ГАЗИНФОРМ СЕРВИС

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

Руководство по инсталляции. Вариант с удаленным управлением

Санкт-Петербург, 2019

Содержание

1 Установка СЗИ «Блокхост-Сеть 3»

1.1 Требования к аппаратной конфигурации

СЗИ «Блокхост-Сеть 3» (вариант с удаленным управлением) поставляется в виде файла Microsoft Windows Installer *BlockHost.Net 3 Server.exe* для установки серверной части СЗИ на 64-битные ОС Windows, а также в состав дистрибутива варианта с удаленным управлением СЗИ «Блокхост-Сеть 3» входит файл *BhNet.Installer.exe*, который содержит в себе дистрибутивы клиентской части СЗИ для ОС Windows 32- и 64-бит ОС.

Серверная часть СЗИ «Блокхост-Сеть 3» функционирует под управлением серверных ОС Windows, перечисленные в п. 1.2.1 настоящего руководства.

Клиентская часть СЗИ может быть установлена на ОС Windows, перечисленные в п. 1.2.1 настоящего руководства. Клиентская части СЗИ может быть установлена при помощи файла *BhNet.Installer.exe,* и в составе серверной части при помощи файла *BlockHost.Net 3 Server.exe*.

СЗИ «Блокхост-Сеть 3» (вариант с удаленным управлением) устанавливается на компьютеры с процессорами, имеющими архитектуру AMD64.

Для корректной работы СЗИ «Блокхост-Сеть 3» 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 (USB-ключ или смарт-карта), ruToken, JaCarta (USB-ключ и смарт-карта), Avest Token, ESMART Token (USB-ключ и смарт-карта) или USB-накопителя;
- 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 3» 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).
- Windows Server 2019 (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 7 Professional SP1 (32-разрядная/64-разрядная);
- Windows 7 Enterprise SP1 (32-разрядная/64-разрядная);
- Windows 7 Ultimate SP1 (32-разрядная/64-разрядная);
- Windows 8.1 Core (32-разрядная/64-разрядная);
- Windows 8.1 Professional (32-разрядная/64-разрядная);
- Windows 8.1 Enterprise (32-разрядная/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/64-разрядная);
- Windows 10 Pro (32-разрядная/64-разрядная);
- Windows 10 Enterprise (32-разрядная/64-разрядная);
- Windows Server 2016 Standard (64-разрядная);
- Windows Server 2016 Datacenter (64-разрядная);
- Windows Server 2016 Essentials (64-разрядная);
- Windows Server 2019 (64-разрядная).

В составе программного установленного обеспечения необходимы следующие компоненты:

- .NET Framework 4.5.2;
- распространяемый пакет Microsoft Visual C++ 2015 Redistributable или более поздней версии, содержащий компоненты Microsoft Visual C++ 2015;
- обновление системы безопасности KB3033929 (для ОС Windows Server 2008/2008R2).

При использовании персональных идентификаторов на ПК должно быть установлено следующее ПО:

- драйверы для устройств eToken и SafeNet eToken, ruToken, JaCarta, ESMART Token, AvBign.

При входе в ОС Windows с использованием цифровых сертификатов пользователей необходимо:

- установить СКЗИ «КриптоПро CSP» версии 3.6 и выше или СКЗИ «ViPNET CSP» версии 3.2;
- при использовании цифровых сертификатов, выработанных с помощью встроенных возможностей ОС, установка дополнительно ПО не требуется.

Для сетевого взаимодействия серверной и клиентских частей СЗИ на сервере безопасности должен быть открыт 999 TCP-порт.

СЗИ «Блокхост-Сеть 3» имеет следующие ограничения:

1) Установка СЗИ «Блокхост-Сеть 3» должна выполняться на диск C:\.
2) На жестком диске не должно быть других установленных операционных систем.
3) На компьютере не должно быть динамических дисков, работу с ними «Блокхост-Сеть 3» не поддерживает. Также не поддерживается гарантированное удаление на твердотельных магнитных накопителях (SSD-дисками).
4) Для устойчивой работы СЗИ и во избежание конфликта с другими программными средствами необходимо удалить ранее установленные и не устанавливать новые программы, следящие за работой файловой системы. К таким программным средствам относятся:

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

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 3» совместно с ОС семейства Windows допускается только в условиях выполненной активации операционной системы.

Для эксплуатации и эффективного применения СЗИ «Блокхост-Сеть 3» 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.

1.2.2 Особенности установки СЗИ «Блокхост-Сеть 3» на ПК под управлением ОС Windows 8.1/2012/2012R2

Перед началом установки СЗИ «Блокхост-Сеть 3» необходимо отключить встроенный в ОС Windows 8.1/2012/2012R2/10/2016/2019 стандартный защитник Windows (Windows Defender), для чего следует:

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

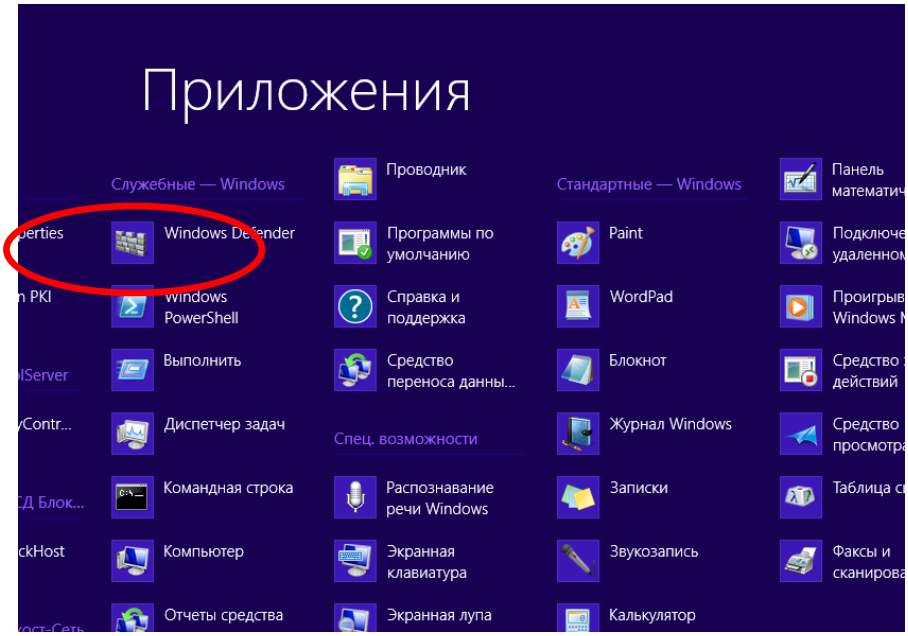


Рисунок 1 – Выбор пункта «Windows Defender»

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

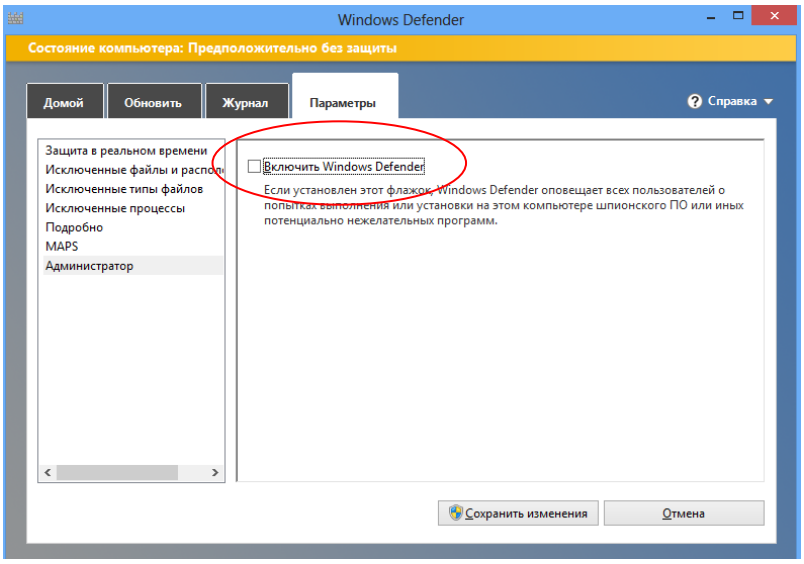


Рисунок 2 – Отключение «Windows Defender»

После завершения процесса установки СЗИ «Блокхост-Сеть 3» стандартный защитник Windows (Windows Defender) можно снова включить.

1.3 Порядок установки серверной части СЗИ «Блокхост-Сеть 3»

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 файла *BlockHost.Net 3 Server.exe* (для 64-bit ОС). Мастер установки серверной части СЗИ «Блокхост-Сеть 3» имеет оконный графический интерфейс.

ПЕРЕД ИНСТАЛЛЯЦИЕЙ СЗИ «БЛОКХОСТ-СЕТЬ 3» НЕОБХОДИМО УБЕДИТЬСЯ, ЧТО ДЛЯ ВСТРОЕННОЙ УЧЕТНОЙ ЗАПИСИ АДМИНИСТРАТОРА В ОС (ДОМЕНЕ) ЗАДАН ПАРОЛЬ!

Не рекомендуется устанавливать СЗИ «Блокхост-Сеть 3» на контроллер домена.

Для инсталляции серверной части СЗИ необходимо войти в операционную систему под учетной записью встроенного администратора ОС Windows (контроллера домена), либо под учетной записью, имеющей административные права. Запустить на выполнение файл-установщик СЗИ (*BlockHost.Net 3 Server.exe* – 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:

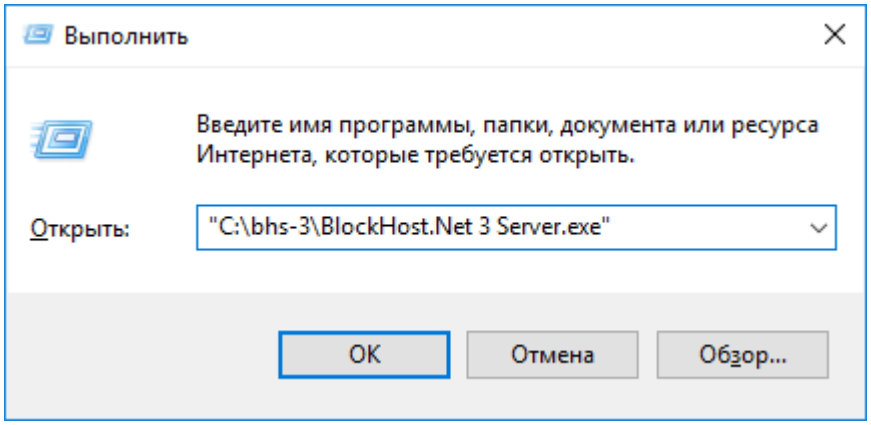


Рисунок 3 – Запуск файла-установщика

В результате запуска файла-установщика на экране монитора появится окно приветствия мастера установки серверной части СЗИ «Блокхост-Сеть 3» (рис. 4).

