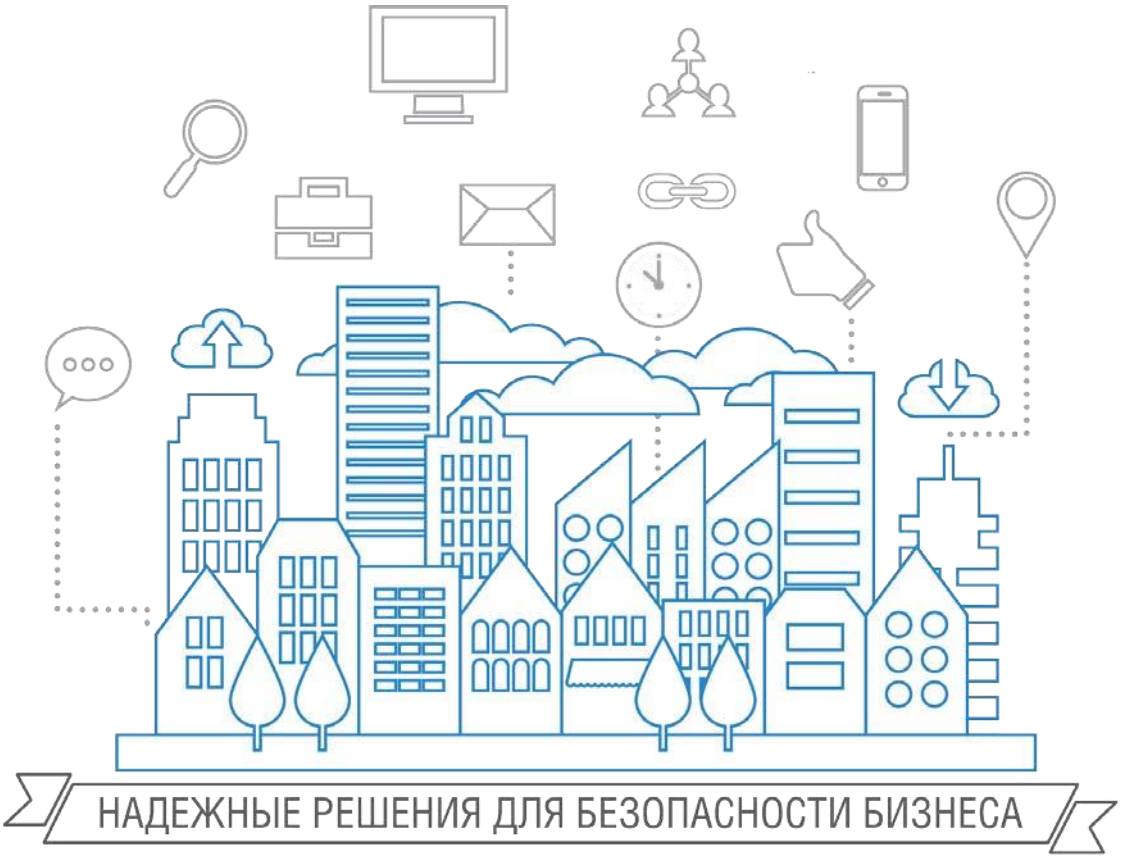
ГАЗИНФОРМСЕРВИС

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 -Пет ербу рге 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

Автономный вариант



Санкт-Петербург, 2018

Содержание

1. Установка СЗИ «Блокхост-сеть 2.0»

1.1. Требования к аппаратной конфигурации

Автономный вариант СЗИ «Блокхост-сеть 2.0» поставляется в виде файлов Microsoft Windows Installer *BlockHost-Net-2.0-Client x32.msi* и *BlockHost-Net-2.0-Client x64.msi* для 32- и 64-битных ОС Windows соответственно. Также в состав дистрибутива автономного 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.

СЗИ «Блокхост-сеть 2.0» 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 клиентской части СЗИ «Блокхост-сеть 2.0» на компьютеры, работающие под управлением операционных систем:

- 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 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 8.1 Core (32-разрядная);
- Windows 8.1 Core (64-разрядная);
- Windows 8.1 Professional (32-разрядная);
- Windows 8.1 Professional (64-разрядная);
- Windows 8.1 Enterprise (32-разрядная);
- Windows 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 (32-разрядная);
- Windows 10 Home (64-разрядная);
- Windows 10 Pro (32-разрядная);
- Windows 10 Pro (64-разрядная);
- Windows 10 Enterprise (32-разрядная);
- Windows 10 Enterprise (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-v2-x64* (*NDP40-KB2468871-v2-x86*) или выше;
- Обновление системы безопасности KB3033929 (для ОС Windows 7 и Windows Server 2008/2008R2);
- драйверы для устройств eToken и SafeNet eToken (любой из вариантов):
  - SafeNet Authentication Client 8.2. Подходит для всех поддерживаемых ОС, в комплект поставки СЗИ не входит.
  - eToken PKI Client 5.1 SP1 или eToken RTE 3.66 – при использовании персональных идентификаторов eToken PRO, eToken NG-FLASH, eToken NG-OTP;
  - eToken PKI Client 5.1 SP1 – при использовании персональных идентификаторов eToken NG-FLASH (Java), eToken NG-OTP (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

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.

Перед началом установки СЗИ на ОС Windows 10 необходимо отключить протокол ***Secure Boot***, отвечающий за безопасную загрузку ОС, в настройках BIOS. Отключение данного протокола, осуществляется установкой параметра ***Secure Boot*** в значение ***Disabled***. Более подробная информация о настройке параметра ***Secure Boot*** описана в документации к материнской плате рабочей станции, на которую устанавливается СЗИ.

1.2.2. Особенности установки СЗИ «Блокхост-сеть 2.0» на ПК под управлением ОС Windows 8.1/2012/2012R2

Перед началом установки СЗИ «Блокхост-сеть 2.0» необходимо отключить встроенный в ОС Windows 8.1/2012/2012R2 стандартный защитник Windows (Windows Defender), для чего следует:

1) запустить ***Windows Defender*** (***Пуск→ Все приложения→ Windows Defender***, см. пример на рис. 1);
2) во вкладке **Параметры** окна **«Windows Defender»** выбрать пункт ***Администратор***, снять флажок с пункта ***Включить Windows Defender*** (рис. 2).

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

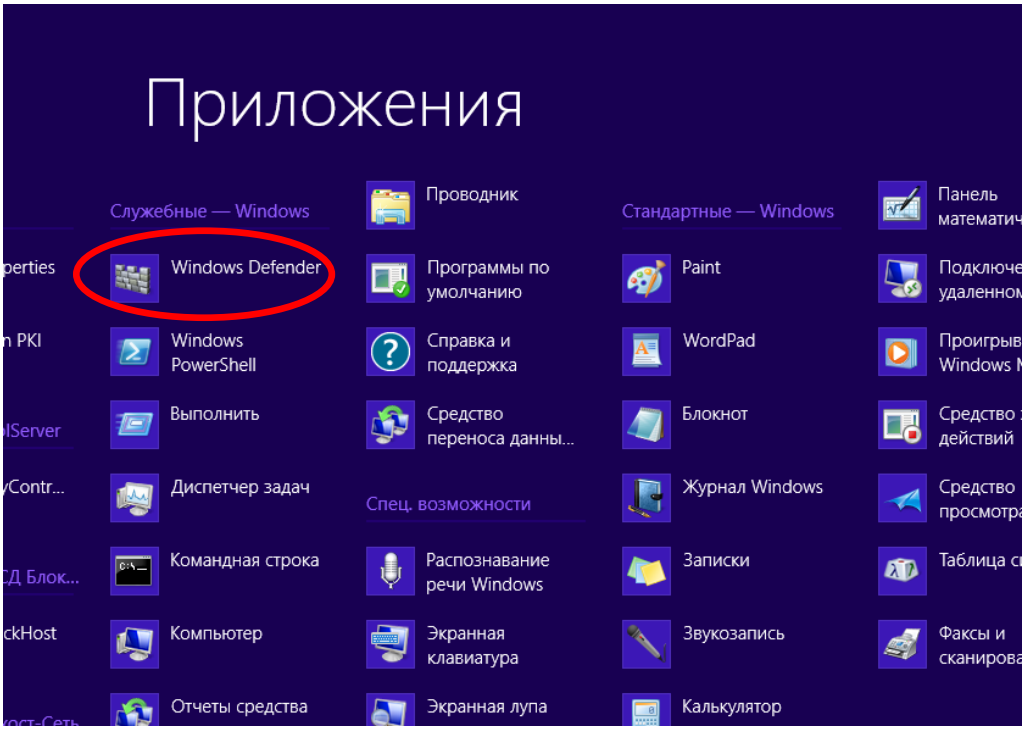


Рисунок 1. Выбор пункта «Windows Defender»

