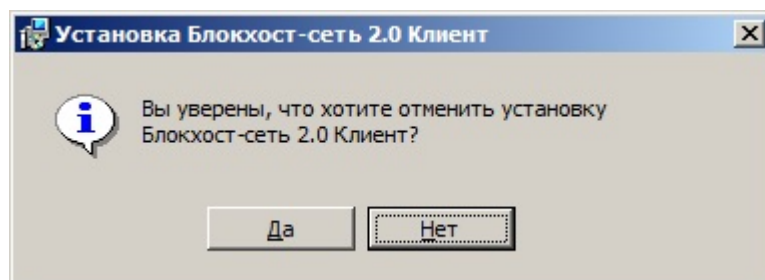


Рисунок 24. Окно прекращения установки

После нажатия в окне приветствия мастера установки СЗИ кнопки *Далее* (рис. 23) на экране монитора появится окно с текстом условий лицензионного соглашения (рис. 25).

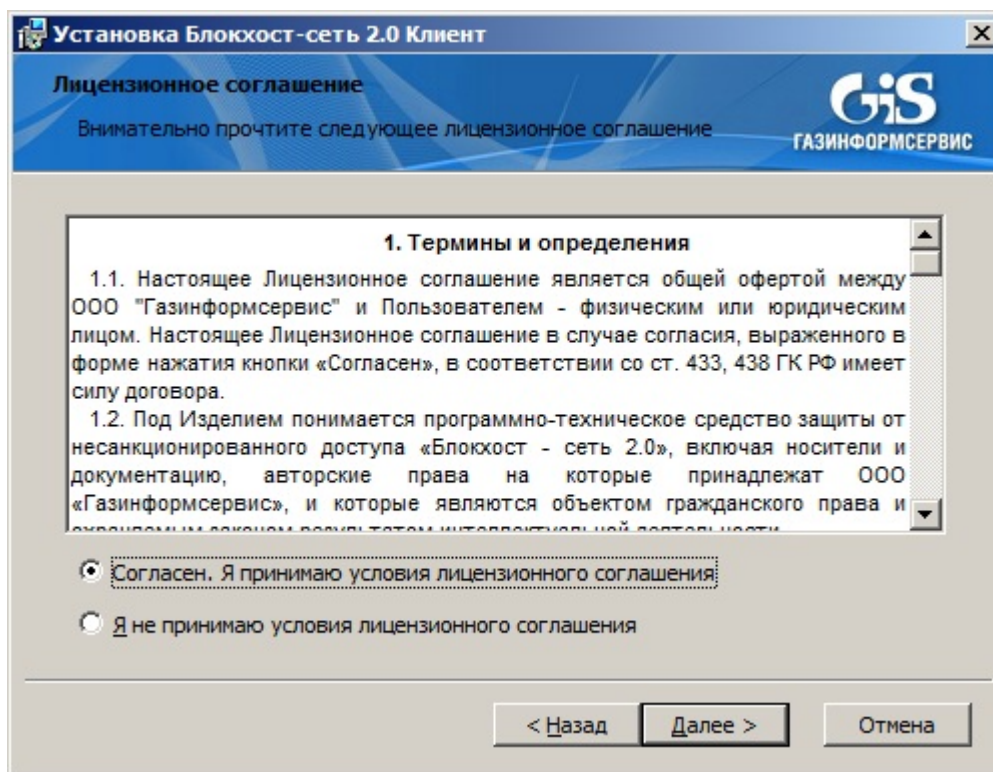
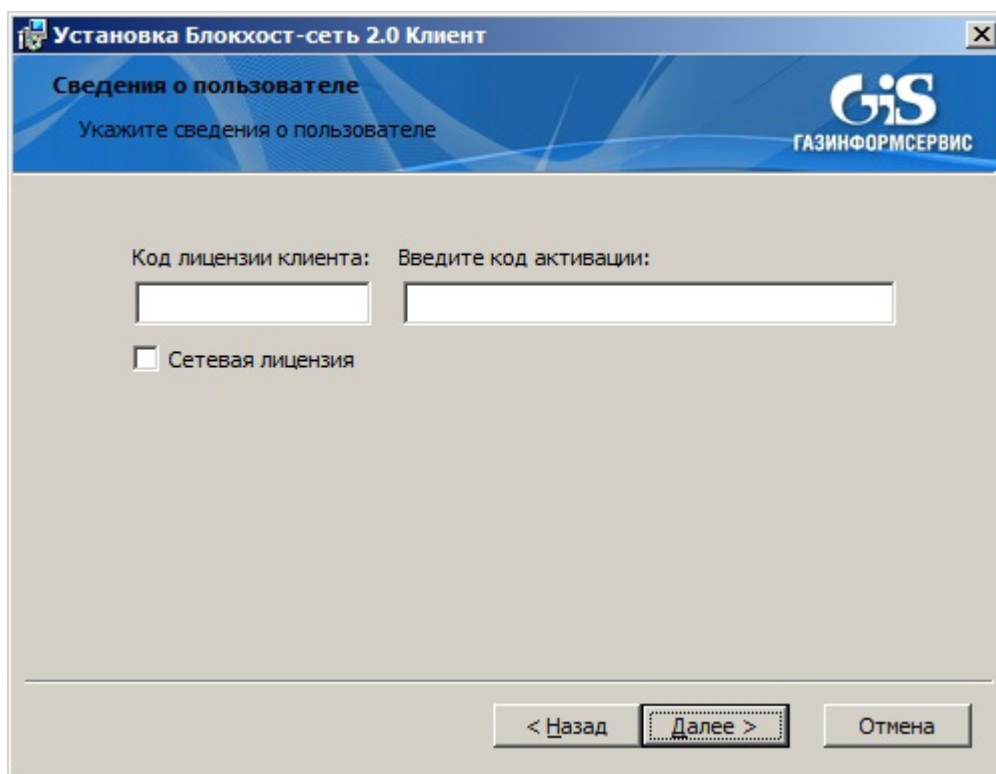


Рисунок 25. Окно мастера установки СЗИ «Блокхост-сеть 2.0» с лицензионным соглашением

Необходимо внимательно прочитать условия лицензионного соглашения. В случае несогласия с условиями лицензионного соглашения (выбран пункт ***Я не принимаю условиями лицензионного соглашения***) дальнейшая установка СЗИ становится невозможна (кнопка *Далее* – неактивна). Для выхода из программы установки СЗИ необходимо нажать кнопку *Отмена*.

В случае принятия условий лицензионного соглашения необходимо выбрать пункт ***Я принимаю условия лицензионного соглашения*** и нажать кнопку *Далее*. После этого появится окно (рис. 26, а), в котором необходимо установить флажок в поле ***Сетевая лицензия*** и ввести в соответствующие поля (рис. 26, б) коды сетевой лицензии и лицензии клиента и коды их активации, которые прописаны в выданной лицензии.

После заполнения полей ввода кода необходимых лицензий и кода их активации нажмите кнопку *Далее*. Если код лицензии или код активации был введен неверно, то на экране появится окно с сообщением об ошибке ввода кода активации лицензии (на рис. 27 показано окно с сообщением о неверном вводе кода активации сетевой лицензии клиентской части СЗИ).