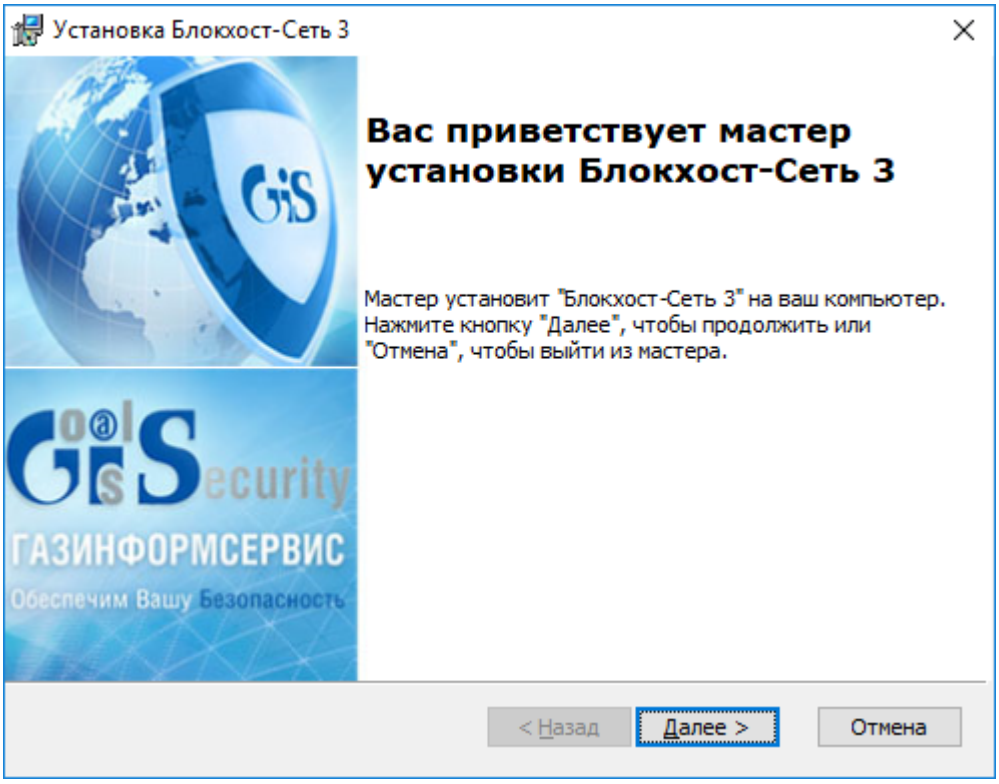


Рисунок 4 – Окно мастера установки сервера СЗИ «Блокхост-Сеть 3»

Перед установкой СЗИ «Блокхост-Сеть 3» необходимо убедиться в выполнении всех требований к установке, описанных в подразделе 1.2 «Требования к составу установленного программного обеспечения» настоящего документа.

В случае отсутствия на ПК распространяемого пакета Microsoft Visual C++ 2015 Redistributable или более поздней версии, содержащий компоненты Microsoft Visual C++ 2015, появится сообщение вида:

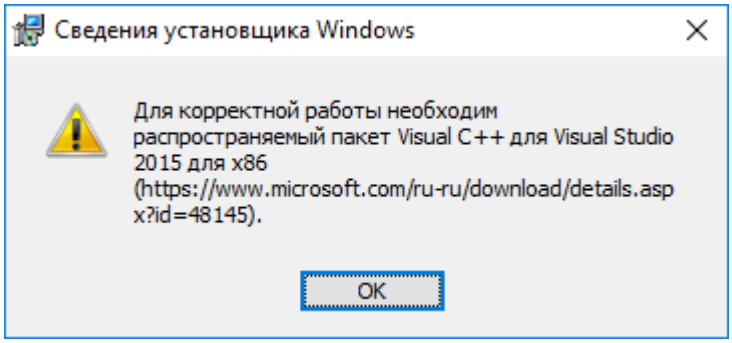


Рисунок 5 – Ошибка установки СЗИ «Блокхост-Сеть 3»

Установка СЗИ «Блокхост-Сеть 3» будет прервана (рис. 6). Для продолжения установки необходимо установить распространяемый пакет Microsoft Visual C++ 2015 Redistributable или более поздней версии, содержащий компоненты Microsoft Visual C++ 2015, и запустить на выполнение файл-установщик СЗИ повторно.

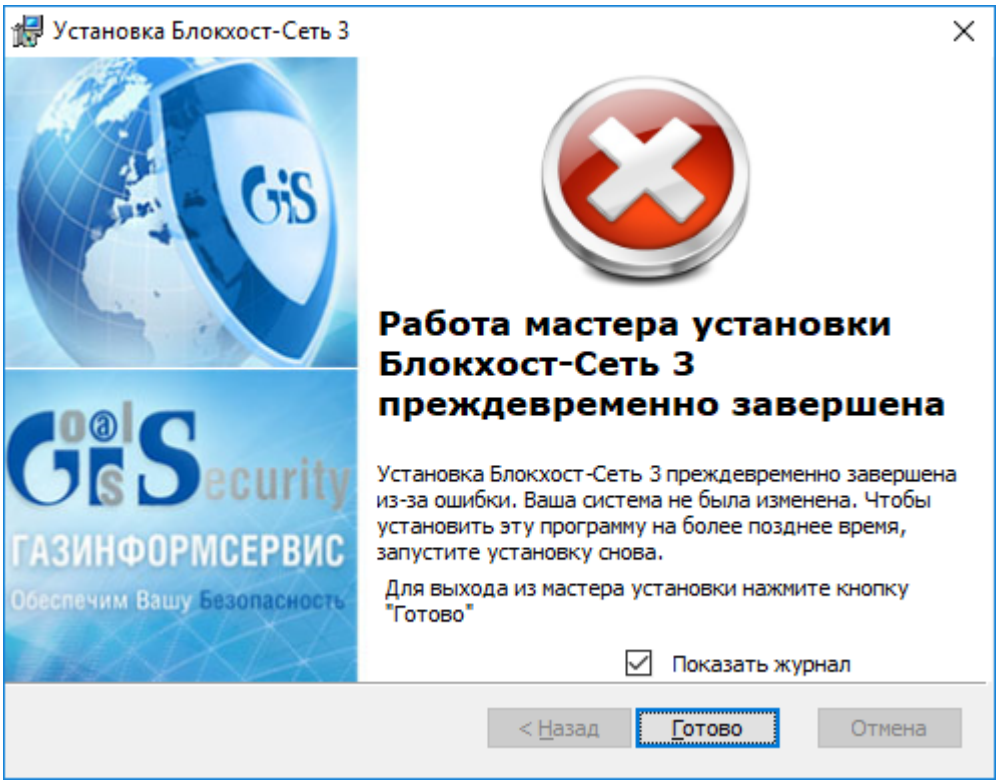


Рисунок 6 – Работа мастер установки преждевременно завершена

При установленном флаге «***Показать журнал***», после нажатия кнопки ***Готово*** откроется окно лога инсталлятора, содержащее ошибки, выявленные при установке СЗИ «Блокхост-Сеть 3».

На любом этапе работы мастера установки серверной части СЗИ можно нажать кнопку ***Отмена***. На экране появится окно, показанное на рисунке 7. При нажатии кнопки ***Да*** установка будет прервана. При нажатии кнопки ***Нет*** установка будет продолжена.

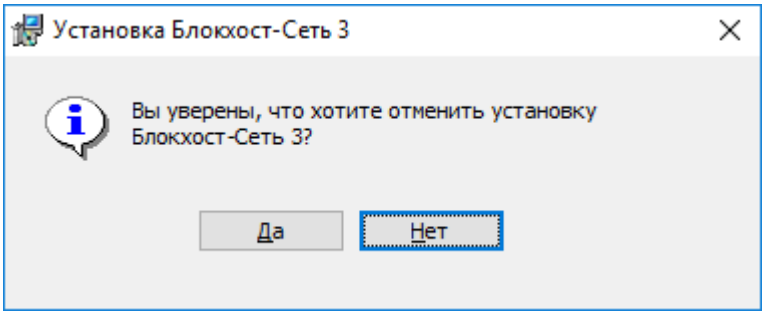


Рисунок 7 – Окно прекращения установки

После нажатия в окне приветствия мастера установки СЗИ кнопки ***Далее*** (см. рис. 4) на экране монитора появится окно с текстом условий лицензионного соглашения (рис. 8).