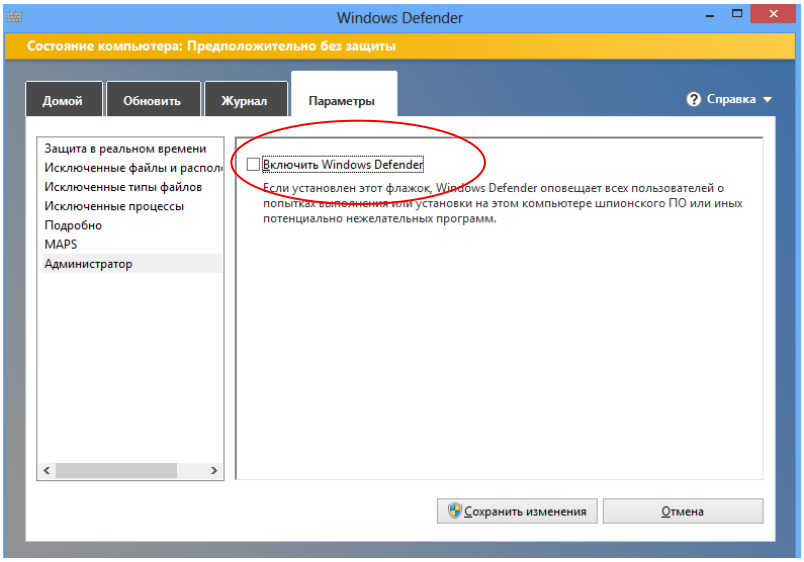


Рисунок 2. Отключение «Windows Defender»

1.3. Порядок установки СЗИ «Блокхост-сеть 2.0»

1.3.1. Локальная установка СЗИ «Блокхост-сеть 2.0»

Инсталляция СЗИ производится с компакт-диска или другого носителя. Программа поставляется в виде файлов Microsoft Windows Installer *BlockHost-Net-2.0-Client x32.msi* (для 32-bit ОС) и *BlockHost-Net-2.0-Client x64.msi* (для 64-bit ОС), а также файла *BhNet.Installer.exe*, который содержит в себе инсталляторы для 32- и 64-bit ОС. Мастер установки клиентской части СЗИ «Блокхост-сеть 2.0» имеет оконный графический интерфейс.

При использовании автономного варианта СЗИ «Блокхост-сеть 2.0» клиентскую часть СЗИ «Блокхост-сеть 2.0» устанавливают на защищаемый локальный ПК.

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

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 или *BlockHost-Net-2.0-Client x64.msi* – для 64-bit ОС). Запустить файл-установщик на выполнение можно дважды щелкнув по нему в окне **Проводника** Windows или выполнить 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:

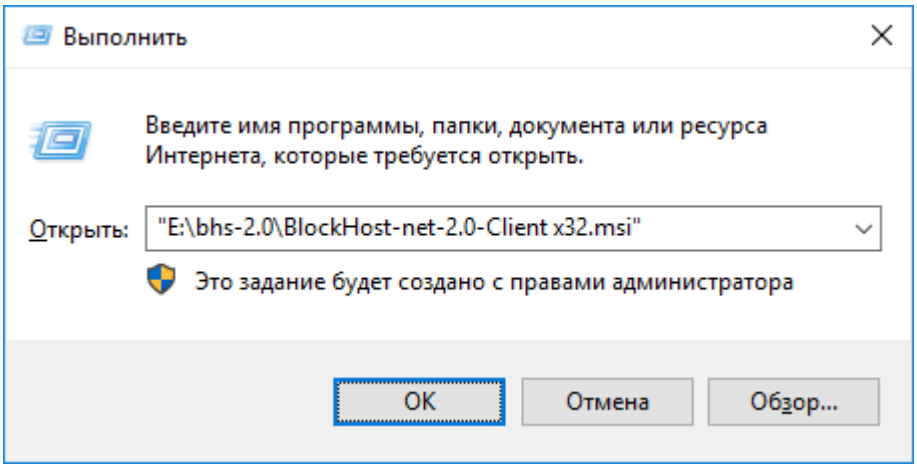


Рисунок 3. Запуск файла-установщика

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

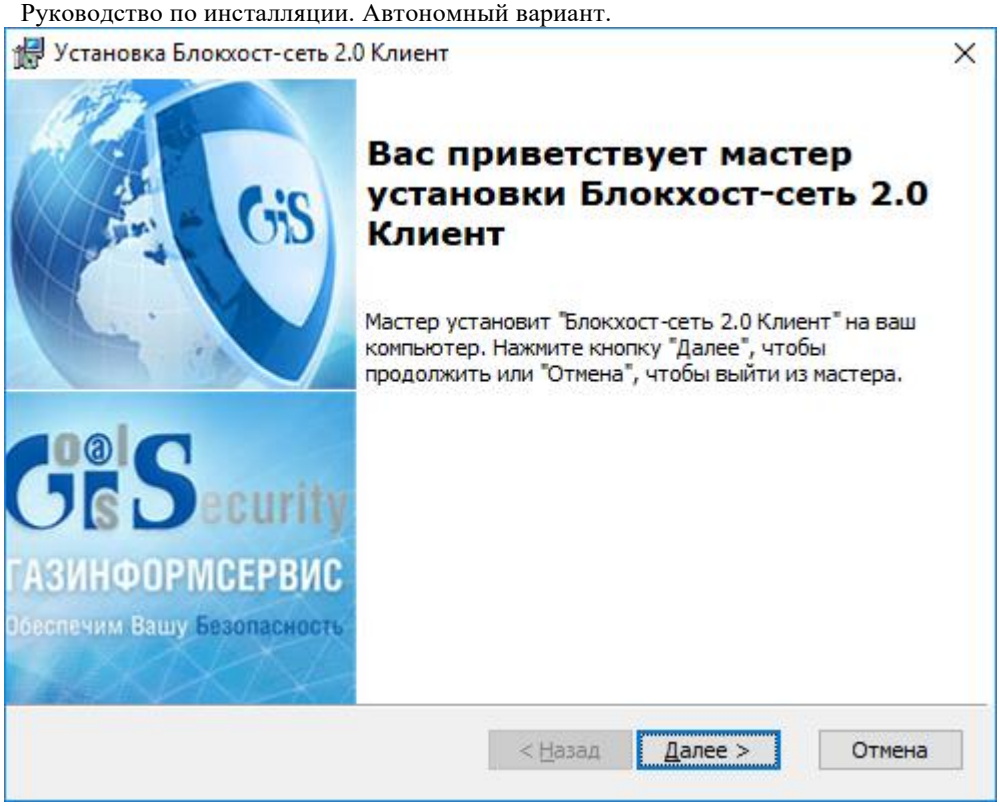


Рисунок 4. Окно установки сервера СЗИ «Блокхост-сеть 2.0»

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

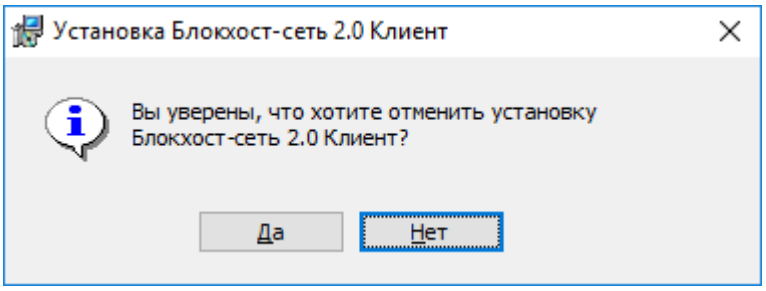


Рисунок 5. Окно прекращения установки

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).

