ГАЗИНФОРМ СЕРВИС

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

Руководство по инсталляции в ОС Windows

Санкт-Петербург, 2024

Содержание

Введение

В настоящем руководстве приведены сведения по установке средства защиты информации от несанкционированного доступа «Блокхост-Сеть 4» (в дальнейшем – СЗИ от НСД «Блокхост-Сеть 4», СЗИ или средство).

Настоящее руководство предназначено для администратора безопасности (АБ), отвечающего за установку программного обеспечения на рабочих местах пользователей, настройку параметров изделия и управление учетными записями пользователей.

Перед началом эксплуатации изделия необходимо внимательно ознакомиться с данным руководством и документами:

– «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Формуляр»;

– «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Описание применения»;

– «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора. Часть 1. Управление политиками»;

– «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора. Часть 2. Развертывание и аудит»;

– «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора. Часть 3. Настройка подсистемы управления токенами, ЦС Microsoft CA»;

– «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора. Часть 4. Настройка подсистемы управления токенами, ЦС DogTag»;

– «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора. Часть 5. Управление токенами»;

– «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора. Часть 6. Подсистема ГУПТ»;

– «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора. Часть 7. Консоль управления клиентом в ОС Linux».

Степени важности примечаний:

Важная информация

Указания, требующие особого внимания.

Дополнительная информация

Указания, позволяющие упростить работу с подсистемой.

1 Условия применения

СЗИ от НСД «Блокхост-Сеть 4» устанавливается на ПК с процессорами, имеющими архитектуру x86 и AMD64. Поддерживаемые ОС MS Windows/Linux, под управлением которых функционирует СЗИ, приведены в таблице 1.1.

Таблица 1.1 – Перечень поддерживаемых операционных систем

ОС
MS Windows
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)
Windows Server 2022 Standard (64-разрядная)
Windows Server 2022 Essentials (64-разрядная)
Windows Server 2022 Datacenter (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 10 Home (32-разрядная/64-разрядная)
Windows 10 Pro (32-разрядная/64-разрядная)
Windows 10 Enterprise (32-разрядная/64-разрядная)
Windows 11 Home (64-разрядная)
Windows 11 Professional (64-разрядная)
Linux
AstraLinux SE (Смоленск)
Альт 8 СП
РЕД ОС 7.3 Муром

1.1 Требования к аппаратному и программному обеспечению

Программные и аппаратные требования к средствам вычислительной техники, на которых функционирует клиентская и серверная часть СЗИ приведены в таблице 1.2.

Таблица 1.2 – Программные и аппаратные требования к средствам вычислительной техники, на которых функционирует клиентская и серверная часть СЗИ

Требования	Наименование	Примечание
Требования к производительности	Обусловлены требованиями используемых ОС	см. таблицу 1.1
Аппаратные требования	**Использование персональных идентификаторов**	
	USB-порт	
Дополнительное программное обеспечение	**Обновления**	
	KB3033929, KB4474419, KB4490628	для ОС Windows 7 и Windows Server 2008/2008R2
	KB2921916	в ОС Windows 7 и Windows Server 2008/2008R2 для механизма «Контроль печати»
	Реализация аутентификации с использованием ГОСТ сертификатов – КриптоПро [1]	
	СКЗИ «КриптоПро CSP»	версии 3.6 и выше
	Драйверы токенов	
	Драйверы устройств производителей	
	Программная платформа	
	NET Framework 4.5.2	При использовании подсистемы ГУПТ
	распространяемый пакет Microsoft Visual C++ 2015-2019 Redistributable	
	обновление «Remote Server Administration Tools»: • для ОС Windows 7 "Remote Server Administration Tools for Windows 7" (https://www.microsoft.com/en-us/download/details.aspx?id=7887); • для ОС Windows 8.1 "Remote Server Administration Tools for Windows 8.1" (https://www.microsoft.com/en-us/download/details.aspx?id=28972); • для ОС Windows 10 до версии 1903 "Remote Server Administration Tools for Windows 10" (https://www.microsoft.com/en-us/download/details.aspx?id=45520).	При использовании подсистемы управления токенами на клиентских ОС
	СУБД «PostgreSQL»	

[1] При использовании цифровых сертификатов, выработанных с помощью встроенных возможностей ОС, установка дополнительно ПО не требуется.

Требования	Наименование	Примечание
Системы управления базами данных (СУБД)	СУБД «Jatoba»	Сертификат соответствия ФСТЭК России № 4327 от 19.11.2020

Ограничения при эксплуатации СЗИ от НСД «Блокхост-Сеть 4» описаны в документе «СЗИ от НСД «Блокхост-Сеть 4». Описание применения».

2 Подготовка к установке СЗИ от НСД «Блокхост-Сеть 4»

СЗИ от НСД «Блокхост-Сеть 4» поставляется заказчику на компакт-диске согласно комплектности, указанной в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Формуляр».

Перед эксплуатацией СЗИ от НСД «Блокхост-Сеть 4» необходимо ознакомиться с сопроводительными документами.

Для обеспечения защиты ПО от угроз безопасности информации, связанных с нарушением целостности в процессе передачи его пользователю необходимо обеспечить контроль соответствия экземпляра ПО, переданного разработчиком и экземпляра ПО, полученного пользователем.

Контроль соответствия на месте эксплуатации ПО осуществляется путем сверки контрольных сумм дистрибутива со значениями, указанными в сопроводительной документации на данное ПО.

Уполномоченному пользователю необходимо рассчитать контрольные суммы дистрибутива, сверится с данными Приложения 1 документа «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Формуляр» и указать ответственного за эксплуатацию СЗИ от НСД «Блокхост-Сеть 4» в таблице 12.

Установка изделия должна осуществляться под руководством специально подготовленного персонала.

При установке изделия на ЭВМ рекомендуется консультироваться с технической поддержкой ООО «Газинформсервис». Контакты технической поддержки указаны в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Формуляр».

2.1 Порты по умолчанию, используемые компонентами СЗИ

Информация о портах, используемых по умолчанию компонентами СЗИ от НСД «Блокхост-Сеть 4», и возможность их настройки, приведены в таблице 2.1.

Таблица 2.1 – Порты по умолчанию, используемые компонентами СЗИ

Компонент системы	Порт по умолчанию	Направление	Назначение	Возможность настройки	Место, где устанавливается значение
Консоль администрирования	16979	исходящий	Для подключения к серверу Блокхост-Сеть	нет	

	55313	исходящий	Для аутентификации на сервере Блокхост-Сеть (на ОС Windows)	нет	
Сервер	59731	входящий	Для построения иерархии серверов	да	В мастере подключения подчиненного сервера
	999	входящий	Для подключения клиентов/подчиненных серверов	да	В мастере настройки сервера
	999	исходящий	Для подключения к мастер-серверу	да	Автоматически при построении иерархии
	16979	входящий	Для подключения консоли управления сервером	нет	
	55313	входящий	Для аутентификации консоли управления сервером на сервере (на ОС Windows)	нет	
	25000	входящий	Для подключения агента Системы Развертывания	да	В мастере настройки сервера
	25001	исходящий	Для подключения к агенту Системы Развертывания	нет	
	5432	исходящий	Для подключения к БД Postgres (по умолчанию)	да	В мастере настройки сервера
	514	исходящий	Для отправки сообщений в SIEM	да	В настройках подключения к SIEM
	587	исходящий	Для уведомлений по почте	да	В настройках почтовых уведомлений
	389	исходящий	Для получения информации по LDAP	нет	
Агент системы развертывания	25000	исходящий	Для подключения к серверу	да	При установке
	25001	входящий	Для подключения сервера	нет	
Клиент	999	исходящий	Для подключения к серверу	да	Автоматически при установке через систему развертывания

2.2 Установка корневых и промежуточных сертификатов для проверки сертификата подписи кода

Перед установкой СЗИ от НСД «Блокхост-Сеть 4» необходимо убедиться в том, что на

сервере установлены необходимые корневые и промежуточные сертификаты для проверки сертификата подписи кода *LLC DATAGILE.cer*:

– Root_R45_GlobalSign_Code.cer - GlobalSign Code Signing Root R45 (корневой);
  - GlobalSign GCC R45 CodeSigning CA 2020.cer - GlobalSign Code Signing Root R45;
– root-r6.crt - GlobalSign Root CA - R6 (корневой);
  - gstsacasha384g4.crt - GlobalSign Timestamping CA - SHA384 - G4.

При отсутствии данных сертификатов в оснастке ***Сертификаты (certmgr.msc)*** в разделах *Доверенные корневые центры сертификации* и *Промежуточные центры сертификации* во время установки СЗИ от НСД «Блокхост-Сеть 4» возможно возникновение ошибки вида:

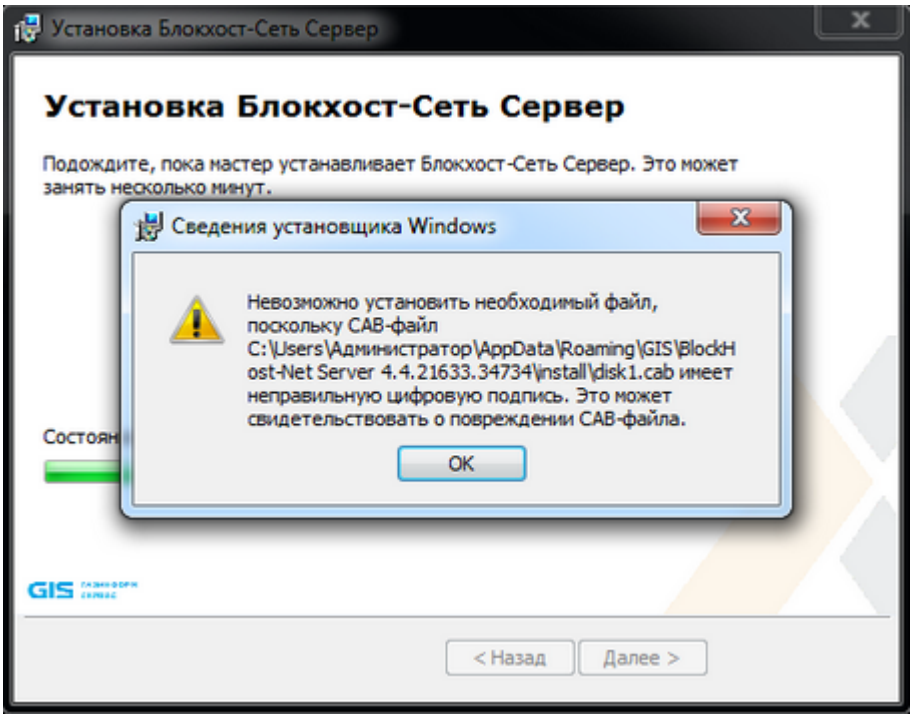


Рисунок 2.1 – Ошибка при установке сервера СЗИ от НСД «Блокхост-Сеть 4»

Для продолжения установки СЗИ от НСД «Блокхост-Сеть 4» необходимо выполнить установку сертификатов. Сертификаты входят в комплект поставляемого носителя СЗИ от НСД «Блокхост-Сеть 4».

3 Комплект поставки СЗИ от НСД «Блокхост-Сеть 4»

В зависимости от приобретаемой лицензии возможны два варианта использования:

– вариант №1 - автономный вариант СЗИ, при котором СЗИ устанавливается на ПК под управлением ОС MS Windows и используется локально;

– вариант №2 - вариант с удаленным управлением СЗИ, при котором клиентские части СЗИ устанавливается на ПК под управлением ОС MS Windows/Linux (РЕД ОС), клиент управления устанавливается на ПК под управлением сертифицированной ОС Linux (Astra Linux SE, Альт 8 СП)[2] и работают под управлением серверной части СЗИ, установленной на сервер безопасности под управлением ОС MS Windows/Linux. В состав установки клиента управления/клиента под управлением ОС Linux включается консоль управления клиентом.

В состав варианта №1 входят консоль управления, серверная и клиентская части СЗИ, функционирующие на одном ПК. Сетевой режим работы для данного варианта использования невозможен и ограничен автономной лицензией.

В комплект поставки варианта №1 входят следующие файлы:

– BlockHost.Net 4 Server.exe – установка СЗИ от НСД «Блокхост-Сеть 4» для эксплуатации на одном ПК (содержит консоль управления, серверную и клиентскую части СЗИ, функционирующие на одном ПК);

– GIS.WipeFiles<номер версии>.msi – установка подсистемы гарантированного удаления по требованию.

В состав варианта №2 входят:

– клиентская часть СЗИ от НСД «Блокхост-Сеть 4», которая устанавливается на клиентские рабочие станции под управлением ОС MS Windows/Linux (РЕД ОС);

– серверная часть СЗИ от НСД «Блокхост-Сеть 4», которая устанавливается на серверы безопасности под управлением ОС MS Windows/Linux;

– клиент управления, который устанавливается на рабочую станцию под управлением сертифицированной ОС Linux (Astra Linux SE, Альт 8 СП);

– консоль управления, которая устанавливается на рабочее место администратора под управлением ОС MS Windows/Linux и позволяет управлять развертыванием СЗИ на

[2] Функциональные возможности клиента управления под управлением ОС Linux (Astra Linux SE, Альт 8 СП) ограничены возможностью управления входом в ОС и двухфакторной аутентификацией пользователей при входе в ОС при помощи персональных электронных идентификаторов, в т.ч. с использованием цифровых сертификатов пользователей, хранящихся на них; возможностью контроля целостности файлов, гарантированным удалением по требованию.

клиентах, подключением клиентских частей к серверной части и настройками сбора событий безопасности.

В комплект поставки варианта №2 входят следующие файлы:

– для ОС MS Windows:

СЗИ от НСД «Блокхост-Сеть 4»	Имя файла	Примечание
Серверная часть	BlockHost.Net 4 Server.exe	установка серверной части СЗИ на 64-разрядные ОС Windows (установка клиентской части СЗИ от НСД «Блокхост-Сеть 4» на клиентские рабочие станции будет доступна после установки серверной части из консоли управления СЗИ)
Клиентская часть	BhNet.Installer.exe	установка клиентской части СЗИ содержит в себе инсталляторы для 32- и 64-разрядных ОС Windows
Консоль	BlockHost.Net 4 Console.msi	консоль управления СЗИ, которая устанавливается на рабочее место администратора и позволяет управлять развертыванием СЗИ на клиентах, подключением клиентских частей к серверной части и настройками сбора событий безопасности
Подсистема ГУПТ	GIS.WipeFiles<номер версии>.msi	установка гарантированного удаления по требованию
Подсистема развертывания	BHNetDeployment Agent <номер версии>.msi	установка агента развертывания для взаимодействия между сервером СЗИ и клиентскими рабочими станциями
Подсистема расширенной аутентификации	BlockHost.Net 4 extended auth.msi	установка модуля расширенной аутентификации, позволяющего проводить двухфакторную аутентификацию по сети и разграничивать доступ на уровне создания сессии пользователя

4 Установка СЗИ от НСД «Блокхост-Сеть 4»

Установка автономного варианта СЗИ от НСД «Блокхост-Сеть 4» или серверной части СЗИ при использовании варианта с удаленным управлением описана в разделе 4.1 «Установка серверной части СЗИ» настоящего документа.

Установка консоли управления при использовании варианта с удаленным управлением СЗИ описана в разделе 4.2 «Установка консоли управления» настоящего документа.

Установка агента системы развертывания описана в разделе 4.5 «Установка агента развертывания» настоящего документа.

Установка клиентской части СЗИ описана в разделе 4.6 «Установка клиентской части СЗИ» настоящего документа.

Установка модуля расширенной аутентификации выполняется с помощью создания задачи на установку программы, подробное описание см. в разделе 8.1 «Установка программы» документа «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит».

Установка гарантированного удаления по требованию описана в разделе 2 «Инсталляция подсистемы ГУПТ» документа Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 6. Подсистема ГУПТ».

Перед началом установки СЗИ от НСД «Блокхост-Сеть 4» необходимо убедиться в том, что на сервере установлены сертификаты

4.1 Установка серверной части СЗИ

Серверная часть СЗИ устанавливается на сервер безопасности под управлением ОС MS Windows с поставляемого носителя с помощью файла *BlockHost.Net 4 Server.exe,* который содержит в себе инсталлятор для 64-разрядных ОС.

Одновременно с установкой серверной части, на сервер безопасности будут установлены консоль управления и клиентская часть СЗИ.

Перед инсталляцией СЗИ от НСД «Блокхост-Сеть 4» необходимо убедиться, что для встроенной учетной записи администратора в ОС (домене) задан пароль!

Не рекомендуется устанавливать СЗИ от НСД «Блокхост-Сеть 4» на контроллер домена.

Перед установкой СЗИ от НСД «Блокхост-Сеть 4» необходимо убедиться в выполнении всех требований к установке, описанных в подразделе 1.1 «Требования к аппаратному и программному обеспечению» настоящего документа.

Для установки серверной части СЗИ необходимо войти в операционную систему сервера под учетной записью встроенного администратора ОС Windows (контроллера домена), либо под учетной записью, имеющей административные права и запустить на выполнение файл-установщик СЗИ (*BlockHost.Net 4 Server.exe*).

В результате запуска файла-установщика на экране монитора появится окно приветствия мастера установки серверной части СЗИ от НСД «Блокхост-Сеть 4» (рисунок 4.1).

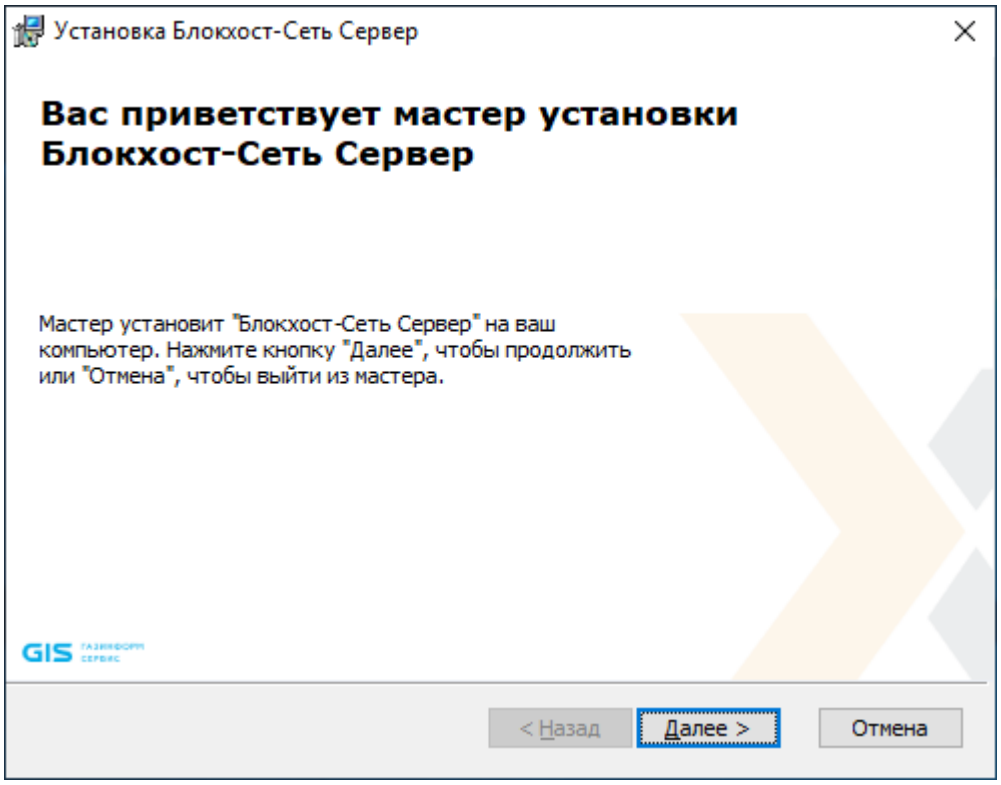


Рисунок 4.1 – Окно мастера установки сервера СЗИ от НСД «Блокхост-Сеть 4»

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 4.2.

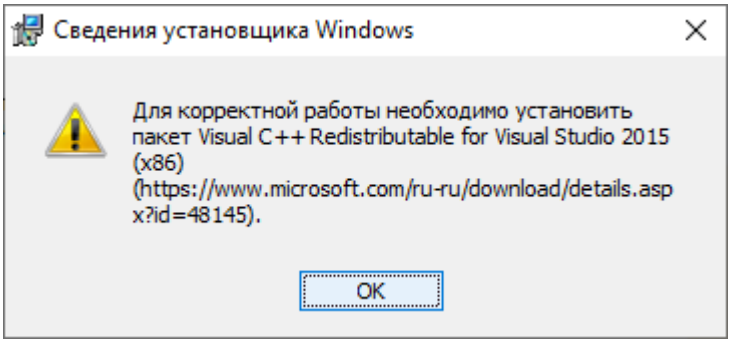


Рисунок 4.2 – Требование установки распространяемого пакета Microsoft Visual C++ 2015 Redistributable

Установка серверной части будет прервана (рисунок 4.3). 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 повторно.

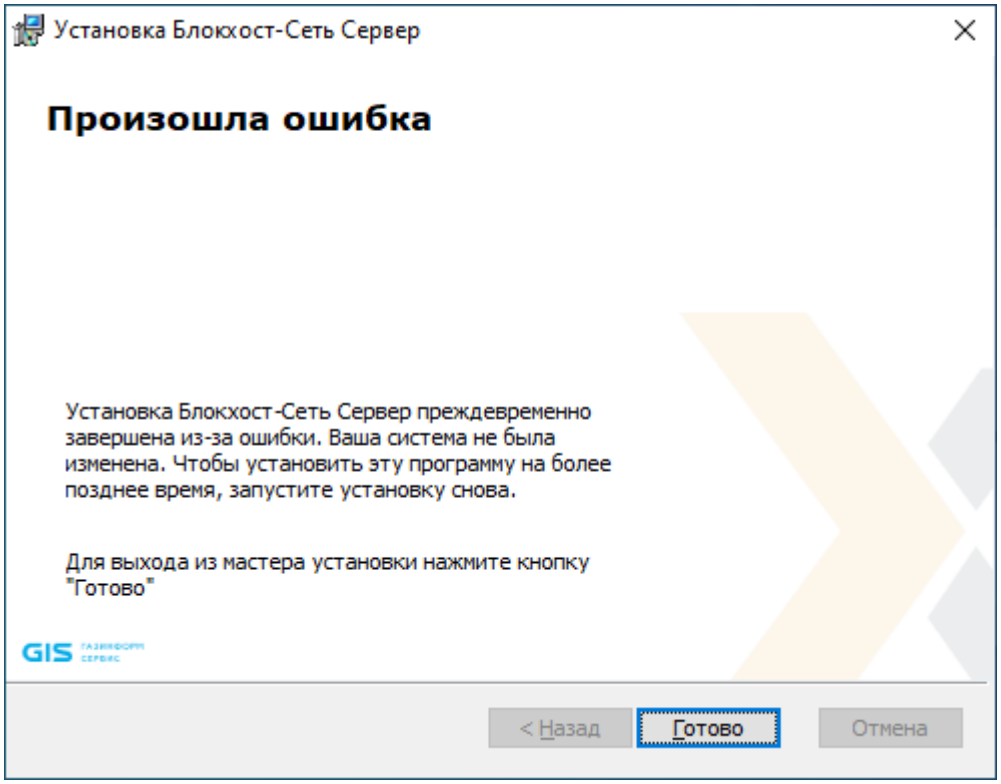


Рисунок 4.3 – Работа мастера установки преждевременно завершена

В следующем окне (рисунок 4.4) необходимо выбрать тип установки СЗИ от НСД «Блокхост-Сеть 4»:

– *обычная* – установка только основных компонент, необходимых для функционирования СЗИ;

– *выборочная* – установка выборочных компонент СЗИ из списка (рисунок 4.5).

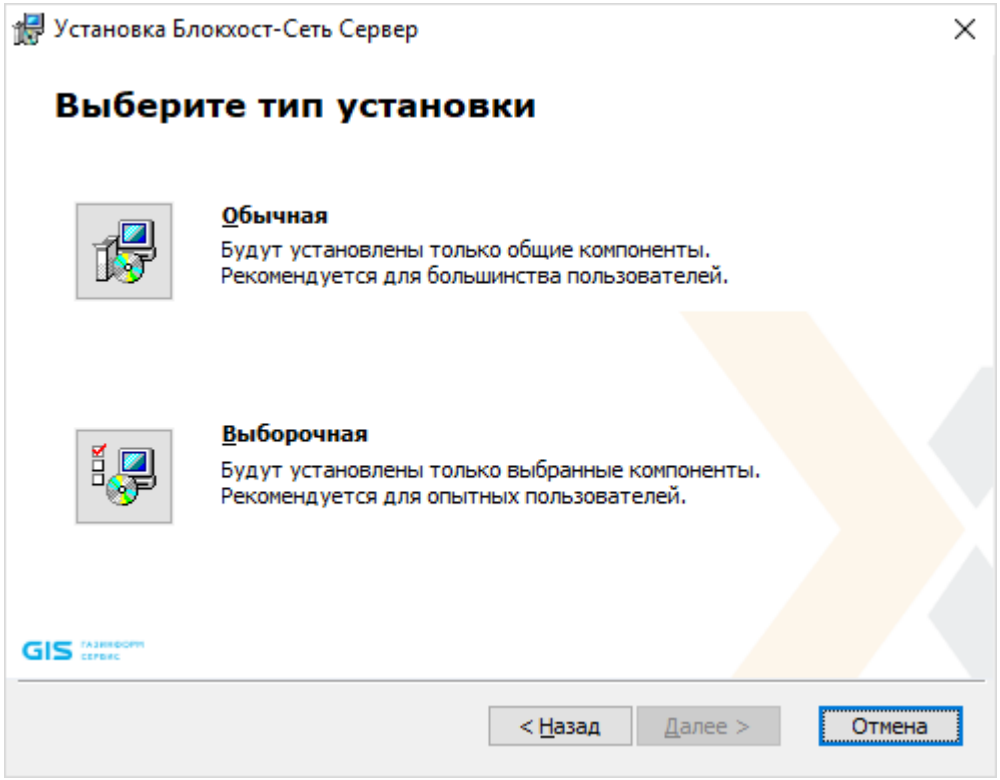


Рисунок 4.4 – Выбор типа установки СЗИ

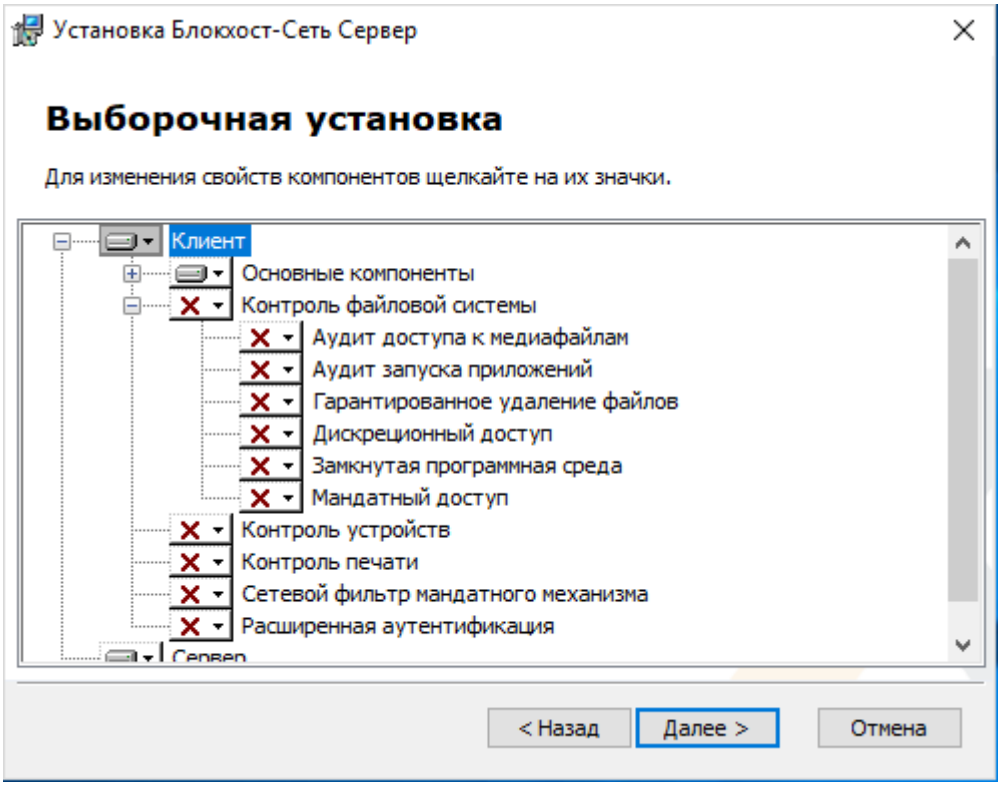


Рисунок 4.5 – Выбор компонент для установки

Для выбора доступны следующие компоненты:

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

- *Аудит доступа к медиафайлам* – контроль доступа к определённым типам файлов: аудиофайлам, видеофайлам и изображениям, путем регистрации событий аудита;
- *Аудит запуска приложений* – контроль отслеживания запуска и прекращения работы исполняемых файлов;
- *Гарантированное удаление файлов* - удаление объектов файловой системы с системных и не системных дисков без возможности их дальнейшего восстановления;
- *Дискреционный доступ* - настройка доступа всех пользователей к объектам файловой системы;
- *Замкнутая программная среда* – формирование списка разрешенных для запуска процессов, доступных для пользователя на клиентской рабочей станции;
- *Мандатный доступ* - разграничение доступа субъектов к объектам путем сочетания назначенных субъектам и объектам допуска квалификационных меток и неиерархических категорий;

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

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

– ***Сетевой фильтр мандатного механизма*** – необходим при использовании мандатного разграничения доступа;

– ***Расширенная аутентификация*** – расширенные настройки механизма аутентификации, позволяющие проводить двухфакторную аутентификацию по сети и разграничивать доступ на уровне создания сессии пользователя[3].

После выбора необходимого типа установки и нажатия кнопки ***Далее*** появится окно, содержащее текст лицензионного соглашения (рисунок 4.6). Для продолжения установки необходимо ознакомиться с лицензионным соглашением на устанавливаемый продукт и принять условия лицензионного соглашения.