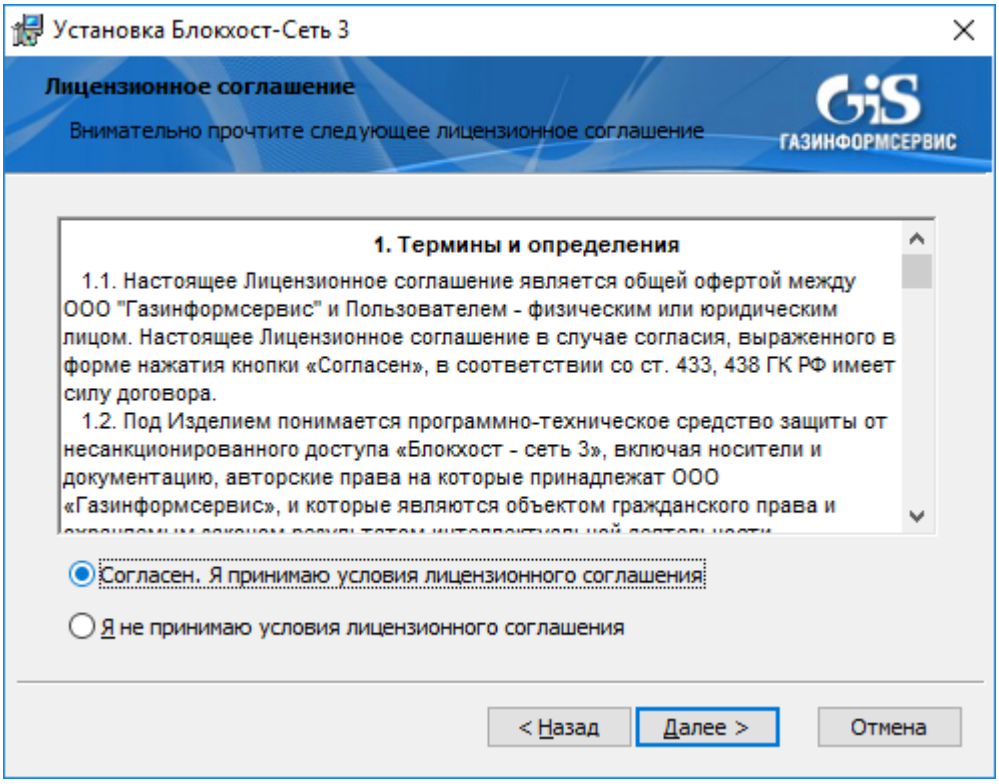


Рисунок 8 – Окно мастера установки СЗИ «Блокхост-Сеть 3» с лицензионным соглашением

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. 9), 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.

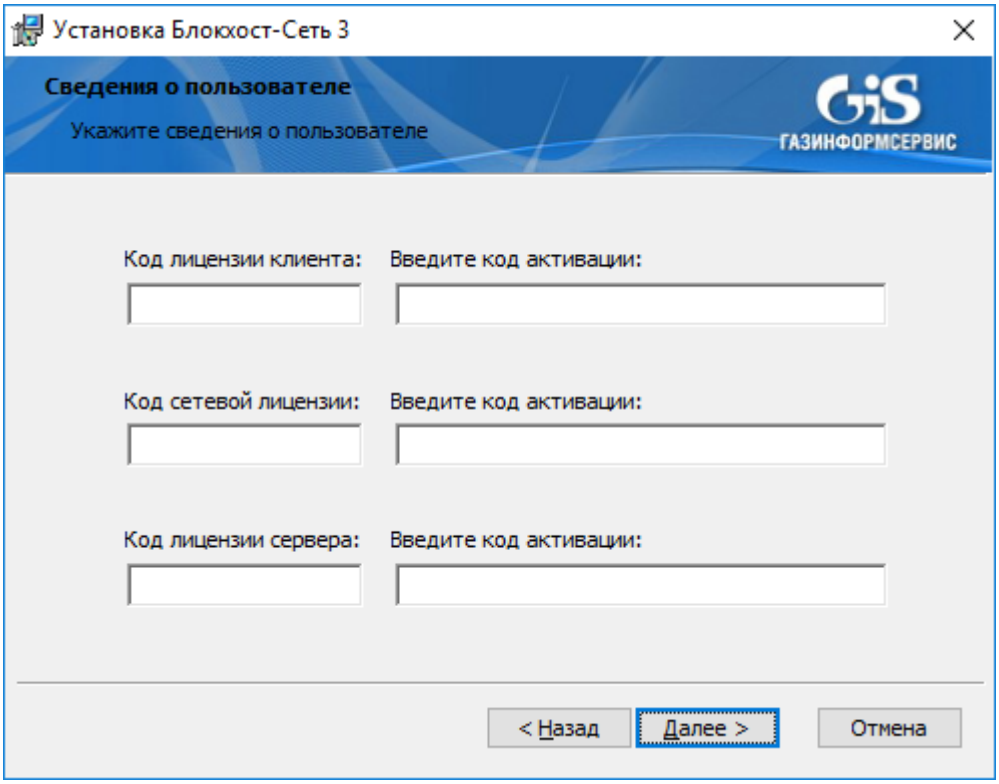


Рисунок 9 – Окно ввода кода лицензии и кода активации СЗИ «Блокхост-Сеть 3»

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. 10 показано окно с сообщением о неверном вводе кода активации лицензии клиентской части).

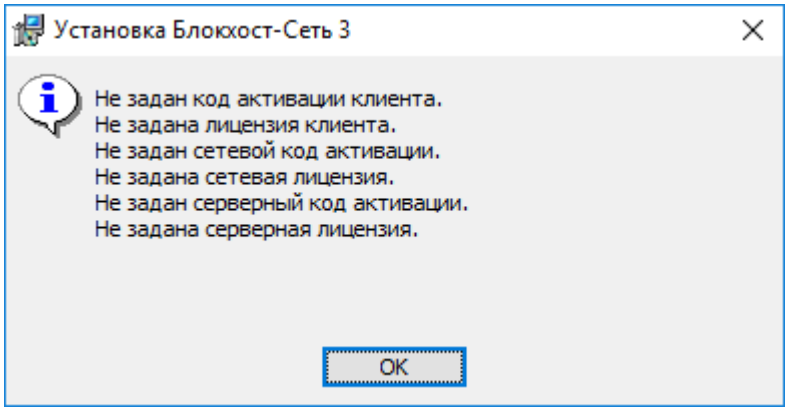


Рисунок 10 – Окно с сообщением о неверно введенном коде

Если код лицензии и код активации были введены верно, установка будет продолжена

и на экране появится окно формирования ключевого носителя администратора безопасности СЗИ (рис. 11).

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 8.1/2012/2012R2/10/2016, 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 3» (если USB-накопитель или дискета использовались ранее в качестве персонального идентификатора администратора в СЗИ «Блокхост-Сеть 3», 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 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 «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Руководство администратора безопасности»).

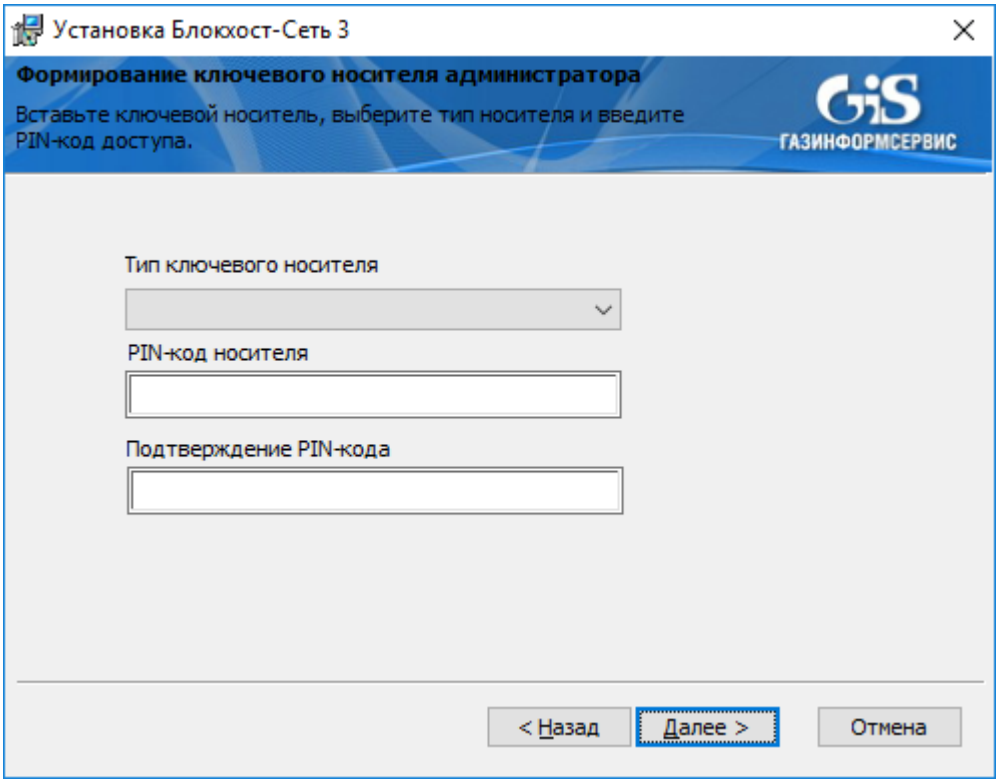


Рисунок 11 – Окно формирования ключевого носителя администратора

Если введен неверный PIN-код доступа к ключевому носителю, то на экране появится сообщение. После нажатия на кнопку ***OK*** происходит возврат в окно формирования ключевого носителя (рис. 11), в котором необходимо заново ввести PIN-код доступа к ключевому носителю.

Если операция проверки PIN-кода доступа к ключевому носителю прошла успешно, то появится следующее окно (рис. 12).