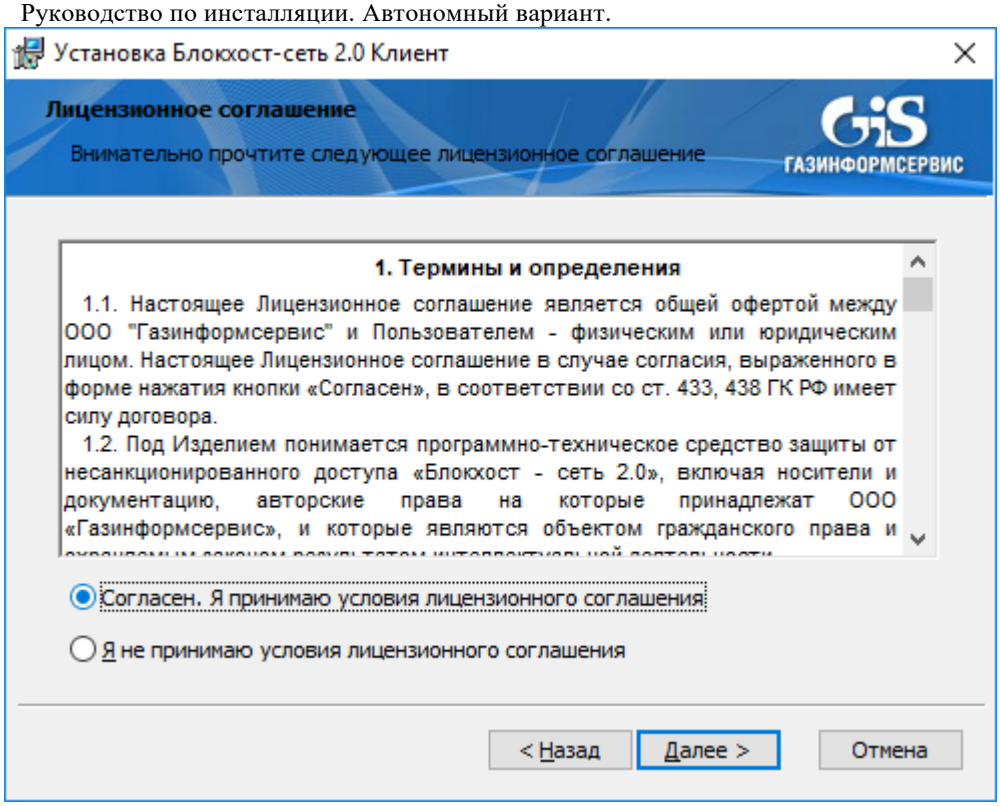


Рисунок 6. Окно мастера установки СЗИ «Блокхост-сеть 2.0» с лицензионным соглашением

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 код лицензии и код активации клиентской части, которые прописаны в выданной лицензии. Поля ввода кода с***етевой*** лицензии клиента и кода ее активации оставить незаполненными.

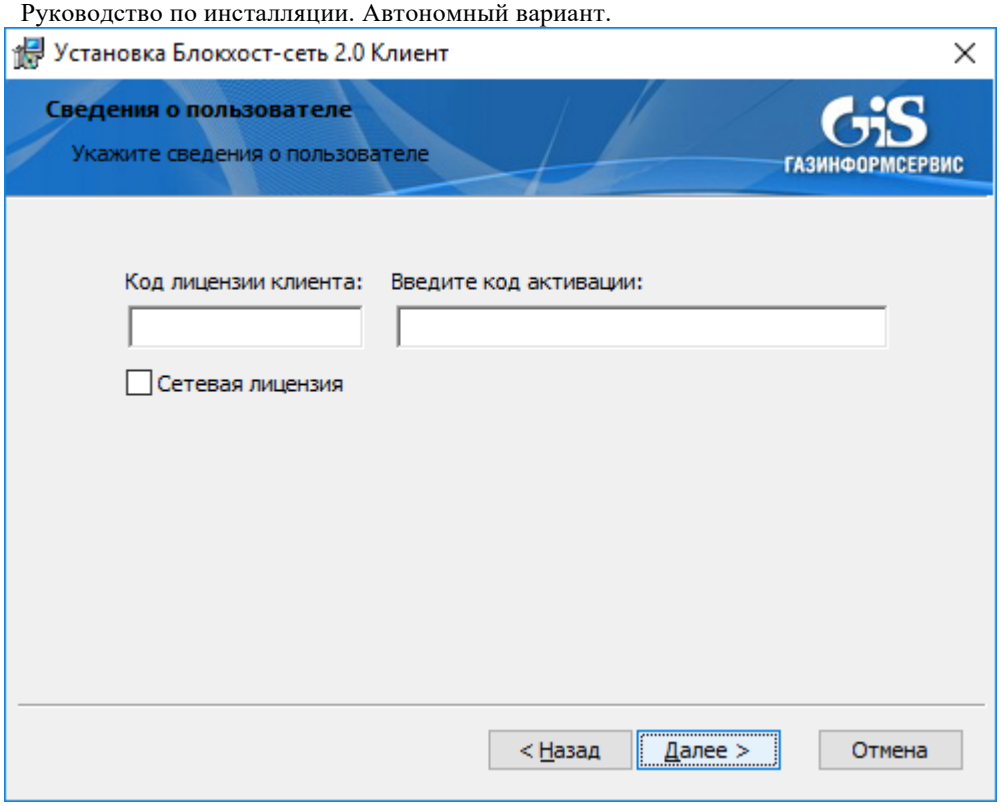


Рисунок 7. Окно ввода кода лицензии и кода активации СЗИ «Блокхост-сеть 2.0»

После заполнения полей ввода кода лицензии клиента и кода ее 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 (рис. 8). После нажатия на кнопку ***ОК*** происходит возврат в окно ввода лицензий, в котором необходимо скорректировать введенные значения кодов лицензии клиента и ее активации и продолжить установку.

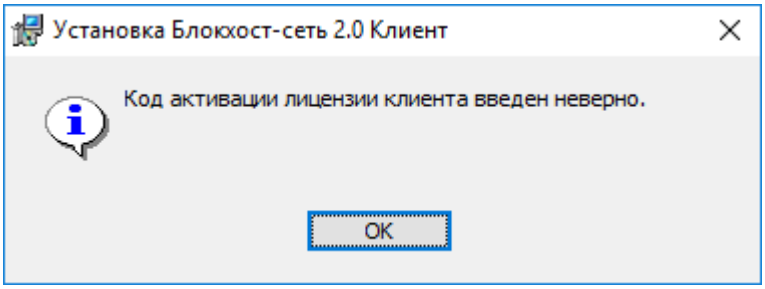


Рисунок 8. Окно с сообщением о неверно введенном коде

На следующем шаге работы мастера установки появится окно формирования ключевого носителя администратора безопасности (рис. 9). 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 8.1/2012/2012R2/10/2016, 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 защищённом 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 (локальная консоль)».

Для продолжения установки нажмите кнопку ***Далее***:

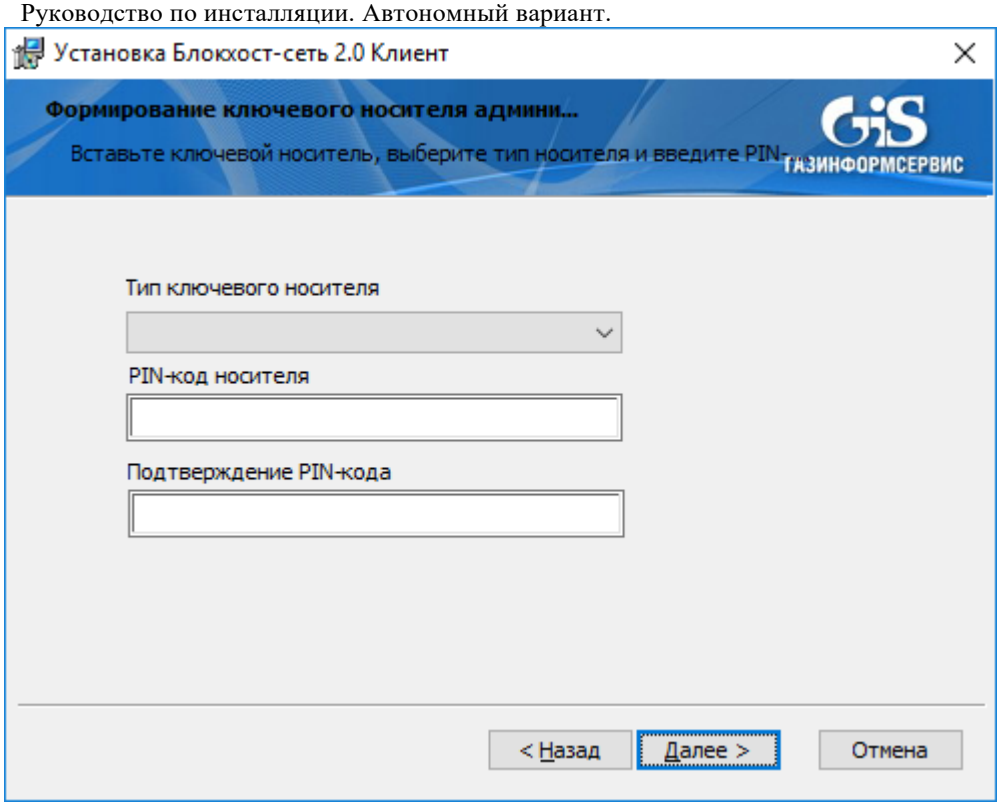


Рисунок. 9. Окно формирования ключевого носителя администратора

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.