Установка Блокхост-сеть 2.0 Клиент

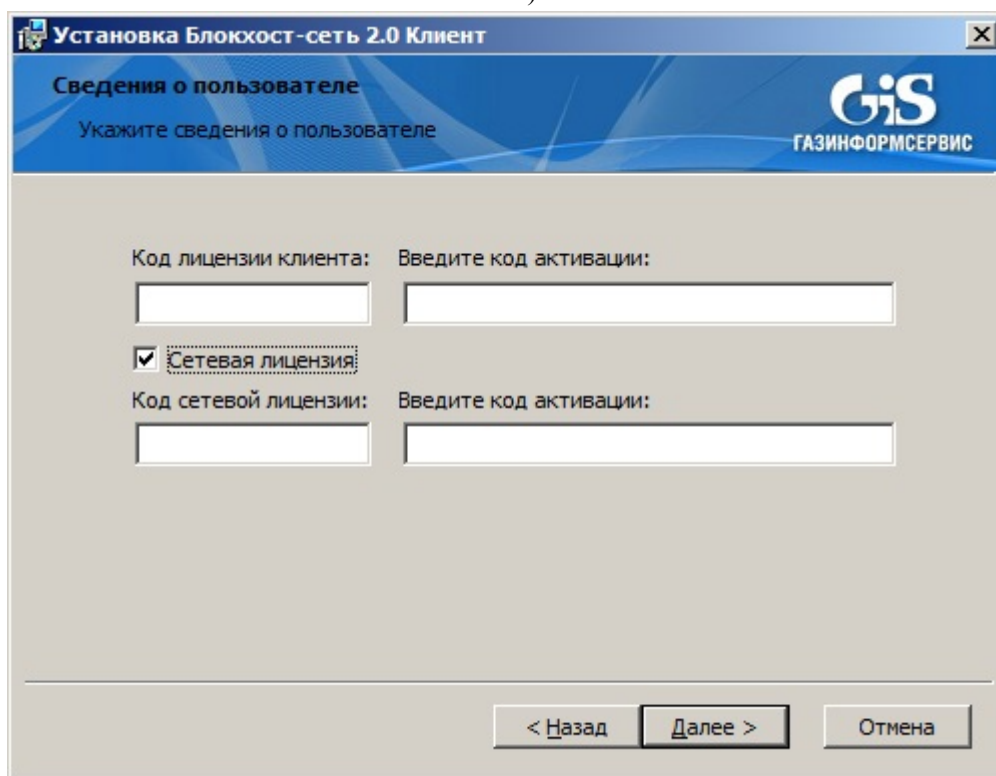
Сведения о пользователе
Укажите сведения о пользователе

Код лицензии клиента: Введите код активации:

☐ Сетевая лицензия

< Назад Далее > Отмена

а)



Установка Блокхост-сеть 2.0 Клиент

Сведения о пользователе
Укажите сведения о пользователе

Код лицензии клиента: Введите код активации:

☒ Сетевая лицензия

Код сетевой лицензии: Введите код активации:

< Назад Далее > Отмена

б)

Рисунок 26. Окно ввода кода лицензии и кода активации СЗИ «Блокхост-сеть 2.0»

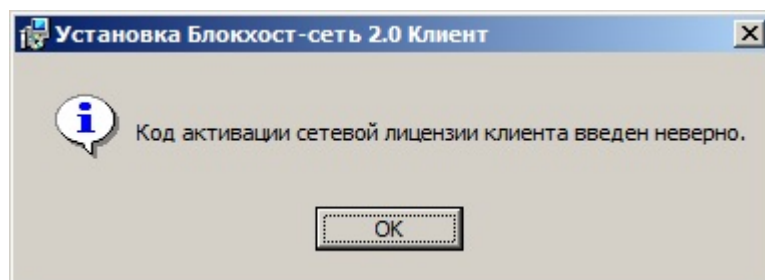


Рисунок 27. Окно с сообщением о неверно введенном коде

Если коды лицензии и коды активации были введены верно, установка будет продолжена и на экране появится окно формирования ключевого носителя администратора безопасности (рис. 28). Необходимо подключить к рабочей станции, на которую производится установка СЗИ, ключевой носитель администратора безопасности, из выпадающего списка поля **Тип ключевого носителя** выбрать тип носителя (eToken, SafeNet eToken, ruToken, eSmart Token, Avest Token, USB-носитель, дискета или персональный идентификатор в реестре Windows; электронный идентификатор JaCarta определится в списке, как eToken), ввести PIN-код доступа к ключевому носителю и его подтверждение в соответствующие поля. PIN-код доступа к ключевому носителю задается с помощью специального программного обеспечения, поставляемого вместе с носителем (ПО для SafeNet eToken, драйверы JaCarta для ОС Windows 8/8.1/2012/2012R2/10/2016, драйверы eSmart Token и Avest Token не входят в комплект поставки СЗИ). По умолчанию PIN-код eToken и SafeNet eToken – «1234567890», ruToken – «12345678», JaCarta – «1234567890», AvBign – «12345678». Для USB-накопителя, дискеты и персонального идентификатора в реестре PIN-код задается средствами СЗИ «Блокхост-сеть 2.0» (если USB-накопитель или дискета использовались ранее в качестве персонального идентификатора администратора в СЗИ «Блокхост-сеть 2.0», то необходимо ввести PIN-код доступа к ним, установленный ранее). Если при установке СЗИ в поле **Тип ключевого носителя** выбрать пункт **Registry Add Device**, в защищенном хранилище реестра Windows рабочей станции будет создан ключ, содержащий информацию, идентичную информации для других типов ключевых носителей.



При использовании электронных идентификаторов SafeNet eToken 7200 и SafeNet eToken 7300 существуют следующие ограничения:

- 1) ограничения по применению SafeNet eToken 7200:
 - для использования eToken-части необходимо наличие интерфейса USB 3.0;
 - не следует выполнять блокировку флеш-части при помощи предустановленного ПО, т.к. в этом случае при использовании флеш-части для установки СЗИ и для входа пользователя в систему она автоматически блокируется после перезагрузки ОС. Для ее разблокировки необходимо войти в систему, запустить предустановленное на носителе ПО и ввести заданный ранее PIN-код. Далее следует выполнить LogOff\LogOn, после чего FLASH-часть будет разблокирована;



- 2) ограничения по применению SafeNet eToken 7300:
- может не отображаться на виртуальных АРМ, построенных на структуре ESXi;
 - не следует использовать флеш-часть данного носителя для установки СЗИ и для входа пользователя в систему, так как флеш-часть после перезагрузки ОС автоматически блокируется. Для ее разблокировки необходимо войти в систему, запустить предустановленный в ROM-области Launcher и ввести PIN-код (PIN-код FLASH-части соответствует PIN-коду, заданному для SafeNet eToken 7300). Далее следует выполнить LogOff\LogOn, после чего флэш-часть будет разблокирована. При использовании LogOff\LogOn флэш-часть работает штатно без блокировки. Подробнее особенности применения данных электронных идентификаторов описаны в пункте 5.2.1.1 «Особенности применения электронных идентификаторов SafeNet eToken 7200 и SafeNet eToken 7300» документа «СЗИ «Блокхост-сеть 2.0». Руководство администратора безопасности».