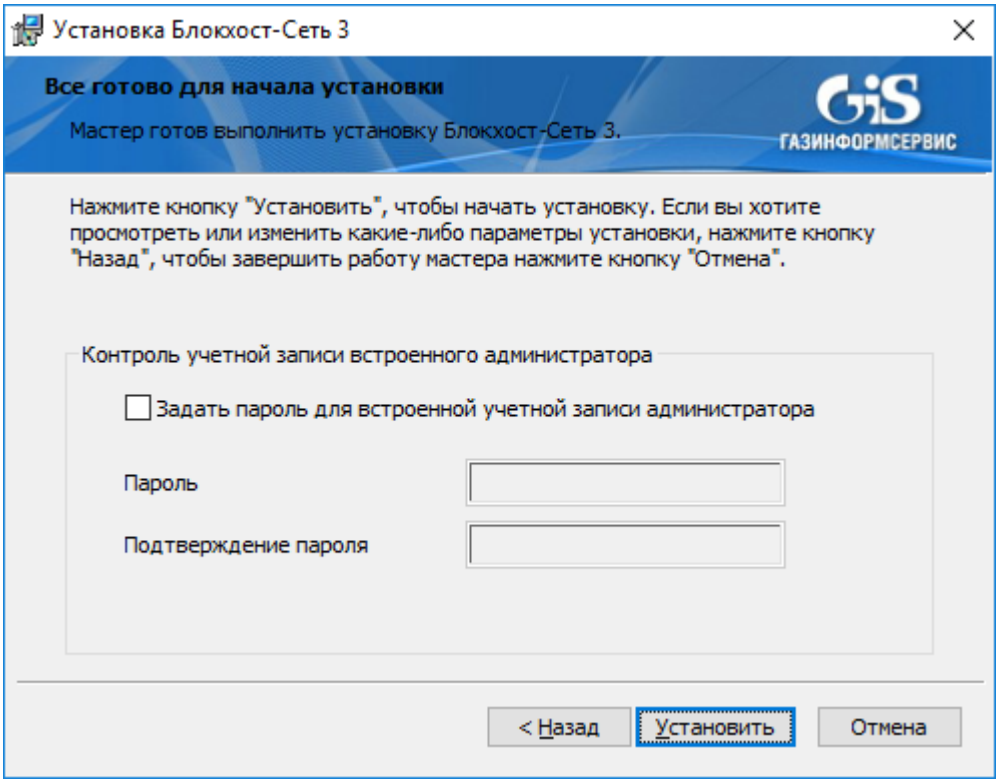


Рисунок 12 – Окно готовности к установке СЗИ «Блокхост-Сеть 3»

Данное окно отвечает за контроль встроенной учетной записью администратора. При установке параметра **Задать пароль для встроенной учетной записи администратора** необходимо в полях **Пароль** и **Подтверждение пароля** ввести пароль, который будет задан для встроенной учетной записи администратора (рис. 13).

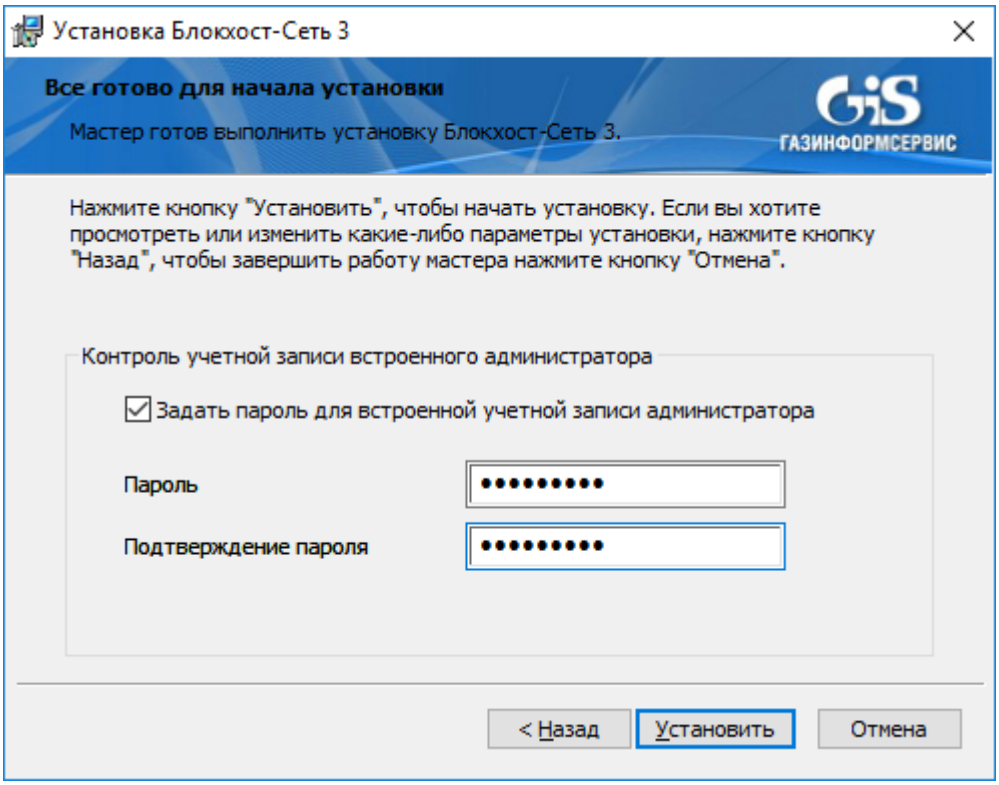


Рисунок 13 – Установка пароля встроенной учетной записи администратора

Далее нажать кнопку ***Установить***, после чего начнется процесс установки СЗИ «Блокхост-Сеть 3». Процесс установки показан на рисунке 14.

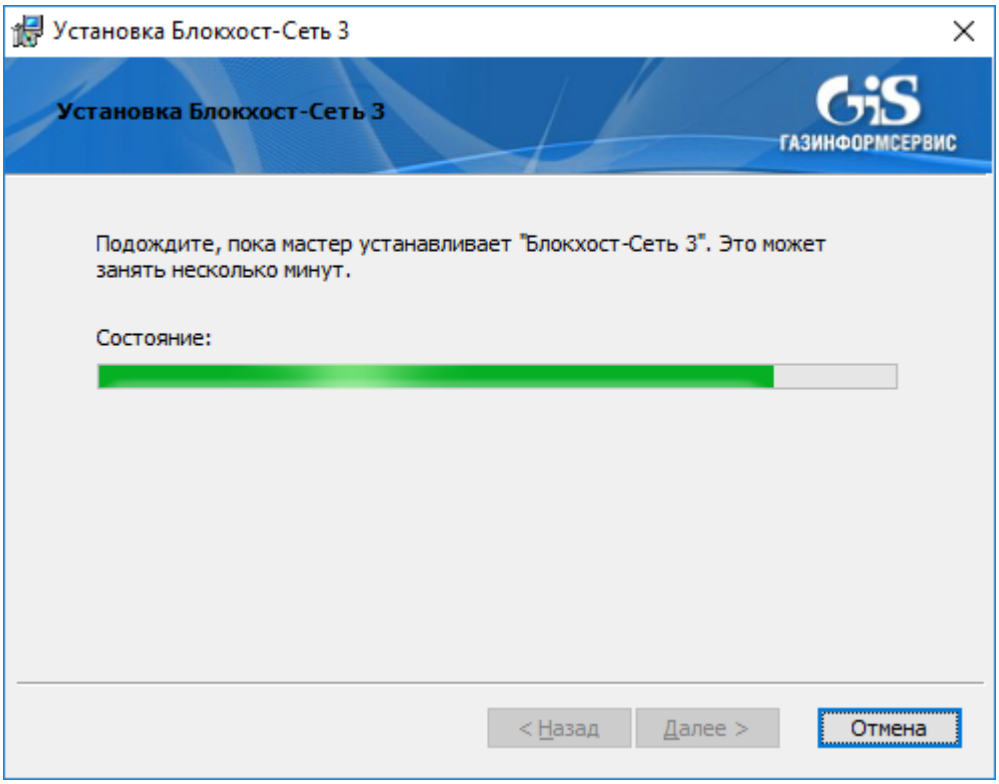


Рисунок 14 – Ход установки СЗИ «Блокхост-Сеть 3»

Если установка закончена успешно, то на экране появится окно окончания установки (рис. 15). Для окончания работы мастера установки СЗИ необходимо нажать кнопку ***Готово***.

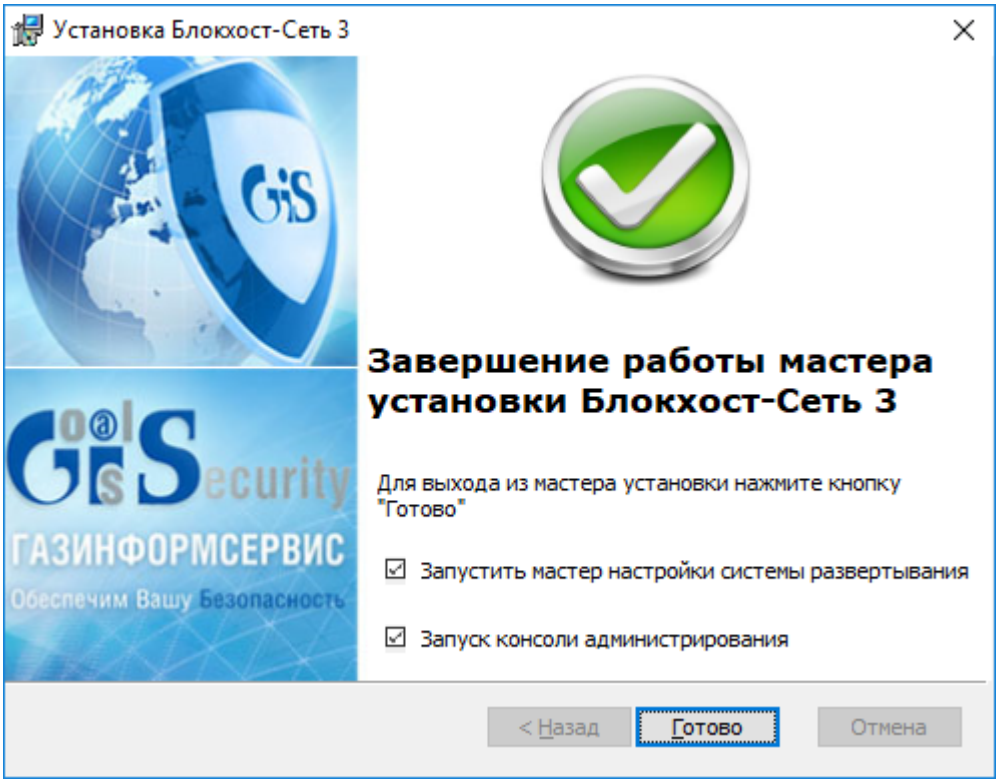


Рисунок 15 – Окно окончания установки серверной части СЗИ «Блокхост-Сеть 3»

В окне завершения работы мастера установки есть дополнительные параметры – ***Запустить мастер настройки системы развертывания*** и ***Запуск консоли администрирования*** (см. рис. 15). При необходимости настройки параметров системы развертывания СЗИ «Блокхост-Сеть 3» сразу после окончания установки серверной части СЗИ следует оставить отмеченным пункт ***Запустить мастер настройки системы развертывания*** – в результате, после закрытия окна работы мастера установки СЗИ (нажата кнопка ***Готово/Finish***), произойдет запуск мастера настройки системы развертывания СЗИ. Описание настройки параметров системы развертывания и аудита СЗИ «Блокхост-Сеть 3» приведено в п. 1.2 документа «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Система развертывания и аудита. Руководство администратора безопасности».