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

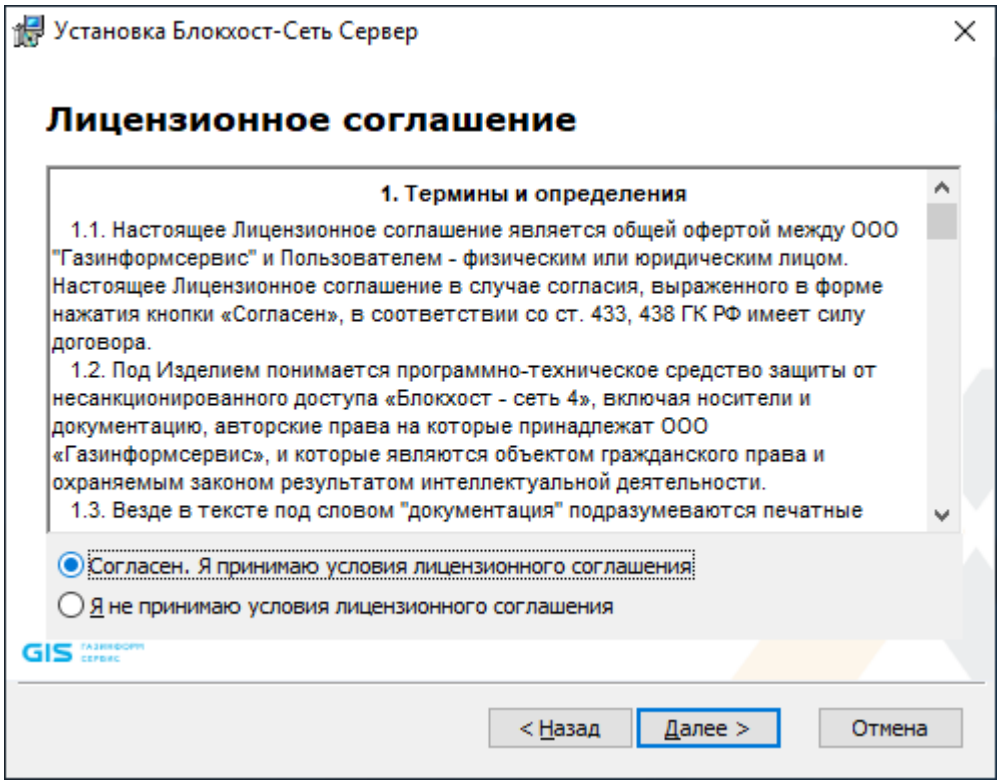


Рисунок 4.6 – Лицензионное соглашение

После принятия соглашения и нажатия кнопки ***Далее*** появится окно, позволяющее задать пароль для встроенной учетной записи администратора (рисунок 4.7).

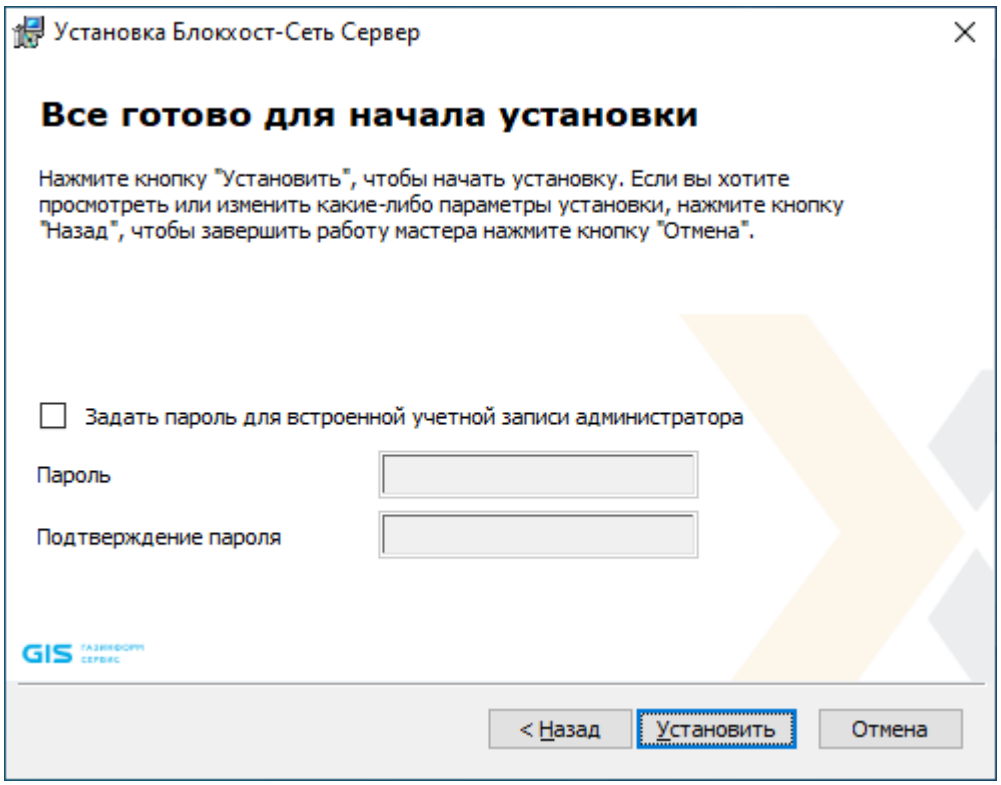


Рисунок 4.7 – Окно готовности к установке СЗИ от НСД «Блокхост-Сеть 4»

После нажатия кнопки ***Установить*** начнется процесс установки СЗИ от НСД «Блокхост-Сеть 4» (рисунок 4.8).

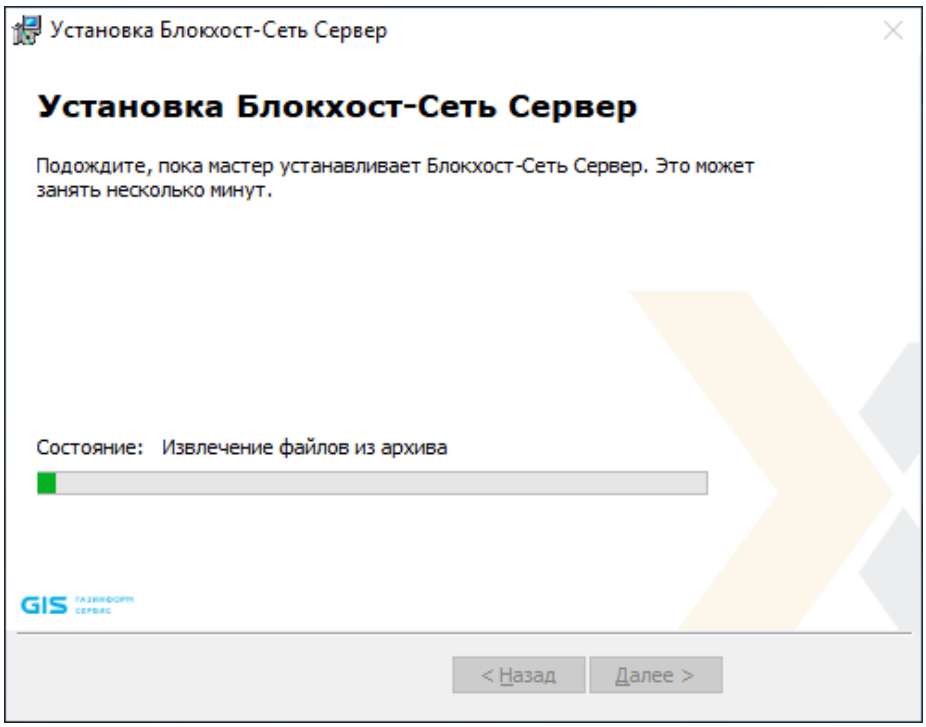


Рисунок 4.8 – Ход установки СЗИ от НСД «Блокхост-Сеть 4»

При успешном завершении установки появится окно окончания работы мастера установки СЗИ (рисунок 4.9) в котором необходимо нажать кнопку ***Готово***.

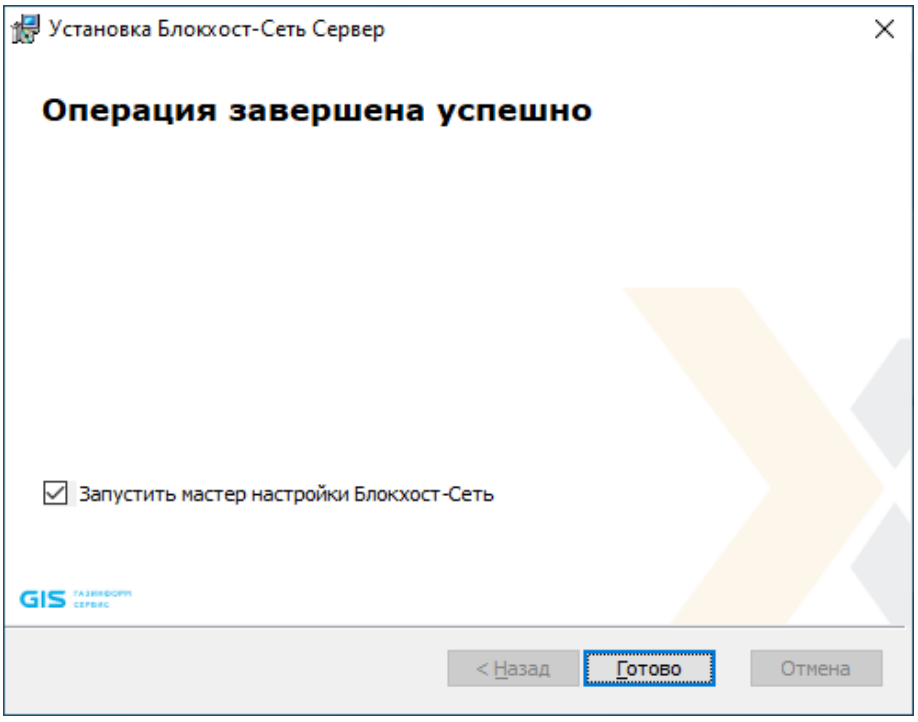


Рисунок 4.9 – Окно окончания установки серверной части СЗИ от НСД «Блокхост-Сеть 4»

Для завершения установки СЗИ необходимо перезагрузить компьютер. Перезагрузка доступна сразу после окончания работы мастера установки СЗИ, по нажатию кнопки ***Да*** в окне на рисунке 4.10, или позднее вручную, для этого нужно отказаться от перезагрузки, нажав кнопку ***Нет*** в окне на рисунке 4.10.

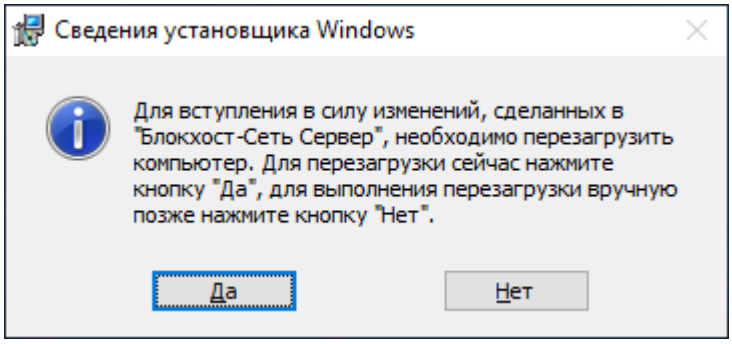


Рисунок 4.10 – Подтверждение выполнения перезагрузки рабочей станции

После выполнения перезагрузки на рабочей станции появится ярлык для запуска консоли управления.

После первичной установки серверной части СЗИ перед запуском консоли управления необходимо выполнить настройку с помощью пункта ***Мастер настройки*** в меню ***Пуск*** → ***Блокхост-Сеть Сервер***. При попытке запуске консоли управления до настройки мастера появится сообщение о необходимости настроить СЗИ (рисунок 4.11).

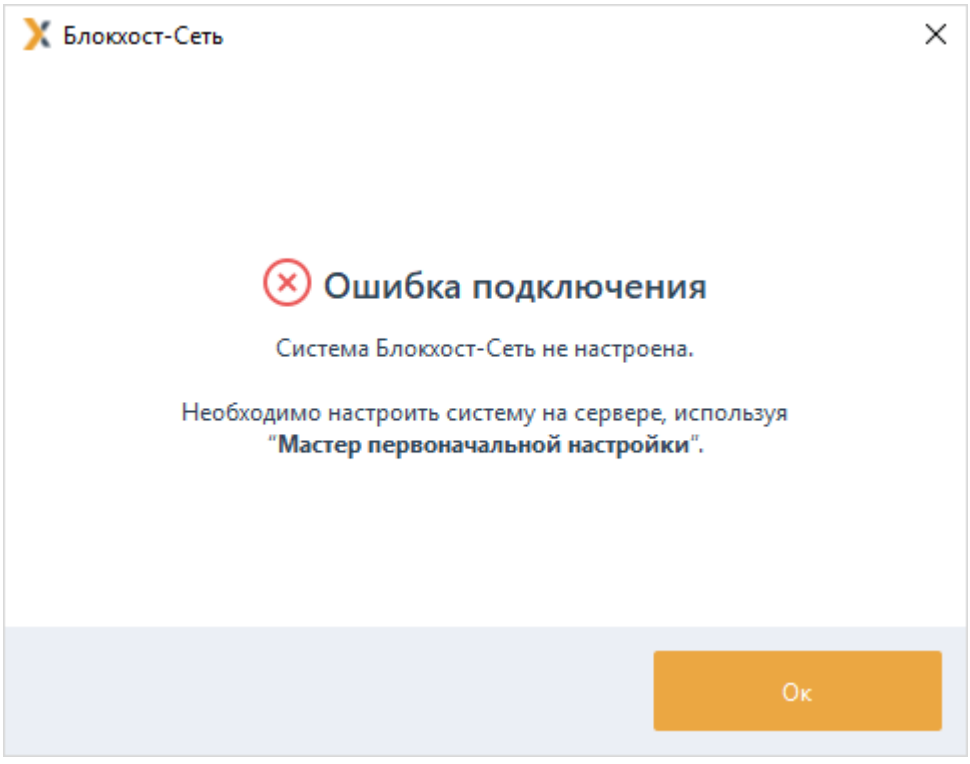


Рисунок 4.11 – Ошибка при запуске консоли управления СЗИ

4.2 Установка консоли управления

При установке серверной части СЗИ консоль управления устанавливается по умолчанию. Никаких дополнительных настроек для запуска консоли производить не нужно.

Консоль управления СЗИ может быть установлена на рабочее место администратора для удобства управления клиентскими рабочими станциями.

Консоль управления должна быть установлена только на рабочую станцию с установленной клиентской частью СЗИ. Перед установкой консоли управления убедитесь, что клиентская часть СЗИ установлена на рабочей станции!

Установка консоли управления осуществляется с поставляемого носителя с помощью файла *BlockHost.Net 4 Console.msi*.

Для установки консоли управления СЗИ необходимо войти в операционную систему под учетной записью, имеющей административные права, и запустить на выполнение файл *BlockHost.Net 4 Console.msi*.

В результате запуска на экране монитора появится окно приветствия мастера установки консоли управления СЗИ (рисунок 4.12).

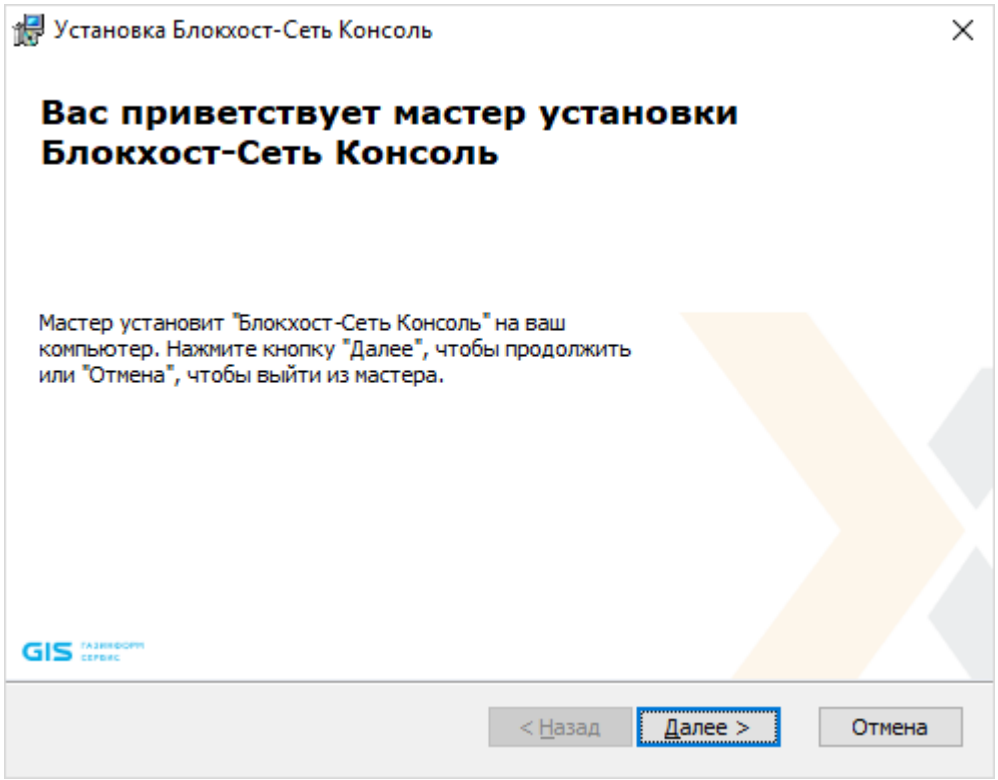


Рисунок 4.12 – Окно установки консоли управления СЗИ

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 4.2.

Установка консоли управления будет прервана (рисунок 4.13). 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 повторно.

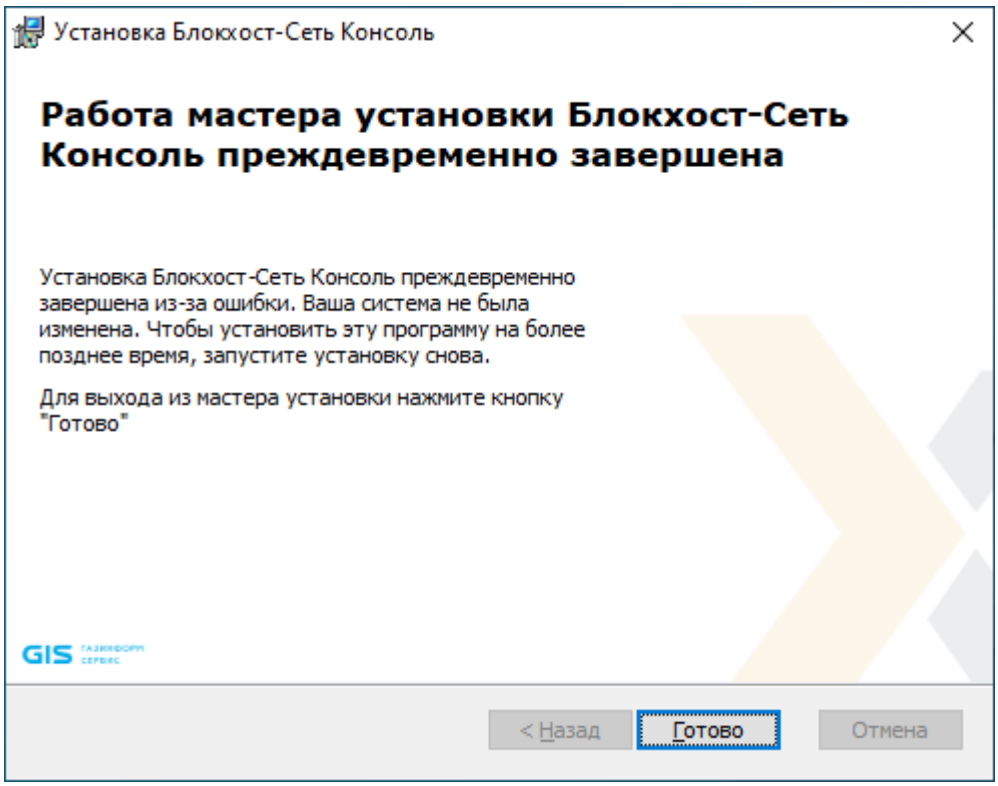


Рисунок 4.13 – Работа мастера установки преждевременно завершена

После нажатия в окне приветствия мастера установки СЗИ кнопки ***Далее*** (рисунок 4.12) появится окно, содержащее текст пользовательского соглашения (рисунок 4.14). Для продолжения установки необходимо ознакомиться с пользовательским соглашением на устанавливаемый продукт и принять условия пользовательского соглашения.

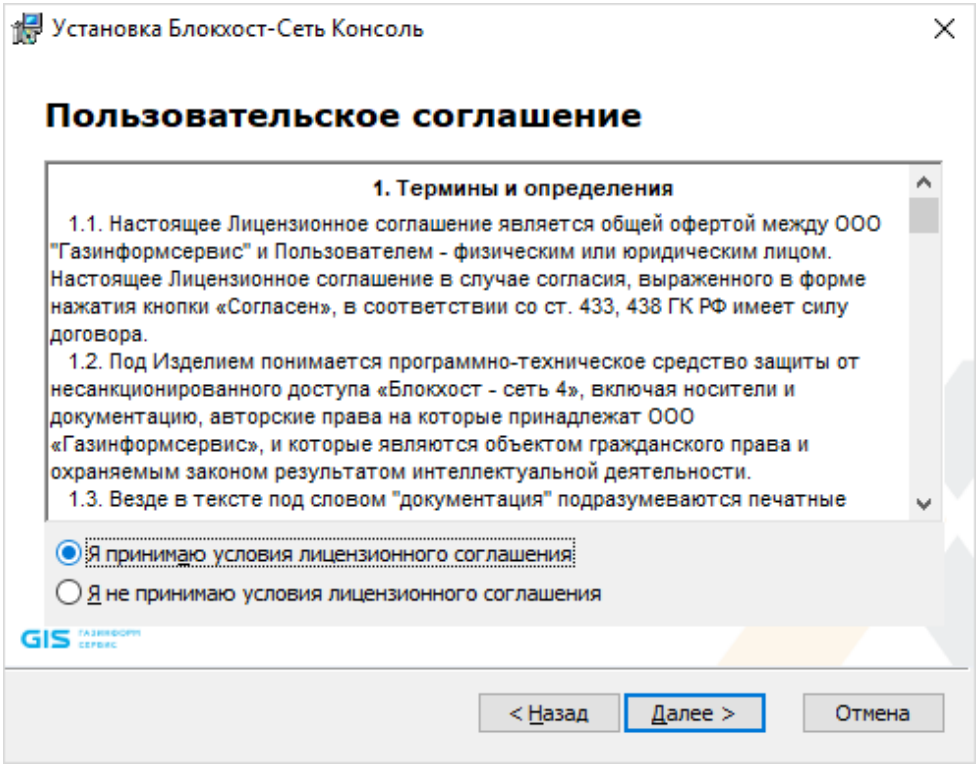


Рисунок 4.14 – Пользовательское соглашение

После принятия соглашения и нажатия кнопки ***Далее*** появится окно выбора директории для установки (рисунок 4.15). Для изменения директории, указанной по умолчанию, нажмите кнопку ***Обзор*** и выберите нужную директорию.

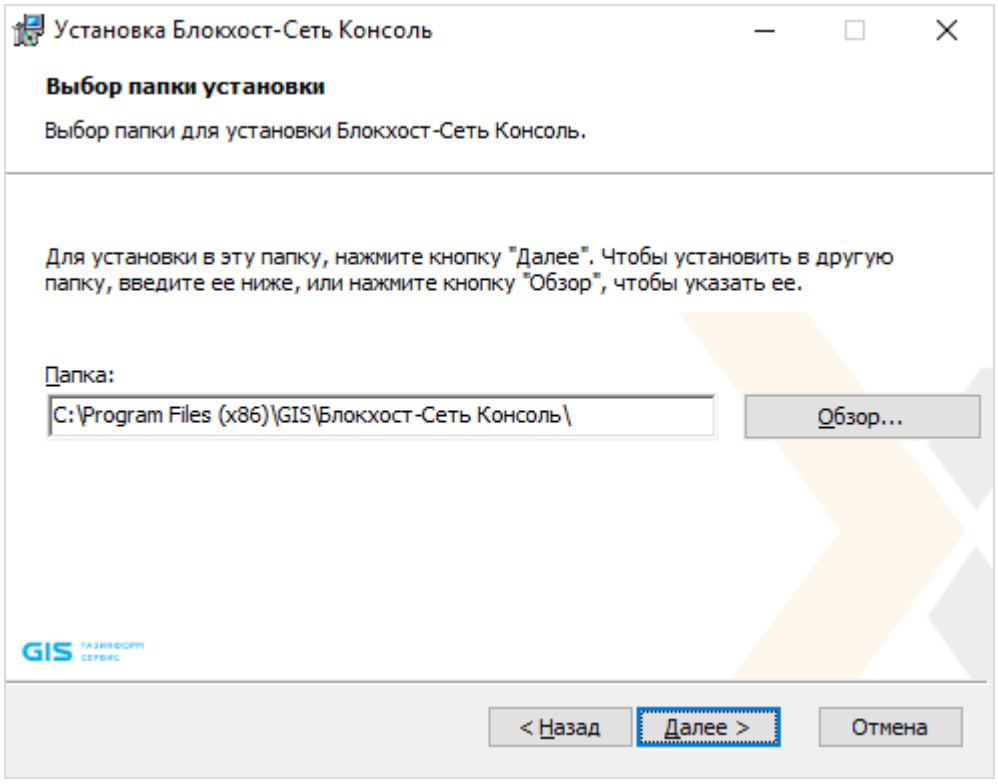


Рисунок 4.15 – Выбор директории для установки

После выбора директории и нажатия кнопки ***Далее*** появится информационное окно с сообщением о готовности к выполнению установки консоли управления (рисунок 4.16).

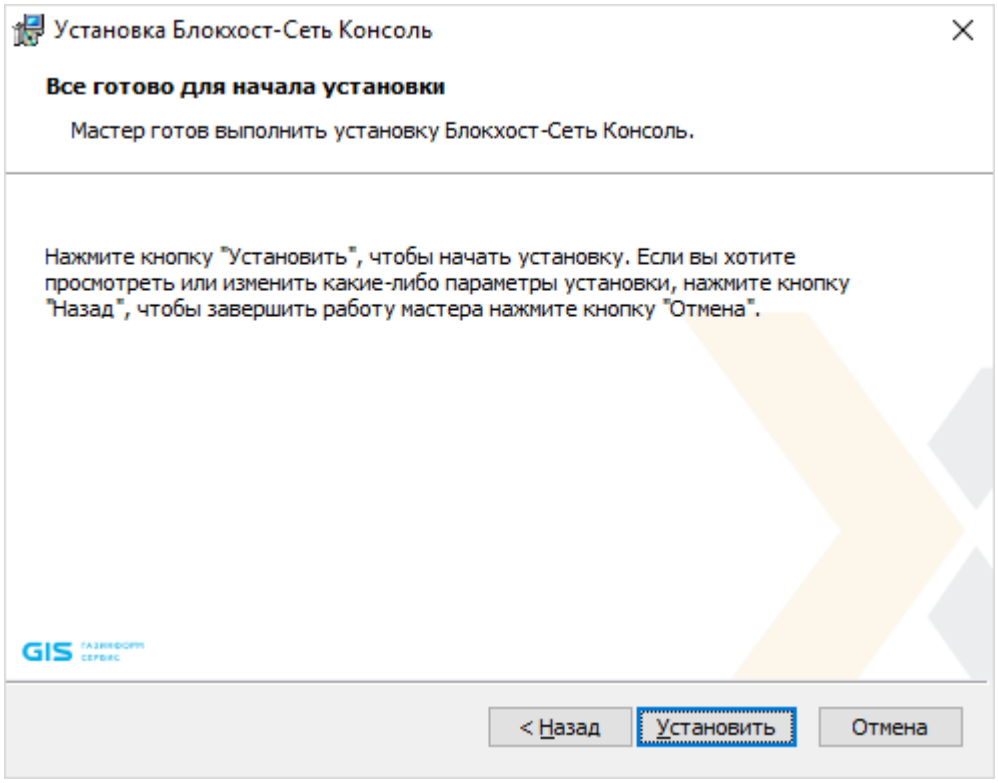


Рисунок 4.16 – Окно готовности к установке консоли управления

После нажатия кнопки ***Установить*** начнется процесс установки консоли управления. При успешном завершении установки появится окно окончания работы мастера установки (рисунок 4.17) в котором необходимо нажать кнопку ***Готово***.

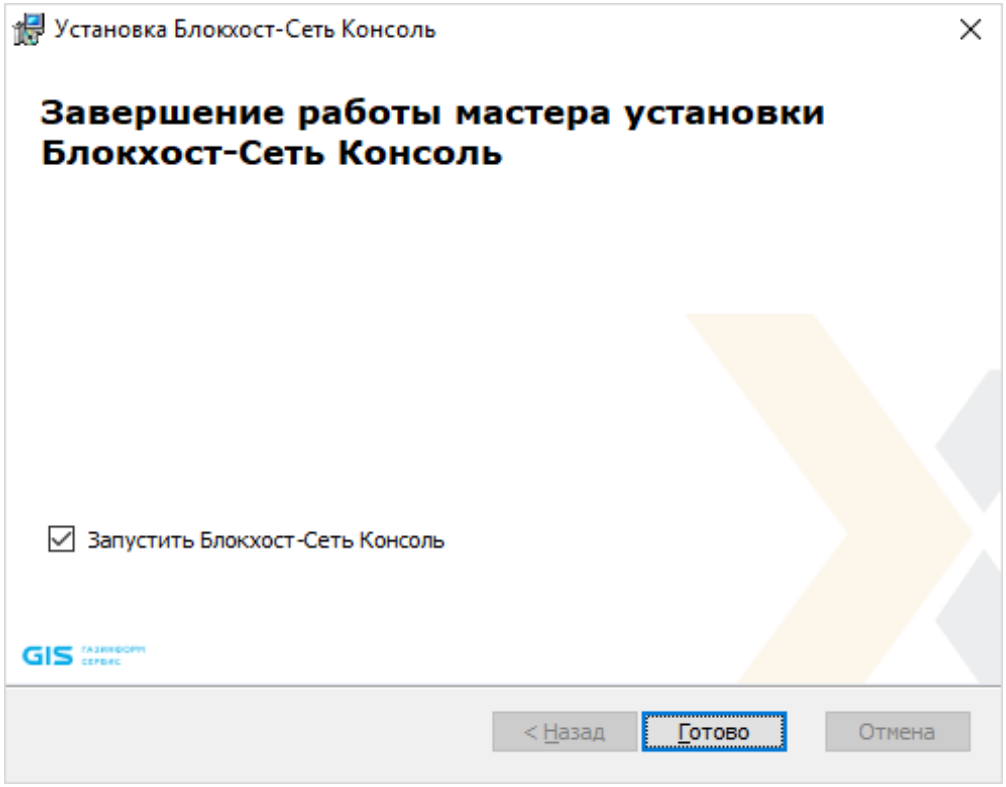


Рисунок 4.17 – Окно окончания установки консоли управления

По завершению установки консоли управления необходимо настроить параметры подключения консоли к серверу СЗИ. Подробнее подключение к серверу описано в разделе ***«Настройка подключения к серверу»*** настоящего документа.

4.3 Первоначальная настройка системы

Перед запуском консоли управления СЗИ от НСД «Блокхост-Сеть 4» необходимо выполнить первоначальную настройку параметров системы.

Запуск мастера первоначальной настройки доступен только на сервере безопасности с установленной серверной частью СЗИ.

Мастер настройки запускается автоматически по завершению установки СЗИ, если в окне завершения установки (рисунок 4.9) установлен флаг ***Запустить мастер настройки СЗИ*** или принудительно после выполнения перезагрузки рабочей станции выбором пункта ***Мастер настройки*** в меню ***Пуск*** → ***Блокхост-Сеть Сервер*** (рисунок 4.18).