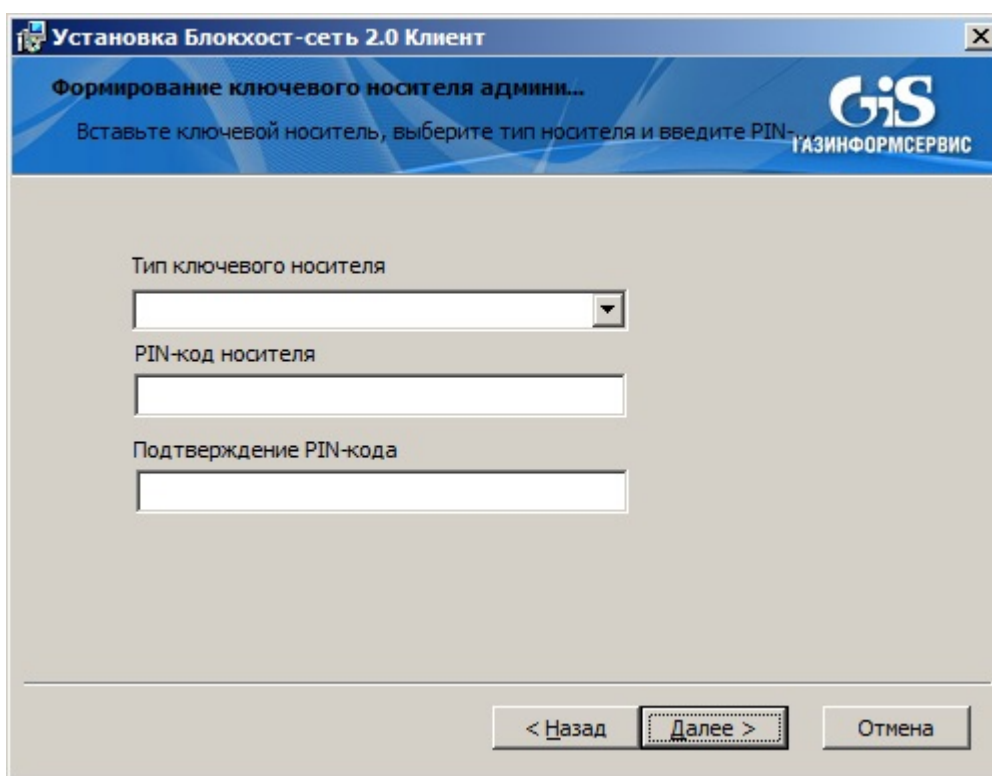


Рисунок. 28. Окно формирования ключевого носителя администратора

Для продолжения установки нажмите кнопку **Далее**.

Если введен неверный PIN-код доступа к ключевому носителю, то на экране появится сообщение, показанное на рис. 29. После нажатия на кнопку **ОК** происходит возврат в окно формирования ключевого носителя (см. рис. 28), в котором необходимо заново ввести PIN-код доступа к ключевому носителю.

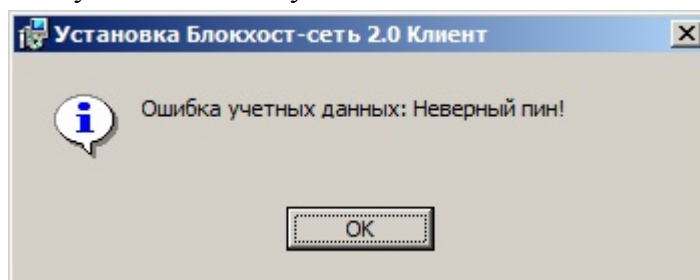


Рисунок 29. Окно сообщения о неверном PIN-коде

Если операция проверки PIN-кода доступа к ключевому носителю прошла успешно, то появится окно начала установки СЗИ (рис. 30), в котором необходимо нажать кнопку **Установить**, после чего начнется процесс установки СЗИ «Блокхост-сеть 2.0».

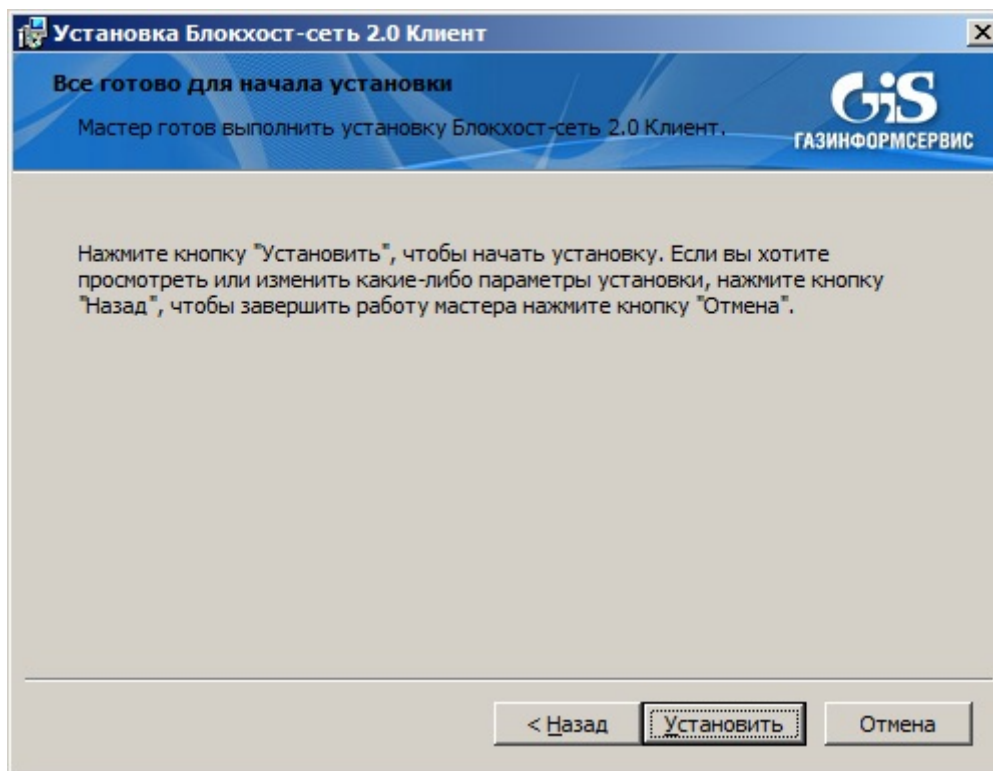


Рисунок 30. Окно готовности к установке СЗИ «Блокхост-сеть 2.0»

Ход установки будет отображаться в окне мастера установки (рис. 31), программный продукт будет установлен на локальный компьютер в папку *C:\BlockHost*.

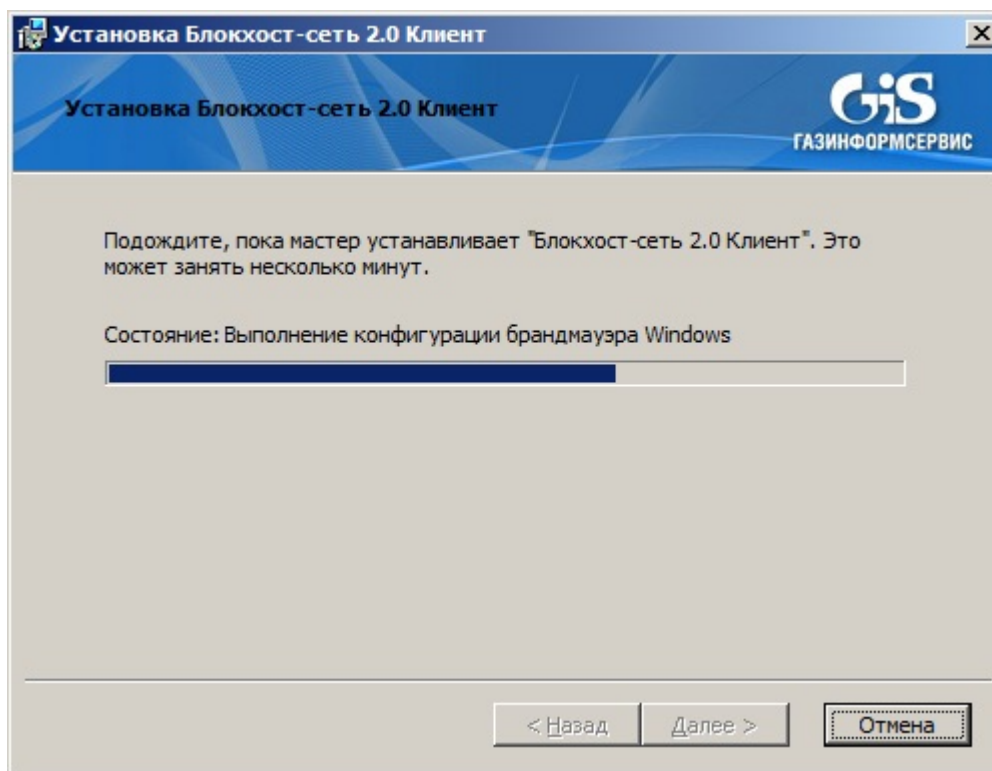


Рисунок 31. Ход установки СЗИ «Блокхост-сеть 2.0»