При необходимости работы в серверной консоли администрирования СЗИ «Блокхост-Сеть 3» 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 3». Руководство администратора безопасности».

1.4 Установка клиентской части СЗИ

Инсталляция клиентской части СЗИ на рабочую станцию может быть выполнена несколькими способами:

- администратором, с помощью консоли «Системы развертывания и аудита»;
- локально администратором рабочей станции с указанием параметров подключения к серверу СЗИ;
- локально администратором рабочей станции с использованием мастера установки клиентской части СЗИ;
- администратором сети – с использованием групповых политик.

Подробно установка СЗИ администратором СЗИ с помощью консоли «Системы развертывания и аудита» и с использованием групповых политик описана в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Система развертывания и аудита. Руководство администратора безопасности».

Клиентская часть СЗИ поставляется в виде файла *BhNet.Installer.exe*, который содержит в себе инсталляторы для 32- и 64-bit ОС.

Установка клиентской части СЗИ «Блокхост-Сеть 3» с использованием групповых политик осуществляется только после подготовки файла-установщика для развертывания средствами AD в консоли «Системы развертывания и аудита» (подробнее в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Система развертывания и аудита. Руководство администратора безопасности»).

Не рекомендуется устанавливать СЗИ «Блокхост-Сеть 3» на контроллер домена.

1.4.1 Локальная установка клиентской части СЗИ с указанием параметров подключения к серверу СЗИ

При локальной установке клиентской части СЗИ «Блокхост-Сеть 3» 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 удаленной установке клиентской части СЗИ при помощи специализированных программных продуктов (в том числе и через групповые политики).

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 (*BhNet.Installer.exe*) ввести необходимые коды и ключи лицензий (локальной и сетевой) и параметры подключения к серверу СЗИ. При локальной установке клиентской части СЗИ с использованием интерпретатора командной строки доступны параметры, описание которых приведено в таблице 1.

Таблица 1 – Параметры конфигурации клиента СЗИ, вводимые в командной строке

Наименование параметра	Назначение	Возможные значения
SERVER_ADDRESS	IP адрес и порт взаимодействия сервера СЗИ в формате IP-adress: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 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	Соответствует значению параметра PIN
LOC	Код локальной лицензии	По умолчанию не задан
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.
MACHINE_KEY	Пароль подключения клиента к серверу СЗИ	Значение устанавливается в серверной консоли администрирования СЗИ во вкладке **Параметры сервера**.
REBOOT	Параметр перезагрузки	*ReallySuppress* – перезагрузка подавляется (по умолчанию); *Force* – 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.
CONNECT	Параметр принудительного подключения клиента к серверу СЗИ, параметры которого указаны в поле ***Параметры*** (командной строке). Указывается для рабочих станций, которые уже подключены к какому-либо серверу СЗИ, при их переподключении к новому серверу СЗИ.	*CONNECT=1*.

Наименование параметра	Назначение	Возможные значения
/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*.

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 MACHINE_KEY=12345 CONNECT=1

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. 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 «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Руководство администратора безопасности».

1.4.2 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 (*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 3» (рис. 16).

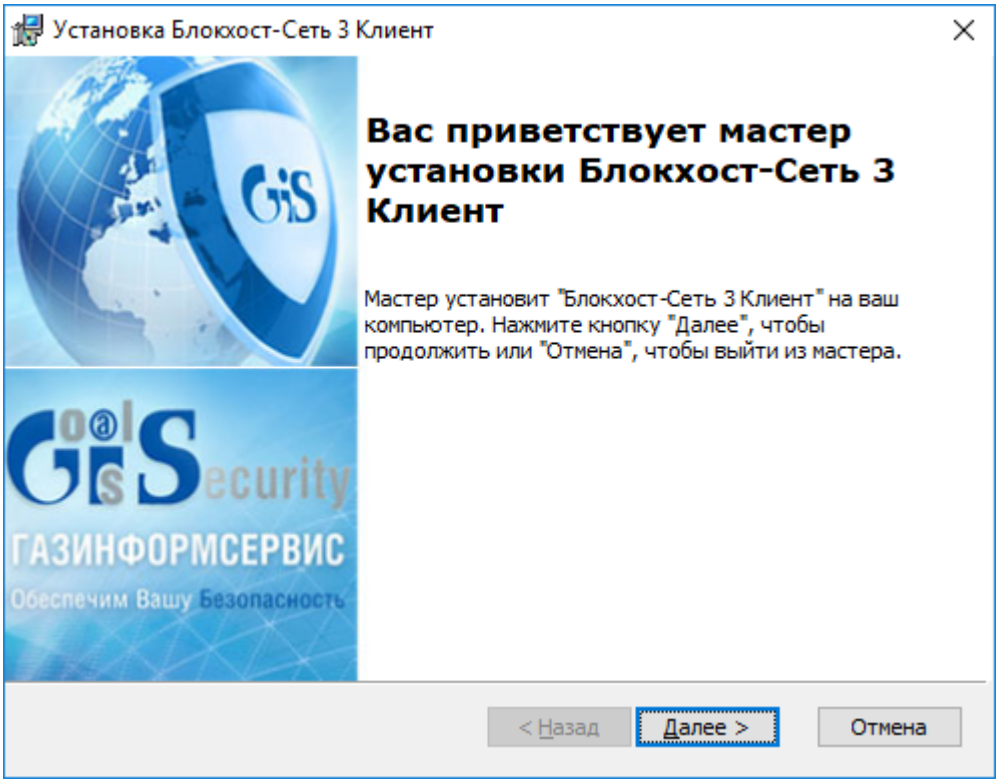


Рисунок 16 – Окно установки сервера СЗИ «Блокхост-Сеть 3»

Перед установкой клиентской части СЗИ «Блокхост-Сеть 3» необходимо убедиться в выполнении всех требований к установке, описанных в подразделе 1.2 «Требования к составу установленного программного обеспечения» настоящего документа.

В случае отсутствия на ПК распространяемого пакета Microsoft Visual C++ 2015 Redistributable или более поздней версии, содержащий компоненты Microsoft Visual C++ 2015, появится сообщение вида, представленного на рисунке 5.

Установка клиентской части СЗИ «Блокхост-Сеть 3» будет прервана (рис. 17). Для продолжения установки необходимо установить распространяемый пакет Microsoft Visual C++ 2015 Redistributable или более поздней версии, содержащий компоненты Microsoft Visual C++ 2015, и запустить на выполнение файл-установщик СЗИ повторно.

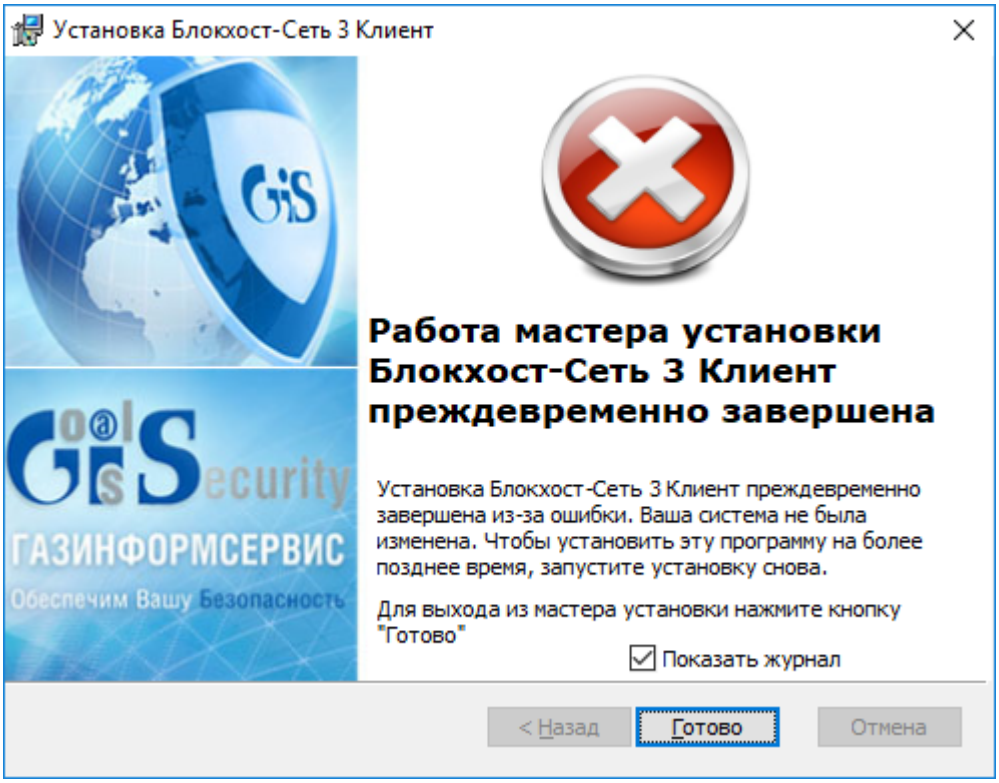


Рисунок 17 – Работа мастера установки преждевременно завершена

При установленном флаге «***Показать журнал***», после нажатия кнопки ***Готово*** откроется окно лога инсталлятора, содержащее ошибки, выявленные при установке СЗИ «Блокхост-Сеть 3».

На любом этапе работы мастера установки СЗИ можно нажать кнопку ***Отмена***. На экране появится окно, показанное на рисунке 18. При нажатии кнопки ***Да*** установка будет прервана. При нажатии кнопки ***Нет*** установка будет продолжена.