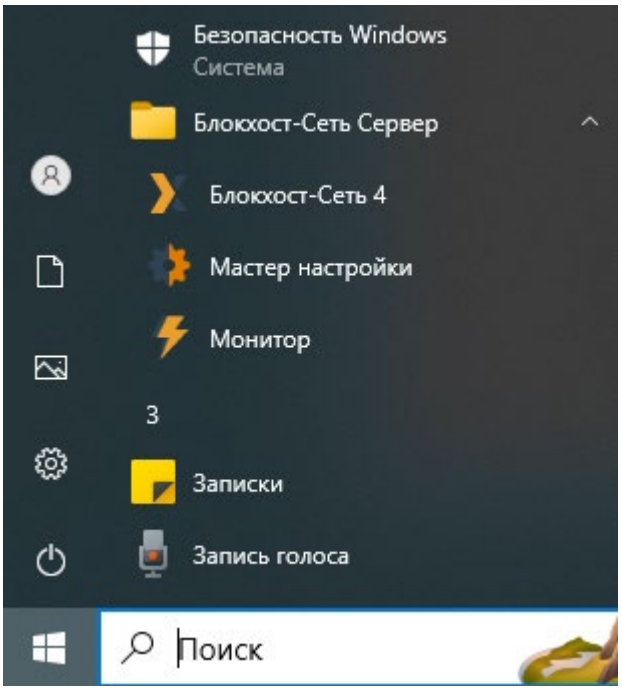


Рисунок 4.18 – Запуск мастера настройки Блокхост-Сеть

Появится окно приветствия мастера настройки системы (рисунок 4.19) в котором необходимо нажать кнопку ***Далее***.

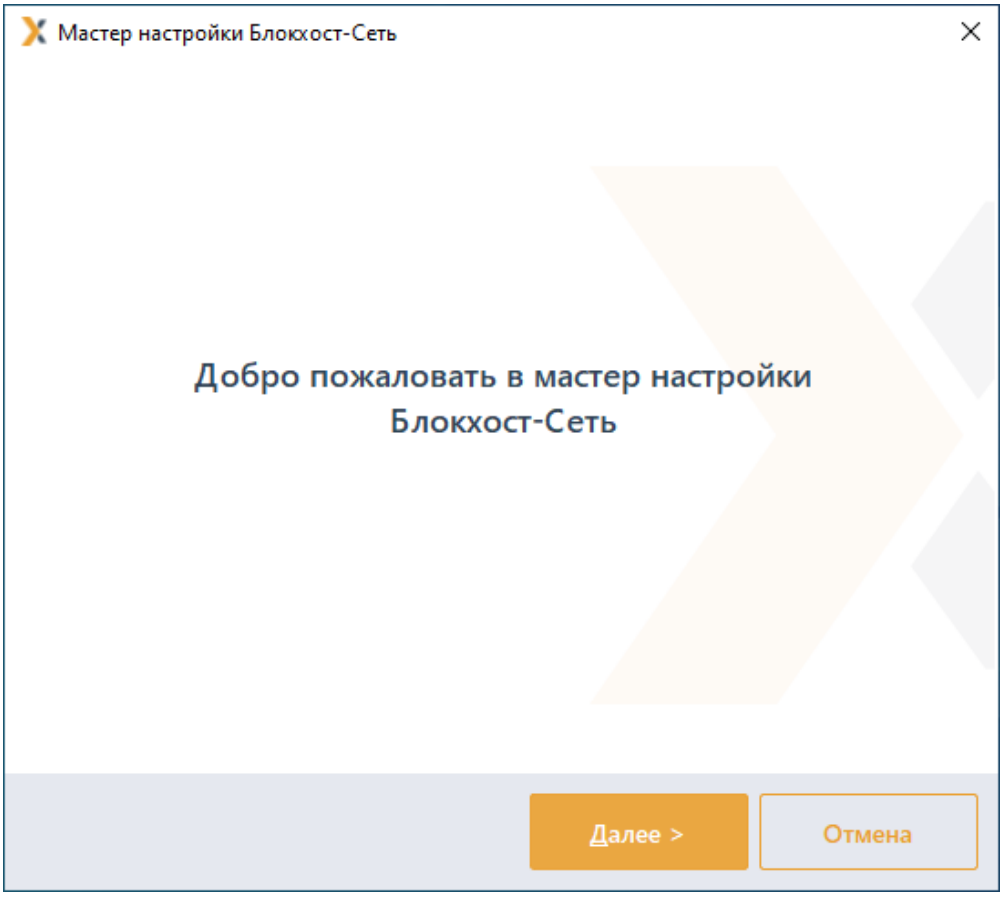


Рисунок 4.19 – Окно приветствия мастера настройки системы

На следующем этапе работы мастера настройки необходимо задать путь к файлу инсталлятора распространяемого пакета Microsoft Visual C++ 2015 Redistributable или более поздней версии, содержащий компоненты Microsoft Visual C++ 2015 (рисунок 4.20). Наличие данного пакета является обязательным для корректной работы компонентов «Агент системы развертывания» и «Клиент Блокхост-Сеть».

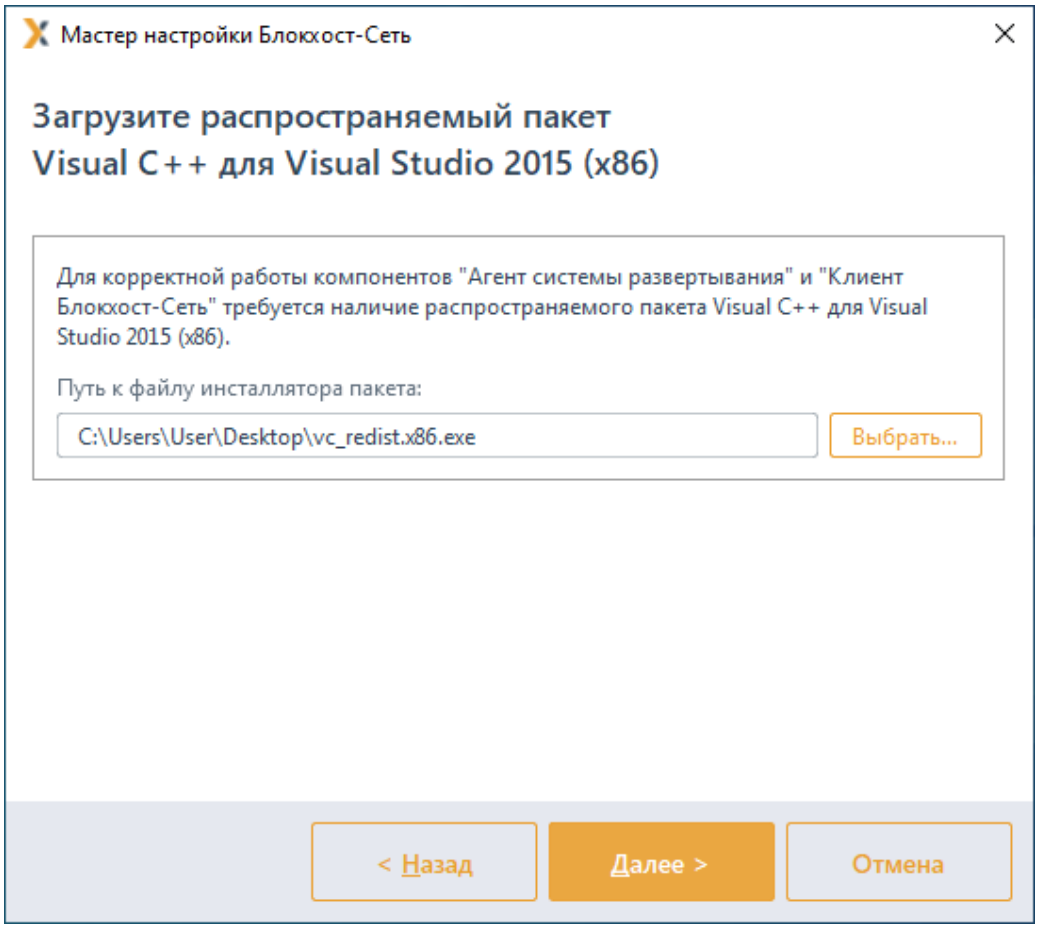


Рисунок 4.20 – Установка пути к распространяемому пакету Microsoft Visual C++ 2015 Redistributable

На следующем этапе работы мастера настройки (рисунок 4.21) необходимо задать параметры соединения с сервером БД (СЗИ от НСД «Блокхост-Сеть 4» поддерживает работу с СУБД «PostgreSQL»[4], «Jatoba» или использовать встроенную БД):

– ***Тип базы данных*** – выбирается тип СУБД:
  - ***PostgreSQL*** (рисунок 4.21 б) – данный тип базы данных выбирается для взаимодействия с СУБД «PostgreSQL» и СУБД «Jatoba»;

[4] В случае использования СУБД «Jatoba», если СУБД «Jatoba» и настраиваемый сервер СЗИ установлены на разных машинах, необходимо вручную сконфигурировать СУБД «Jatoba». Описание необходимых настроек приведено в разделе «Особенности подключения к СУБД «Jatoba»».

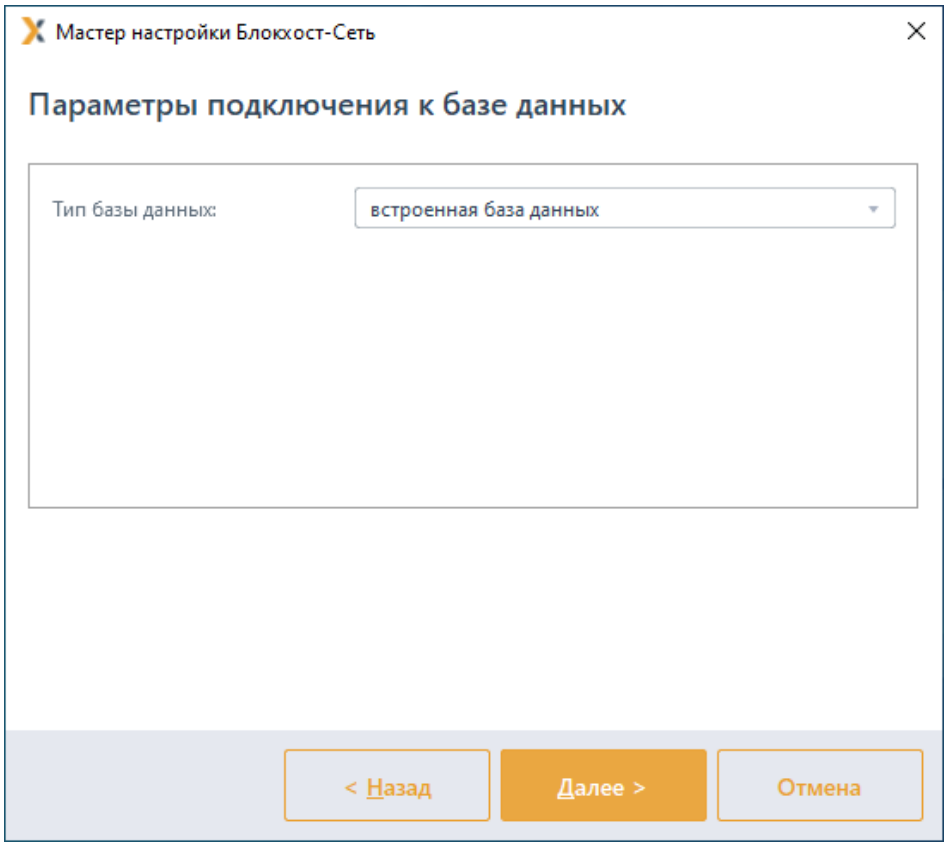
- ***встроенная база данных*** (рисунок 4.21 а) – при выборе встроенной базы данных, используется база данных СЗИ, подключение к серверу не потребуется, параметры подключения не задаются);

– ***Адрес сервера базы данных*** – указывается IP-адрес или DNS-имя рабочей станции, на которой установлена СУБД «PostgreSQL» или СУБД «Jatoba». При размещении СУБД PostgreSQL/Jatoba и сервера СЗИ на одной ЭВМ в поле ***Адрес*** можно оставить значение по умолчанию *localhost*;

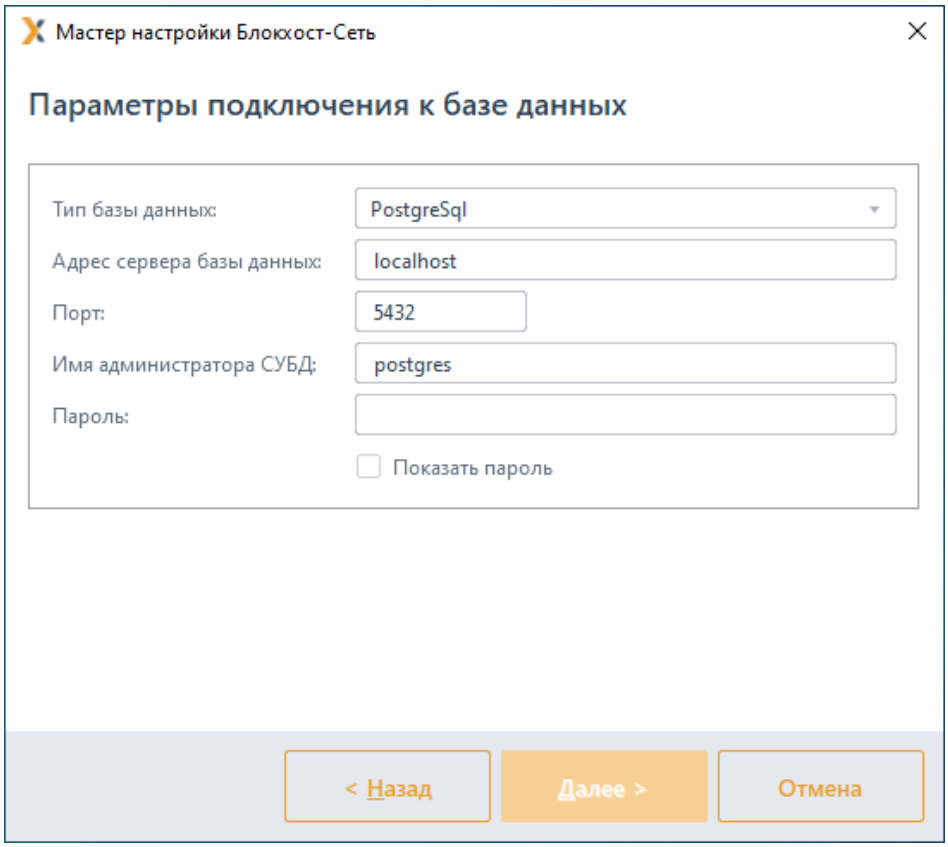
– ***Порт*** – указывается значение TCP-порта, по которому осуществляется работа СУБД PostgreSQL/Jatoba;

– ***Имя администратора СУБД*** – имя учетной записи, обладающей полномочиями создания и редактирования баз данных. «Суперпользователь» – в терминологии СУБД «PostgreSQL», «администратор СУБД» в терминологии СУБД «Jatoba»;

– ***Пароль*** – пароль указанной выше учетной записи (суперпользователь или администратор СУБД в зависимости от используемой БД). Отмеченный параметр ***Показать пароль*** позволяет отобразить, введенное в поле ***Пароль*** значение. В противном случае в поле отображаются символы «*».



а)



б)

Рисунок 4.21 – Окно настройки параметров соединения системы развертывания и сервера баз данных

После ввода всех необходимых параметров соединения с СУБД необходимо нажать кнопку ***Далее***, откроется окно по выбору сетевого интерфейса (рисунок 4.22).

IP-адрес выбранного сетевого интерфейса используется для подключения агентов развертывания и клиентов Блокхост-Сеть к серверу СЗИ. В списке сетевых интерфейсов отображаются только включенные сетевые адаптеры типа Ethernet и Wireless, имеющие IP-адреса протокола IPv4. Для выбора необходимого интерфейса следует выделить его в окне мастера настройки и нажать кнопку ***Далее***.

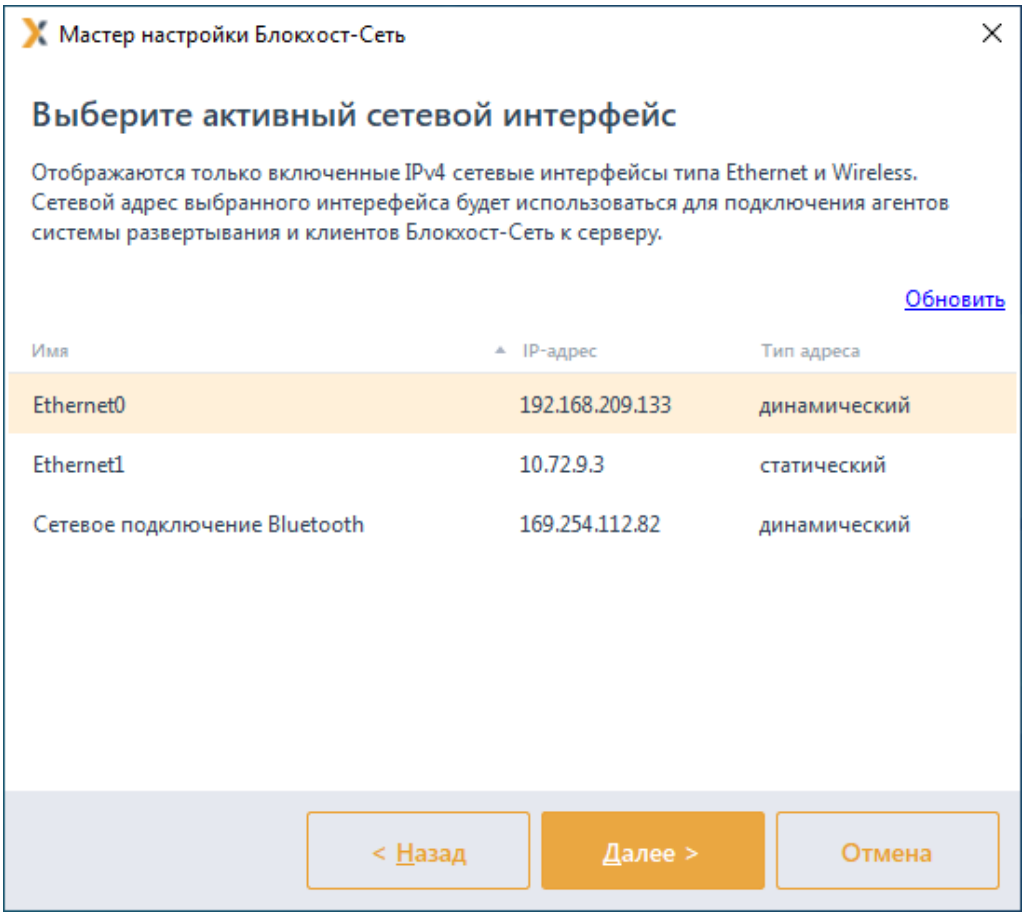


Рисунок 4.22 – Окно выбора сетевого интерфейса

На следующем шаге откроется окно по редактированию параметров удаленного соединения агентов развертывания и клиентов Блокхост-Сеть с системой развертывания (рисунок 4.23):

– ***Порт сервера системы развертывания для входящих соединений*** (по умолчанию 25000), при необходимости установленное значение можно изменить, указав новое значение в соответствующем поле;

– ***Порт сервера Блокхост-Сеть для входящих соединений (по умолчанию 999***), при необходимости установленное значение можно изменить, указав новое значение в соответствующем поле;

– ***Порт сервера Блокхост-Сеть для построения иерархии серверов***, при необходимости установленное значение можно изменить, указав новое значение в соответствующем поле;

– ***Выполнять логирование работы системы развертывания*** (по умолчанию логирование установлено), при необходимости логирование можно отключить;

– Каталог для записи логов (по умолчанию *localhost C:\BlockHost\DeploymentSystem\log*) при включенном логировании работы лог-файлы системы развертывания будут храниться в указанной директории.

Рекомендуется не отключать параметр ***Выполнять логирование работы системы развертывания,*** так как в лог-файлы записывается отладочная информация, позволяющая разработчикам быстрее разобраться с возможными проблемами в работе системы развертывания.

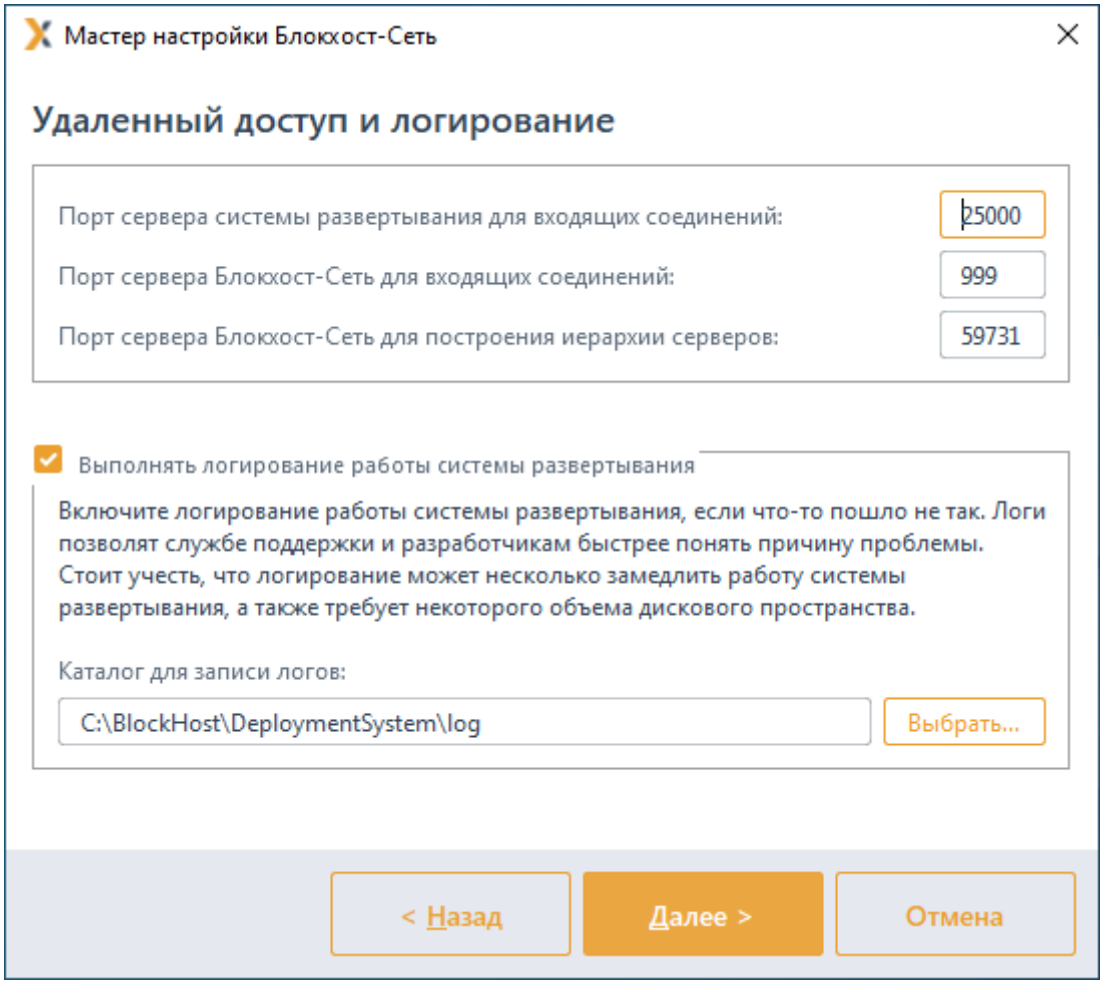


Рисунок 4.23 – Окно настройки параметров удаленного доступа и логирования

После нажатия кнопки ***Далее*** откроется окно с сообщением о готовности к выполнению процесса подготовки Блокхост-Сеть к работе (рисунок 4.24).

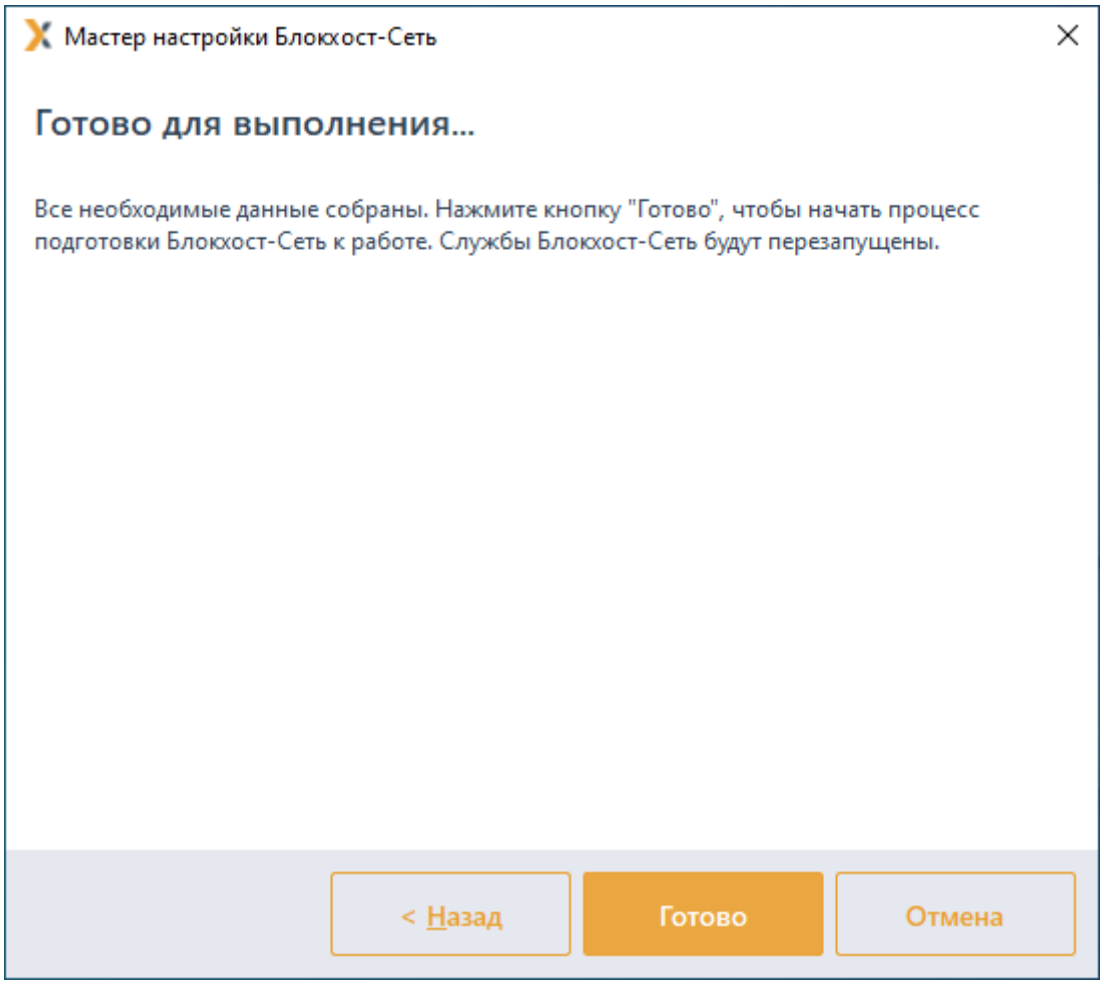


Рисунок 4.24 – Окно готовности к выполнению настройки

После нажатия кнопки ***Готово*** появится окно завершения работы мастера настройки (рисунок 4.25). Нажмите кнопку ***Завершить*** для начала работы с консолью управления с настроенными параметрами.

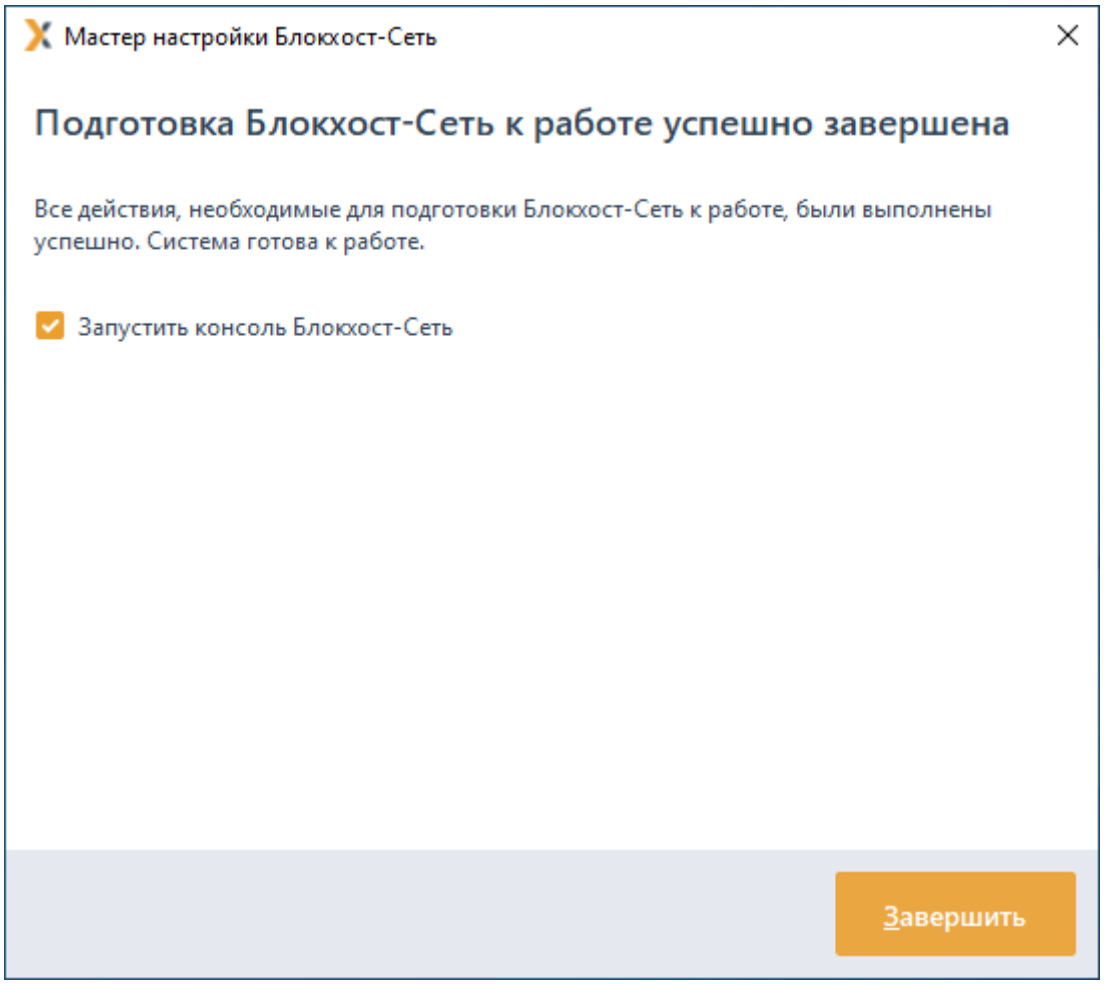


Рисунок 4.25 – Окно окончания работы мастера настройки

4.4 Первый запуск консоли управления

4.4.1 Настройка подключения к серверу

При первом запуске консоли управления необходимо выполнить настройку подключения консоли к серверу безопасности. Для этого после перезагрузки рабочей станции запустите консоль управления СЗИ по ярлыку на рабочем столе или в меню кнопки ***Пуск***.

В появившемся окне (рисунок 4.26) укажите необходимые настройки для подключения к серверу:

– ***Адрес сервера*** – указывается IP-адрес сервера;

– ***Имя пользователя*** – имя пользователя, обладающего полномочиями администратора;

– ***Пароль*** – пароль указанного выше пользователя.