Если установка закончена успешно, то на экране появится окно окончания установки (рис. 32). Для окончания работы мастера установки СЗИ необходимо нажать кнопку **Готово**:

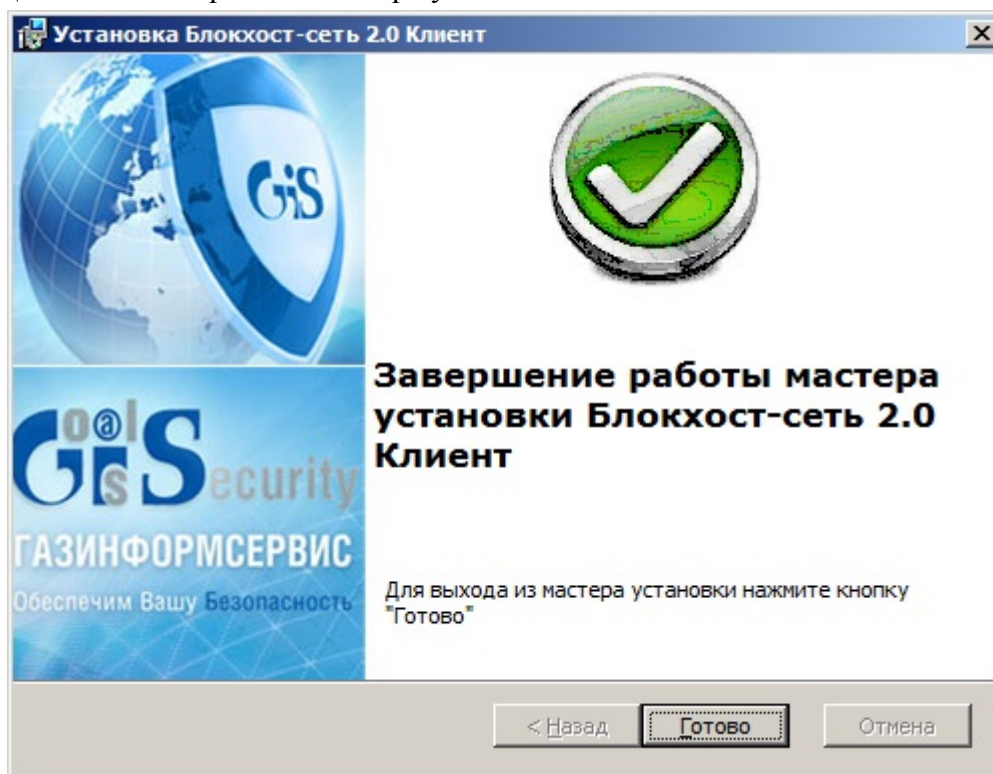


Рисунок 32. Окно окончания установки СЗИ «Блокхост-сеть 2.0»

После окончания процесса установки все службы СЗИ будут запущены, и администратор безопасности сможет сразу запустить локальную консоль администрирования СЗИ и произвести необходимые настройки.

1.4.3.1. Экспорт сетевых настроек

Настройка сетевых параметров рабочих станций, добавляемых в группу контролируемых на сервере СЗИ, выполняется администратором безопасности в серверной консоли СЗИ «Блокхост-сеть 2.0» в следующей последовательности:

1. В окне «Список машин» выделить группу, в которую будут добавлены рабочие станции (в примере на рис. 33 выделена группа **Все машины**);
2. В меню **Развертывание** выбрать пункт **Ручное развертывание** (см. пример на рис. 14). Откроется вкладка **Ручное развертывание** (рис. 33);
3. Во вкладке **Ручное развертывание** сформировать список рабочих станций, для которых будет производиться экспорт параметров сетевого взаимодействия (подробнее о создании списка контролируемых рабочих станций см. подраздел 1.4.1 настоящего руководства);

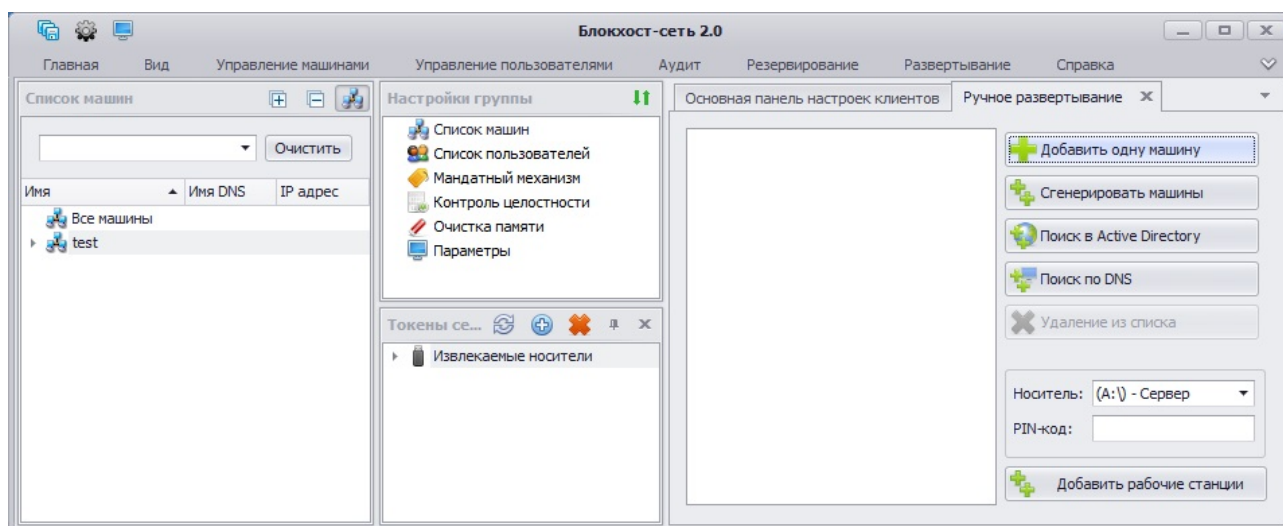


Рисунок 33 Вкладка «Ручное развертывание»

4. Подключить к серверу СЗИ ключевой носитель, на который будет осуществлен экспорт сетевых настроек и ключей аутентификации клиента, и выбрать его из выпадающего списка поля **Носитель**;



1. Для экспорта сетевых настроек сервера СЗИ и ключей аутентификации клиента может быть использован носитель, отличный от того, с которым производилась установка серверной и клиентских частей СЗИ.

2. Следует учесть, что, если при установке серверной части СЗИ в качестве ключевого носителя был использован персональный идентификатор в реестре Windows, то для экспорта сетевых настроек сервера безопасности необходимо использовать другой вид носителя, например, eToken. Персональный идентификатор в реестре не предназначен для переноса настроек и может применяться только на той рабочей станции, на которой он был создан.

5. В поле **PIN-код** ввести PIN-код доступа к выбранному носителю;

6. Для записи сетевых настроек и ключей взаимной аутентификации удаленных рабочих станций на выбранный ключевой носитель нажать кнопку **Добавить рабочие станции**.