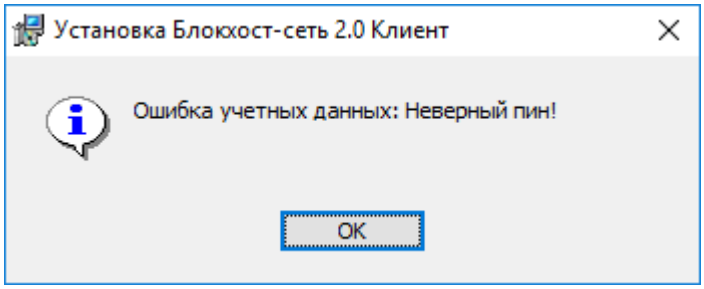


Рисунок 10. Окно сообщения о неверном PIN-коде

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 СЗИ «Блокхост-сеть 2.0».

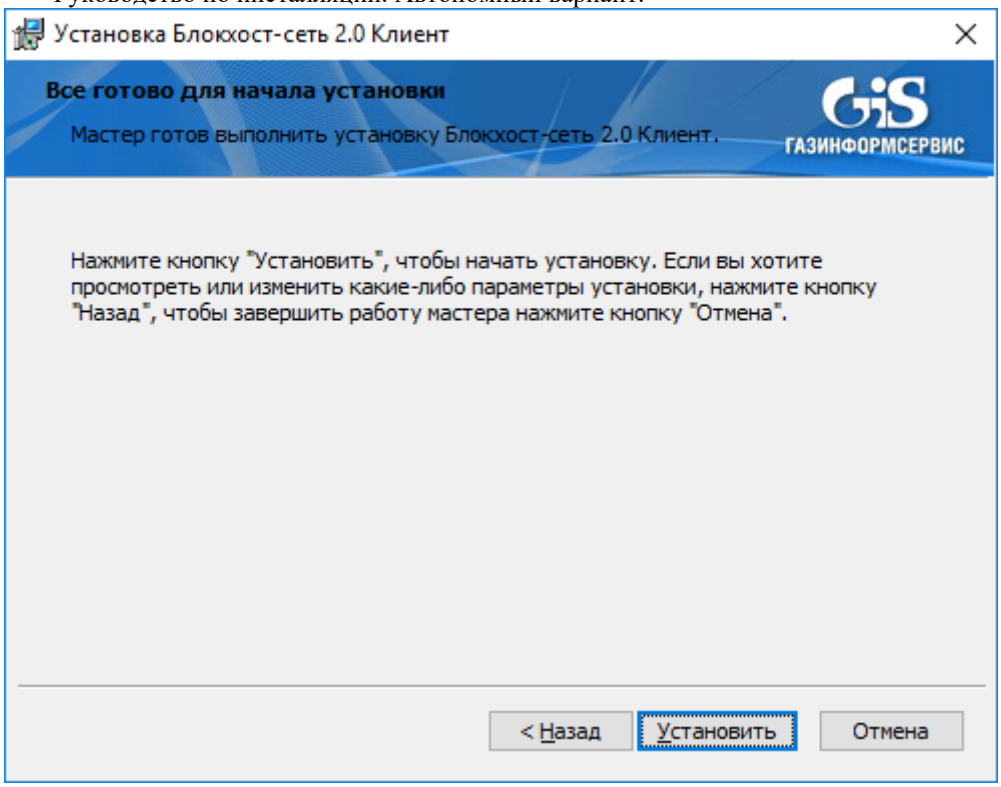


Рисунок 11. Окно готовности к установке СЗИ «Блокхост-сеть 2.0»

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

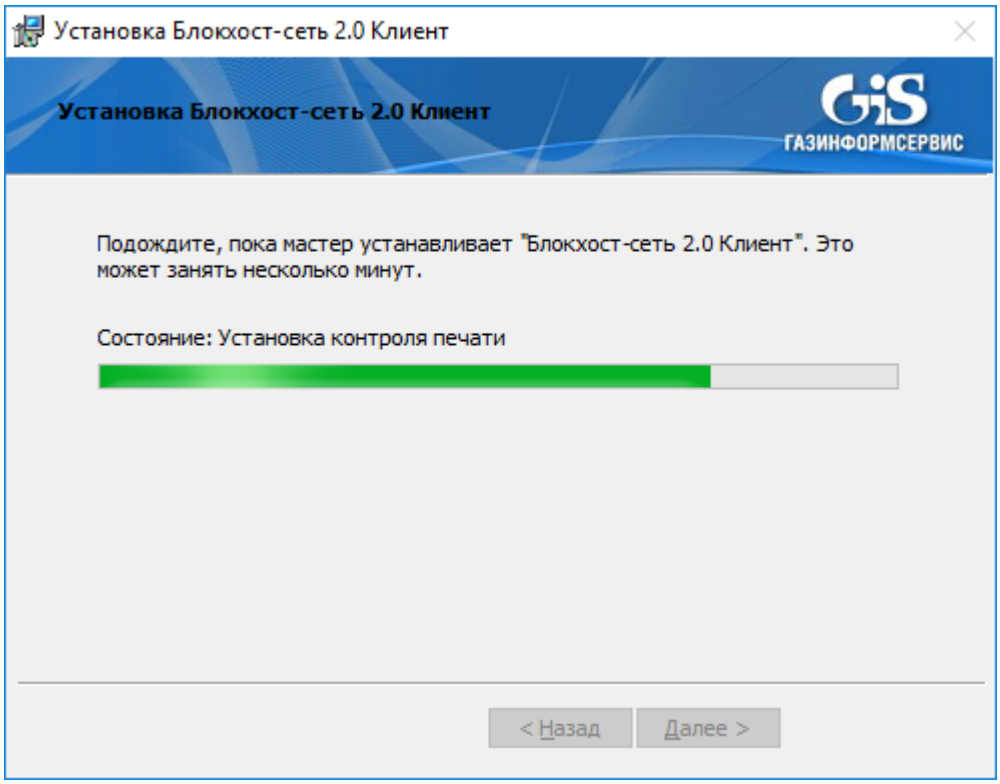


Рисунок 12. Ход установки СЗИ «Блокхост-сеть 2.0»

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

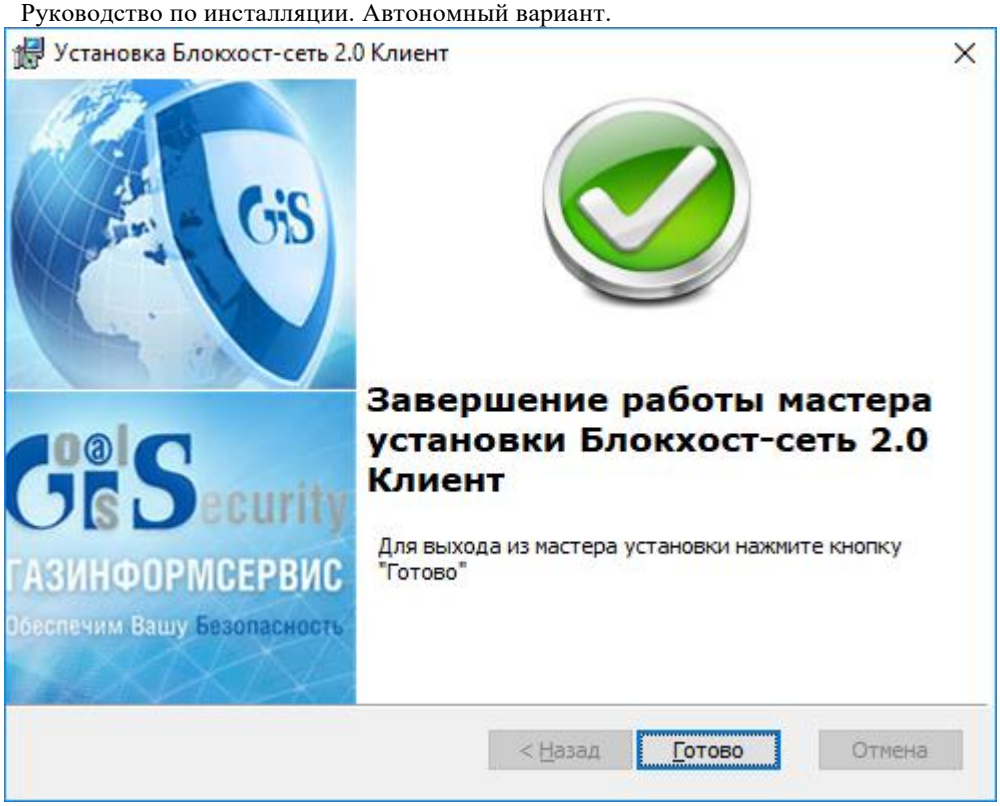


Рисунок 13. Окно окончания установки СЗИ «Блокхост-сеть 2.0»

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

1.3.2. Инсталляция СЗИ из окна интерпретатора командной строки Windows

Для установки СЗИ «Блокхост-сеть 2.0» из командной строки необходимо после указания файла дистрибутива СЗИ ввести необходимые коды лицензии и ее активации и параметры первоначальной настройки работы СЗИ. Список параметров, их описание, возможные значения и значения по умолчанию приведены в табл. 1.