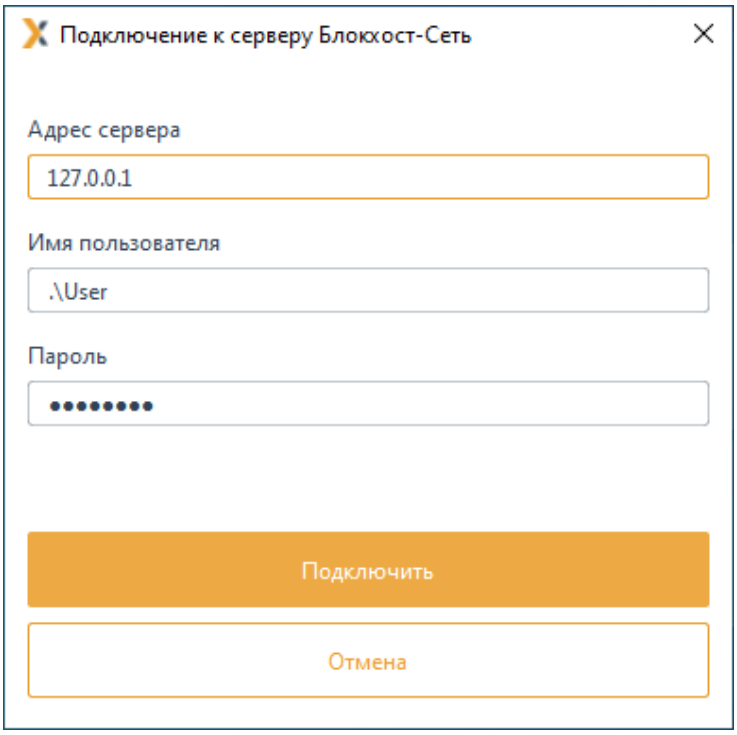


Рисунок 4.26 – Подключение к серверу безопасности

После нажатия кнопки ***Подключить*** появится окно в котором необходимо проверить сертификат подключения к серверу и согласиться или отказаться от продолжения установки (рисунок 4.27).

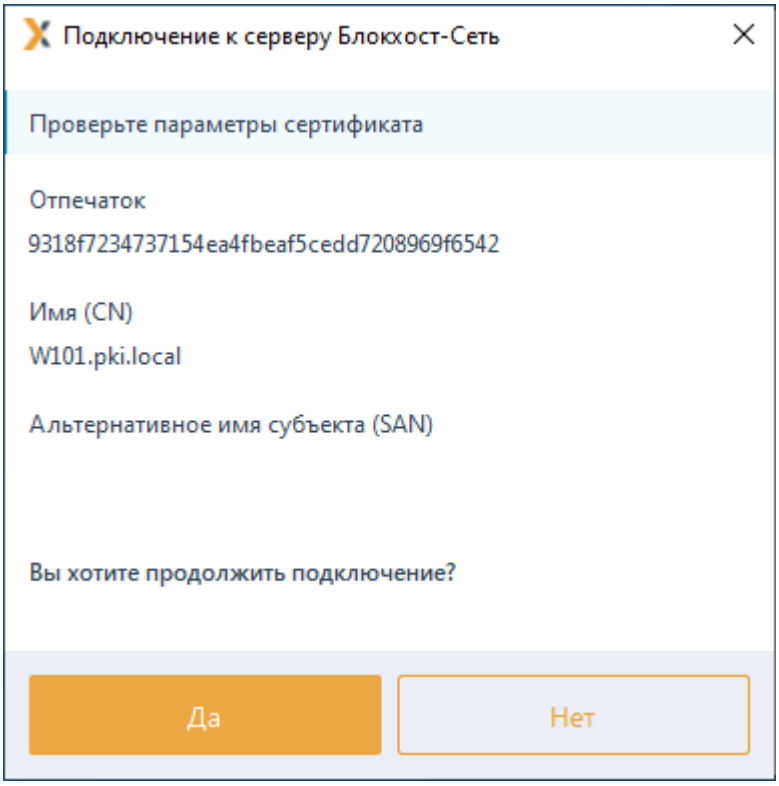


Рисунок 4.27 – Подтверждение продолжения установки

После нажатия кнопки ***Да*** появится главное окно консоли управления СЗИ (рисунок 4.28).

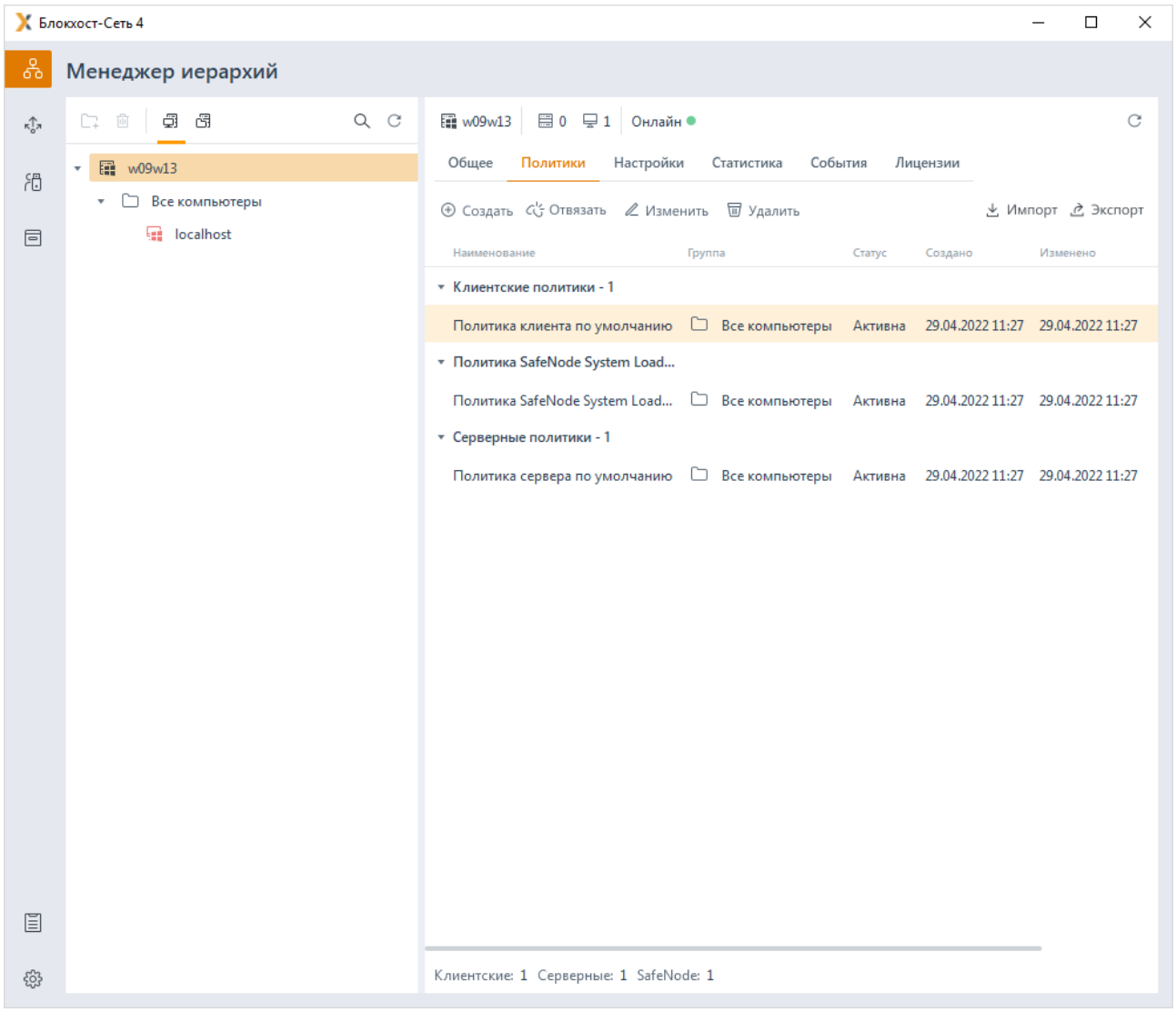


Рисунок 4.28 – Главное окно консоли управления СЗИ

До первого запуска консоли управления необходимо выполнить настройку системы с помощью мастера первоначальной настройки. Если этот шаг был пропущен, при попытке запуска консоли управления появится сообщение о необходимости выполнить первоначальную настройку до запуска консоли (рисунок 4.11).

4.4.2 Особенности подключения к СУБД «Jatoba»

В случае подключения к СУБД «Jatoba», если СУБД «Jatoba» и настраиваемый сервер СЗИ установлены на разных машинах, необходимо вручную сконфигурировать СУБД «Jatoba», чтобы избежать ошибки при открытии базы данных:

```
FATAL: no pg_hba.conf entry for host "<IP адрес>", user "jatobaUser", database "deploymentsystem", SSL off)
```

Для корректного взаимодействия сервера СЗИ с СУБД «Jatoba» необходимо изменить конфигурационный файл ***pg_hba.conf*** по умолчанию расположенный в директории *C:\Program Files\GIS\Jatoba\1\data\pg_hba.conf* добавив в конец файла строку, предоставляющую подключение к СУБД «Jatoba» по сети:

```
host "имя базы данных или all" "имя пользователя или all" " описание сегмента сети, в котором находятся хосты, которым разрешен коннект к СУБД" "md5 - проверка по логину/паролю"
```

например:

```
host all all 172.17.21.0/24 md5
```

После внесения изменений в конфигурационный файл необходимо перезапустить службу базы данных (JatobaServer).

После выполнения указанных действий настройка подключения сервера СЗИ к удаленной СУБД «Jatoba» проходит корректно.

4.5 Настройка входа в консоль управления доменными пользователями

Приведенные настройки необходимо выполнить только в случае подключения доменными пользователями через консоль под управлением ОС Linux к серверу под управлением ОС Windows.

Для входа в консоль управления доменными пользователями необходимо создать SPN и keytab-файл.

SPN (Service Principal Name) – уникальный идентификатор экземпляра сервиса. SPN используется аутентификацией Kerberos для сопоставления экземпляра сервиса с учетной записью сервиса (service logon account). Это позволяет клиентским приложением аутентифицироваться в роли сервиса без имени пользователя.

До того, как аутентификация Kerberos сможет использовать SPN для аутентификации сервиса, SPN должен быть привязан к учетной записи, которая будет использоваться для входа. SPN может быть привязан только к одной учетной записи. Если учетная запись, привязанная к SPN, изменяется, необходимо заново выполнить привязку.

Для того, чтобы воспользоваться сервисом клиент находит экземпляр сервиса и составляет SPN для этого экземпляра, далее использует этот SPN для аутентификации.

Keytab-файл – это файл, содержащий пары Kerberos принципалов и их ключей (полученных с использованием Kerberos пароля). Эти файлы используются для аутентификации в системах, использующих Kerberos, без ввода пароля. Если пароль принципала изменится, то keytab-файл необходимо будет сгенерировать заново.

Каждый имеющий разрешения на чтение keytab-файла может воспользоваться любыми ключами в нем. Для предотвращения нежелательного использования ограничивайте права доступа при создании keytab-файла.

4.5.1 Настройки домена Active Directory

Все команды выполняются в PowerShell на контроллере домена от имени администратора.

Для входа в консоль управления доменными пользователями Active Directory необходимо выполнить следующие действия:

1. Создать на контроллере домена (DC) пользователя, к которому впоследствии будет привязан SPN, например, *bhsconsole*.

2. Запретить созданному пользователю смену пароля и не ограничивать срок действия пароля.

Если ограничить срок действия пароля, при его истечении, потребуется не только изменять пароль, но и заново генерировать keytab-файлы, привязанные к созданному пользователю:

3. В целях безопасности рекомендуется исключить сервисного пользователя из доменных групп.

4. Создать SPN для веб-сервера BHConsoleService/BHConsoleService/rdos1.pki.local и привязать его к пользователю *bhsconsole* (этот шаг делать отдельно не обязательно, т.к. его автоматически выполняет утилита ktpass при создании keytab-файла) с помощью команды:

```
setspn -S BHConsoleService/rdos1.pki.local pki.local\bhsconsole
```

5. Если сервер Блокхост-Сеть установлен на РЕД ОС, необходимо включить дополнительные методы шифрования:

```
Set-ADUser BHConsoleService -KerberosEncryptionType 28
```

где:

BHConsoleService – имя сервисного аккаунта;

28 – типы шифрования (RC4, AES256, AES128).

6. Создать keytab-файл с помощью следующей команды:

```
ktpass -princ BHConsoleService/rdos1.pki.local@PKI.LOCAL -mapuser bhsconsole -crypto ALL -ptype KRB5_NT_PRINCIPAL -pass Gazprom09 -target s09dc.pki.local -out c:\tmp\BHConsoleService.keytab
```

где:

rdos1.pki.local – имя машины на которой установлен сервер Блокхост-Сеть;

pki.local – имя домена;

Gazprom09 – пароль пользователя bhsconsole;

s09dc.pki.local – имя машины доменного контроллера;

c:\tmp\BHConsoleService.keytab – путь куда будет сгенерирован файл.

Перед генерацией нового keytab-файла при полном совпадении пути и имени файла рекомендуется удалить предыдущий keytab-файл.

7. Скопировать keytab-файл на машину с установленным сервером Блокхост-Сеть в папку *C:\BlockHost\DeploymentSystem* для ОС семейства Windows или */opt/Blockhost/server* для ОС семейства Linux.

8. Перезапустить службу *gis_server_consoleservice*.

9. Удалить keytab-файл с контроллера домена.

10. Создать отдельного пользователя и повторить все предыдущие шаги для каждого сервера Блокхост-Сеть.

11. До входа на сервер Блокхост-Сеть выдать права на вход для доменных пользователей в серверной политике.

4.5.2 Настройки домена FreeIPA

Для входа в консоль управления доменными пользователями FreeIPA необходимо выполнить следующие действия:

1. Для добавления SPN в веб-интерфейсе сервера FreeIPA выбрать «Идентификация» → «Службы» и нажать кнопку «Добавить» «Identity» → «Services» → «Add» (рисунок 4.29).

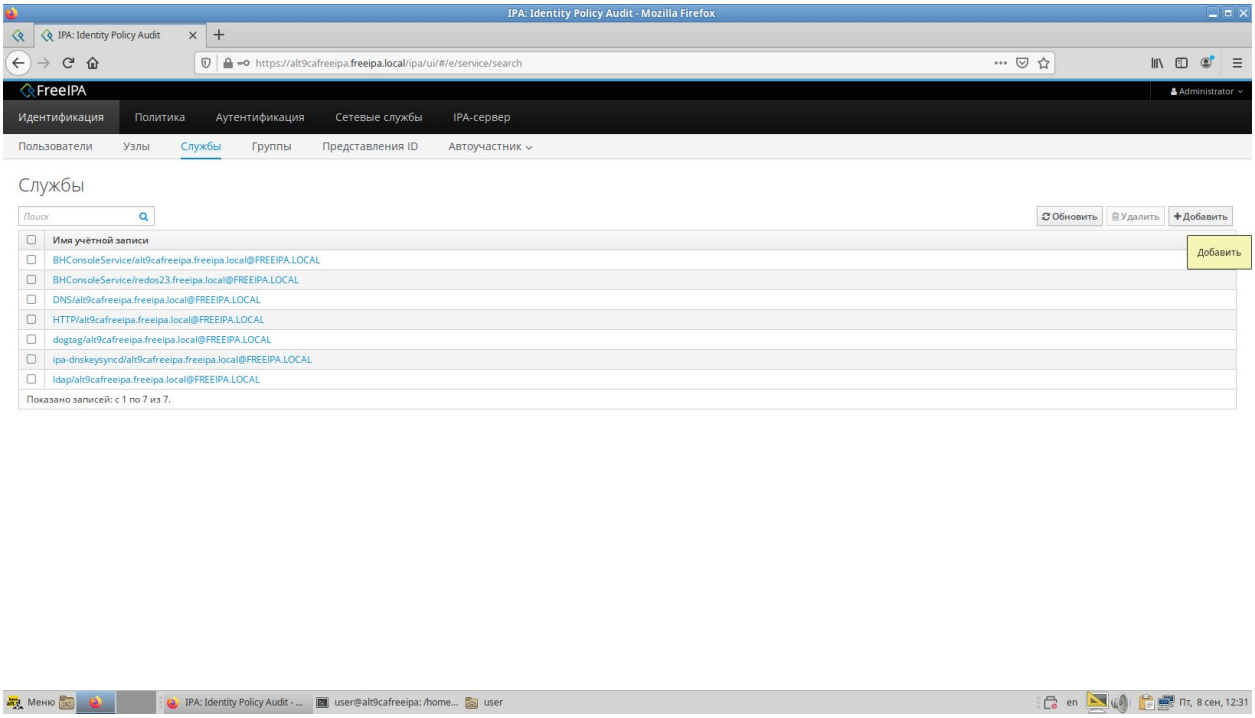


Рисунок 4.29 – Добавление SPN в веб-интерфейсе FreeIPA

2. В открывшемся окне выбрать имя сервиса и имя узла, к которому будет привязан сервис (рисунок 4.30).

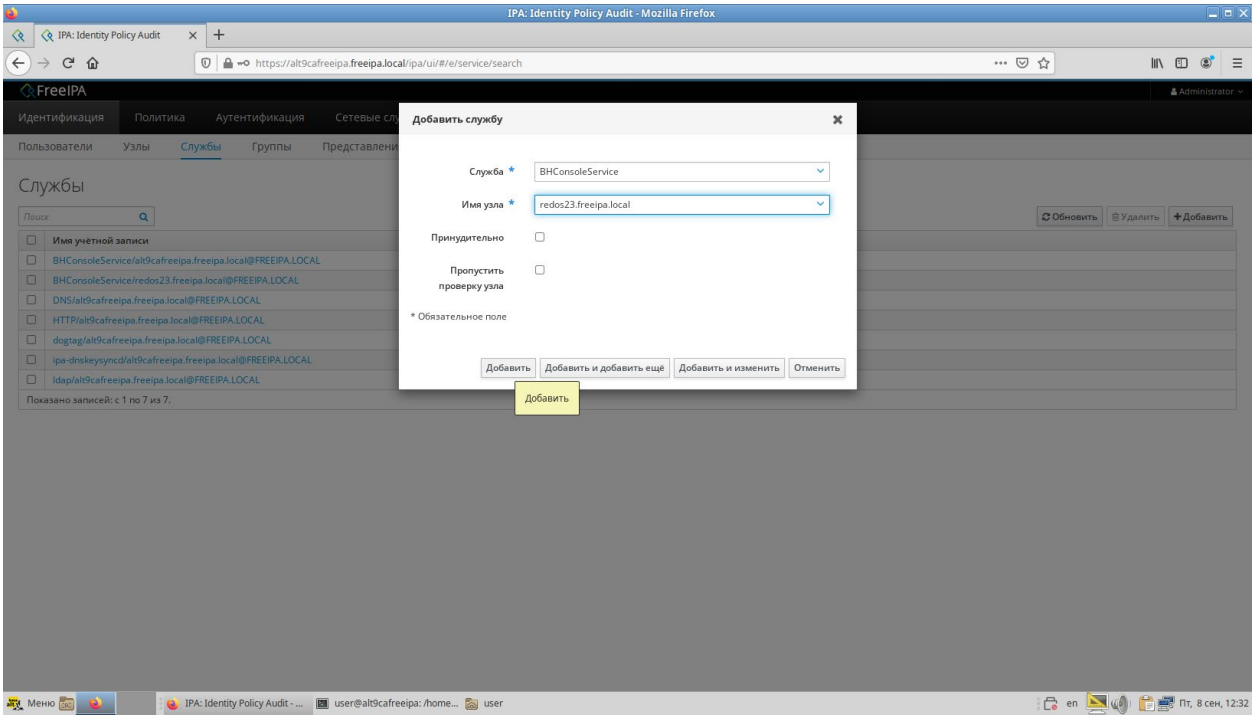


Рисунок 4.30 – Выбор имени сервиса и имени узла

3. Повысить привилегии с помощью команды:

```
sudo -i
```

4. Получить билет администратора домена:

```
kinit admin
```

где:

admin – доменный администратор.

5. Добавить сервисный аккаунт:

```
ipa service-add BHConsoleService/alt103.freeipa.local@FREEIPA.LOCAL
```

где:

alt103.freeipa.local – имя машины на которой установлен сервер Блокхост-Сеть;

@FREEIPA.LOCAL – имя домена (прописными буквами).

6. Сгенерировать keytab-файл с помощью команды:

```
ipa-getkeytab -p BHConsoleService/alt103.freeipa.local@FREEIPA.LOCAL -k /tmp/BHConsoleService.keytab
```

где:

BHConsoleService/alt103.freeipa.local@FREEIPA.LOCAL – имя сервиса из предыдущего шага;

/tmp/BHConsoleService.keytab – имя и путь сохранения keytab файла.

Перед генерацией нового keytab-файла при полном совпадении пути и имени файла рекомендуется удалить предыдущий keytab-файл.

7. Скопировать keytab-файл на машину с установленным сервером Блокхост-Сеть в папку */opt/Blockhost/server*.

8. Перезапустить службу *gis_server_consoleservice*.

```
sudo systemctl restart gis_server_consoleservice
```

9. Удалить keytab-файл с контроллера домена.

10. Повторить все предыдущие шаги для каждого сервера Блокхост-Сеть.

11. До входа на сервер Блокхост-Сеть выдать права на вход для доменных пользователей в серверной политике.

4.5.3 Настройки домена SAMBA

Для входа в консоль управления доменными пользователями SAMBA необходимо выполнить следующие действия:

1. Создать на контроллере домена пользователя *BHConsoleService* любым удобным способом и выставить «Password never expires»:

```
sudo samba-tool user create --random-password BHConsoleService
sudo samba-tool user setexpiry BHConsoleService --noexpiry
```

2. Задать SPN с помощью команды:

```
sudo samba-tool spn add BHConsoleService/alt103.domain.test BHConsoleService
```

где:

alt103.domain.test – имя машины на которой установлен сервер Блокхост-Сеть;

BHConsoleService – имя сервисного аккаунта из шага 1.

3. Если сервер Блокхост-Сеть установлен на РЕД ОС, необходимо включить дополнительные методы шифрования:

```
kinit Administrator
```

где:

Administrator – администратор домена.

```
net ads enctypes set BHConsoleService 28
```

где:

BHConsoleService – имя сервисного аккаунта;

28 – типы шифрования (RC4, AES256, AES128).

4. Создать keytab-файл с помощью следующей команды:

```
sudo samba-tool domain exportkeytab /tmp/BHConsoleService.keytab --principal BHConsoleService/alt103.domain.test@DOMAIN.TEST
```

где:

/tmp/BHConsoleService.keytab – путь сохранения и имя keytab файла

BHConsoleService/alt103.domain.test@DOMAIN.TEST – SPN из шага 2 с указанием домена прописными буквами (realm).

5. Скопировать keytab-файл на машину с установленным сервером Блокхост-Сеть в папку *C:\BlockHost\DeploymentSystem* для ОС семейства Windows или */opt/Blockhost/server* для ОС семейства Linux.

6. Перезапустить службу *gis_server_consoleservice*.

```
sudo systemctl restart gis_server_consoleservice
```

7. Удалить keytab-файл с контроллера домена.

8. Создать отдельного пользователя и повторить все предыдущие шаги для каждого сервера Блокхост-Сеть.

9. До входа на сервер Блокхост-Сеть выдать права на вход для доменных пользователей в серверной политике.

4.5.4 Общие рекомендации по настройке домена

Рекомендуется добавить два SPN – для полного (alt103.domain.test) и короткого (alt103) имени сервера.

Рекомендуется добавить поддержку современных методов шифрования, даже если РЕД ОС не используется в качестве сервера Блокхост-Сеть.

Рекомендуется ограничить доступ к keytab-файлу.

4.5.5 Разрешение возможных ошибочных ситуаций

Ошибка	Возможные пути решения

"На узле нет соответствующей записи DNS A/AAAA" при добавления SPN	**Решение**: на РЕД ОС отредактировать /etc/sssd/sssd.conf:
	`pluma /etc/sssd/sssd.conf`
	добавить:
	# Включить обновление прямых записей (A/AAAA записей):
	`dyndns_update = true`
	# Включить обновление обратных записей (PTR записей):
	`dyndns_update_ptr = true`
	# Интервал обновления в секундах. По умолчанию - 0, и обновление выполняется только один раз при запуске службы SSSD.

	# Если интервал менее 60 секунд, то обновление выполняется раз в 60 секунд. # Если адрес после предыдущего обновления не изменялся - обновление не выполняется. `dyndns_refresh_interval = 60`
Предупреждение о невозможности записать UPN для учетной записи bhsconsole: *Failed to set property 'userPrincipalName' to...*	**Решение**: включить bhsconsole в группу Domain Admins.
При подключении к консоли выводится ошибка *"KDC has no support for encryption type"*.	**Решение**: для bhsconsole в оснастке "Active Directory Users Nad Computers" выставить параметры *"This account supports Kerberos AES 128bit encryption"* и *"This account supports Kerberos AES 256bit encryption".*
При подключении к консоли выводится ошибка *"Socket connect Failed"*	**Причина**: отсутствует keytab-файл или он не подхвачен сервисом gis_server_consoleservice . **Решение**: создать и установить keytab по инструкции (на каждую машину создается свой keytab). **Внимание:** при добавлении/замене keytab-файла нужно перезапустить сервис gis_server_consoleservice или перезагрузить машину.
При подключении к консоли выводится ошибка *"Krb5 sendauth error: Server not found in Kerberos database..*	**Причина**: Krb5 не может подключиться по указанному адресу сервера. **Решение**: использовать DNS имя машины или отредактировать hosts.
При подключении к консоли выводится ошибка *"krb5 sendauth error: Bad SAM flags in obtain_sam_padata (KRB5_SAM_UNSUPPORTED"*	В протоколе krb5 ошибка: error-code: eRR-S-PRINCIPAL-UNKNOWN (7) **Причина**: скорее всего не было найдено соответствие SPN. На сервере запись вида BHConsoleService/astra17.pki.local. На клиенте билет формировался с записью вида BHConsoleService/astra17. **Решение**: формировать SPN на клиенте корректно (наш баг) или (обходной путь) на kdc добавить необходимую запись для этого пользователя (setspn -S)
SAMBA. При подключении к консоли выводится ошибка *"krb5 sendauth error:*	**Причина**: некорректная запись пользователя - для bhsconsole в оснастке "Active Directory Users Nad

Unsupported pre-authentification type..."	Computers", вкладка "Account", поле "User logon name" имеет значение "bhsconsole". **Решение**: для bhsconsole в оснастке "Active Directory Users Nad Computers", вкладка "Account", поле "User logon name" установить в "BHConsoleService/pc43.domain.test" где: pc43.domain.test – имя хоста где установлен сервер Блокхост-Сеть и keytab-файл.

4.6 Установка агента системы развертывания

Установка агента системы развертывания на рабочую станцию может быть выполнена несколькими способами:

– в серверной консоли управления с использованием функциональных возможностей подсистемы развертывания;

– локально на рабочей станции с использованием мастера установки клиентской части СЗИ;

– с использованием сторонних систем развертывания.

4.6.1 Установка агента системы развертывания с помощью серверной консоли управления

При установке серверной части СЗИ автоматически создаются задачи на установку агента развертывания и клиента Блокхост-Сеть на клиентские рабочие станции. Для настройки взаимодействия между сервером СЗИ и клиентскими рабочими станциями необходимо последовательно выполнить задачи на установку агента развертывания на требуемых клиентских рабочих станциях и на установку клиента Блокхост-Сеть.

Агент системы развертывания устанавливается на рабочую станцию с помощью пакета установки ***Агент системы развертывания <номер версии>*** (*BHNetDeploymentAgent <номер версии>.msi*).

Подробно установка агента системы развертывания с помощью серверной консоли управления описана в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит».

4.6.2 Локальная установка агента системы развертывания

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

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

Откроется окно приветствия мастера установки агента развертывания (рисунок 4.31). Для продолжения установки агента нажмите кнопку ***Далее***.

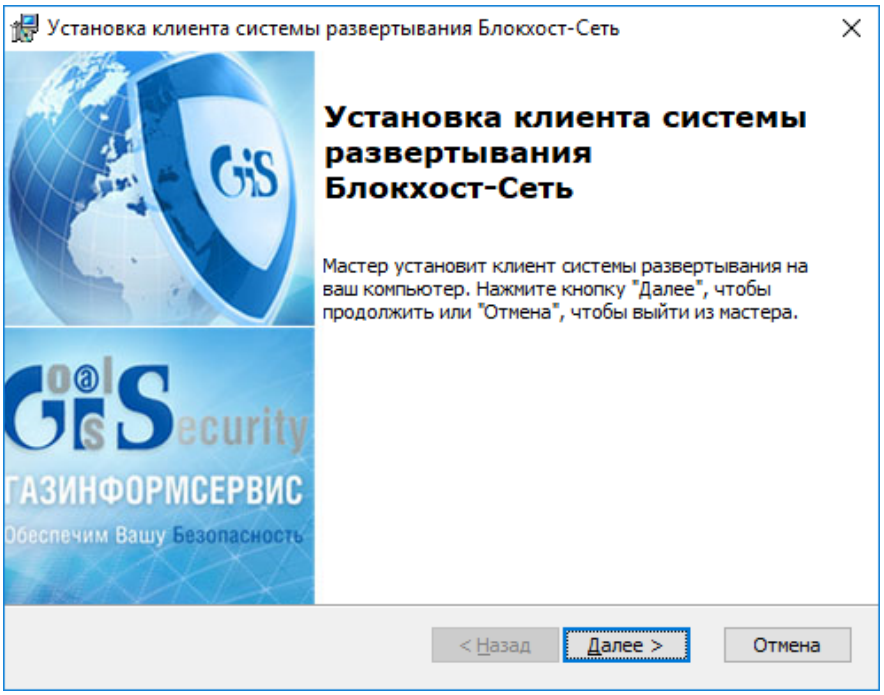


Рисунок 4.31 – Окно мастера установки агента развертывания

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 4.2.

Установка агента развертывания будет прервана (рисунок 4.13). 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 повторно.