После этого сетевые настройки и ключи взаимной аутентификации сервера СЗИ и рабочих станций будут созданы и экспортированы на ключевой носитель администратора, а в окне «Список машин» появятся рабочие станции, список которых был сформирован во вкладке **Ручное развертывание**.



Необходимо учитывать, что количество генерируемых ключей аутентификации клиентов СЗИ ограничено размерами носителя (например, на eToken Pro 32K можно сгенерировать ключи аутентификации приблизительно для 100 машин). Если необходимо подключать к серверу СЗИ большее количество машин, то по мере подключения рабочих станций к серверу СЗИ можно добавлять ключи аутентификации для новых машин на тот же самый носитель, либо использовать дополнительный носитель, в остальном процедура экспорта сетевых настроек сервера и ключей аутентификации клиента аналогична.

1.4.3.2. Импорт сетевых настроек на рабочие станции

Импорт сетевых настроек осуществляется непосредственно на рабочих станциях с ключевого носителя, на который из вкладки **Ручная генерация** серверной консоли администрирования СЗИ выполнялся экспорт сетевых настроек и ключей аутентификации

клиента. Для импорта сетевых настроек администратор безопасности должен выполнить следующие действия:

7. Подключить к рабочей станции, для которой осуществляется импорт сетевых настроек, ключевой носитель администратора, на который были экспортированы сетевые настройки, и запустить на ней локальную консоль администрирования СЗИ «Блокхост-сеть 2.0»;

8. В локальной консоли администрирования СЗИ в окне «Список машин» раскрыв группу **Все машины** выделить рабочую станцию **localhost**, а в окне «Настройки машины» выделить механизм **Параметры**:

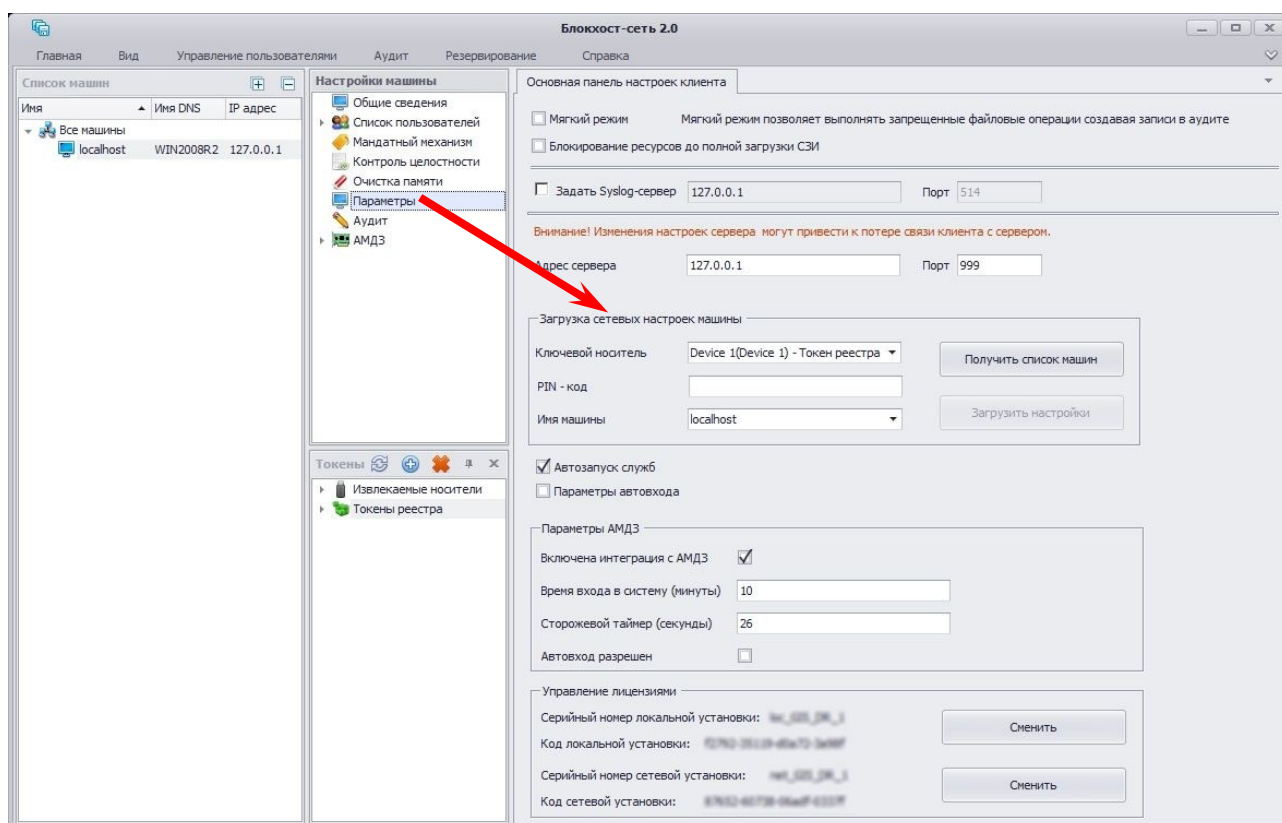


Рисунок 34. Импорт сетевых настроек

9. Во вкладке **Основная панель настроек клиентов** в области **Загрузка сетевых настроек машины**:

- в выпадающем списке поля **Ключевой носитель** выбрать ключевой носитель администратора, подключенный в п.1, и ввести PIN-код доступа к нему в поле **PIN-код**;
- Нажать кнопку **Получить список машин**;
- Из выпадающего списка поля **Имя машины** выбрать имя сгенерированной, во вкладке **Ручное развертывание** серверной консоли, рабочей станции;
- Загрузить настройки сервера СЗИ и рабочей станции, нажав кнопку **Загрузить настройки**;



Поле **Адрес сервера** заполняется автоматически на основе информации, содержащейся на ключевом носителе администратора (подробнее о сетевых параметрах см. п. 3.3.2 документа «СЗИ «Блокхост-сеть 2.0». Руководство администратора безопасности»). В дальнейшем, в ходе администрирования СЗИ «Блокхост-сеть 2.0» администратор безопасности может изменить значения в указанном поле (данная операция может потребоваться, если в сети параметры IP-адресации определяются автоматически).

10. Сохранить произведенные настройки с помощью пункта меню **Главная** → **Сохранить**, или воспользоваться кнопкой **Сохранить все** , расположенной в левом верхнем углу консоли администрирования СЗИ;

11. Аналогичные действия выполняются на всех рабочих станциях, с установленной клиентской частью СЗИ, которые необходимо подключить к серверу СЗИ.