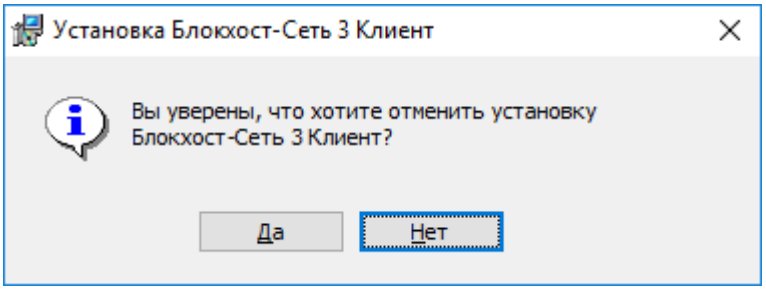


Рисунок 18 – Окно прекращения установки

После нажатия в окне приветствия мастера установки СЗИ кнопки ***Далее*** (рис. 16) на экране монитора появится окно с текстом условий лицензионного соглашения (рис. 19).

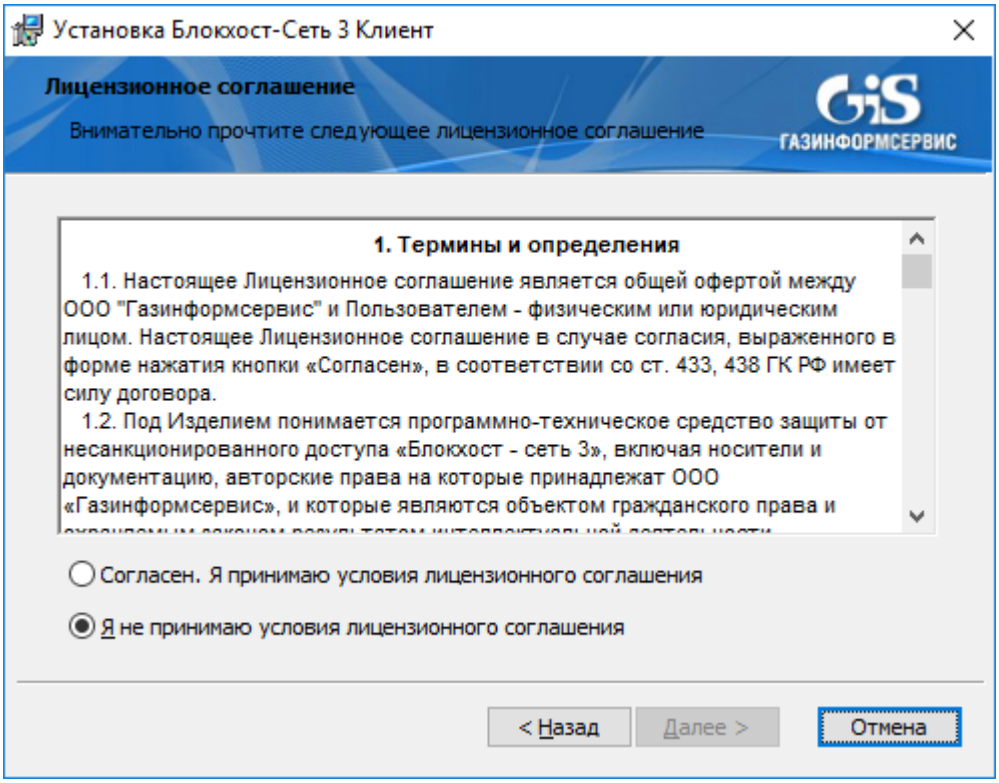
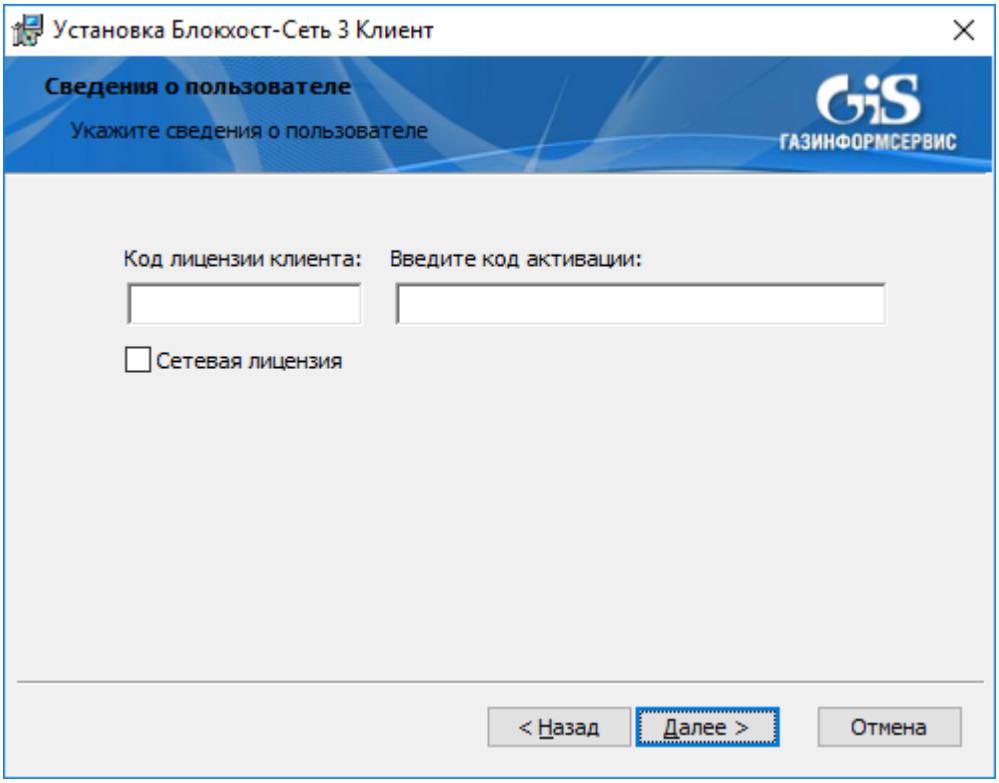


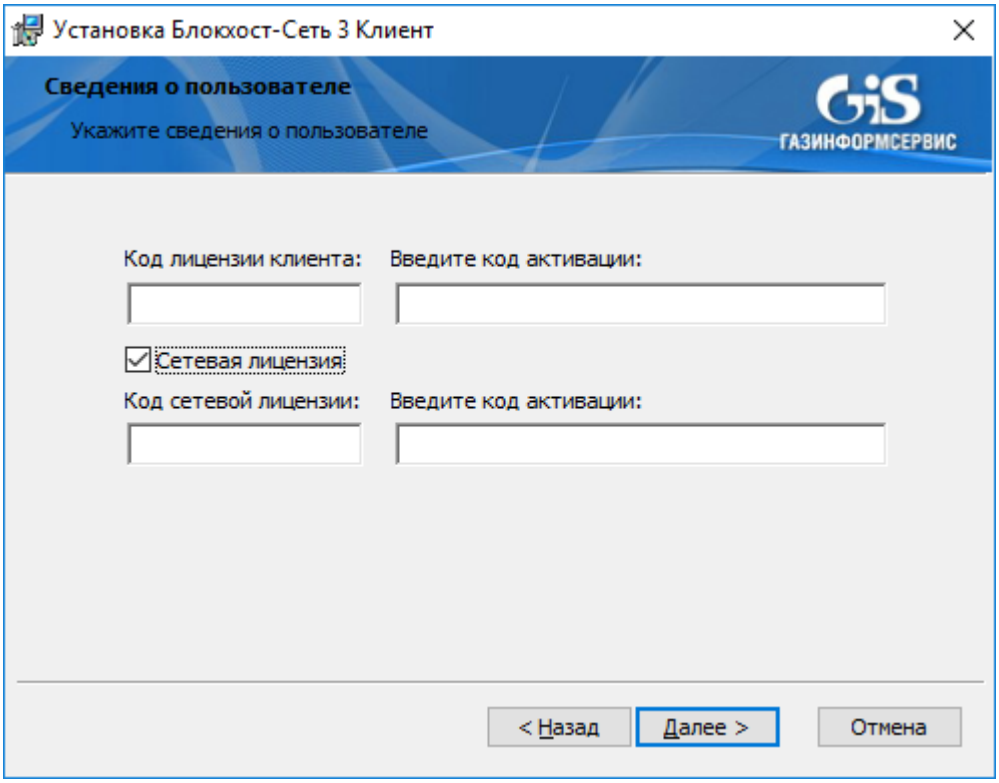
Рисунок 19 – Окно мастера установки СЗИ «Блокхост-Сеть 3» с лицензионным соглашением

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. 20, а), в котором необходимо установить флажок в поле ***Сетевая лицензия*** и ввести в соответствующие поля (рис. 20, б) коды сетевой лицензии и лицензии клиента и коды их активации, которые прописаны в выданной лицензии.



а)



б)

Рисунок 20 – Окно ввода кода лицензии и кода активации СЗИ «Блокхост-Сеть 3»

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. 21 показано окно с сообщением о неверном вводе кода активации сетевой лицензии клиентской части СЗИ).

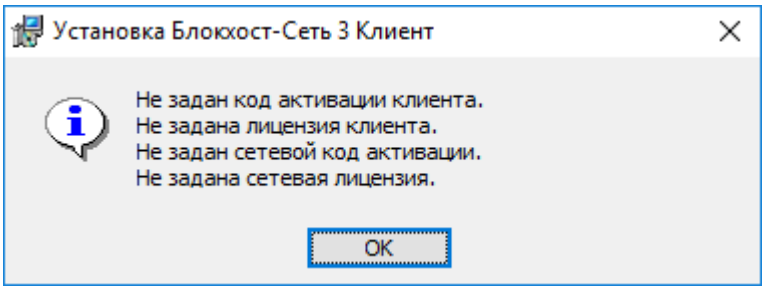


Рисунок 21 – Окно с сообщением о неверно введенном коде

Если коды лицензии и коды активации были введены верно, установка будет продолжена и на экране появится окно формирования ключевого носителя администратора безопасности (рис. 22). 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 3» (если USB-накопитель или дискета использовались ранее в качестве персонального идентификатора администратора в СЗИ «Блокхост-Сеть 3», 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 реестре 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.