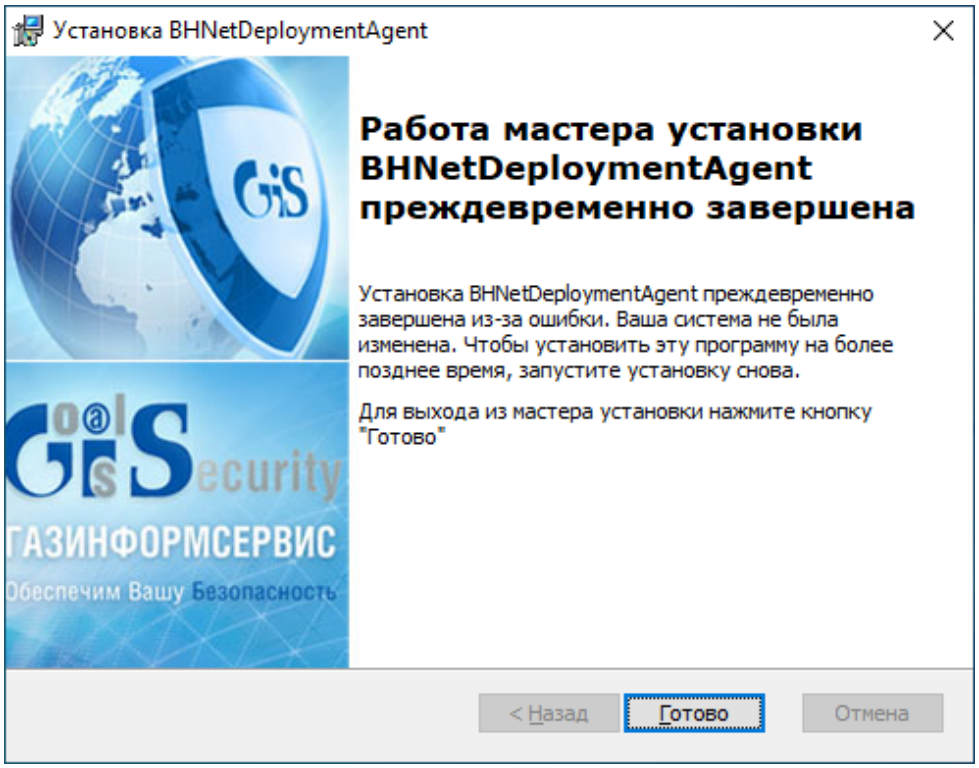


Рисунок 4.32 – Работа мастера установки преждевременно завершена

В следующем диалоговом окне (рисунок 4.33) выбирается директория для установки агента. При необходимости изменить указанный по умолчанию каталог установки, нажмите кнопку ***Обзор*** и укажите нужную директорию.

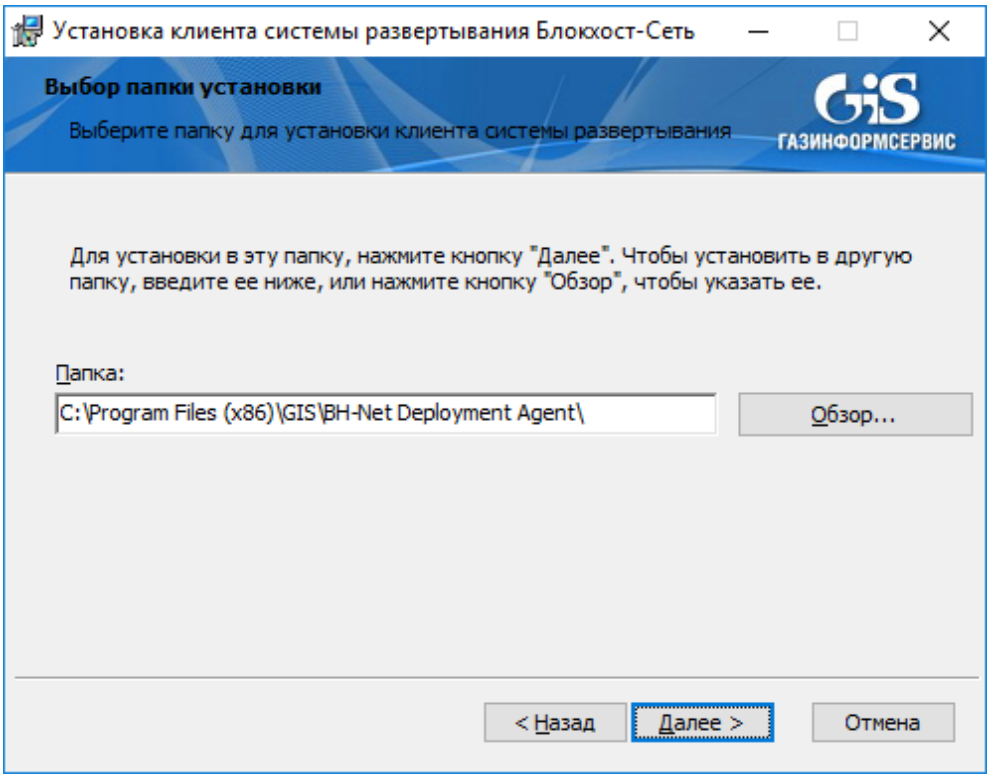


Рисунок 4.33 – Диалоговое окно выбора каталога установки программы

После нажатия кнопки ***Далее*** в открывшемся окне установите настройки параметров подключения агента развертывания к серверу СЗИ (рисунок 4.34), включающие IP-адрес и TCP-порт сервера СЗИ, к которому будет подключаться агент. По умолчанию в окне указан локальный адрес и TCP-порт сервера, на который был сгенерирован инсталляционный пакет.

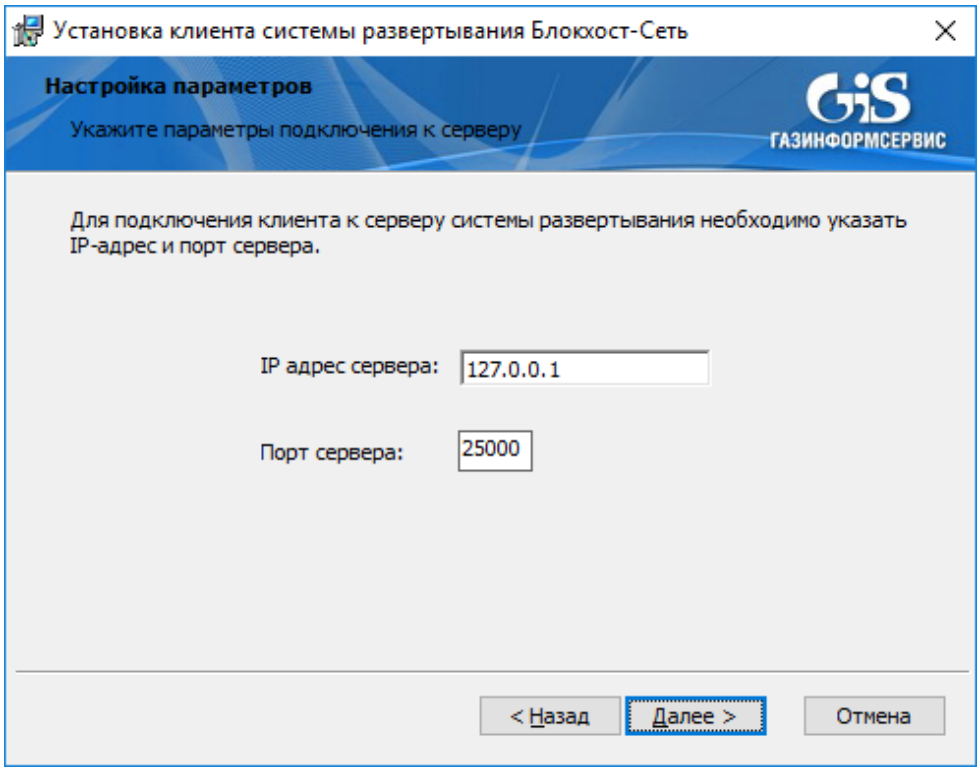


Рисунок 4.34 – Диалоговое окно ввода параметров подключения агента к серверу СЗИ

После нажатия кнопки ***Далее*** откроется диалоговое окно готовности мастера к установке (рисунок 4.35). По кнопке ***Установить*** начнется фактическая установка агента развертывания на рабочую станцию.

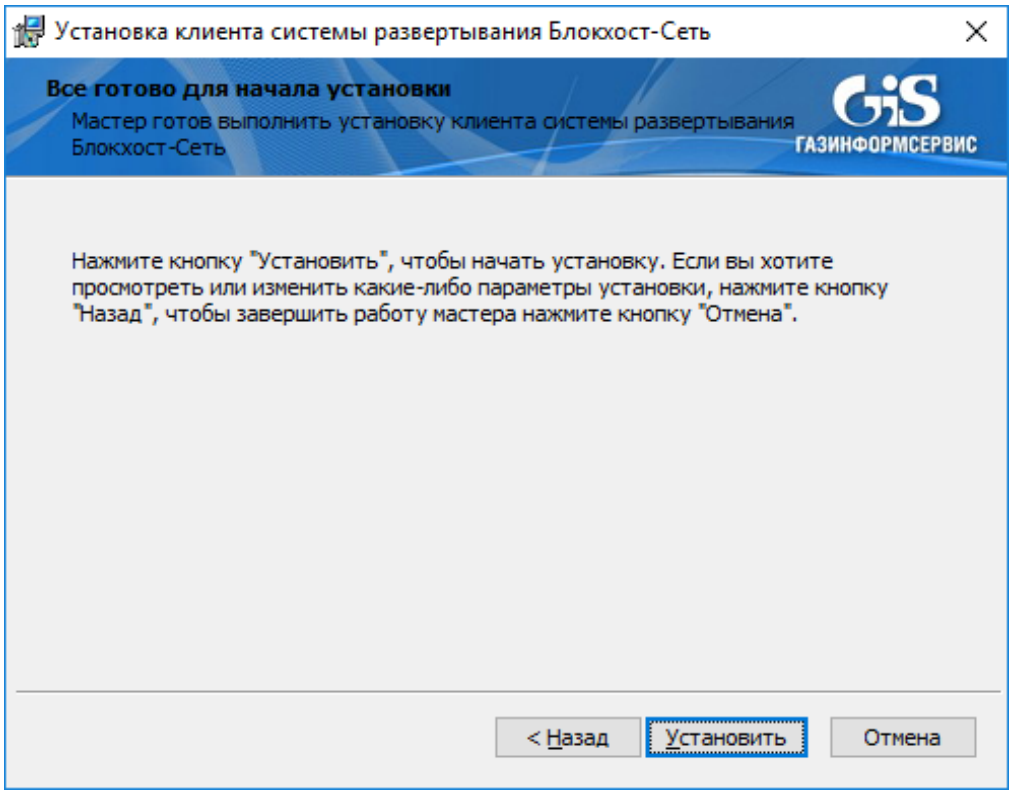


Рисунок 4.35 – Диалоговое окно готовности мастера к установке

По окончанию установки появится окна завершения работы мастера установки, в котором необходимо нажать кнопку ***Готово*** (рисунок 4.36).

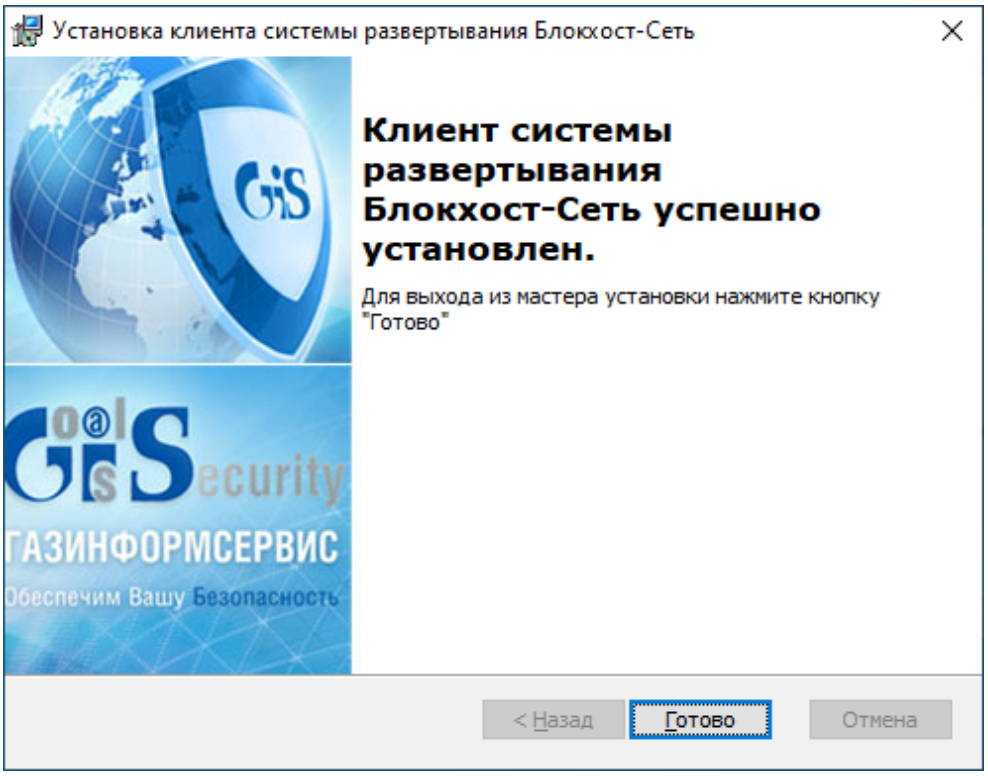


Рисунок 4.36 – Окно завершения установки агента развертывания

После завершения установки на рабочей станции будет установлен агент системы развертывания, не имеющий оконного интерфейса.

4.6.3 Установка агента развертывания с помощью сторонних систем развертывания

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

4.7 Установка клиентской части СЗИ

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

– с помощью консоли управления;

– локально на рабочей станции с использованием мастера установки клиентской части СЗИ;

– с помощью сторонних систем развертывания.

4.7.1 Установка клиентской части СЗИ с помощью консоли управления

При установке серверной части СЗИ автоматически создаются задачи на установку агента развертывания и клиента Блокхост-Сеть на клиентские рабочие станции. Для настройки взаимодействия между сервером СЗИ и клиентскими рабочими станциями необходимо последовательно выполнить задачи на установку агента развертывания на требуемых клиентских рабочих станциях и на установку клиента Блокхост-Сеть.

Клиентская часть СЗИ устанавливается на рабочую станцию с помощью пакета установки ***Клиент Блокхост-Сеть <номер версии>*** (*BhNet.Installer.exe*), который содержит в себе инсталляторы для 32- и 64-разрядных ОС Windows.

Подробно установка клиентской части СЗИ с помощью консоли управления описана в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит».

4.7.2 Локальная установка клиентской части СЗИ

Перед локальной установкой клиентской части СЗИ с использованием мастера установки необходимо сформировать автономный пакет установки клиентской части СЗИ. Автономный пакет установки клиента создается с помощью системы развертывания в консоли управления.

Для формирования автономного пакета перейдите во вкладку ***Пакеты установки*** по кнопке , выберите из списка дистрибутив, содержащий установку клиента Блокхост-Сеть ***Клиент Блокхост-Сеть <номер версии>*** (*BhNet.Installer.exe*) и нажмите на кнопку Создать автономный пакет установки (рисунок 4.37), укажите каталог, в который будет сохранен подготовленный пакет и нажмите кнопку ***Подготовить***.

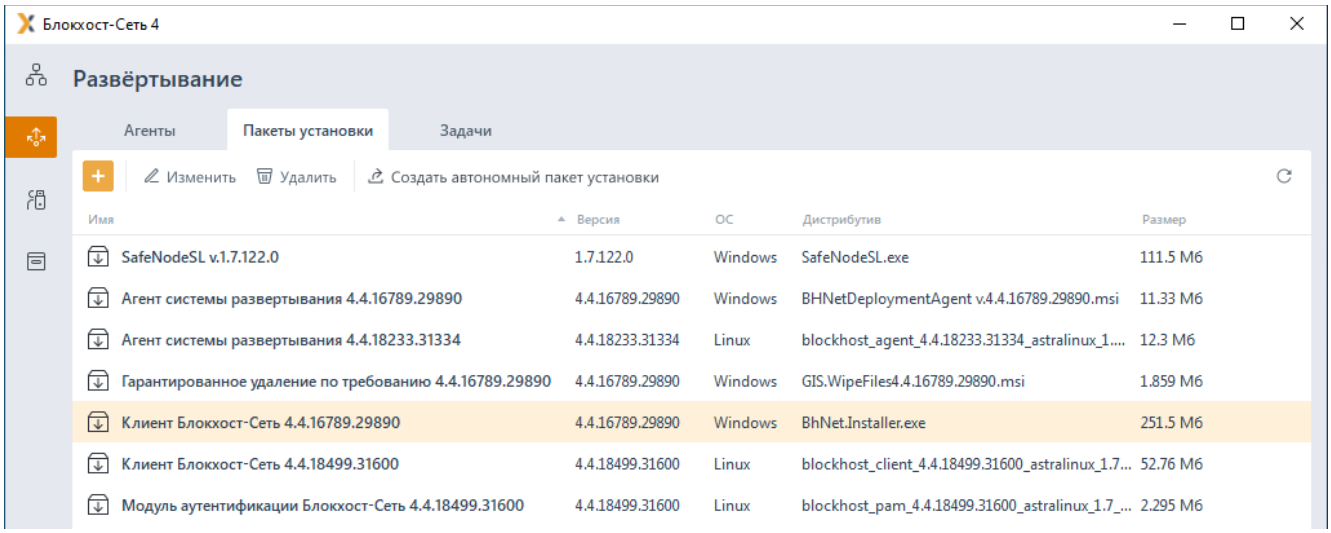


Рисунок 4.37 – Подготовка автономного пакета клиентской части СЗИ

В случае успешного завершения операции подготовки дистрибутива появится окно, содержащее директорию и наименование подготовленного пакета установки (рисунок 4.38).

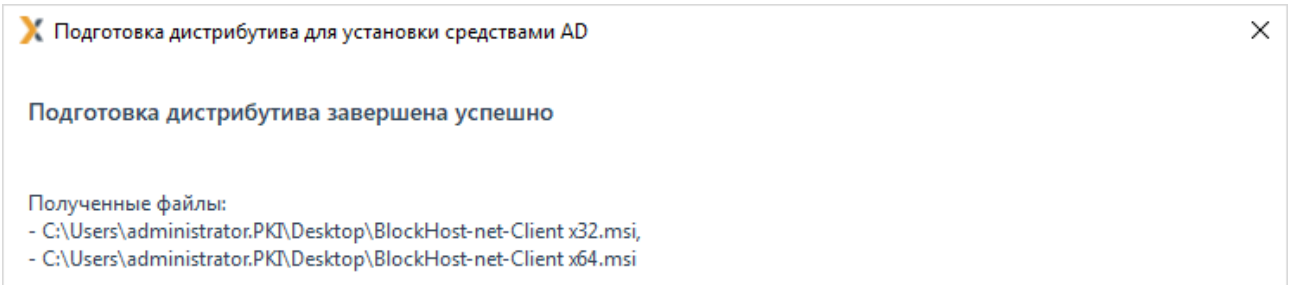


Рисунок 4.38 – Сформированные автономные пакеты

Выберите пакет установки в соответствии с разрядностью используемой ОС (*BlockHost-net-Client x64.msi* или *BlockHost-net-Client x32.msi*), скопируйте пакет установки клиента на рабочую станцию (или съемный носитель), войдите в ОС рабочей станции под учетной записью, имеющей административные права (состоящей в локальной группе **Администраторы**) и запустите автономный пакет на выполнение.

Перед установкой клиентской части СЗИ необходимо убедиться в выполнении всех требований к установке, описанных в подразделе ***«Требования к аппаратному и программному обеспечению»*** настоящего документа.

В результате запуска файла-установщика на экране монитора появится окно приветствия мастера установки клиентской части СЗИ от НСД «Блокхост-Сеть 4» (рисунок 4.39).

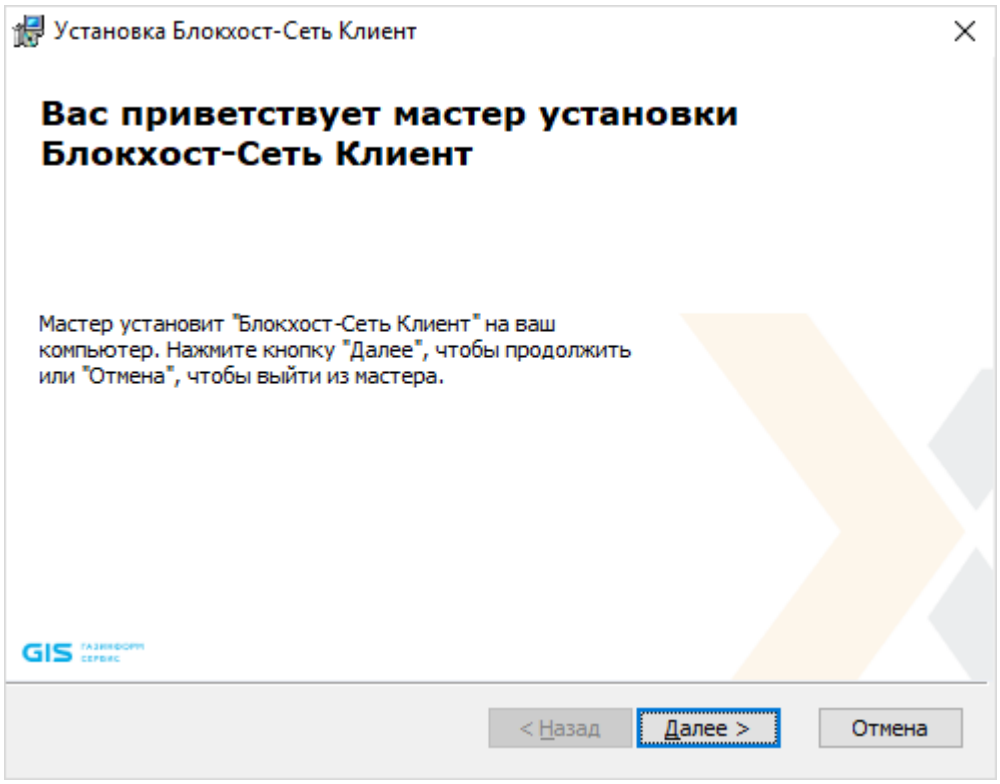


Рисунок 4.39 – Окно установки клиентской части СЗИ

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 4.2.

Установка клиента будет прервана (рисунок 4.40). 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 повторно.

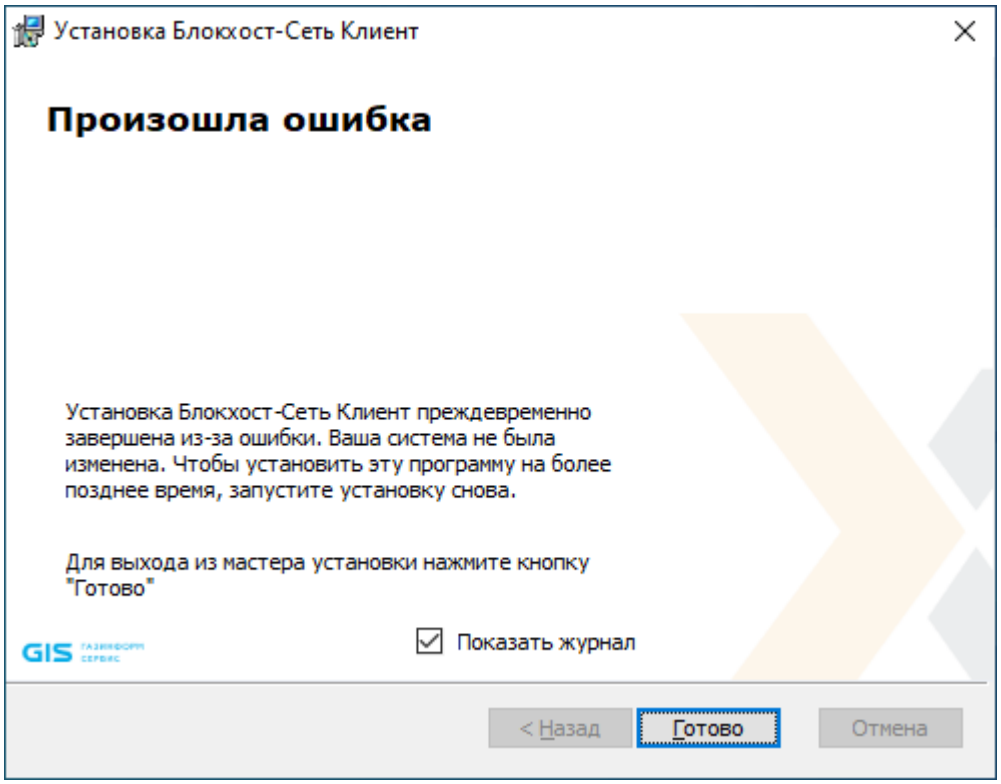


Рисунок 4.40 – Работа мастера установки преждевременно завершена

При установленном флаге «***Показать журнал***», после нажатия кнопки ***Готово*** откроется окно лога инсталлятора, содержащее ошибки, выявленные при установке СЗИ от НСД «Блокхост-Сеть 4».

После нажатия в окне приветствия мастера установки СЗИ кнопки ***Далее*** (рисунок 4.39) появится окно, в котором необходимо выбрать тип установки СЗИ от НСД «Блокхост-Сеть 4» (рисунок 4.41):

– *обычная* – установка только основных компонент, необходимых для функционирования СЗИ;

– *выборочная* – установка выборочных компонент СЗИ из списка (рисунок 4.42).

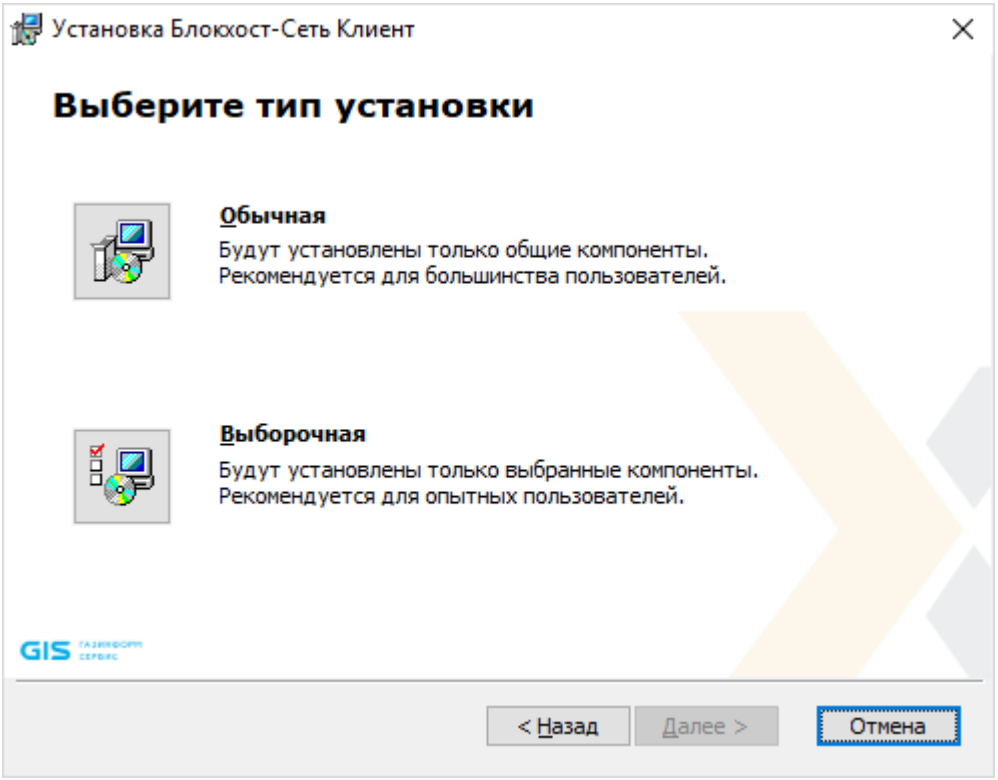


Рисунок 4.41 – Выбор типа установки СЗИ

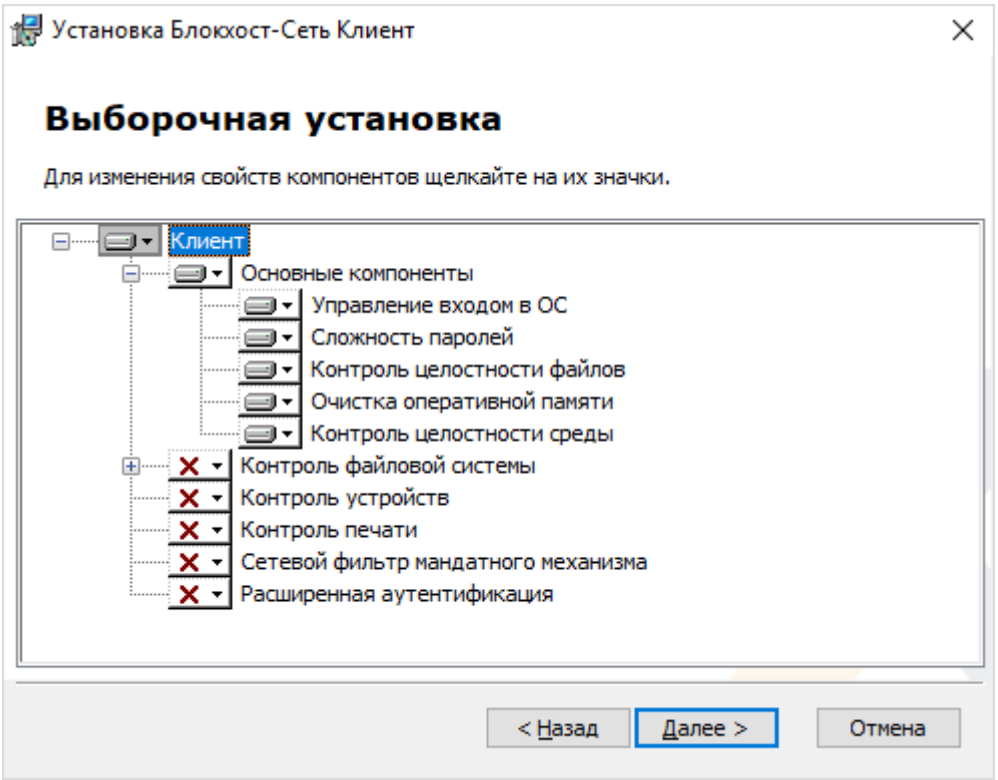


Рисунок 4.42 – Выбор компонент для установки

Для выбора доступны следующие компоненты:

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

- *Аудит доступа к медиафайлам* – контроль доступа к определённым типам файлов: аудиофайлам, видеофайлам и изображениям, путем регистрации событий аудита;
- *Аудит запуска приложений* – контроль отслеживания запуска и прекращения работы исполняемых файлов;
- *Гарантированное удаление файлов* - удаление объектов файловой системы с системных и не системных дисков без возможности их дальнейшего восстановления;
- *Дискреционный доступ* - настройка доступа всех пользователей к объектам файловой системы;
- *Замкнутая программная среда* – формирование списка разрешенных для запуска процессов, доступных для пользователя на клиентской рабочей станции;
- *Мандатный доступ* - разграничение доступа субъектов к объектам путем сочетания назначенных субъектам и объектам допуска квалификационных меток и неиерархических категорий;

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

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

– ***Сетевой фильтр мандатного механизма*** – необходим при использовании мандатного разграничения доступа;

– ***Расширенная аутентификация*** – расширенные настройки механизма аутентификации, позволяющие проводить двухфакторную аутентификацию по сети и разграничивать доступ на уровне создания сессии пользователя[5].

После выбора необходимого типа установки и нажатия кнопки ***Далее*** появится окно, содержащее текст лицензионного соглашения (рисунок 4.43). Для продолжения установки необходимо ознакомиться с лицензионным соглашением на устанавливаемый продукт и принять условия лицензионного соглашения.