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 PIN=12345 PIN2=12345 LOC=<код лицензии клиента> LOCKEY=<ключ активации лицензии клиента>
```

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

```
BhNet.Installer.exe /qn /qn PIN=12345 PIN2=12345 LOC=<код лицензии клиента> LOCKEY=<ключ активации лицензии клиента>
```

Таблица 1. Параметры конфигурации клиента СЗИ

Наименование параметра	Назначение	Возможные значения
/qn	Параметры Windows Installer, позволяющие проводить установку без участия пользователя в скрытом режиме	

Наименование параметра	Назначение	Возможные значения
PIN	PIN-код доступа к ключевому носителю	Если параметр отсутствует, то при инсталляции СЗИ не будет создан ключевой идентификатор в реестре Windows рабочей станции. При установке PIN-кода ключевого носителя запрещено использовать символы русского алфавита и спецсимволы: ~ / \ | ; ? $ & % @ ^ = * ’ + ” [ ] ` { } ( ) < >
PIN2	Подтверждение PIN-кода доступа к ключевому носителю	Если параметр отсутствует, то при инсталляции СЗИ не будет создан ключевой идентификатор в реестре Windows рабочей станции. При установке PIN-кода ключевого носителя запрещено использовать символы русского алфавита и спецсимволы: ~ / \ | ; ? $ & % @ ^ = * ’ + ” [ ] ` { } ( ) < >
LOC	Код лицензии клиента	По умолчанию не задан
LOCKEY	Ключ активации лицензии клиента	По умолчанию не задан
SOFTMODE	Работа СЗИ в мягком режиме	1 – мягкий режим включен; отсутствие параметра – мягкий режим отключен.
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.
REBOOT	Параметр перезагрузки рабочей станции	*ReallySuppress* – перезагрузка подавляется (по умолчанию); *Force* – по окончании инсталляции СЗИ выполняется перезагрузка рабочей станции
USERS	Список SID-ов пользователей, указанных через запятую.	При отсутствии параметра, в список пользователей СЗИ 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.

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 (локальная консоль)».

1.3.3 Установка СЗИ «Блокхост-сеть 2.0» с использованием групповых политик.

Для установки СЗИ «Блокхост-сеть 2.0» 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 2008R2):

1. Поместить msi-файл установщика клиентской части СЗИ в папку с общим доступом (например, *%WINDIR%\SYSVOL\domain\scripts*).

> К каталогу должен быть предоставлен доступ на ***Чтение*** и ***Выполнение*** для учетных записей компьютеров.
> 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 компьютеров, на которые планируется осуществить установку клиента СУ. 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 →Управление групповой политикой*** (рис. 14).