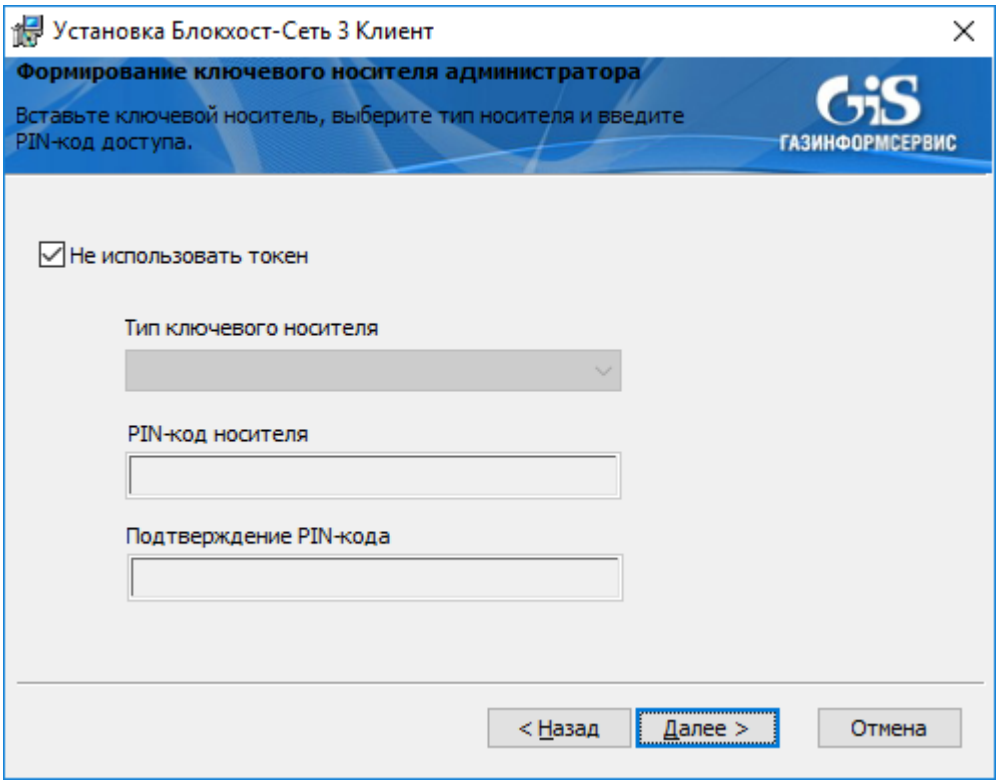


Рисунок. 22 – Окно формирования ключевого носителя администратора

Для продолжения установки нажмите кнопку ***Далее***.

Если введен неверный PIN-код доступа к ключевому носителю, то на экране появится сообщение. После нажатия на кнопку ***ОК*** происходит возврат в окно формирования ключевого носителя (см. рис. 22), в котором необходимо заново ввести PIN-код доступа к ключевому носителю.

Если операция проверки PIN-кода доступа к ключевому носителю прошла успешно, то появится следующее окно (рис. 23).

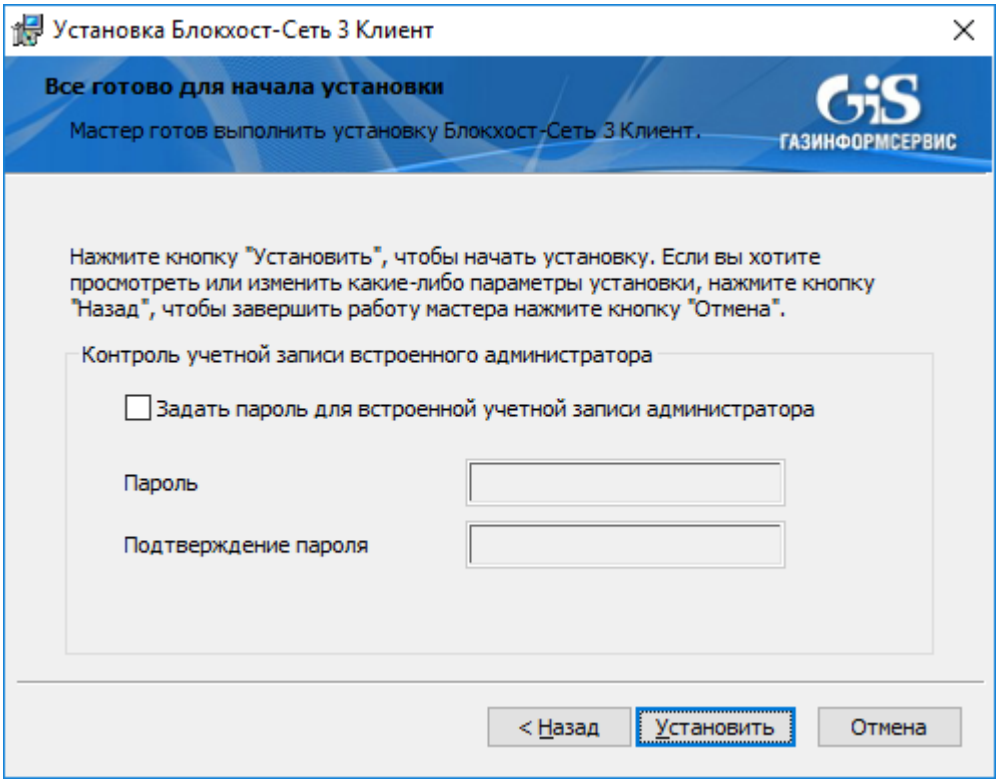


Рисунок 23 – Окно готовности к установке СЗИ «Блокхост-Сеть 3»

Данное окно отвечает за контроль встроенной учетной записью администратора. При установке параметра **Задать пароль для встроенной учетной записи администратора** необходимо в полях **Пароль** и **Подтверждение пароля** ввести пароль, который будет задан для встроенной учетной записи администратора.

Далее нажать кнопку ***Установить***, после чего начнется процесс установки СЗИ «Блокхост-Сеть 3» (рис. 24).

Ход установки будет отображаться в окне мастера установки (рис.24), программный продукт будет установлен на локальный компьютер в папку *C:\BlockHost*.

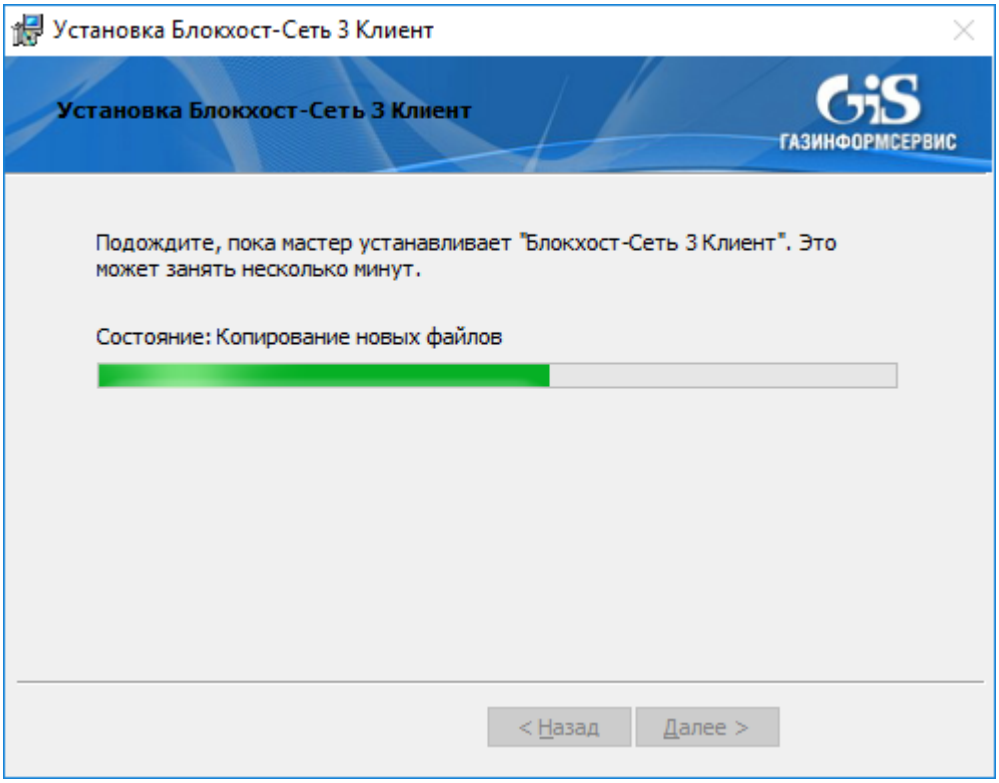


Рисунок 24 – Ход установки СЗИ «Блокхост-Сеть 3»

Если установка закончена успешно, то на экране появится окно окончания установки (рис. 25). Для окончания работы мастера установки СЗИ необходимо нажать кнопку ***Готово***.