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

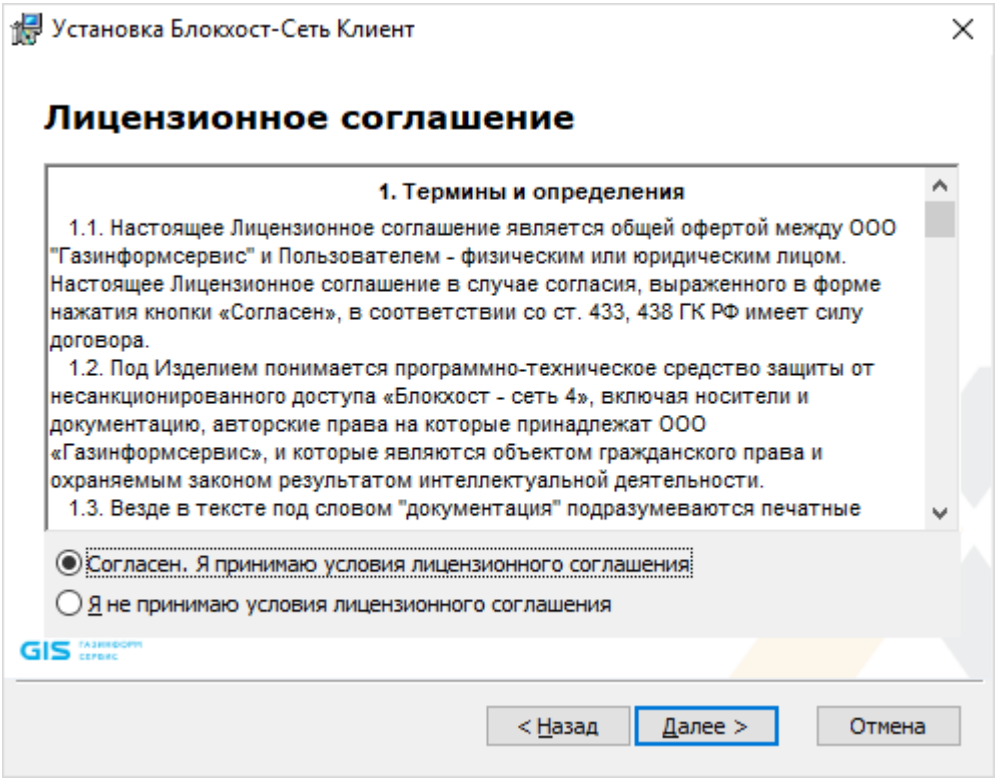


Рисунок 4.43 – Лицензионное соглашение

После принятия соглашения и нажатия кнопки ***Далее*** появится окно, позволяющее задать пароль для встроенной учетной записи администратора (рисунок 4.44).

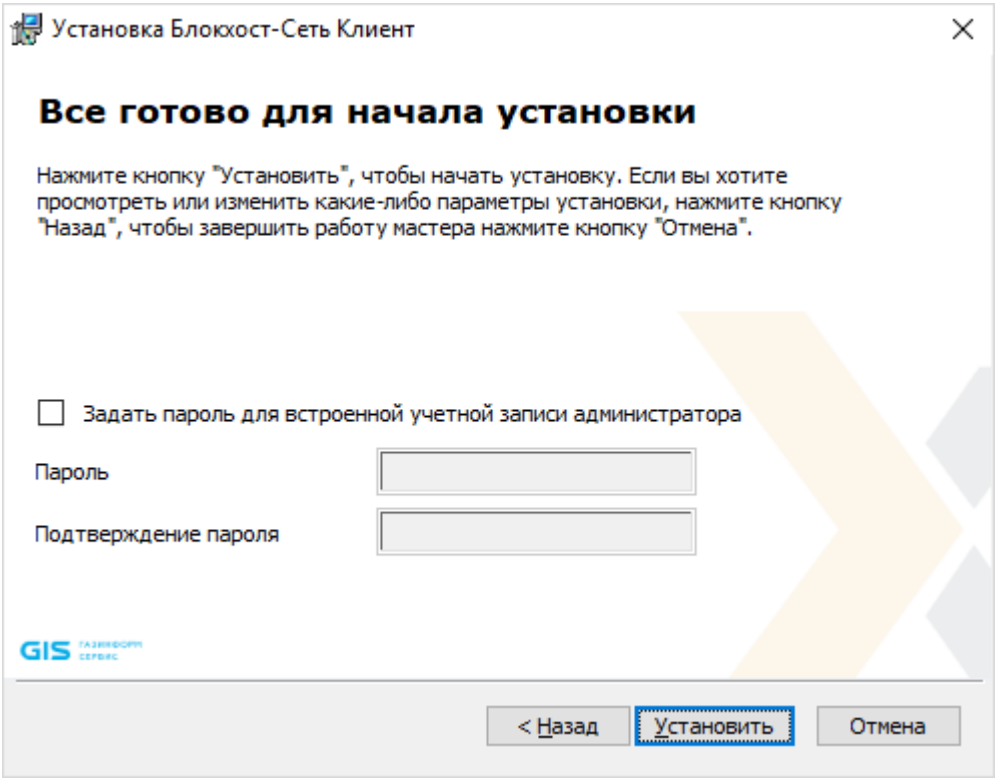


Рисунок 4.44 – Окно готовности к установке СЗИ от НСД «Блокхост-Сеть 4»

После нажатия кнопки ***Установить*** начнется процесс установки СЗИ от НСД «Блокхост-Сеть 4» (рисунок 4.45).

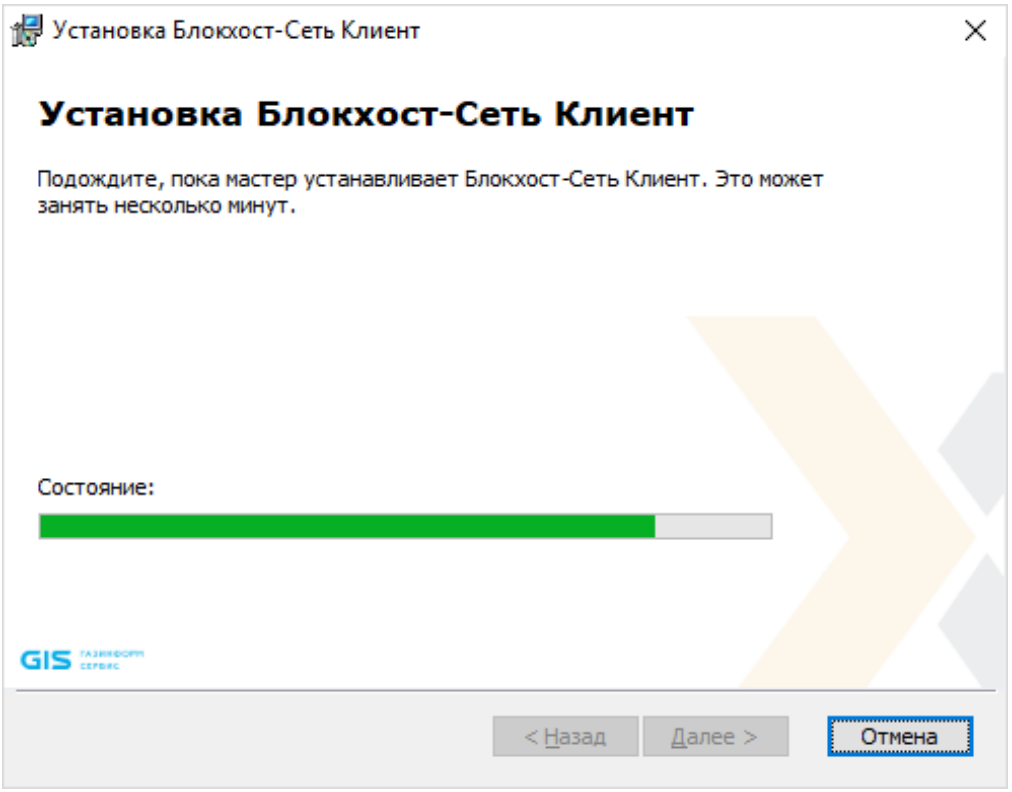


Рисунок 4.45 – Ход установки СЗИ от НСД «Блокхост-Сеть 4»

При успешном завершении установки появится окно окончания работы мастера установки СЗИ (рисунок 4.46) в котором необходимо нажать кнопку ***Готово***.

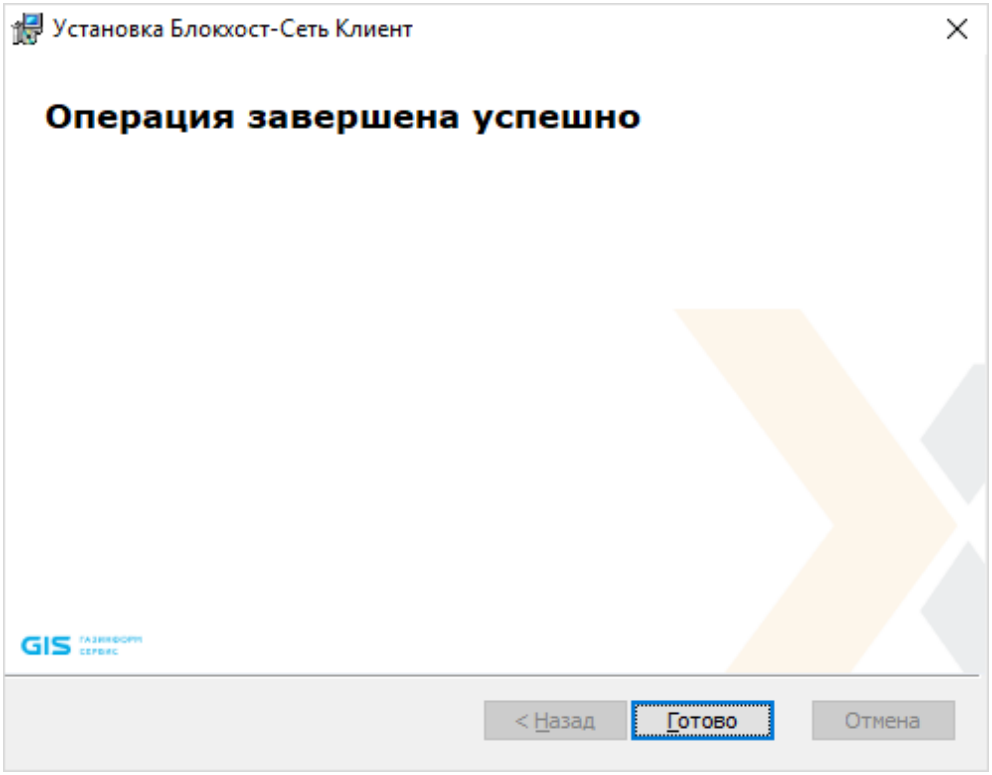


Рисунок 4.46 – Окно окончания установки клиентской части СЗИ от НСД «Блокхост-Сеть 4»

Для завершения установки клиента необходимо перезагрузить компьютер. Перезагрузка доступна сразу после окончания работы мастера установки клиентской части, по нажатию кнопки ***Да*** в окне на рисунке 4.47, или позднее вручную, для этого нужно отказаться от перезагрузки, нажав кнопку ***Нет*** в окне на рисунке 4.47.

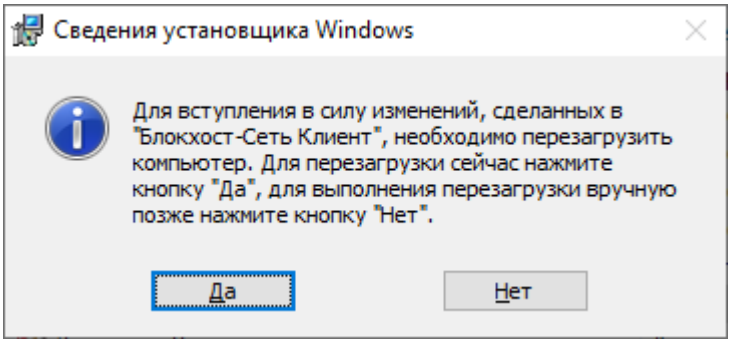


Рисунок 4.47 – Подтверждение выполнения перезагрузки рабочей станции

После завершения установки на рабочей станции будет установлена клиентская часть СЗИ не имеющая оконного интерфейса. Управление клиентами СЗИ доступно из консоли управления.

4.7.3 Установка клиентской части СЗИ с помощью сторонних систем развертывания

Установка клиентской части СЗИ от НСД «Блокхост-Сеть 4» с использованием

сторонних систем развертывания осуществляется только после подготовки файла-установщика для развертывания средствами Active Directory (AD) в консоли управления (подробнее в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развёртывание и аудит»).

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

5 Деинсталляция СЗИ от НСД «Блокхост-Сеть 4»

Удаление автономного варианта СЗИ от НСД «Блокхост-Сеть 4» или серверной части СЗИ при использовании варианта с удаленным управлением описано в разделе 5.1 «Деинсталляция серверной части СЗИ» настоящего документа.

Удаление агента системы развертывания описано в разделе 5.2 «Деинсталляция агента развертывания» настоящего документа.

Удаление клиентской части СЗИ при использовании варианта с удаленным управлением описано в разделе 5.3 «Деинсталляция клиентской части СЗИ» настоящего документа.

Удаление консоли управления СЗИ при использовании варианта с удаленным управлением описано в разделе 5.4 «Деинсталляция консоли управления» настоящего документа.

Удаление модуля расширенной аутентификации выполняется с помощью создания задачи на удаление программы, подробное описание см. в разделе 8.2 «Удаление программы» документа «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит».

Удаление гарантированного удаления по требованию описано в разделе 3 «Деинсталляция подсистемы ГУПТ» документа Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 6. Подсистема ГУПТ».

5.1 Деинсталляция серверной части СЗИ

Удаление серверной части СЗИ от НСД «Блокхост-Сеть 4» 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 Сервер*** и нажать кнопку ***Удалить***.

В результате запустится мастер удаления серверной части СЗИ с рабочей станции (рисунок 5.1). Для продолжения удаления в окне необходимо нажать ***Далее***.

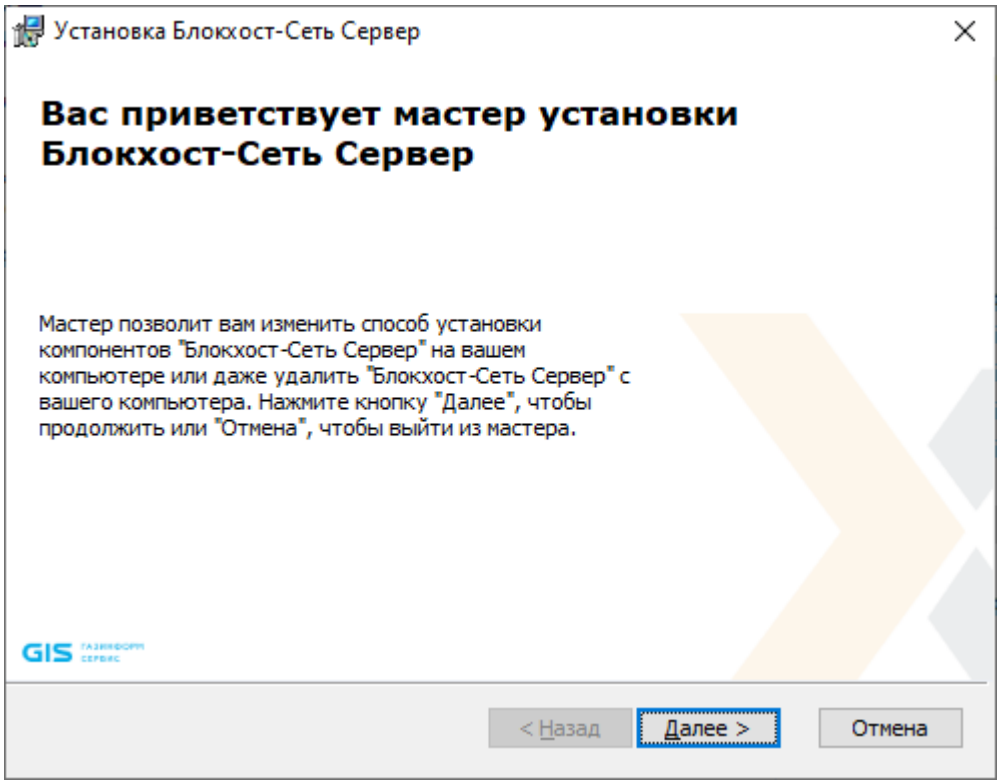


Рисунок 5.1 – Запуск мастер удаления серверной части СЗИ

Если мастеру удаления СЗИ не удалось остановить работающие службы, откроется окно с сообщением об ошибке остановки этих приложений.

После нажатия кнопки ***ОК*** (рисунок 5.2) начнется процесс удаления серверной части СЗИ.

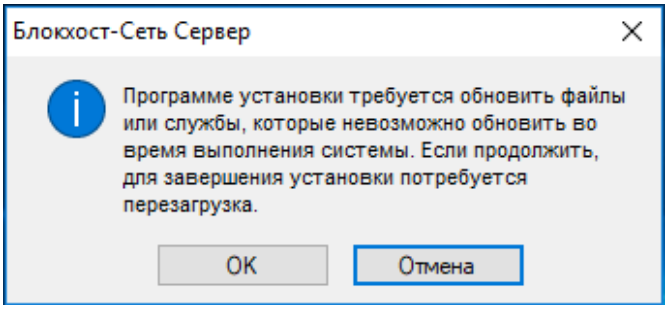


Рисунок 5.2 – Предупреждение об ошибке остановки работающих служб СЗИ

В следующем окне (рисунок 5.3) необходимо выбрать операцию удаления.

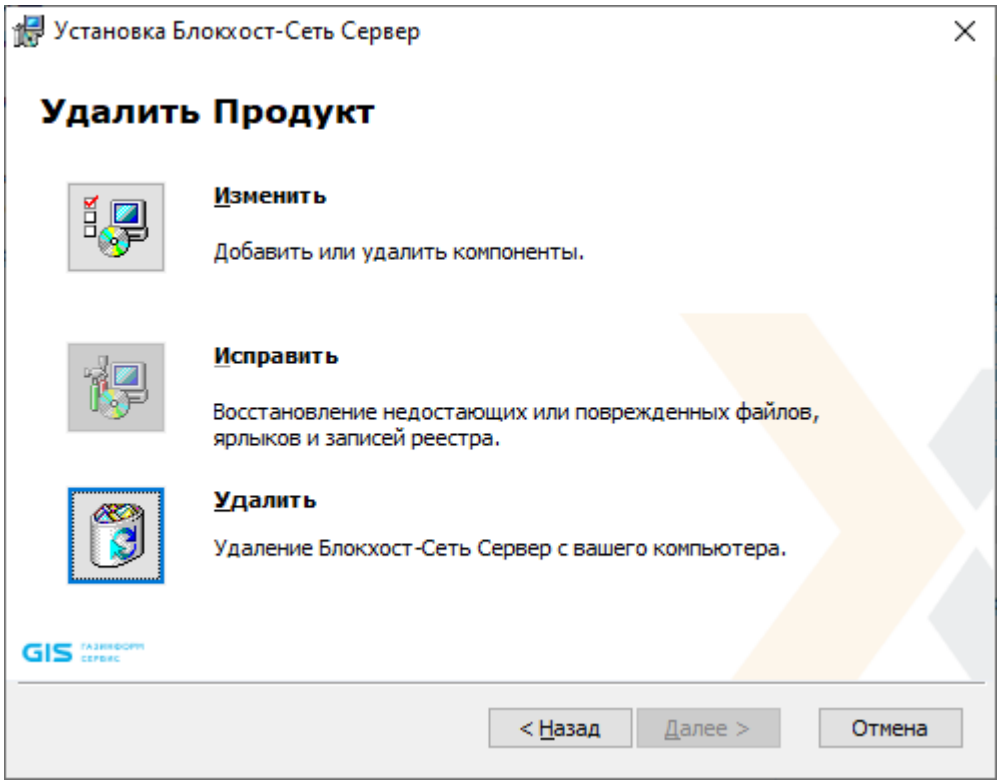


Рисунок 5.3 – Выбор операции удаления серверной части СЗИ

Для подтверждения удаления серверной части СЗИ необходимо ввести пароль встроенной учетной записи администратора, заданный при установке продукта (рисунок 5.4).

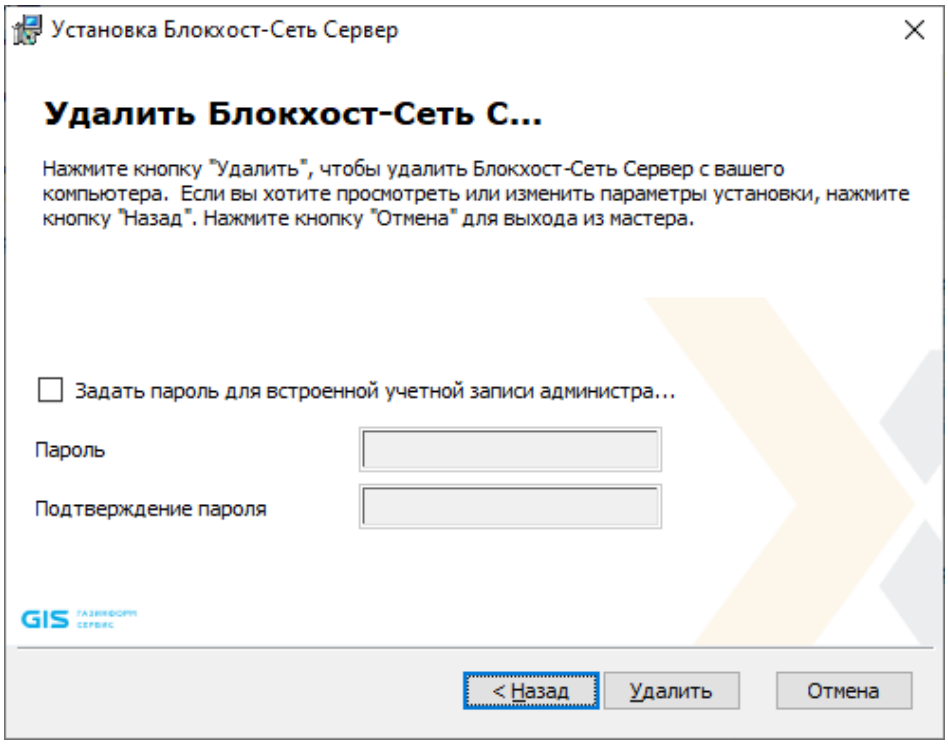


Рисунок 5.4 – Ввод учетных данных встроенного администратора

После нажатия кнопки ***Удалить*** (рисунок 5.5) начнется процесс удаления серверной части СЗИ.

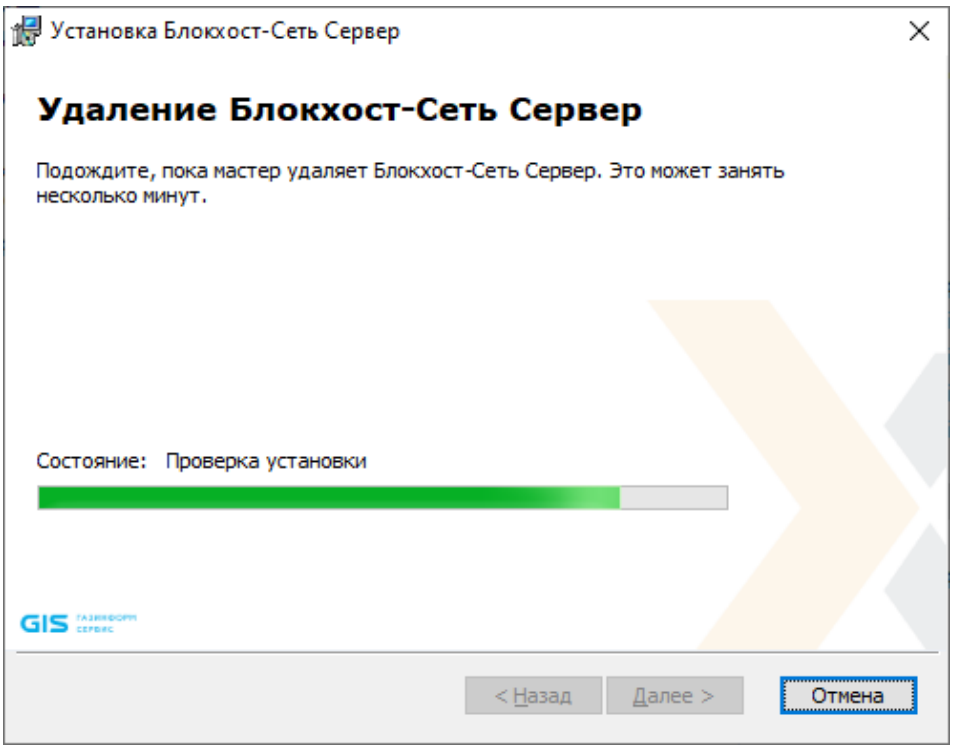


Рисунок 5.5 – Удаление серверной части СЗИ

При успешном завершении удаления появится окно окончания работы мастера СЗИ (рисунок 5.6) в котором необходимо нажать кнопку ***Готово***.

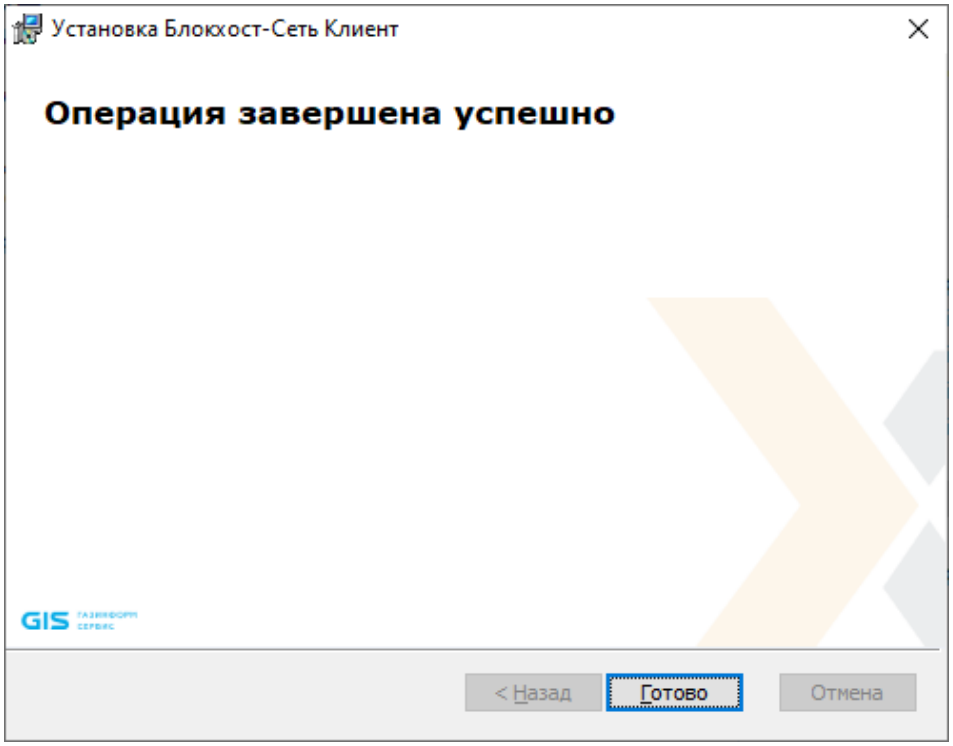


Рисунок 5.6 – Окно окончания удаления серверной части

По окончании удаления серверной части СЗИ от НСД «Блокхост-Сеть 4» откроется окно с предложением выполнить перезагрузку компьютера (рисунок 5.7). Перезагрузка доступна сразу после завершения удаления СЗИ, по нажатию кнопки ***Да*** в окне на рисунке 5.7, или позднее вручную, для этого нужно отказаться от перезагрузки, нажав кнопку ***Нет*** в окне на рисунке 5.7.

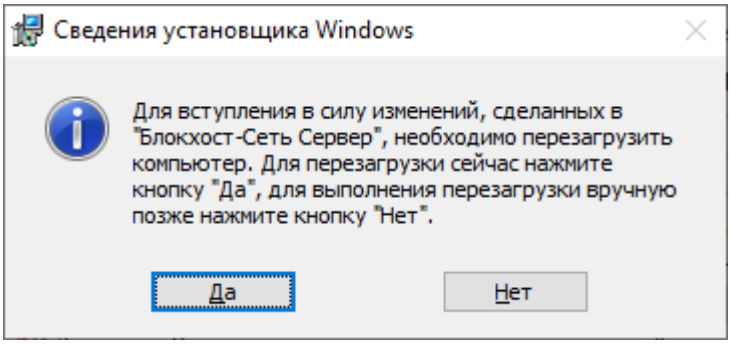


Рисунок 5.7 – Подтверждение немедленной перезагрузки

5.2 Деинсталляция агента управления

Удаление агента развертывания с рабочей станции может быть выполнено локально на рабочей станции.

Удаление агента развертывания СЗИ от НСД «Блокхост-Сеть 4» 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 агента развертывания с рабочих станций запустите апплет панели **Программы и компоненты** (***Пуск→ Панель управления→ Программы и компоненты***), в списке установленных программ рабочей станции выберите *BHNetDeploymentAgent* и нажмите кнопку ***Удалить***.

В результате откроется окно апплета **Программы и компоненты**, в котором необходимо подтвердить операцию удаления агента развертывания (рисунок 5.11).

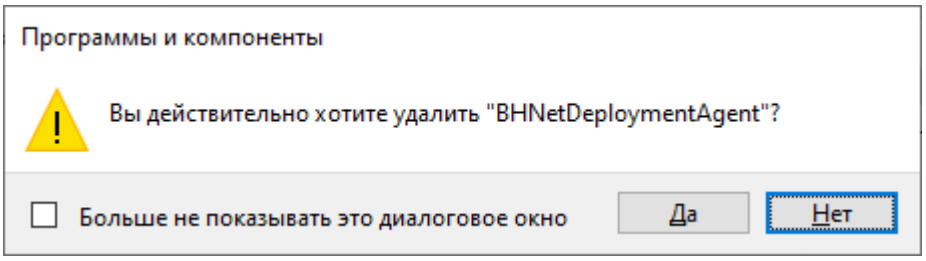


Рисунок 5.8 – Подтверждение удаления агента развертывания

После подтверждения операции агент управления будет удален.

5.3 Деинсталляция клиентской части СЗИ

Удаление клиентской части СЗИ с рабочей станции может быть выполнено несколькими способами:

– с помощью консоли управления;

– локально на рабочей станции.

5.3.1 Удаление клиентской части СЗИ с помощью консоли управления

Для удаления клиентской части СЗИ с помощью консоли управления необходимо создать задачу на удаление клиента через систему развертывания и запустить ее на выполнение.

Подробно удаление клиентской части СЗИ с помощью консоли управления описано в документе «Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит».

5.3.2 Локальное удаление клиентской части СЗИ

Удаление клиентской части СЗИ от НСД «Блокхост-Сеть 4» 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 Клиент*** и нажать кнопку ***Удалить***.

В результате запустится мастер удаления клиентской части СЗИ с рабочей станции (рисунок 5.9). Для продолжения удаления в окне необходимо нажать ***Далее***.