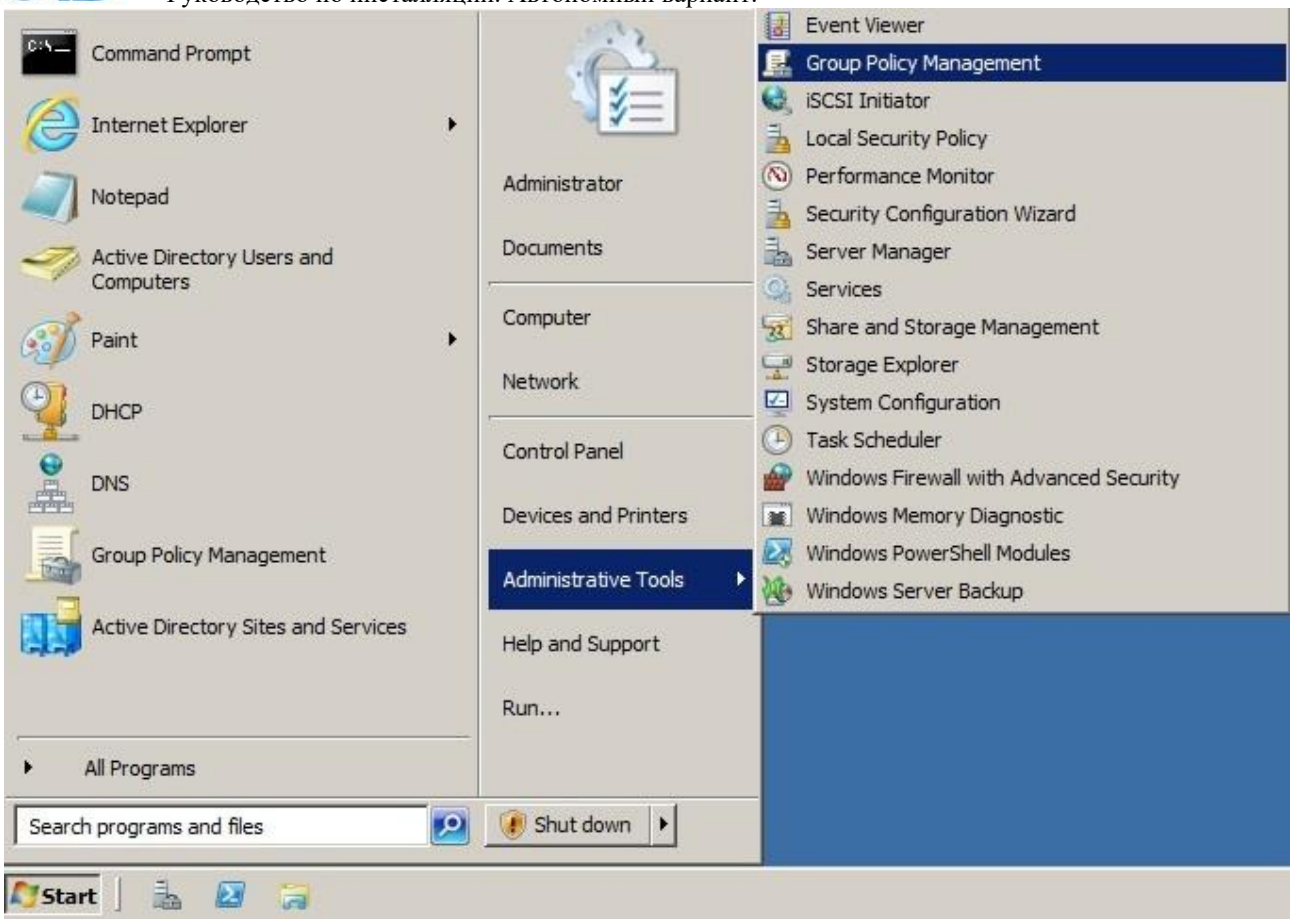


Рисунок 14. Запуск консоли управления групповой политикой

3. В открывшемся окне **«Управление групповой политикой»** (рис. 15) 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***.

При использовании файлов-установщиков *BlockHost-Net-2.0-Client x32.msi*, *BlockHost-Net-2.0-Client x64.msi* необходимо создавать два объекта групповой политики для инсталляции 32- и 64-bit клиентской части СЗИ на рабочие станции с ОС соответствующей разрядности.

При использовании в объекте групповой политики файла-инсталлятора *BhNet.Installer.exe* для установки клиентской части СЗИ, в зависимости от разрядности ОС, будет использован файл-установщик необходимой разрядности.

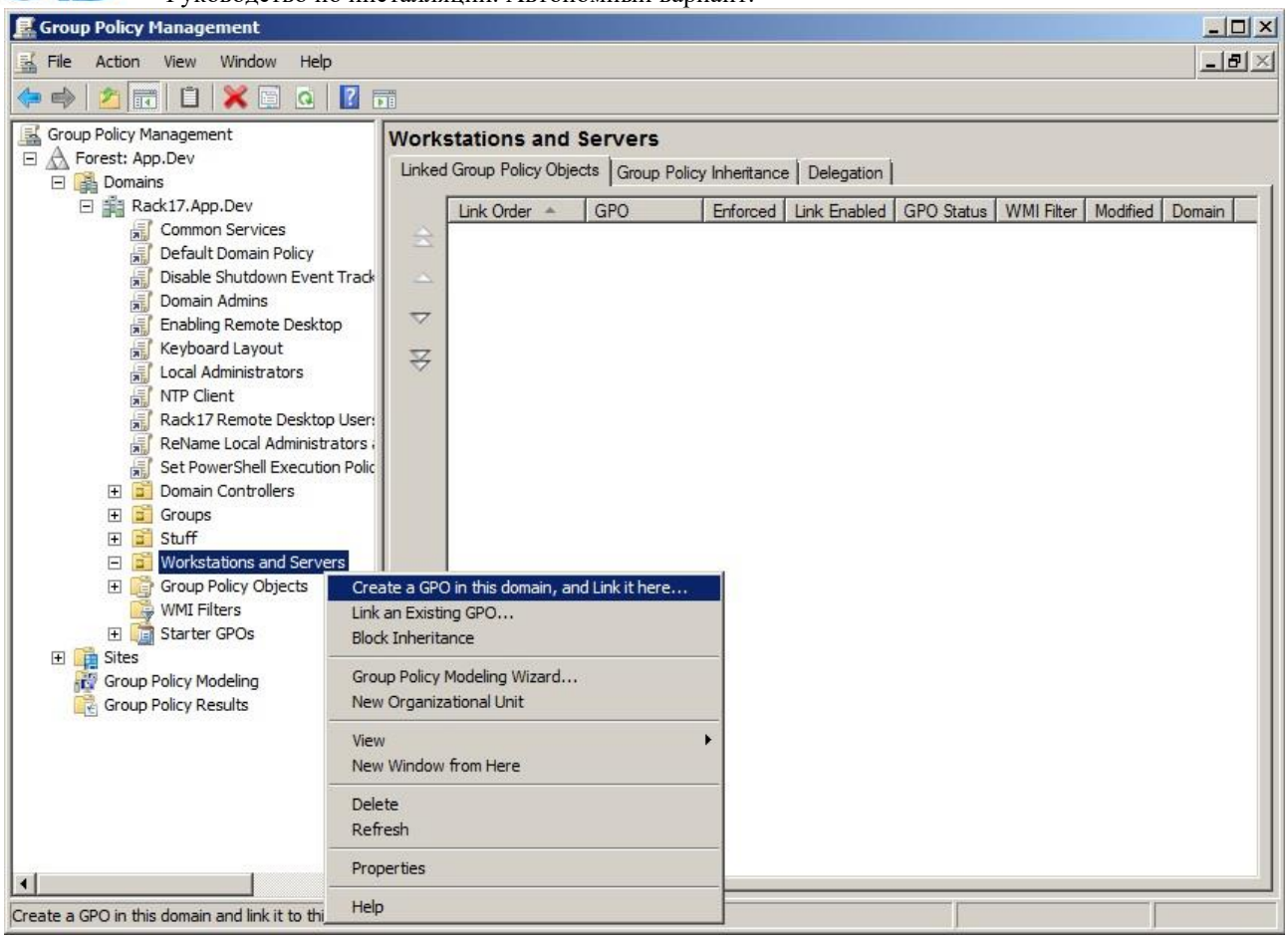


Рисунок 15. Меню создания объекта групповой политики

4. Ввести описательное имя объекта групповой политики в поле ***Имя*** диалогового окна **«Новый объект групповой политики»** и нажать кнопку ***ОК***:

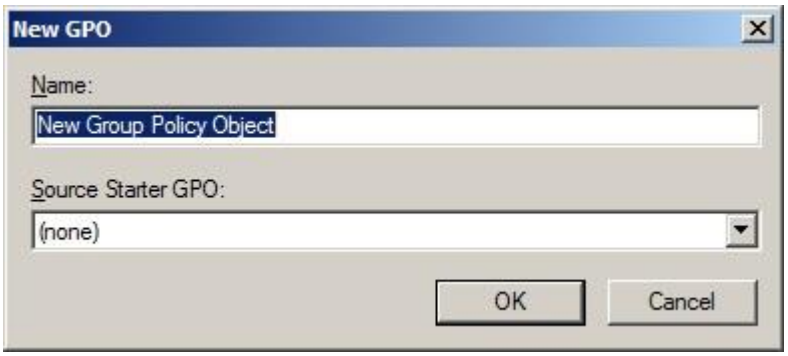


Рисунок 16. Окно создания объекта групповой политики

5. Выделить созданный объект групповой политики (рис. 17), щелкнуть на нем правой кнопкой мыши и выбрать пункт контекстного меню ***Изменить*** для редактирования этого объекта.

6. В окне **«Редактор объектов групповой политики»** (рис. 18) перейти к пункту ***Сценарии (Запуск/Завершение)***, раскрыв дерево ***Конфигурация компьютера →Политики →Конфигурация Windows***. В открывшейся вкладке **Сценарии (Запуск/Завершение)** щелкнуть два раза левой кнопкой мыши на параметре **Автозагрузка**.

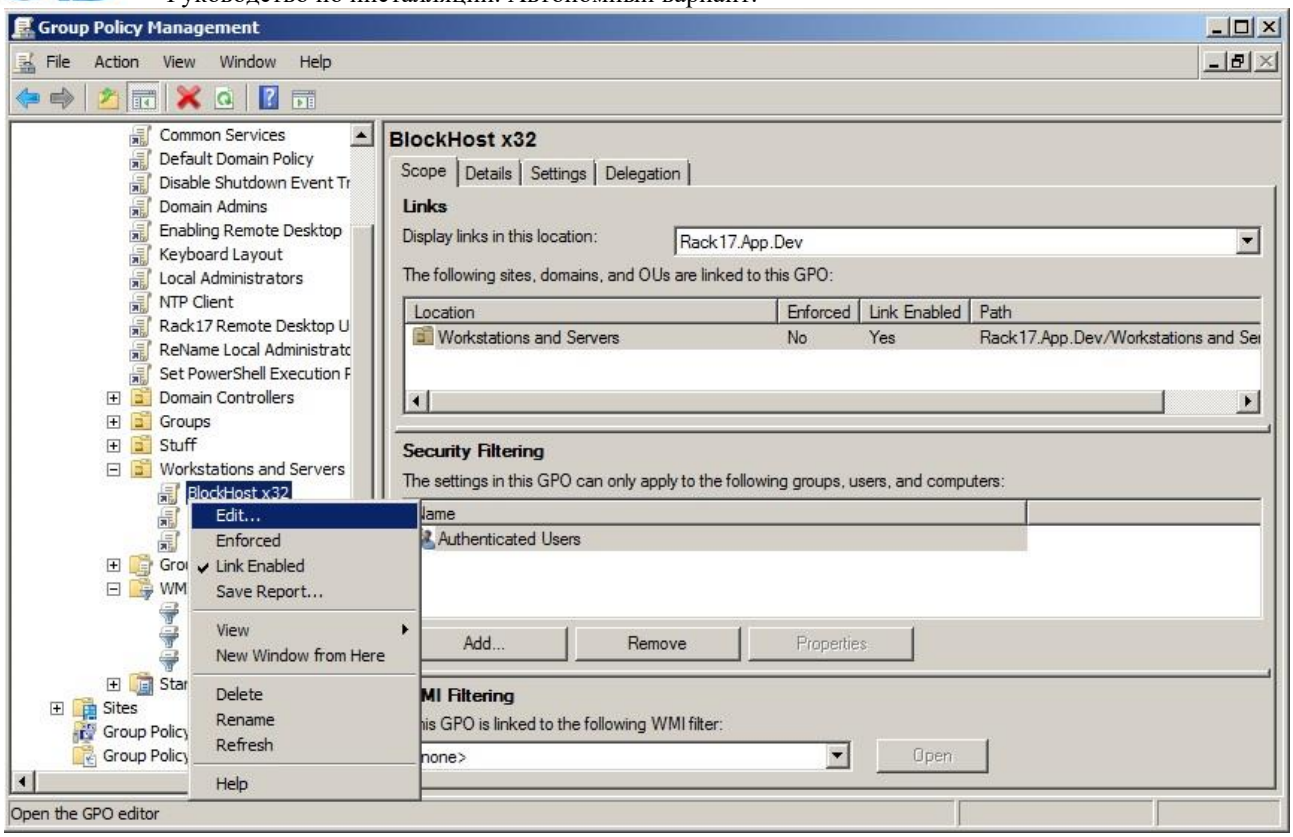


Рисунок 17. Меню вызова редактора групповой политики

Рисунок 18. Окно редактора групповой политики

7. В открывшемся окне **«Свойства: Автозагрузка»** (рис. 19) нажать кнопку ***Добавить***.

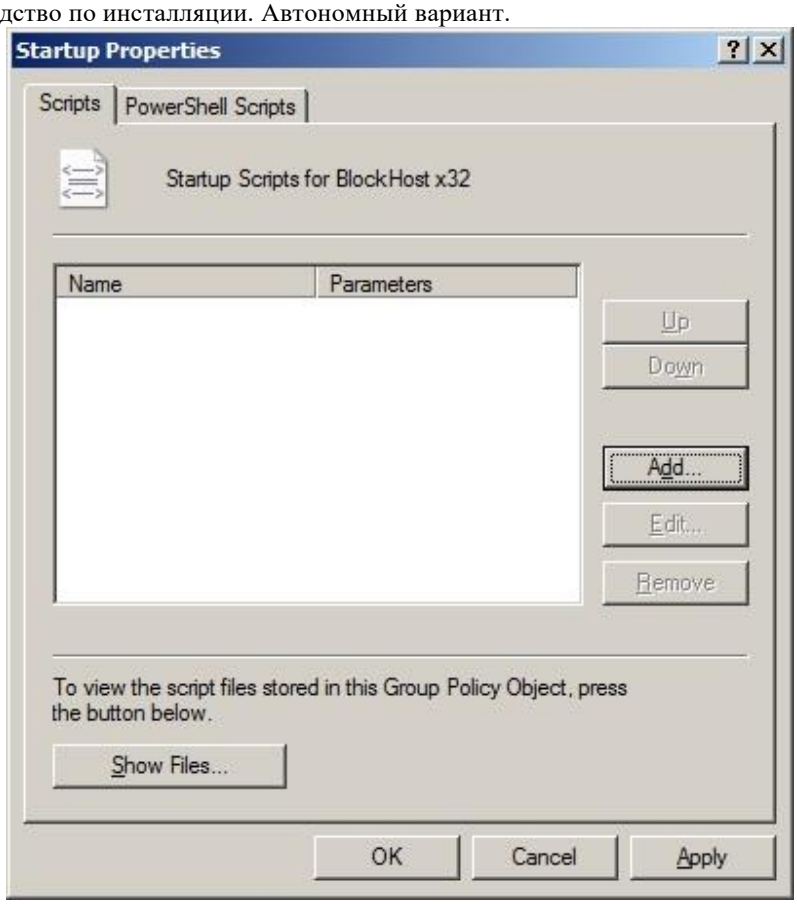


Рисунок 19. Окно свойств сценария автозагрузки

8. В открывшемся окне **«Добавление сценария»** (рис. 20):
   - в поле ***Имя сценария*** необходимо указать путь к дистрибутиву клиентской части СЗИ. Путь можно ввести вручную или воспользовавшись кнопкой ***Обзор***, указать месторасположение файла-установщика с помощью стандартного окна Windows **«Обзор»**;

Путь к файлу-установщику должен быть задан в формате UNC, например: `\\server_name\share_name\BlockHost-Net-2.0-Client x32.msi`.