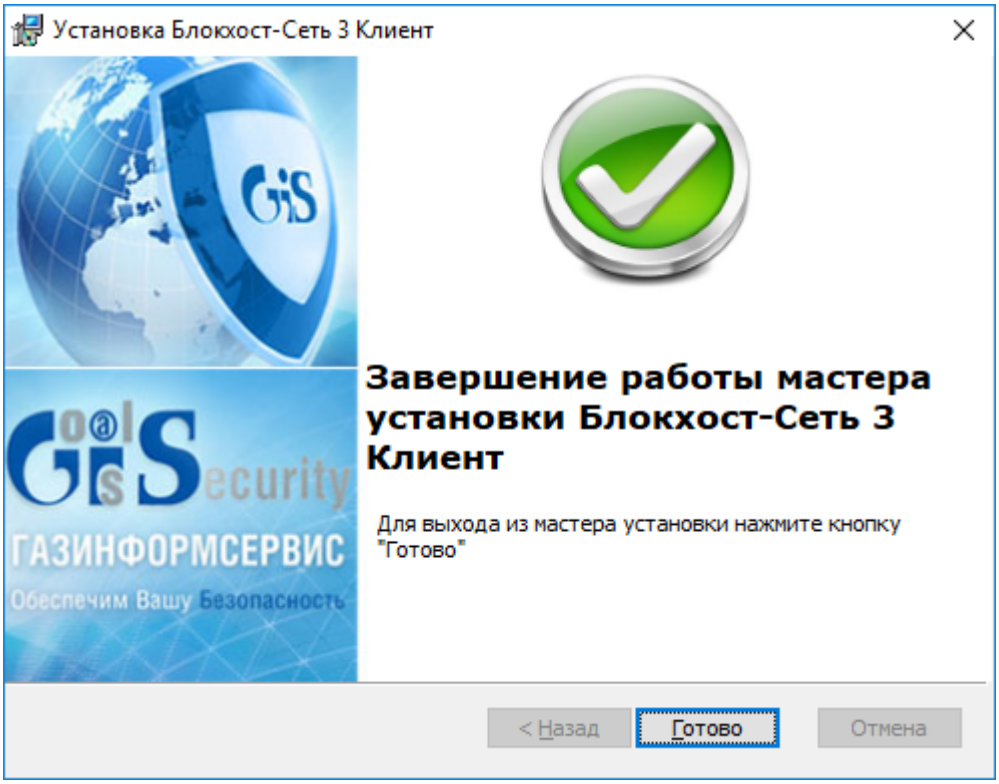


Рисунок 25 – Окно окончания установки СЗИ «Блокхост-Сеть 3»

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

2 Деинсталляция СЗИ «Блокхост-Сеть 3»

2.1 Деинсталляция сервера СЗИ «Блокхост-Сеть 3»

Удаление сервера СЗИ «Блокхост-Сеть 3» может произвести только пользователь, вошедший в систему под встроенной учетной записью администратора ОС Windows или под учетной записью, имеющей административные права. 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 3*** (***BlockHost-Net 3***) и нажать кнопку ***Удалить***. Также для удаления программы можно воспользоваться пунктом главного меню ***Удалить Блокхост-Сеть 3***, расположенном в группе программ ***Пуск→ Все программы→ Блокхост-Сеть 3***. В результате откроется окно установщика Windows, в котором необходимо подтвердить операцию удаления СЗИ «Блокхост-Сеть 3»:

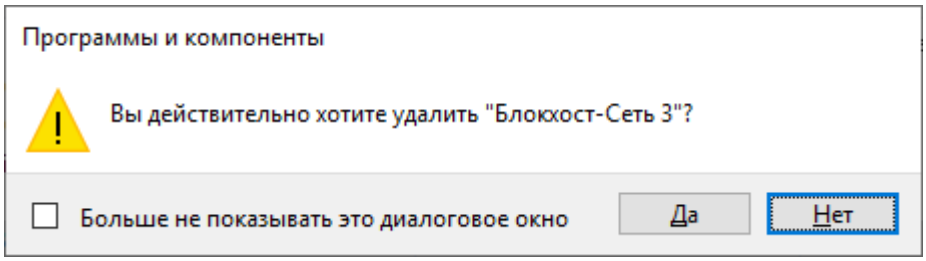


Рисунок 26 – Окно запроса удаления СЗИ

После подтверждения операции удаления СЗИ запустится мастер удаления, который выполнит удаление СЗИ с компьютера. Если мастеру удаления СЗИ не удалось остановить работающие службы, откроется окно с сообщением об ошибке остановки этих приложений. После нажатия кнопки ***ОК*** начнется процесс удаления СЗИ.

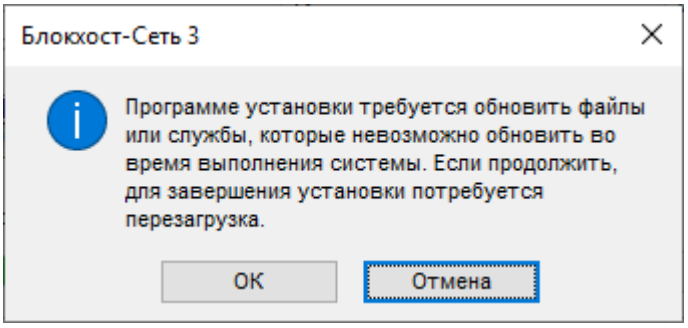


Рисунок 27 – Предупреждение об ошибке остановки работающих служб СЗИ

Если в окнах мастера удаления СЗИ нажать кнопку ***Отмена*** (***Нет***) – процесс удаления будет прекращен, система останется без изменений.

Состояние процесса удаления СЗИ отображается в окне мастера удаления. Работа мастера удаления СЗИ «Блокхост-Сеть 3» 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 сервера СЗИ «Блокхост-Сеть 3» откроется окно с предложением выполнить перезагрузку компьютера (рис. 30). 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. 30), или выполнить это позже, перезагрузив компьютер вручную (нажата кнопка ***Нет*** в окне, показанном на рис. 30).

2.2 Деинсталляция клиентской части СЗИ «Блокхост-Сеть 3»

Удаление клиентской части СЗИ «Блокхост-Сеть 3» может произвести только пользователь, вошедший в систему под встроенной учетной записью администратора ОС Windows локальной рабочей станции или контроллера домена или под учетной записью, имеющей административные права. 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 3 Клиент*** (***BlockHost-Net 3 Client***) и нажать кнопку ***Удалить***. Также для удаления программы можно воспользоваться пунктом главного меню ***Удалить Блокхост-Сеть 3 Клиент*** (***Uninstall BlockHost-Net 3 Client***), расположенном в группе программ ***Пуск→ Все программы→ Блокхост-Сеть 3 Клиент*** (***Start→ All Programs→ BlockHost-Net 3 Client***). В результате откроется окно установщика Windows, в котором необходимо подтвердить операцию удаления СЗИ «Блокхост-Сеть 3»:

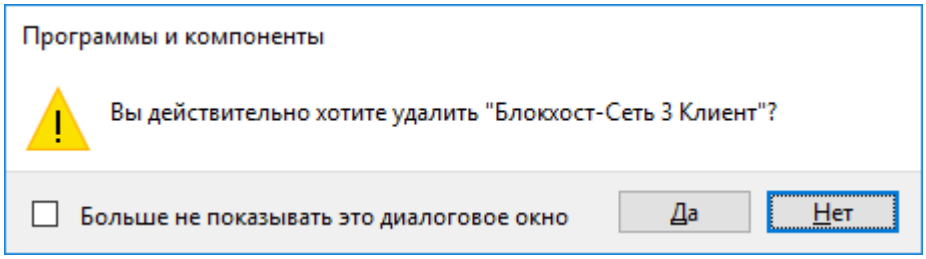


Рисунок 28 – Окно запроса удаления СЗИ

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

Состояние процесса удаления СЗИ отображается в окне мастера удаления:

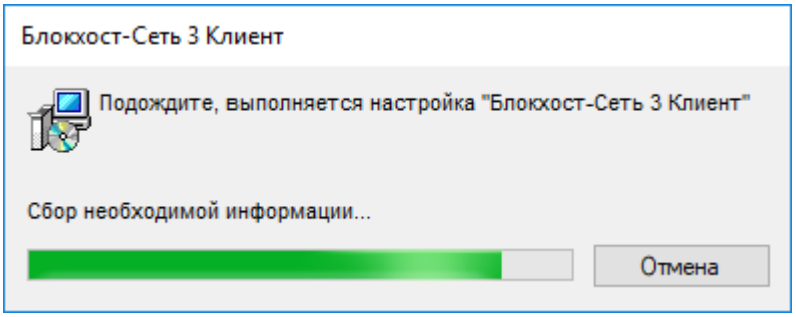


Рисунок 29 – Ход удаления СЗИ «Блокхост-Сеть 3»

Работа мастера удаления СЗИ «Блокхост-Сеть 3» 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 3» откроется окно с предложением выполнить перезагрузку компьютера (рис. 30). 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. 30), или выполнить это позже, перезагрузив компьютер вручную (нажата кнопка ***Нет*** в окне, показанном на рис. 30).

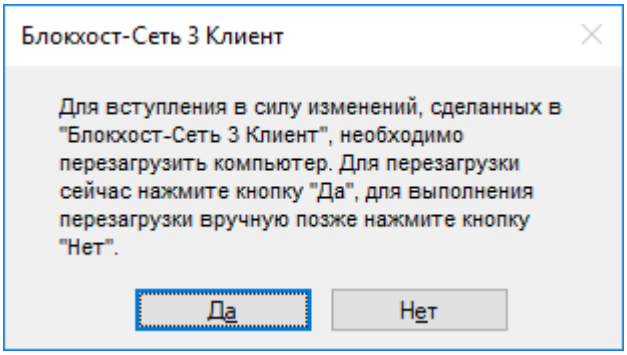


Рисунок 30 – Окно завершения удаления СЗИ «Блокхост-Сеть 3»

3 Обновление СЗИ «Блокхост-Сеть 3»

3.1 Обновление серверной части СЗИ

Обновление более ранних версий серверной части СЗИ до сертифицированной версии СЗИ «Блокхост-Сеть 3» производится установкой новой версии СЗИ «Блокхост-Сеть 3» поверх уже установленной с помощью файла-установщика *BlockHost.Net 3 Server.exe (*под управлением 32-bit и 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 3 Server.exe* 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 3» производится установкой новой версии СЗИ «Блокхост-Сеть 3» поверх уже установленной:

- BlockHost-Net-3-Client x32.msi / BlockHost-Net-3-Client x64.msi (для клиентской части СЗИ под управлением 32-bit/64-bit ОС);
- BhNet.Installer.exe (для клиентской части СЗИ под управлением 32- и 64-bit ОС).

Обновление клиентской части с использованием групповых политик осуществляется только после подготовки файла-установщика для развертывания средствами AD в консоли «Системы развертывания и аудита» (подробнее в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 3». Система развертывания и аудита. Руководство администратора безопасности»).

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 *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 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. 30). Для завершения обновления клиентской части СЗИ необходимо перезагрузить компьютер, сделать это можно сразу же после окончания работы мастера обновления СЗИ (нажата кнопку ***Да*** в окне, показанном на рис. 30), или выполнить это позже, перезагрузив компьютер вручную (нажата кнопка ***Нет*** в окне, показанном на рис. 30).

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.