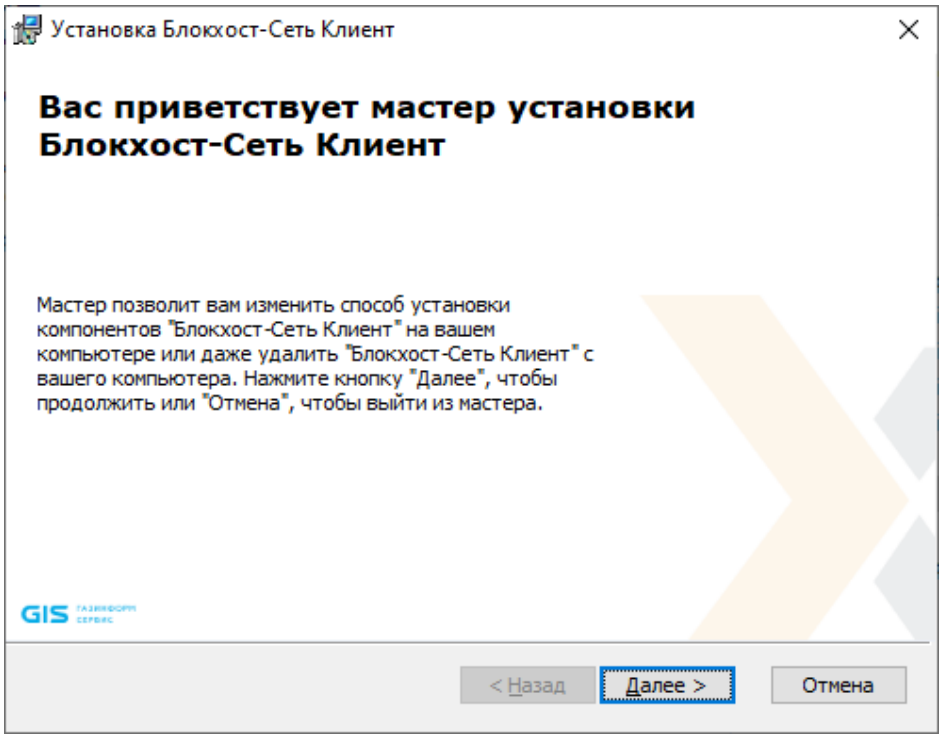


Рисунок 5.9 – Запуск мастер удаления клиента

В следующем окне (рисунок 5.10) необходимо выбрать операцию удаления.

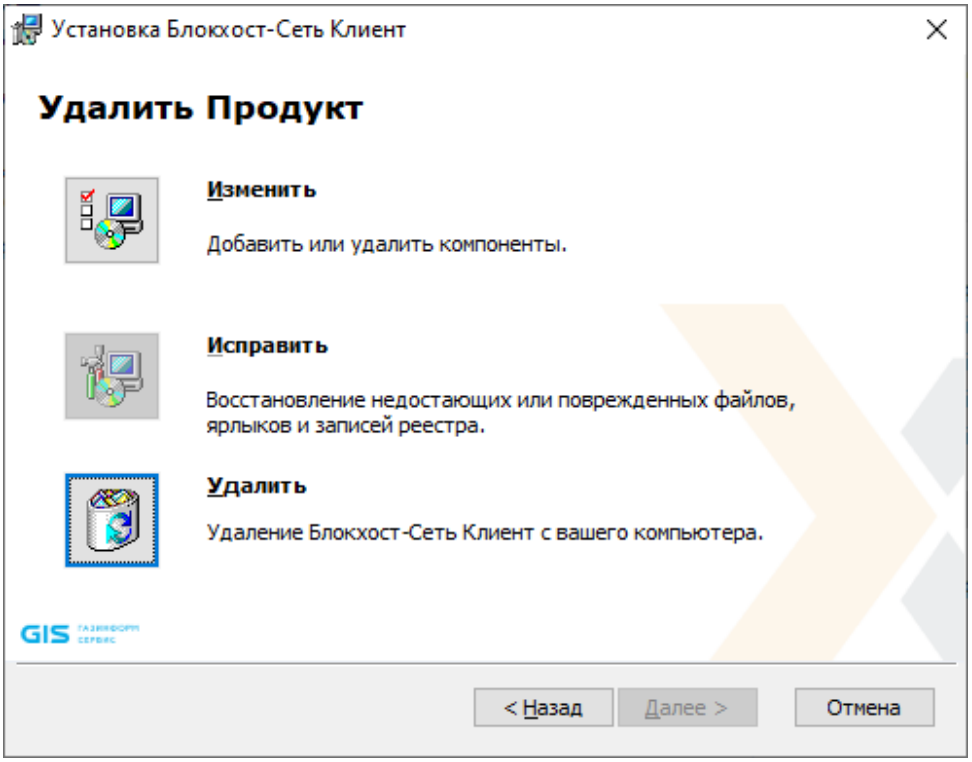


Рисунок 5.10 – Выбор операции удаления клиента

Для подтверждения удаления клиента необходимо ввести пароль встроенной учетной записи администратора, заданный при установке продукта (рисунок 5.11).

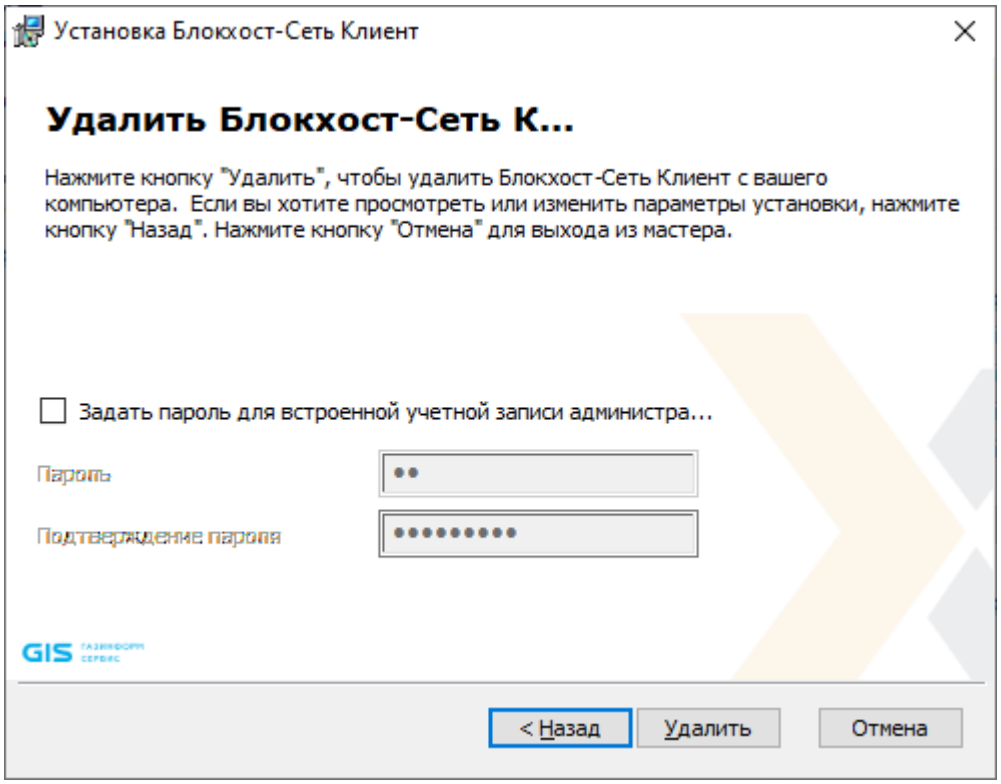


Рисунок 5.11 – Ввод учетных данных встроенного администратора

После нажатия кнопки ***Удалить*** начнется процесс удаления клиентской части СЗИ (рисунок 5.12).

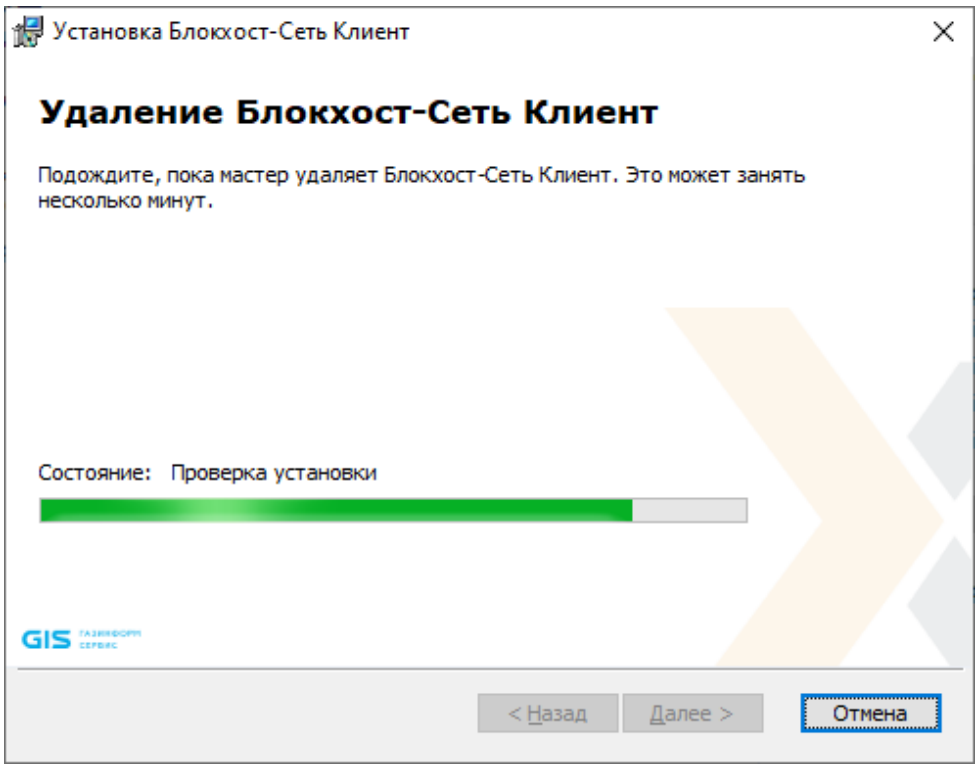


Рисунок 5.12 – Удаление клиента СЗИ

При успешном завершении удаления появится окно окончания работы мастера СЗИ (рисунок 5.13) в котором необходимо нажать кнопку ***Готово***.

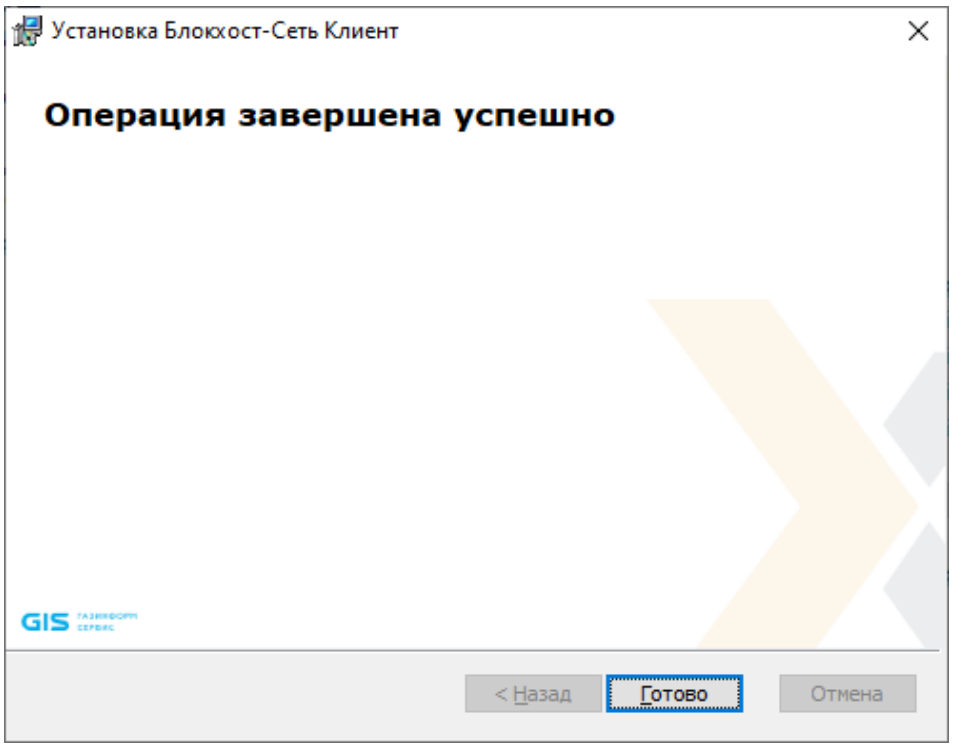


Рисунок 5.13 – Окно окончания удаления клиента

По окончании удаления клиентской части СЗИ откроется окно с предложением выполнить перезагрузку компьютера (рисунок 5.14). Перезагрузка доступна сразу после завершения удаления клиента СЗИ, по нажатию кнопки ***Да*** в окне на рисунке 5.14, или позднее вручную, для этого нужно отказаться от перезагрузки, нажав кнопку ***Нет*** в окне на рисунке 5.14.

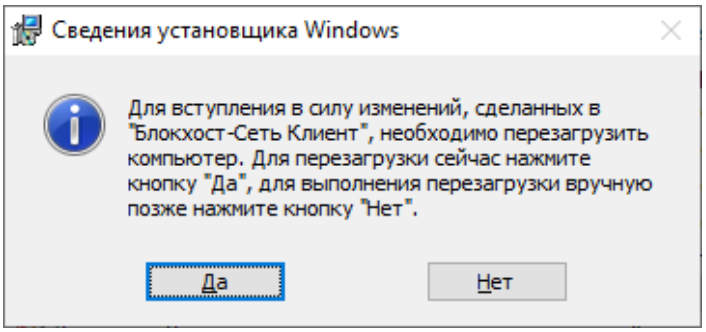


Рисунок 5.14 – Перезагрузка рабочей станции

5.4 Деинсталляция консоли управления

Удаление консоли управления 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.

Удаление консоли возможно с помощью:

– апплета панели управления ***Программы и компоненты***;

– пункта главного меню ***Удалить Блокхост-Сеть Консоль***.

Для удаления консоли с помощью апплета нужно запустить апплет панели управления **Программы и компоненты** (***Пуск → Панель управления → Программы и компоненты***), в списке установленных программ выбрать пункт ***Блокхост-Сеть Консоль*** и нажать кнопку ***Удалить***.

В результате откроется окно апплета **Программы и компоненты**, в котором необходимо подтвердить операцию удаления консоли управления (рисунок 5.15).

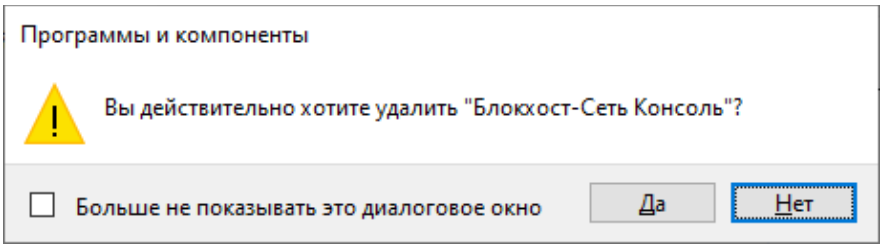


Рисунок 5.15 – Подтверждение удаления консоли управления

Для удаления консоли с помощью пункта главного меню нужно вызвать пункт главного меню ***Удалить Блокхост-Сеть Консоль***, расположенный в группе программ ***Пуск→ Все программы→ Блокхост-Сеть Консоль*** (рисунок 5.16).

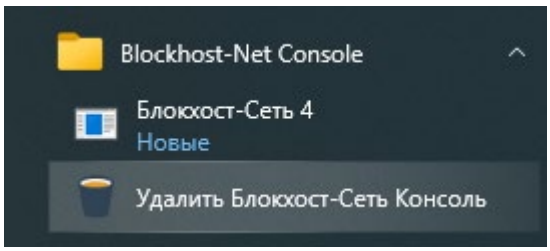


Рисунок 5.16 – Удаление консоли управления

В результате откроется окно установщика Windows, в котором необходимо подтвердить операцию удаления консоли управления (рисунок 5.17).

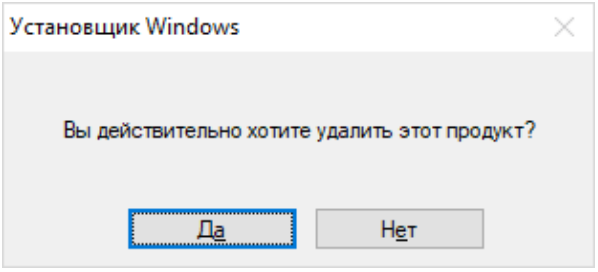


Рисунок 5.17 – Подтверждение удаления продукта

После подтверждения операции консоль управления СЗИ будет удалена.

6 Обновление СЗИ от НСД «Блокхост-Сеть 4»

6.1 Обновление серверной части СЗИ

Обновление более ранних версий серверной части СЗИ до сертифицированной версии СЗИ от НСД «Блокхост-Сеть 4» производится установкой новой версии СЗИ от НСД «Блокхост-Сеть 4» поверх уже установленной с помощью файла-установщика *BlockHost.Net 4 Server.exe* (под управлением 32- и 64-разрядных ОС).

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

Для обновления серверной части СЗИ необходимо запустить файл *BlockHost.Net 4 Server.exe* и последовательно пройти все шаги мастера установки СЗИ (подробное описание установки сервера СЗИ см. в подразделе 4.1 настоящего документа).

В процессе обновления серверной части СЗИ также будет обновлена и клиентская часть со всеми установленными модулями, а также консоль управления.

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, а также лицензия на продукт, добавленная ранее.

Обновление подчиненных серверов производится также, как и обновление мастер-сервера, при этом иерархия серверов сохраняется.

После обновления серверной части СЗИ необходимо обновить клиентскую часть на каждой рабочей станции, подключенной к серверу.

При обновлении сервера с подключением к СУБД никаких дополнительных действий предпринимать не требуется. После обновления сервер останется подключен к СУБД.

6.2 Обновление клиентской части СЗИ

Обновить более ранние версии клиентской части СЗИ на рабочей станции до сертифицированной версии можно удаленно из консоли управления СЗИ.

Перед обновлением клиентской части необходимо обновить сервер, к которому подключен клиент.

Обновление клиентской части состоит из двух этапов:

– обновление агента развертывания;

– обновление клиента.

Обновление производится аналогично первоначальной установке. Более подробная информация по установке приведена в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 2. Развертывание и аудит» в разделах ***«Установка агента подсистемы развертывания»*** и ***«Установка клиента Блокхост-Сеть»***.

При обновлении клиента важно правильно указать все необходимые модули. Модули, которые не были указаны при обновлении, но были установлены до обновления, будут удалены.

6.3 Обновление консоли управления

Обновление консоли управления производится установкой новой версии консоли СЗИ от НСД «Блокхост-Сеть 4» поверх уже установленной с помощью файла-установщика *BlockHost.Net 4 Console.msi*.

Для обновления консоли управления необходимо запустить файл *BlockHost.Net 4 Console.msi* и последовательно пройти все шаги мастера установки СЗИ (подробное описание установки консоли управления см. в подразделе 4.2 настоящего документа).

7 Активация СЗИ от НСД «Блокхост-Сеть 4»

По окончании установки СЗИ для использования функциональных возможностей СЗИ в полном объеме необходимо активировать лицензию на право использования продукта.

7.1 Активация при наличии подключения к сети Интернет

Для активации СЗИ от НСД «Блокхост-Сеть 4» при имеющемся подключении к сети Интернет необходимо выполнить следующие действия:

1) Выбрать в дереве иерархии сервер и перейти во вкладку **Лицензии** (рисунок 7.1).

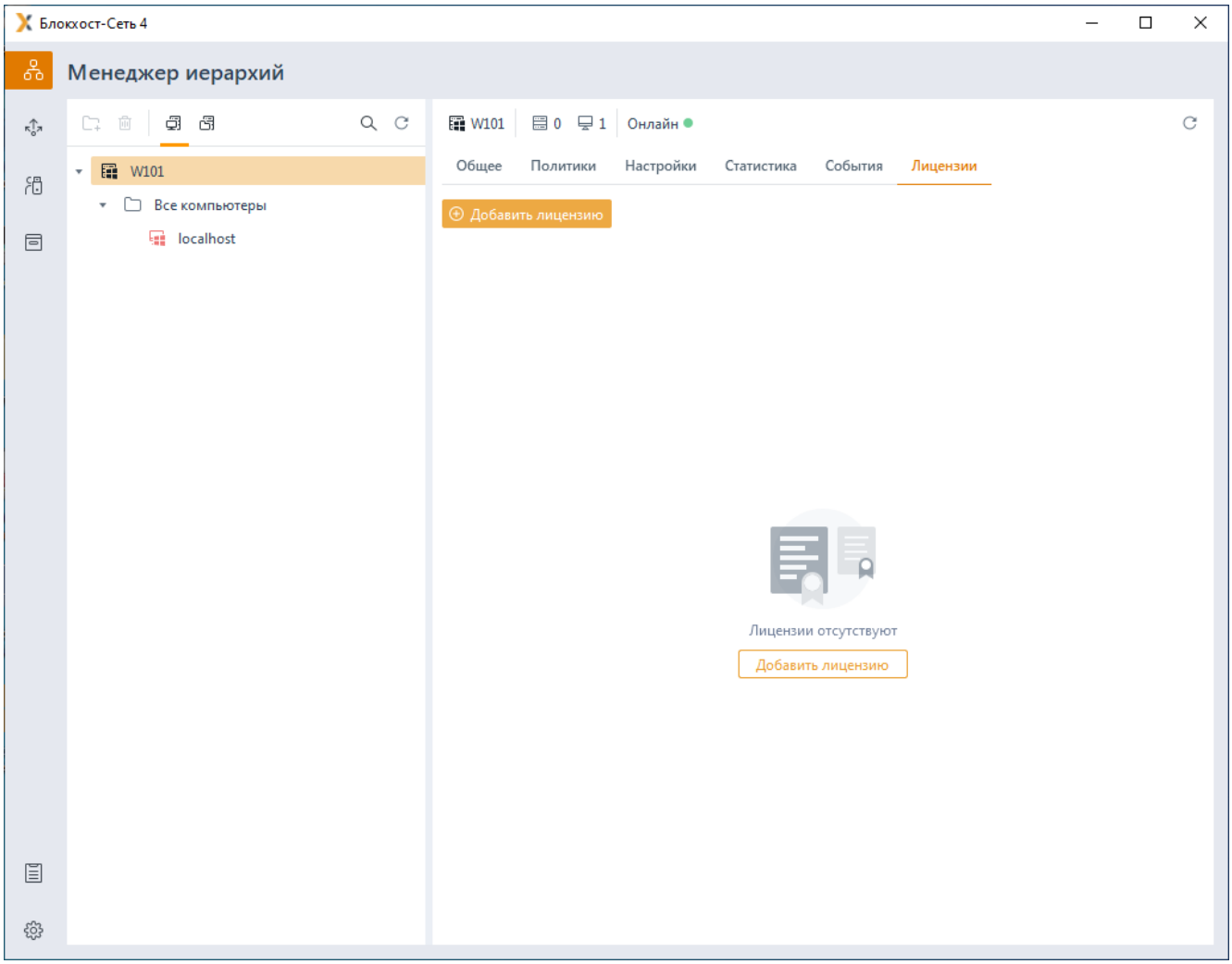
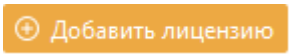


Рисунок 7.1 – Вкладка **Лицензии**

2) Нажать на кнопку добавления лицензии 

и выбрать активацию используя интернет (рисунок 7.2).

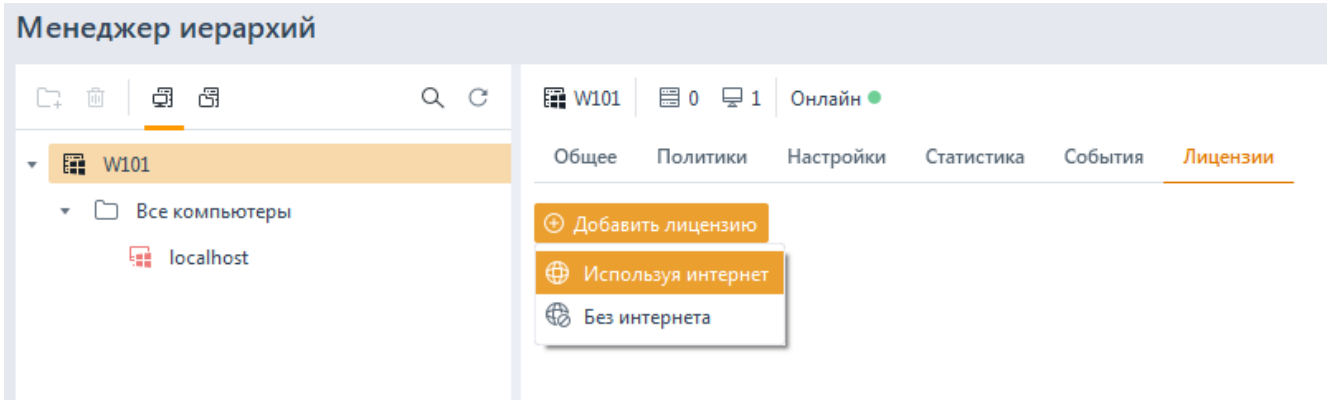


Рисунок 7.2 – Активация с использованием интернет

3) В появившемся окне *Активация лицензии онлайн* (рисунок 7.3) необходимо ввести ключ лицензии, полученный от поставщика программного продукта. Адрес сервера лицензирования, добавлен по умолчанию.

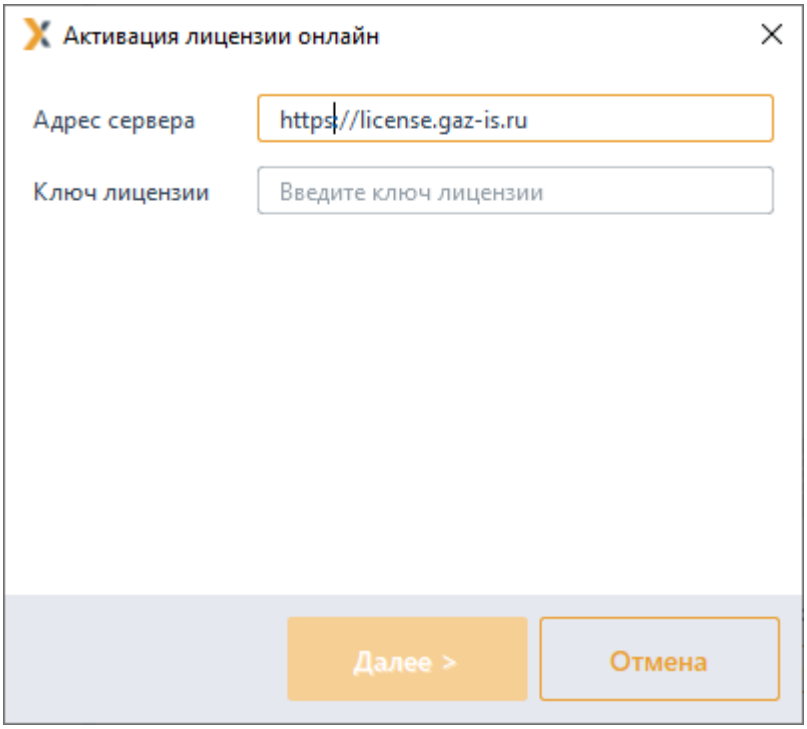


Рисунок 7.3 – Добавление лицензии

4) Нажать кнопку ***Далее***.

5) Если электронный адрес получателя при выпуске лицензии поставщиком программного продукта не был добавлен, после нажатия на кнопку ***Далее*** появится дополнительное поле, в котором необходимо ввести e-mail адрес получателя (рисунок 7.4), и нажать кнопку ***Активировать***.

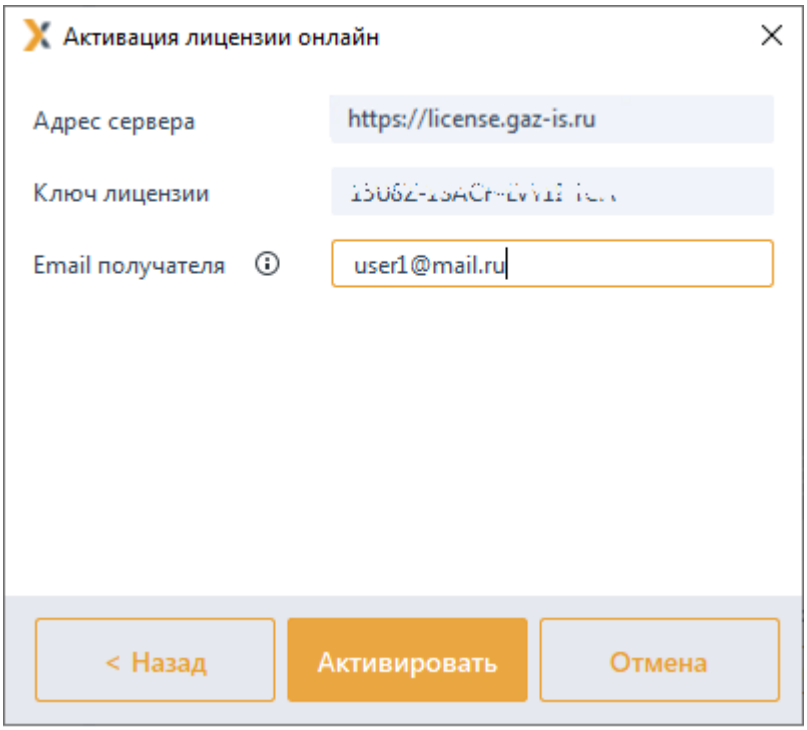


Рисунок 7.4 – Добавление электронного адреса получателя

Если при выпуске лицензии поставщиком программного продукта уже был добавлен электронный адрес получателя, дополнительный ввод электронного адреса получателя не потребуется.

6) В появившемся окне (рисунок 7.5) с сообщением об отправке ключа активации на указанный адрес нажмите ***Ок*** и перейдите в почту для просмотра письма, содержащего ключ активации.

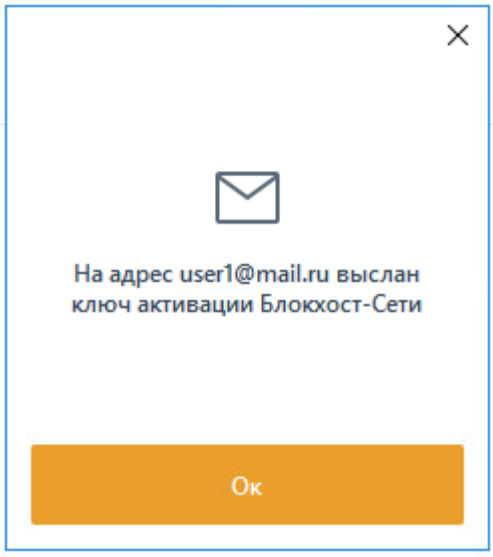


Рисунок 7.5 – Сообщение об отправке письма с ключом активации

7) В открывшемся окне введите ключ активации из полученного по электронной почте письма и нажмите кнопку ***Активировать*** (рисунок 7.6).