   - в поле ***Параметры сценария*** необходимо ввести необходимые для установки клиентской части СЗИ параметры: лицензию на использование СЗИ на рабочих станциях и параметры первоначальной настройки режимов работы СЗИ. Список параметров, их описание, возможные значения и значения по умолчанию приведены в табл. 1;
   - нажать кнопку ***OK***.

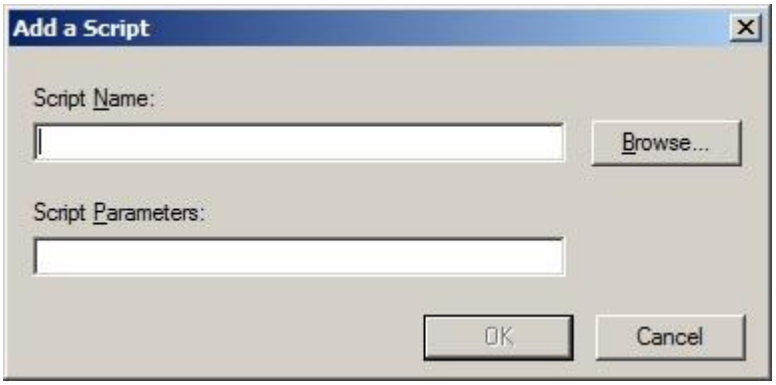


Рисунок 20. Окно добавления сценария

9. Нажать кнопку ***ОК*** в окне **«Свойства: Автозагрузка»**;
10. Закрыть окно редактора объектов групповой политики (рис. 18);
11. Затем необходимо задать фильтр выбора разрядности рабочих станций (серверов) домена, к которым будет применена созданная групповая политика:

- в окне **«Управление групповой политикой»** (см. рис. 17) выделить параметр ***Фильтры WMI*** и выбрать пункт меню ***Действие →Создать***, или воспользоваться аналогичным пунктом контекстного меню выделенного параметра;
- в открывшемся окне **«Новый фильтр WMI»** в поле ***Имя*** ввести имя создаваемого фильтра, которое будет однозначно определять его назначение. При необходимости в поле ***Описание*** можно ввести описание назначения создаваемого фильтра. Нажать кнопку ***Добавить***:

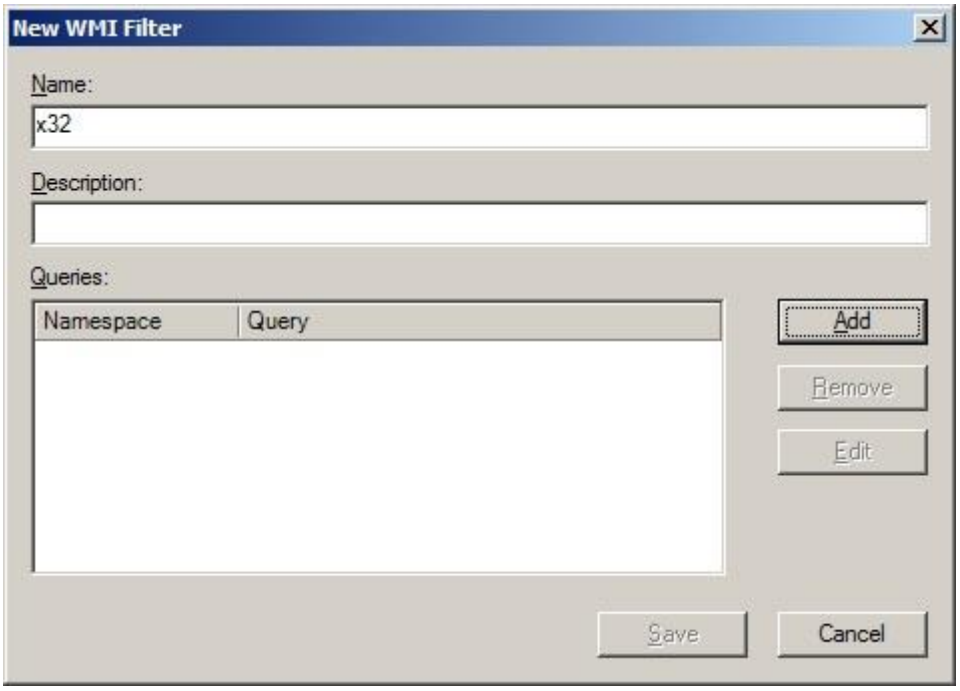


Рисунок 21. Окно создания WMI-фильтра

- в открывшемся окне **«Запрос WMI»** (рис. 22) ввести в поле ***Запрос*** строку
  *Select * from Win32_Processor where AddressWidth = "32"* или
  *Select * from Win32_Processor where AddressWidth = "64"* для выбора 32- или 64-разрядных ОС соответственно.
  В случае необходимости выбора только рабочих станций или только серверов в поле ***Запрос*** необходимо добавить строку
  *Select * from Win32_OperatingSystem where ProductType = 1* – в случае установки СЗИ на рабочие станции (если СЗИ устанавливается на серверные ОС, то указать значение параметра *ProductType = 3*).
  Нажать кнопку ***ОК***;
- в окне **«Новый фильтр WMI»** (см. рис. 21) нажать кнопку ***Сохранить***;
- в окне **«Управление групповой политикой»** выделить созданную групповую политику и на вкладке ***Область*** в выпадающем списке раздела *Фильтрация WMI* выбрать имя соответствующего фильтра (рис. 23). Подтвердить выбор фильтра WMI к выделенному объекту групповой политики в открывшемся окне-запросе.

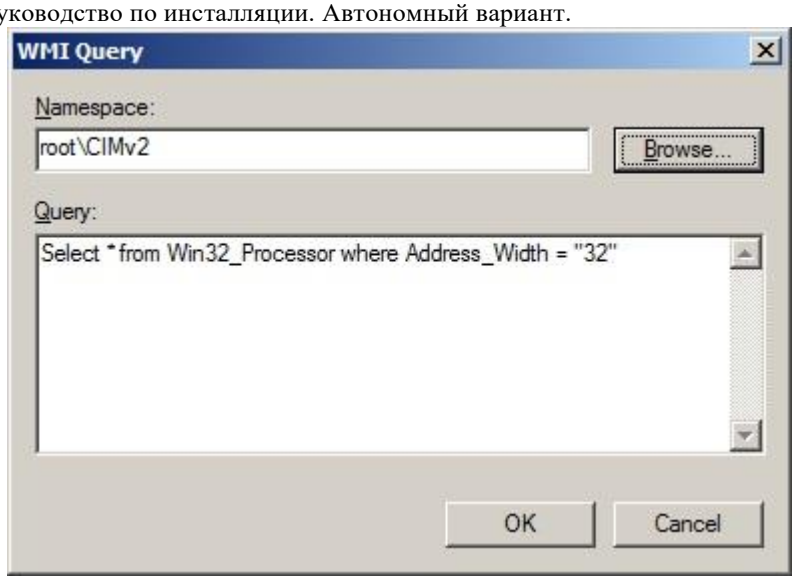


Рисунок 22. Окно создания запроса WMI-фильтра

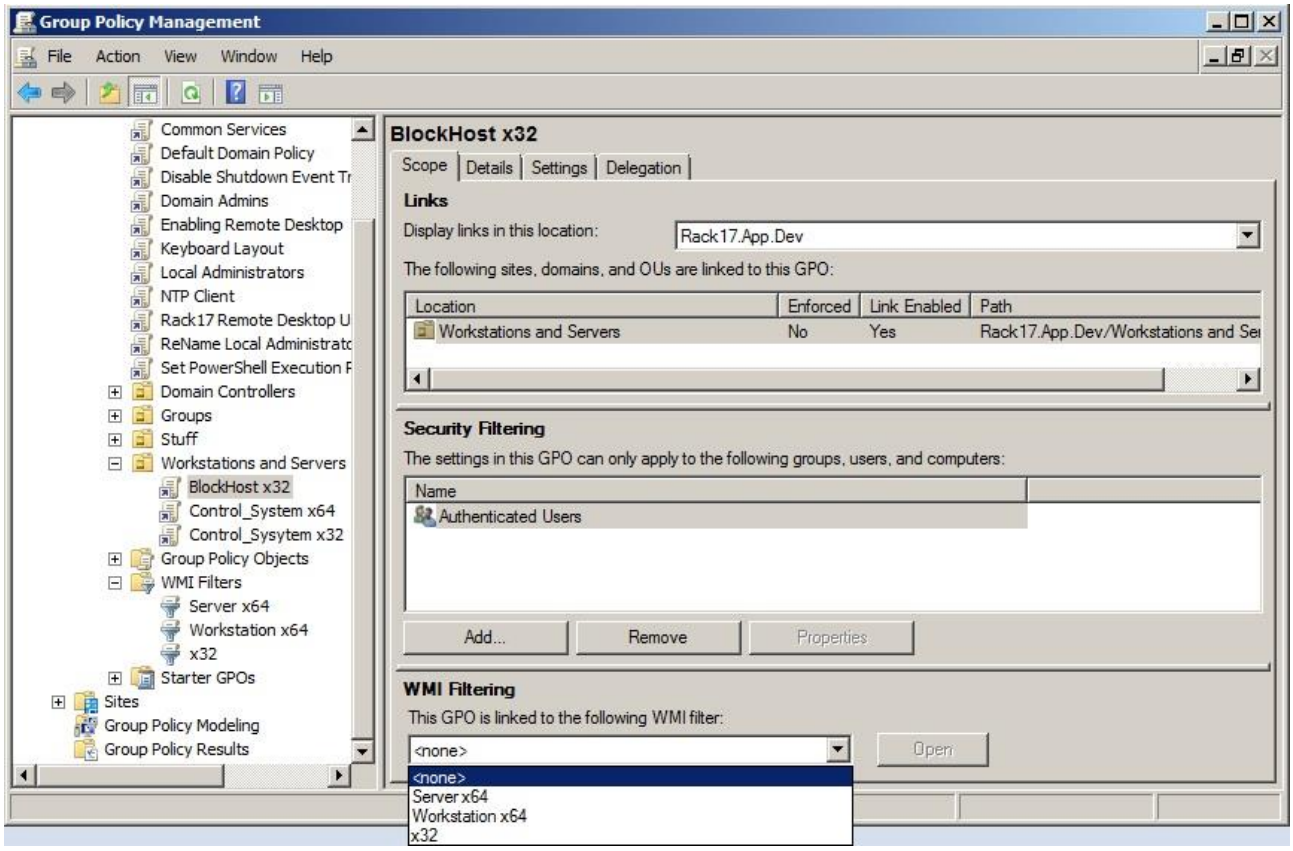


Рисунок 23. Привязка WMI-фильтра к объекту групповой политики

12. Закрыть консоль управления групповой политикой.