2. Деинсталляция СЗИ «Блокхост-сеть 2.0»

2.1. Деинсталляция сервера СЗИ «Блокхост-сеть 2.0»

Удаление сервера СЗИ «Блокхост-сеть 2.0» может произвести только пользователь, вошедший в систему под встроенной учетной записью администратора ОС Windows. Для удаления СЗИ нужно запустить апплет панели управления **Программы и компоненты** (**Пуск**→ **Панель управления**→ **Программы и компоненты**), в списке установленных программ выбрать пункт **Блокхост-сеть 2.0 (BlockHost-Net 2.0)** и нажать кнопку **Удалить**. Также для удаления программы можно воспользоваться пунктом главного меню **Удалить Блокхост-Сеть 2.0**, расположенном в группе программ **Пуск**→ **Все программы**→ **Блокхост-Сеть 2.0**. В результате откроется окно установщика Windows, в котором необходимо подтвердить операцию удаления СЗИ «Блокхост-сеть 2.0»:

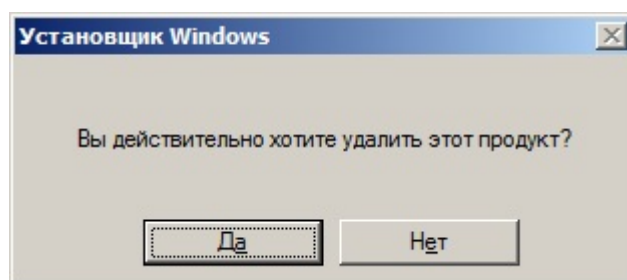


Рисунок 35. Окно запроса удаления СЗИ

После подтверждения операции удаления СЗИ запустится мастер удаления, который предложит выбрать вариант удаления СЗИ – с остановкой служб, препятствующих корректному процессу удаления СЗИ, или без их остановки:

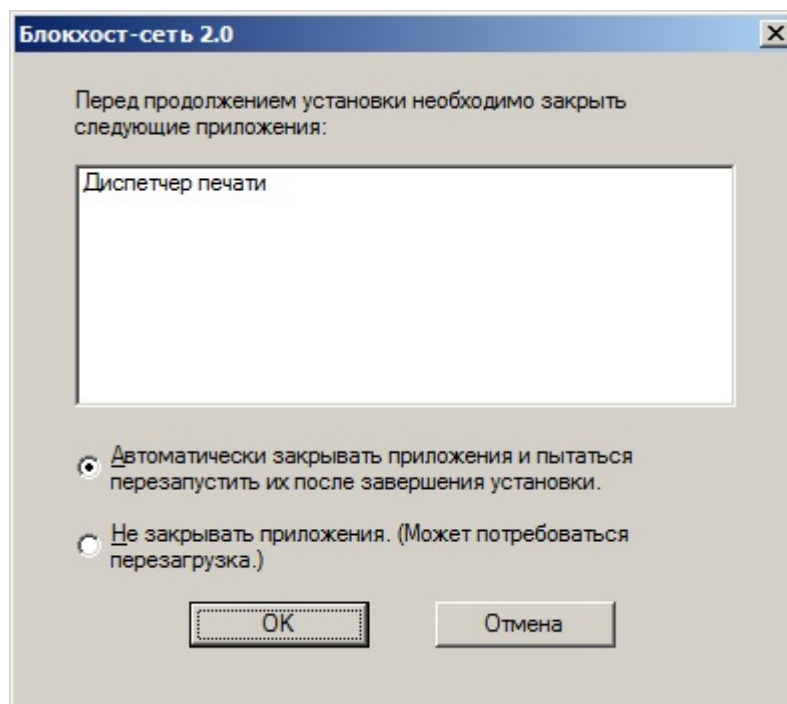


Рисунок 36. Окно запроса остановки служб СЗИ

Для корректного удаления сервера СЗИ «Блокхост-сеть 2.0» рекомендуется выбрать вариант удаления с принудительным завершением работающих служб (**Автоматически**

закрывать приложения и пытаться их перезапустить после завершения установки) и нажать кнопку **ОК**.

Если мастеру удаления СЗИ не удалось остановить работающие службы, откроется окно с сообщением об ошибке остановки этих приложений (рис. 37). После нажатия кнопки **ОК** начнется процесс удаления сервера СЗИ. Если в окнах мастера удаления СЗИ (см. рис. 35-37) нажать кнопку **Отмена (Нет)** – процесс удаления сервера СЗИ будет прекращен, система останется без изменений.

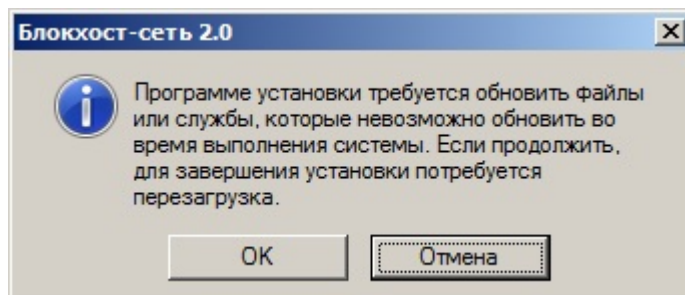


Рисунок 37. Предупреждение об ошибке остановки работающих служб СЗИ

Состояние процесса удаления серверной части СЗИ отображается в окне мастера удаления:

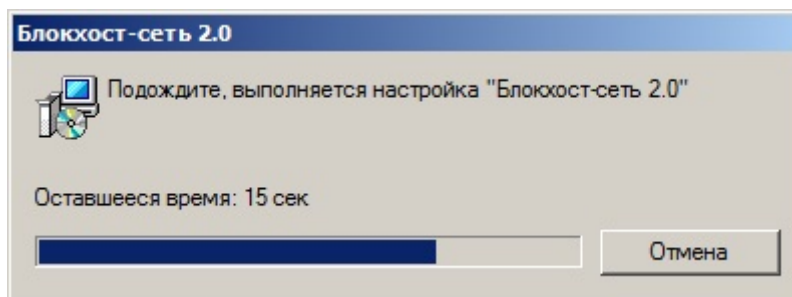


Рисунок 38. Ход удаления СЗИ «Блокхост-сеть 2.0»

По окончании удаления сервера СЗИ «Блокхост-сеть 2.0» откроется окно с предложением выполнить перезагрузку компьютера (рис. 39). Для завершения удаления СЗИ необходимо перезагрузить компьютер, сделать это можно сразу же после окончания работы мастера удаления СЗИ (нажата кнопка **Да** в окне, показанном на рис. 39), или выполнить это позже, перезагрузив компьютер вручную (нажата кнопка **Нет** в окне, показанном на рис. 39).

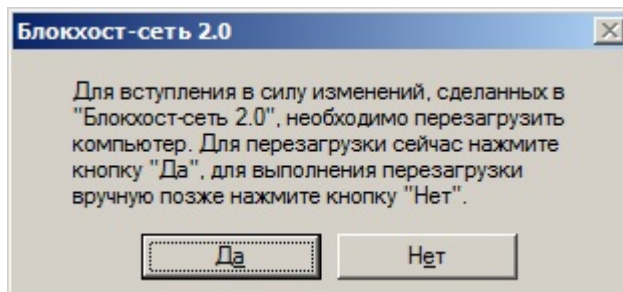


Рисунок 39. Окно завершения удаления СЗИ «Блокхост-сеть 2.0»

2.2. Деинсталляция клиентской части СЗИ «Блокхост-сеть 2.0»

Удаление клиентской части СЗИ «Блокхост-сеть 2.0» может произвести только пользователь, вошедший в систему под встроенной учетной записью администратора ОС Windows локальной рабочей станции или контроллера домена. Для удаления СЗИ нужно запустить апплет панели управления **Программы и компоненты** (**Пуск**→ **Панель управления**→ **Программы и компоненты**), в списке установленных программ выбрать пункт **Блокхост-сеть 2.0 Клиент (BlockHost-Net 2.0 Client)** и нажать кнопку **Удалить**. Также для удаления программы можно воспользоваться пунктом главного меню **Удалить Блокхост-Сеть 2.0 Клиент (Uninstall BlockHost-Net 2.0 Client)**, расположенном в группе программ **Пуск**→ **Все программы**→ **Блокхост-сеть 2.0 Клиент (Start**→ **All Programs**→ **BlockHost-Net 2.0 Client)**. В результате откроется окно установщика Windows, в котором необходимо подтвердить операцию удаления СЗИ «Блокхост-сеть 2.0»:

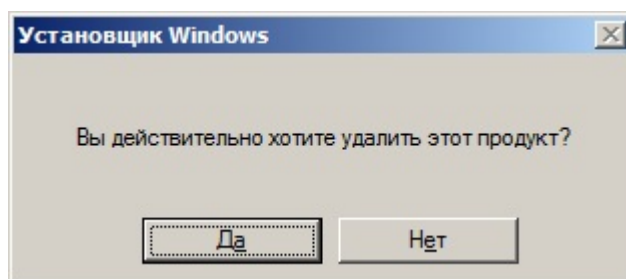


Рисунок 40. Окно запроса удаления СЗИ

После подтверждения операции удаления СЗИ запустится мастер удаления, который предложит выбрать вариант удаления СЗИ – с остановкой служб, препятствующих корректному процессу удаления СЗИ, или без их остановки:

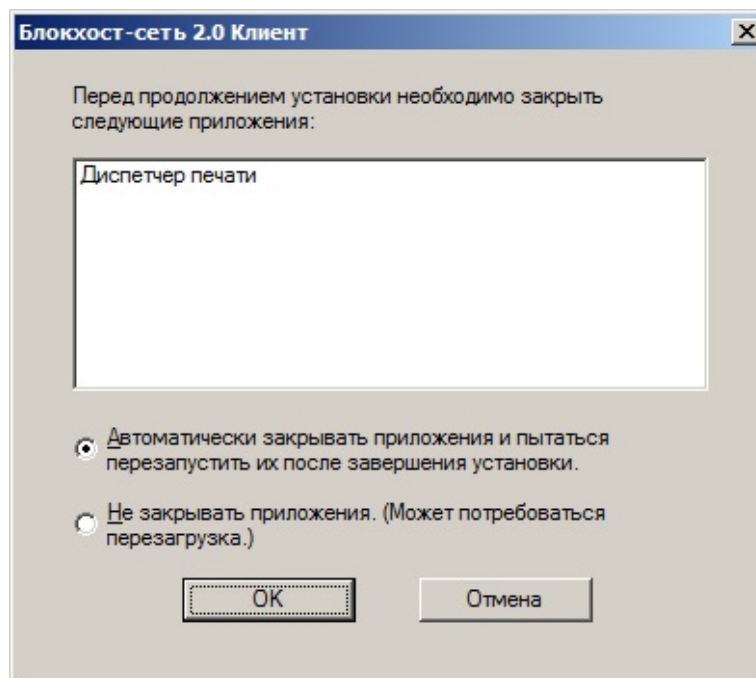


Рисунок 41. Окно запроса остановки служб СЗИ

Для корректного удаления СЗИ «Блокхост-сеть 2.0» рекомендуется выбрать вариант удаления с принудительным завершением работающих служб (**Автоматически закрывать**

приложения и пытаться их перезапустить после завершения установки) и нажать кнопку **ОК**.

Если мастеру удаления СЗИ не удалось остановить работающие службы, откроется окно с сообщением об ошибке остановки этих приложений (рис. 42). После нажатия кнопки **ОК** начнется процесс удаления СЗИ. Если в окнах мастера удаления СЗИ (см. рис. 40-42) нажать кнопку **Отмена (Нет)** – процесс удаления будет прекращен, система останется без изменений.

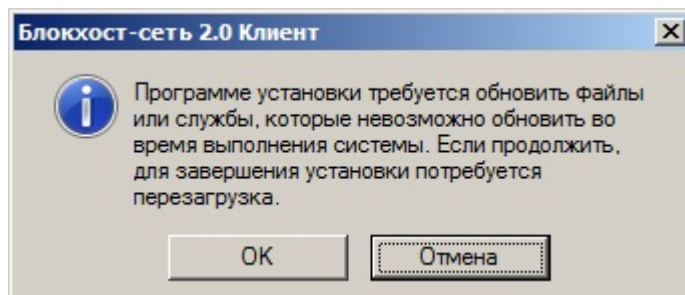


Рисунок 42. Предупреждение об ошибке остановки работающих служб СЗИ
Состояние процесса удаления СЗИ отображается в окне мастера удаления:

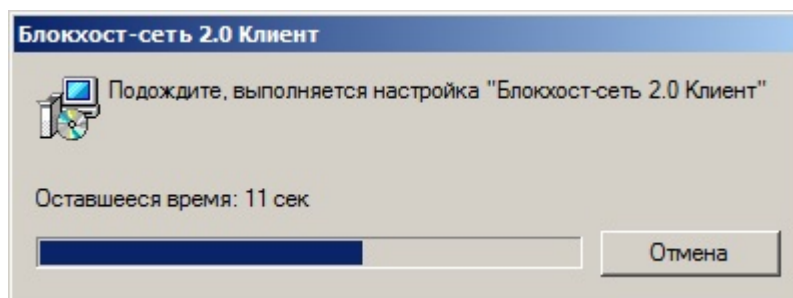


Рисунок 43. Ход удаления СЗИ «Блокхост-сеть 2.0»

По окончании удаления СЗИ «Блокхост-сеть 2.0» откроется окно с предложением выполнить перезагрузку компьютера (рис. 44). Для завершения удаления СЗИ необходимо перезагрузить компьютер, сделать это можно сразу же после окончания работы мастера удаления СЗИ (нажата кнопка **Да** в окне, показанном на рис. 44), или выполнить это позже, перезагрузив компьютер вручную (нажата кнопка **Нет** в окне, показанном на рис. 44).

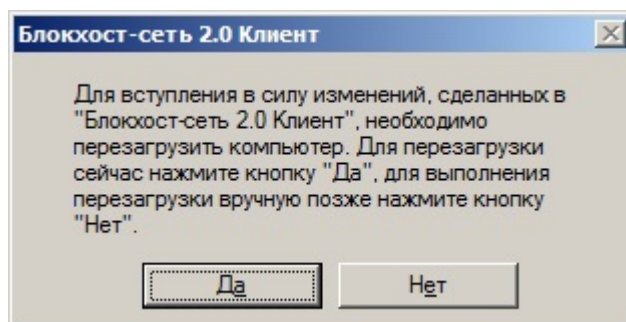


Рисунок 44. Окно завершения удаления СЗИ «Блокхост-сеть 2.0»

3. Обновление СЗИ «Блокхост-сеть 2.0»

3.1. Обновление серверной части СЗИ

Обновление более ранних версий серверной части СЗИ до сертифицированной версии СЗИ «Блокхост-сеть 2.0» производится установкой новой версии СЗИ «Блокхост-сеть 2.0» поверх уже установленной:

- *BlockHost-Net-2.0 x32.msi* (для серверной части СЗИ под управлением 32-bit ОС);
- *BlockHost-Net-2.0 x64.msi* (для серверной части СЗИ под управлением 64-bit ОС);

Обновление СЗИ производится под встроенной учетной записью администратора ОС Windows или контроллера домена.

Для обновления серверной части СЗИ необходимо запустить файл *BlockHost-Net-2.0 x64.msi* (*BlockHost-Net-2.0 x32.msi*) и последовательно пройти все шаги мастера установки СЗИ (подробное описание установки сервера СЗИ см. в подразделе 1.3 настоящего документа). Во время процесса обновления серверной части СЗИ также требуется ввод кодов лицензий СЗИ.

В процессе обновления серверной части СЗИ также будет обновлена и клиентская часть.

После завершения обновления СЗИ компьютер необходимо перезагрузить – во время процесса обновления останавливаются все службы СЗИ, а их последующий запуск возможен только после перезагрузки компьютера.

При обновлении серверной части СЗИ сохраняются все настройки, произведенные в СЗИ до ее обновления:

- для клиентской части СЗИ – индивидуальные и системные механизмы разграничения доступа и пр.;
- для серверной части СЗИ – список контролируемых на сервере рабочих станций.