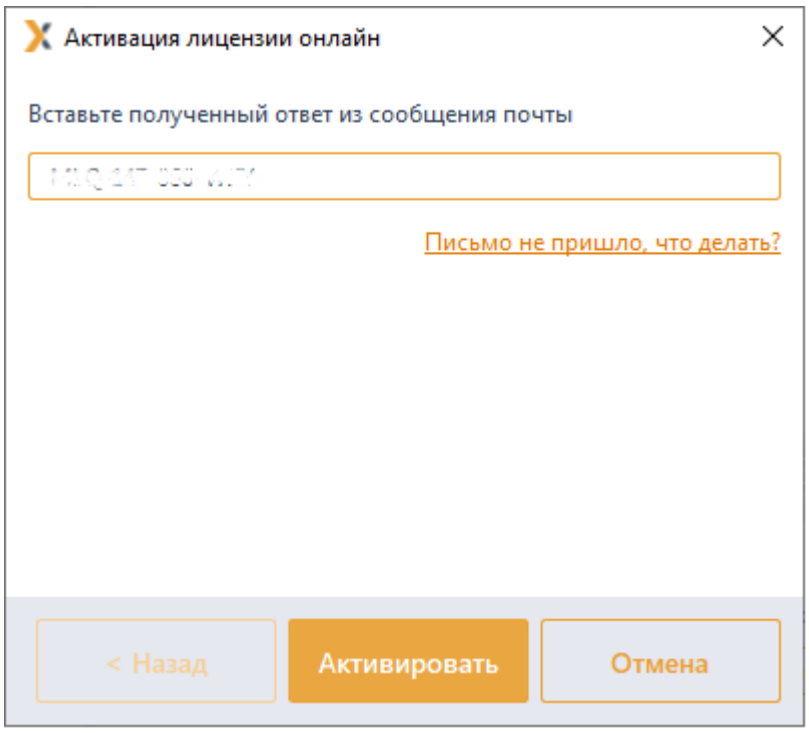


Рисунок 7.6 – Ввод ключа активации

В результате успешно пройденной активации будет выведено сообщение о завершении активации копии продукта (рисунок 7.7). На указанный адрес электронной почты придет сообщение о завершении активации продукта.

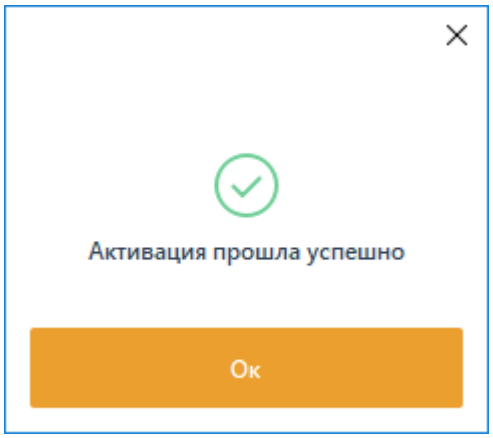


Рисунок 7.7 – Сообщение об успешной активации продукта

Во вкладке **Лицензии** отобразится информация об активированной лицензии (рисунок 7.8).

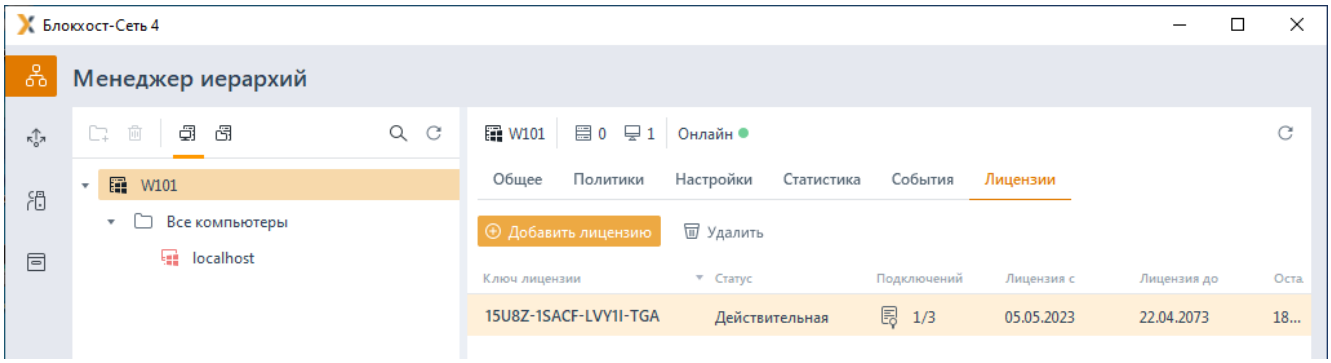


Рисунок 7.8 – Отображение добавленных лицензий во вкладке **Лицензии**

Описание полей добавленной лицензии:

– *Ключ лицензии* – код лицензии, полученный от поставщика программного продукта.

– *Статус* – статус в котором находится добавленная лицензия.

– *Подключений* – соотношение максимально возможного количества подключаемых рабочих станций в рамках выбранной лицензии и количества уже подключенных устройств.

– *Лицензия с* – дата, с которой лицензия входит в действие.

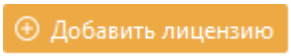
– *Лицензия до* – срок окончания выбранной лицензии.

– *Осталось дней* – количество дней, оставшихся до окончания срока действия лицензии.

7.2 Активация при отсутствии подключения к сети Интернет

Для активации комплекса при отсутствии подключения к сети Интернет необходимо выполнить следующие действия:

1) Перейти в дереве иерархии во вкладку **Лицензии** (рисунок 7.1).

2) Нажать на кнопку добавления лицензии 

и выбрать активацию без сети интернет (рисунок 7.9).

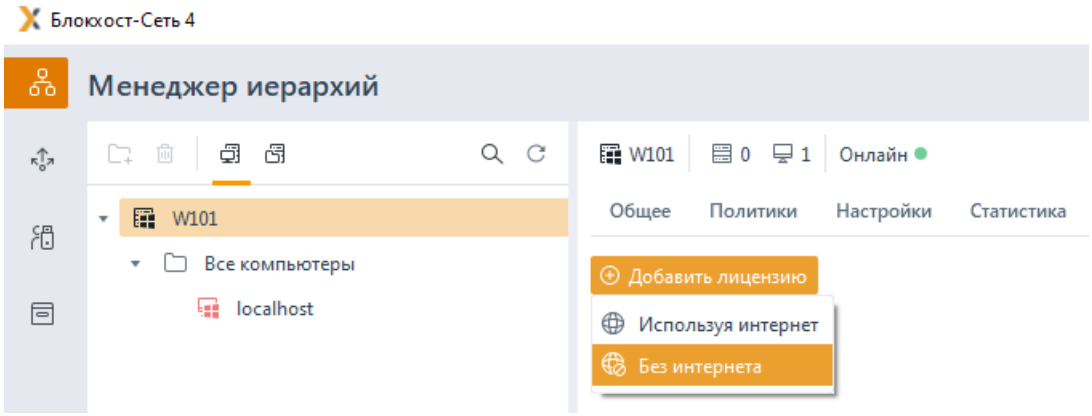


Рисунок 7.9 – Активация без сети интернет

3) В появившемся окне *Активация лицензии офлайн* (рисунок 7.10) ввести ключ лицензии, полученный от поставщика программного продукта, и электронный адрес получателя.

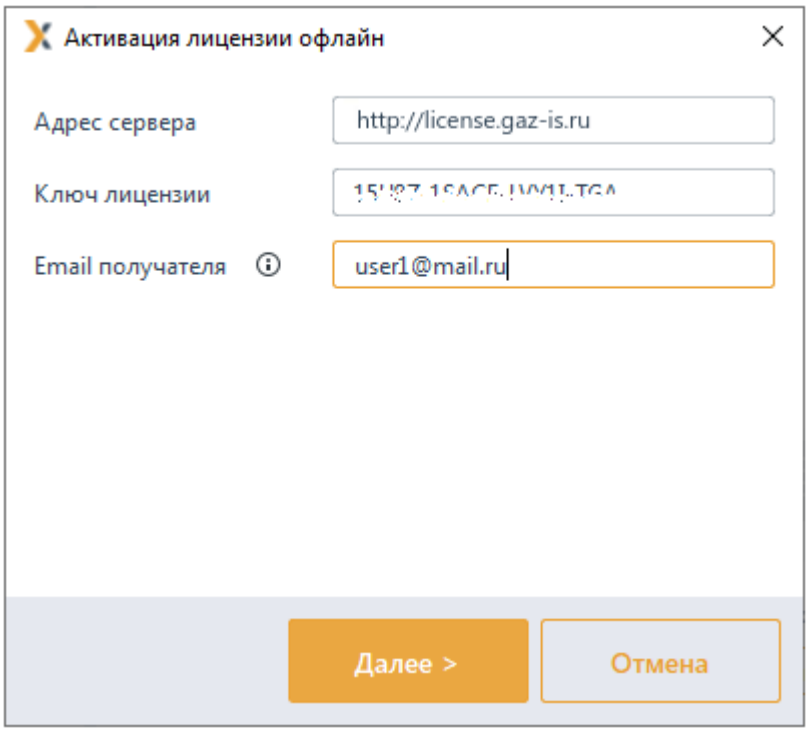


Рисунок 7.10 – Ввод лицензии и адреса электронной почты

4) Нажать кнопку ***Далее***.

5) В появившемся окне (рисунок 7.11) в указанном порядке выполните следующие действия:

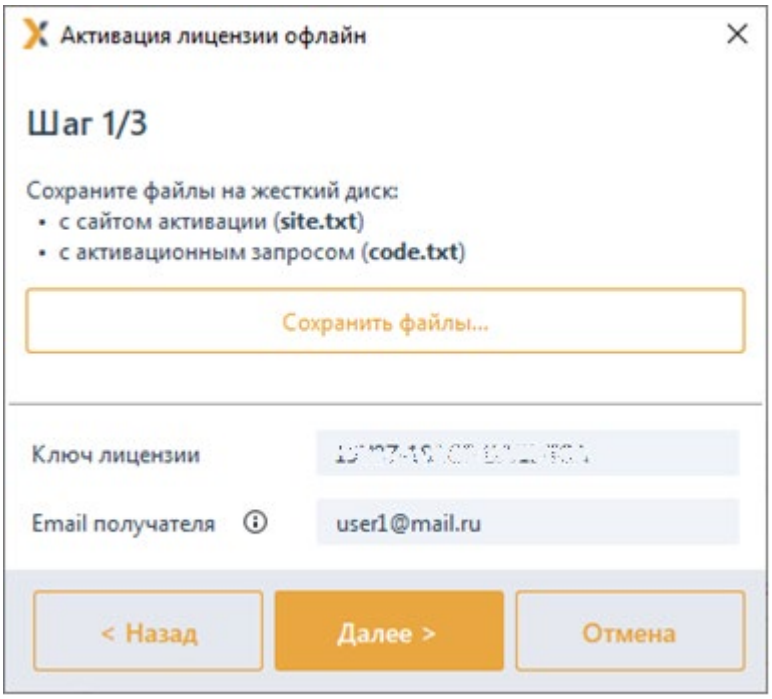


Рисунок 7.11 – Шаг 1 по активации лицензии офлайн

– по кнопке ***Сохранить файлы…*** сохраните поочередно текстовый файл с инструкцией *«site.txt»* и текстовый файл с активационном запросом *«code.txt»* на выбранное устройство;

– перейдите на рабочую станцию с имеющимся подключением к сети Интернет, откройте текстовый файл с инструкцией «*site.txt*» (рисунок 7.12);

Рисунок 7.12 – Шаг 2 по активации лицензии офлайн

– откройте страницу сервиса офлайн активации по ссылке https://license.gaz-is.ru/offlineActivate и в появившемся окне (рисунок 7.13) нажмите на кнопку ***Обзор…*** и вставьте активационный запрос из текстового файла *«code.txt»*;

– нажмите кнопку ***Активировать***;

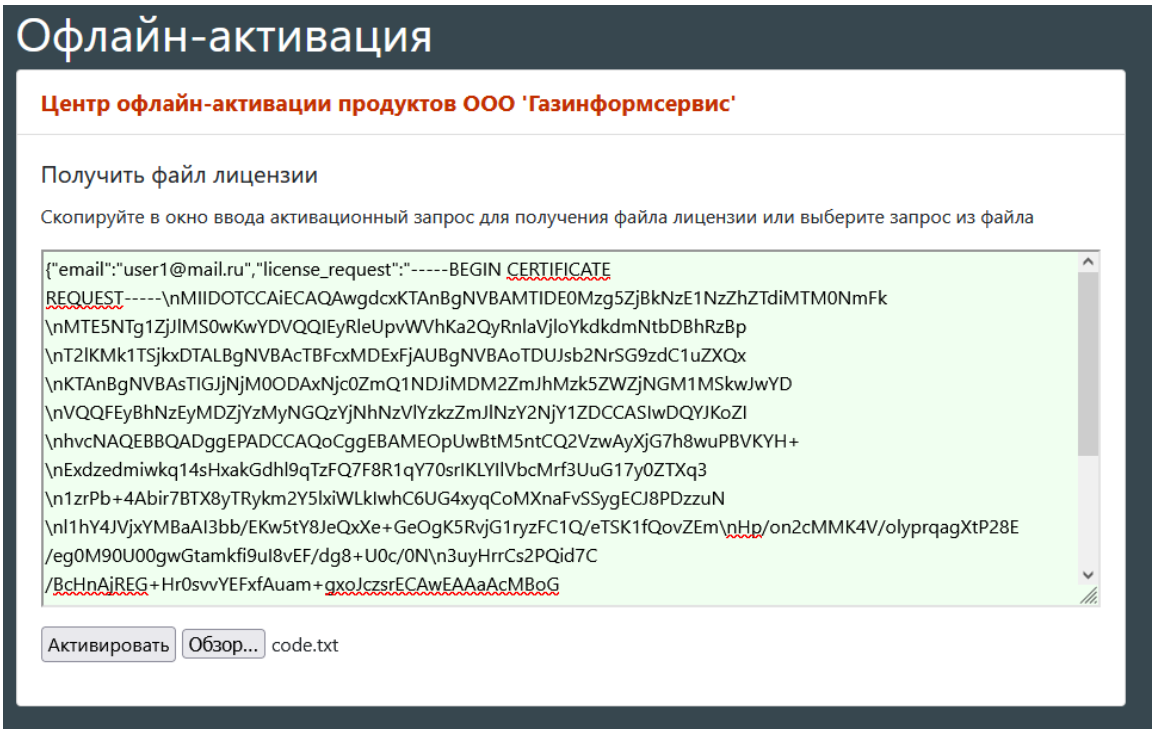


Рисунок 7.13 – Вставка активационного запроса при офлайн активации

– в появившемся окне (рисунок 7.14) введите ключ, полученный на указанную ранее электронную почту и нажмите кнопку ***Активировать***;

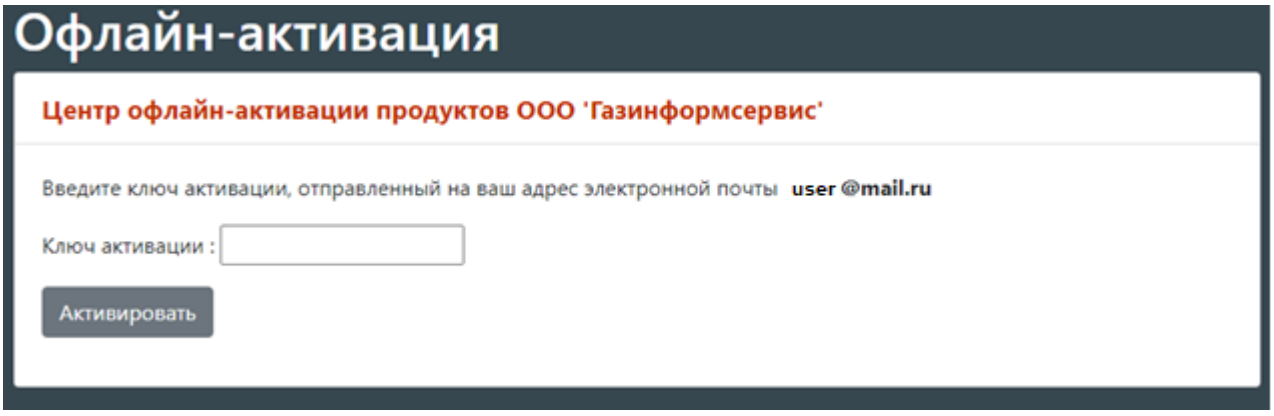


Рисунок 7.14 – Ввод ключа активации

– в появившемся окне (рисунок 7.15) нажмите на кнопку ***Сохранить в файл,*** получите файл *«license.bin»* и сохраните его на выбранное устройство;

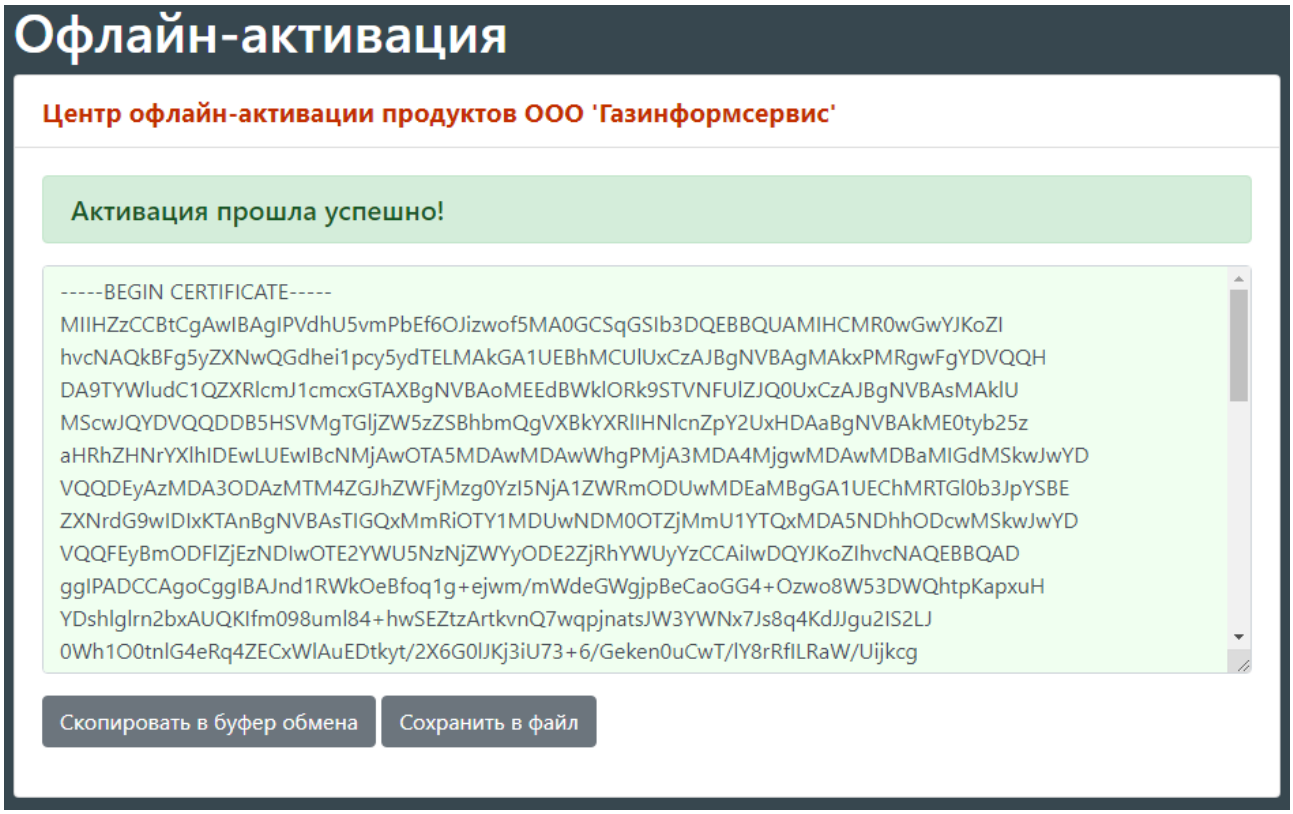
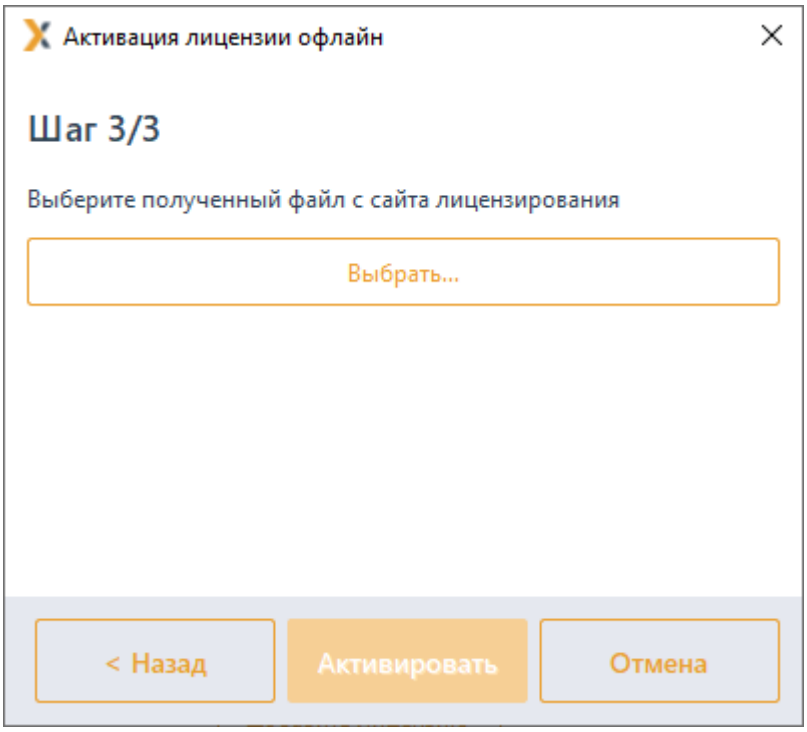
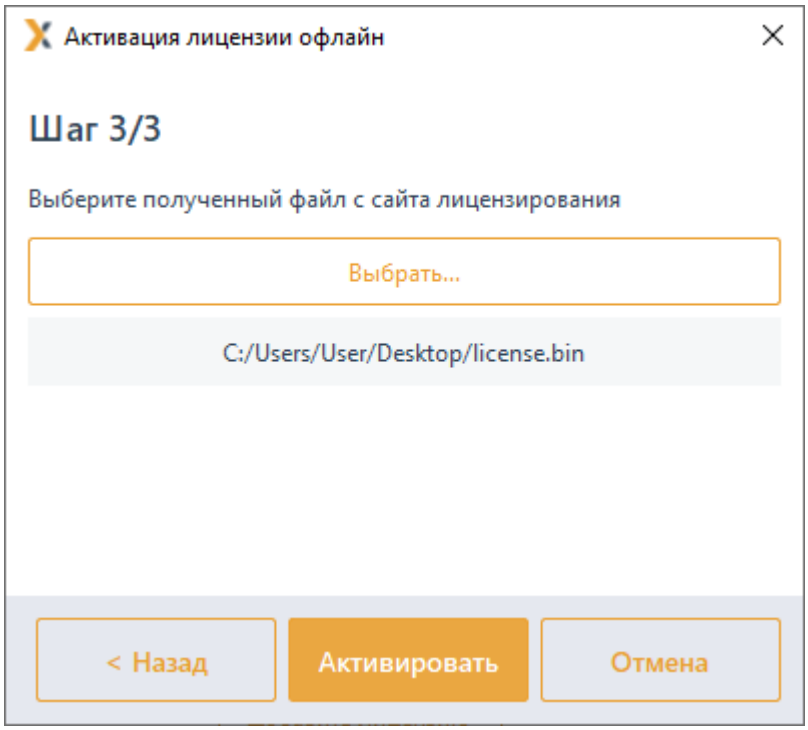


Рисунок 7.15 – Сохранение запроса

– перейдите на рабочую станцию, где необходимо активировать лицензию и нажмите кнопку ***Выбрать*** для добавления сохраненного файла с кодом (рисунок 7.16 а, б);



а)



б)

Рисунок 7.16 – Шаг 3 по активации лицензии офлайн

– нажмите кнопку ***Активировать***.

В результате успешно пройденной активации будет выведено сообщение о завершении активации копии продукта (рисунок 7.7). На указанный адрес электронной почты придет сообщение о завершении активации продукта.

7.3 Активация лицензии на клиентах

Для подключаемых клиентских рабочих станций и подчиненных серверов требуется клиентская лицензия. Количество клиентских лицензий (максимально возможное количество подключаемых рабочих станций) определяется поставщиком программного продукта при выпуске основной лицензии.

Активация клиентских лицензии на клиентах или подчиненных серверах осуществляется в момент подключения к головному серверу.

При наличии возможности подключения (максимально возможное количество подключаемых рабочих станций в рамках выбранной лицензии больше количества уже подключенных устройств) клиентская рабочая станция или подчиненный сервер привязывается к лицензии головного сервера в автоматическом режиме.

Если слоты подключения отсутствуют (максимально возможное количество подключаемых рабочих станций в рамках выбранной лицензии равно количеству уже подключенных устройств) клиентская рабочая станция или подчиненный сервер функционируют в мягком режиме.

Необходимо учитывать, что при «привязке» к лицензии приоритет имеют:
– локальная клиентская рабочая станция сервера по сравнению с обычными клиентскими рабочими станциями и подчиненными серверами;
– подчиненные сервера по сравнению с обычными клиентскими рабочими станциями.

Если сервер имеет несколько активных лицензий, при удалении одной из лицензий клиентские рабочие станции и подчиненные сервера автоматически привязываются к другой лицензии (при наличии свободных слотов). Если свободные слоты отсутствуют, клиентские рабочие станции переходят в мягкий режим работы.

7.4 Повторная активация лицензии

В случае, если лицензия уже активирована на клиентской рабочей станции или подчиненном сервере, и необходимо освободить имеющуюся лицензию от данного клиента с одновременной активацией на другой клиентской рабочей станции или подчиненном сервере, выполняется реактивация (повторная активация) лицензии.

Для выполнения повторной активации лицензии необходимо на выбранной клиентской рабочей станции или подчиненном сервере последовательно выполнить шаги по активации, описанные в подразделах ***«Активация при наличии подключения к сети Интернет»*** или ***«Активация при отсутствии подключения к сети Интернет»*** в зависимости от наличия на клиенте подключения к сети Интернет.

Повторная активация лицензии происходит в автоматическом режиме. Лицензия удаляется с клиента, привязанного к ней ранее (клиент функционирует в мягком режиме), и активируется на выбранной клиентской рабочей станции или подчиненном сервере.

При этом письмо, содержащее ключ активации, придет на электронный адрес получателя, заведенный при выпуске лицензии поставщиком программного продукта.

Если электронный адрес получателя при выпуске лицензии поставщиком программного продукта не был добавлен, потребуется ввод e-mail получателя, идентичный введенному при активации ранее. В противном случае реактивация не осуществится.

Если в лицензии имеется несколько слотов подключения, потребуется ввести файл лицензии клиента, чтобы указать какой слот необходимо освободить для повторной активации лицензии.

7.5 Удаление лицензии

Для удаления лицензии необходимо выполнить следующие действия:

1) Перейти в дереве иерархии во вкладку **Лицензии** (рисунок 7.1).

2) Выбрать в списке лицензию, которую необходимо удалить.

3) Нажать на кнопку удаления Удалить .

4) Подтвердить операцию удаления выбранной лицензии, нажав кнопку ***Удалить*** в открывшемся окне (рисунок 7.17).

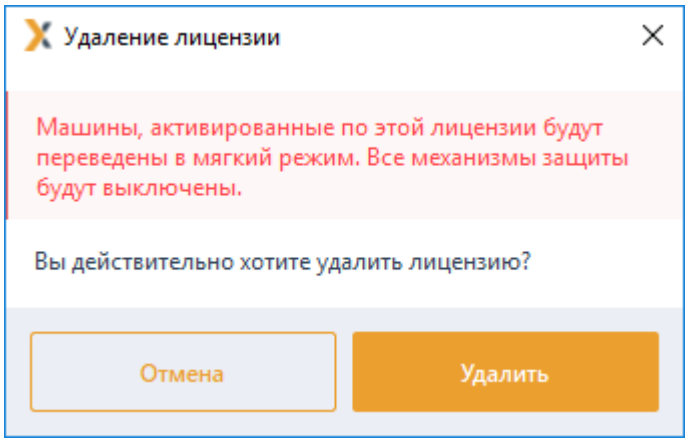


Рисунок 7.17 – Удаление лицензии

По завершению удаления лицензии, рабочие станции, привязанные к данной лицензии, будут переведены в мягкий режим работы.

8 Сбор диагностической информации

В СЗИ от НСД «Блокхост-Сеть 4» реализована возможность сбора технической информации по выявлению проблем функционирования некоторых механизмов СЗИ. В большинстве случаев необходимость сбора такой информации требуется для рассмотрения проблемы функционирования СЗИ и запрашивается специалистами технической поддержки.

8.1 Включение логирования работы механизма контроля печати

При необходимости сбора технической информации о работе механизма контроля печати следует провести ряд настроек на рабочей станции:

1) Создать в корне диска ***C:*** каталог ***Temp*** для размещения в нем лог-файлов работы механизма контроля печати. Предоставить доступ к этому каталогу с правами «Чтение» и «Запись» группе «Пользователи» рабочей станции;

2) В ключе реестра HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\ GIS.Client.PrintControl следует добавить параметр DebugFlag (тип REG_DWORD) и присвоить ему значение «1»;

3) Перезагрузить рабочую станцию.

В результате выполненных настроек, в процессе работы механизма контроля печати СЗИ, в зависимости от выполняемых действий в каталоге *C:\Temp* будут вестись текстовые лог-файлы:

– fpc.txt – информационные сообщения о работе сервиса GIS.Client.PrintControl;

– fpp.txt – информационные сообщения о работе принт-процессора pp_ctrl.dll:

– ff.txt, fc.txt – информационные сообщения о работе библиотеки PCInjDLL.dll;

– fe.txt – информационные сообщения о работе помощника для 64-битного окружения EnumProcess64.exe.

8.2 Включение логирования работы подсистемы аутентификации

При необходимости сбора технической информации о работе подсистемы аутентификации СЗИ следует провести ряд настроек на рабочей станции:

1) Создать в корне диска ***C:*** каталог ***Temp*** для размещения в нем лог-файлов работы подсистемы аутентификации СЗИ. Предоставить доступ к этому каталогу с правами «Чтение» и «Запись» группе «Пользователи» рабочей станции;

2) В ключе реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\WinLogon следует добавить параметр DebugFlag (тип REG_DWORD) и присвоить ему значение:

– «1» - будет вестись минимальный лог работы подсистемы аутентификации;

– «2» - будет вестись полный лог работы подсистемы аутентификации с записью сообщений о пошаговом выполнении команд программы;

3) Перезагрузить рабочую станцию.

В результате выполненных настроек в процессе работы подсистемы аутентификации СЗИ в каталоге *C:\Temp* будет вестись текстовый лог-файл *LogonUI.exe.txt*.

Перечень сокращений

AD	–	Active Directory (служба каталогов Microsoft)
DC	–	Domain Controller (контроллер домена)
DNS	–	Domain Name System (система распределения имен доменов)
SIEM	–	Security Information and Event Management (управление информацией о безопасности и управление событиями безопасности)
SPN	–	Service Principal Name (уникальный идентификатор экземпляра сервиса)
TCP/IP	–	Transmission Control Protocol/Internet Protocol (протокол управления передачей данных)
АБ	–	Администратор безопасности
БД	–	База данных
ГУПТ	–	Гарантированное удаление по требованию
НСД	–	Несанкционированный доступ
ОС	–	Операционная система
ПК	–	Программный комплекс
ПО	–	Программное обеспечение
СЗИ	–	Средство защиты информации
СКЗИ	–	Средство криптографической защиты информации
СУБД	–	Система управления базами данных
ЦС	–	Центр сертификации
ЭВМ	–	Электронная вычислительная машина