В дальнейшем, созданную групповую политику для установки клиента СЗИ «Блокхост-сеть 2.0» 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 клиентской части СЗИ с указанными в сценарии установки параметрами работы СЗИ.

В ходе установки на рабочей станции будет создан персональный идентификатор пользователя, хранящийся в реестре ОС Windows. PIN-код доступа к этому идентификатору задается в параметрах установки. В список пользователей СЗИ рабочей станции будут добавлены все учетные записи локальных пользователей ОС Windows, а также учетные записи пользователей домена, профили которых существуют на рабочей станции. Всем пользователям, включенным в список СЗИ рабочей станции, будет присвоен, созданный в ходе установки, персональный идентификатор, хранящийся в реестре ОС Windows.

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

2. Деинсталляция 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»:

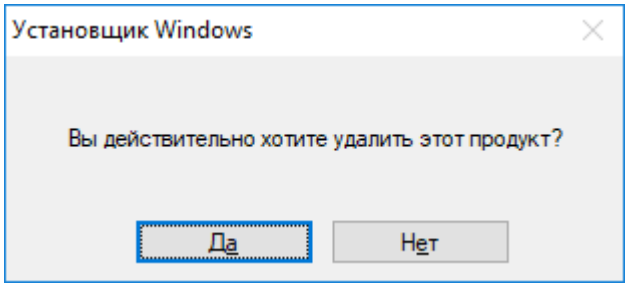


Рисунок 24. Окно запроса удаления СЗИ

После подтверждения операции удаления СЗИ запустится мастер удаления, который выполнит удаление СЗИ с рабочей станции.

Состояние процесса удаления СЗИ отображается в окне мастера удаления:

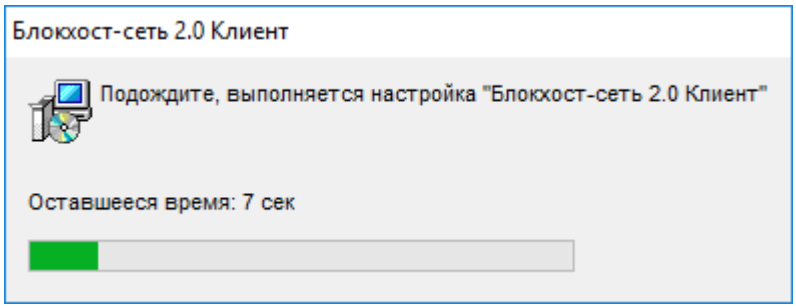


Рисунок 25. Ход удаления СЗИ «Блокхост-сеть 2.0»

Работа мастера удаления СЗИ «Блокхост-сеть 2.0» зависит от используемой операционной системы – в некоторых операционных системах в работе мастера удаления СЗИ могут присутствовать дополнительные шаги по выбору варианта удаления СЗИ (с остановкой служб, препятствующих корректному процессу удаления СЗИ, или без их остановки).

По окончании удаления СЗИ «Блокхост-сеть 2.0» откроется окно с предложением выполнить перезагрузку компьютера (рис. 26). Для завершения удаления СЗИ необходимо перезагрузить компьютер, сделать это можно сразу же после окончания работы мастера удаления СЗИ (нажата кнопку ***Да*** в окне, показанном на рис. 26), или выполнить это позже, перезагрузив компьютер вручную (нажата кнопка ***Нет*** в окне, показанном на рис. 26).

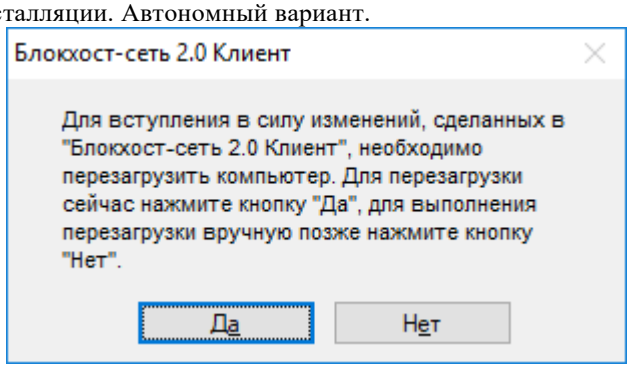


Рисунок 26. Окно завершения удаления СЗИ «Блокхост-сеть 2.0»

3. Обновление СЗИ

Обновление более ранних версий 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-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).

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 1.3 настоящего документа). Во время процесса обновления клиентской части СЗИ также потребуется ввести коды лицензии и ее активации.

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

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