3.2. Обновление клиентской части СЗИ

Обновить более ранние версии клиентской части СЗИ на рабочей станции до сертифицированной версии можно несколькими способами: локально на рабочей станции (запустив файл установки СЗИ) или удаленно из консоли администрирования на сервере СЗИ.

Обновление клиентской части до сертифицированной версии СЗИ «Блокхост-сеть 2.0» производится установкой новой версии СЗИ «Блокхост-сеть 2.0» поверх уже установленной:

- *BlockHost-Net-2.0-Client x32.msi* (для клиентской части СЗИ под управлением 32-bit ОС);
- *BlockHost-Net-2.0-Client x64.msi* (для клиентской части СЗИ под управлением 64-bit ОС);
- *BhNet.Installer.exe* (для клиентской части СЗИ под управлением 32- и 64-bit ОС)

При обновлении клиентской части СЗИ сохраняются все настройки, произведенные в СЗИ до его обновления (индивидуальные и системные механизмы разграничения доступа и пр.).

3.2.1 Локальное обновление клиентской части СЗИ

Обновление клиентской части СЗИ производится под встроенной учетной записью администратора ОС Windows рабочей станции или контроллера домена.

Для обновления СЗИ необходимо запустить файл *BlockHost-Net-2.0-Client x32.msi* или *BlockHost-Net-2.0-Client x64.msi*, в зависимости от разрядности используемой ОС, или файл *BhNet.Installer.exe* (для ОС любой разрядности) и последовательно пройти все шаги мастера установки СЗИ (подробное описание установки клиентской части СЗИ см. в подразделе 1.4.3 настоящего документа). Во время процесса обновления клиентской части СЗИ также потребуется ввести все необходимые коды лицензий СЗИ.

После завершения работы мастера обновления клиентской части СЗИ появится окно с предложением перезагрузки рабочей станции (см. пример на рис. 44). Для завершения обновления клиентской части СЗИ необходимо перезагрузить компьютер, сделать это можно сразу же после окончания работы мастера обновления СЗИ (нажата кнопка **Да** в окне, показанном на рис. 44), или выполнить это позже, перезагрузив компьютер вручную (нажата кнопка **Нет** в окне, показанном на рис. 44).



Следует иметь в виду, что возможность администрирования рабочей станции из серверной консоли администрирования СЗИ по окончании процесса обновления СЗИ появится только после перезагрузки рабочей станции и запуска служб СЗИ на ней – во время процесса обновления останавливаются все службы СЗИ, а их последующий запуск возможен только после перезагрузки компьютера.

3.2.2 Обновление клиентской части СЗИ из окна серверной консоли администрирования

Для обновления клиентской части администратору безопасности необходимо:

1. Выделив в окне «**Список машин**» консоли администрирования СЗИ пункт **Все машины** перейти во вкладку **Развертывание MSI пакетов**, для чего выбрать пункт меню **Развертывание** → **Развертывание MSI пакетов** (см. пример на рис. 14).
2. Для формирования списка рабочих станций для обновления клиентской части СЗИ нажать кнопку **Поиск по списку машин**.
3. В открывшемся окне «**Добавление клиентов на основе списка машин**» выделить рабочие станции, на которых будет обновляться клиентская часть СЗИ (для выделения нескольких рабочих станций можно воспользоваться клавишами <Ctrl> или <Shift>) и при помощи кнопок управления (>> и <<) сформировать список рабочих станций для обновления версии СЗИ, затем нажать кнопку **Добавить** (рис. 45).
4. Дальнейшие действия по обновлению клиентской части СЗИ на выбранных рабочих станциях аналогичны процессу установки СЗИ из окна серверной консоли администрирования, описанному в пунктах 6-8, 10 подраздела 1.4.1 настоящего руководства.

При обновлении клиентской части СЗИ из серверной консоли администрирования отсутствует необходимость заполнения поля **Параметры** вкладки **Развертывание MSI пакетов** (см. пример на рис. 22) – в данное поле автоматически будут добавлены параметры подавления перезагрузки после окончания процесса обновления СЗИ

(*REBOOT=ReallySuppress*) и ведения файла-журнала процесса обновления СЗИ на рабочей станции (*/L *V "C:\<имя_файла_установщика>.log"*).

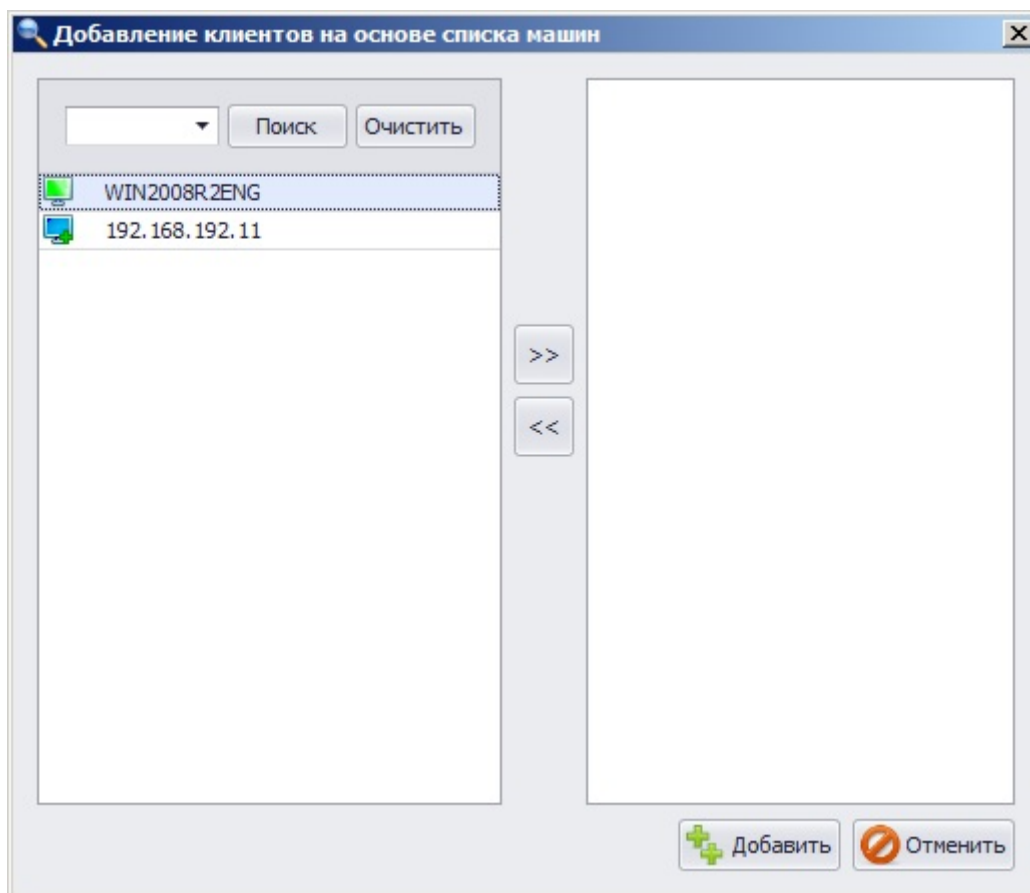


Рисунок 45. Окно добавления рабочих станции на основе списка контролируемых на сервере СЗИ



Следует иметь в виду, что если при обновлении СЗИ использовался параметр подавления перезагрузки рабочей станции, то возможность ее администрирования по окончании процесса обновления СЗИ из серверной консоли администрирования появится только после перезагрузки рабочей станции и запуска служб СЗИ на ней – во время процесса обновления останавливаются все службы СЗИ, а их последующий запуск возможен только после перезагрузки компьютера.