КОД безопасности

Средство защиты информации

Secret Net Studio

Руководство администратора

Установка, обновление, удаление

RU.88338853.501400.001 91 2

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Список сокращений

AD	Active Directory
IIS	Internet Information Services
LDAP	Lightweight Directory Access Protocol
NTFS	New Technology File System
OID	Object Identifier
SID	Security Identifier
SP	Service Pack
USB	Universal Serial Bus
VPN	Virtual Private Network
XML	Extensible Markup Language
БД	База данных
ИС	Информационная система
КЦ	Контроль целостности
ОС	Операционная система
ОСР	Общедоступный сетевой ресурс
ОУ	Оперативное управление
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СБ	Сервер безопасности
СОВ	Средство обнаружения вторжений
СУБД	Система управления базами данных
ЦУ	Централизованное управление
ЭИ	Электронный идентификатор

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio" RU.88338853.501400.001 (далее — Secret Net Studio, система защиты, изделие). В нем содержатся сведения, необходимые администраторам для установки ПО изделия, его обновления, исправления или удаления. Перед изучением данного руководства необходимо ознакомиться с общими сведениями о Secret Net Studio, изложенными в документе [**1**].

Условные обозначения

В руководстве для выделения некоторых элементов текста используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.

- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.

- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Примечания могут не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в интернете. Вы можете посетить сайт компании "Код Безопасности" (https://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru/company/education/training- courses/ . Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Глава 1
Общие сведения о развертывании системы

Структура системы Secret Net Studio является модульной. Подробные сведения об архитектуре системы Secret Net Studio содержатся в документе [**1**].

Состав устанавливаемых компонентов

Система Secret Net Studio состоит из следующих программных пакетов, устанавливаемых на компьютерах:

1. "Secret Net Studio" (далее — клиент).
2. "Secret Net Studio — Сервер безопасности" (далее — сервер безопасности или СБ).
3. "Secret Net Studio — Центр управления" (далее — программа управления).

Требования к аппаратному и программному обеспечению

Клиент

Компонент "Secret Net Studio" устанавливается на компьютеры, работающие под управлением следующих ОС (поддерживаются 32- и 64-разрядные версии ОС с установленными пакетами обновлений не ниже указанных):

- Windows 10;
- Windows 8.1 Rollup Update KB2919355;
- Windows 7 SP1;
- Windows Server 2019;
- Windows Server 2016;
- Windows Server 2012 R2 Rollup Update KB2919355;
- Windows Server 2012;
- Windows Server 2008 R2 SP1.

Внимание!
Во избежание конфликтов средств защиты необходимо до установки Secret Net Studio убедиться в отсутствии на защищаемых компьютерах других установленных антивирусных средств, средств защиты информации от несанкционированного доступа, межсетевых экранов.

Для установки клиента в сетевом режиме функционирования компьютер должен быть включен в домен Active Directory.

Требования к аппаратной конфигурации компьютера:

Элемент	Минимально
Процессор	В соответствии с требованиями ОС [1]
Оперативная память	2 ГБ
Жесткий диск (свободное пространство)	4 ГБ

[1] При использовании компонента "Антивирус" необходим процессор с двумя физическими или логическими (технология hyper-threading) ядрами.

Внимание!
При использовании доверенной среды компьютер должен удовлетворять требованиям, указанным в документе [**8**].

Системный каталог ОС Windows %SystemRoot% должен располагаться на томе с файловой системой NTFS или NTFS5.

Для установки клиента на компьютере должно быть установлено следующее ПО:

- Internet Explorer версии 8 или выше.

Если на компьютере будут использоваться аппаратные средства защиты (ПАК "Соболь" или другие поддерживаемые средства), рекомендуется выполнить подготовку устройств к использованию до установки клиентского ПО системы Secret Net Studio. Действия для подготовки устройств выполняются в соответствии с документацией на изделие. Установку программного обеспечения для поддерживаемых USB-ключей и смарт-карт можно выполнять с установочного диска системы Secret Net Studio. Файлы для установки расположены в соответствующих подкаталогах каталога \Tools\ (сведения о размещении файлов см. в приложении на стр.**69**).

Установка клиента в сетевом режиме функционирования может выполняться централизованно под управлением сервера безопасности. В этом случае в брандмауэре, если он включен, необходимо разрешить использование портов для доступа к общим ресурсам: UDP – 137, 138; TCP – 139, 445. Данные порты по умолчанию закрыты брандмауэром при отсутствии на компьютере сетевых папок общего доступа. Кроме того, должны быть открыты все TCP, UDP-порты, необходимые для функционирования компонентов ОС Windows в домене AD.

Пояснение.

Список всех портов, которые должны быть открыты для корректного функционирования Secret Net Studio, приведен на стр.**67**.

Программа установки клиента до начала модификации системы автоматически создает точку восстановления ОС. В процессе установки проверяются и при необходимости автоматически устанавливаются следующие распространяемые пакеты компании Microsoft:

- Microsoft C/C++ Runtime для Visual Studio 2017;
- Microsoft .NET Framework 4.5;
- пакет обновлений KB2462317;
- службы Microsoft Core XML Services (MSXML) 6.0;
- Microsoft XML Paper Specification Essentials Pack (пакет XPS EP).

После установки обновлений может потребоваться перезагрузка компьютера.

Сервер безопасности

Компонент "Secret Net Studio — Сервер безопасности" устанавливается на компьютеры, включенные в домен Active Directory и работающие под управлением следующих ОС:

- Windows Server 2019;
- Windows Server 2016;
- Windows Server 2012 R2 Rollup Update KB2919355;
- Windows Server 2012;
- Windows Server 2008 R2 SP1.

Требования к аппаратной конфигурации компьютера:

Элемент	Минимально	Рекомендуется
Процессор	В соответствии с требованиями ОС	Intel Core i5/Xeon E3 и выше
Оперативная память	8 ГБ	16 ГБ [1]
Жесткий диск (свободное место)	150 ГБ Рекомендуется использовать высокоскоростной жесткий диск	

[1] При размещении СБ и сервера СУБД на одном компьютере.

Для функционирования компонента требуется наличие системы управления базами данных, реализуемой сервером СУБД MS SQL. Сервер безопасности и сервер СУБД могут быть установлены на разных компьютерах (рекомендуется) или на одном компьютере.

Версии программного обеспечения серверов баз данных, совместимые с сервером безопасности (поддерживаются 32- и 64-разрядные версии, включая свободно распространяемые варианты SQL Server Express):

- Microsoft SQL Server 2019;
- Microsoft SQL Server 2017;
- Microsoft SQL Server 2016;
- Microsoft SQL Server 2014;
- Microsoft SQL Server 2012 с пакетом обновления 1 (SP1) и выше;

  Пояснение.
  Установку СУБД MS SQL Server 2012 SP1 Express можно выполнить с установочного диска комплекта поставки — см. стр.70

- Microsoft SQL Server 2008 R2 с пакетом обновления 1 (SP1) и выше.

Пояснение.
Корректное взаимодействие сервера безопасности и СУБД MS SQL обеспечивается при выполнении условий, изложенных в приложении на стр.70.

Дополнительно к компьютеру предъявляются следующие требования:

- на компьютере должны быть свободны и открыты TCP-порты 50000–50003. Если эти порты заняты другими приложениями, при установке сервера безопасности будет предложено выбрать другие порты для использования службами каталогов. Кроме того, должны быть открыты все TCP, UDP-порты, необходимые для функционирования компонентов ОС Windows в домене AD;

  Пояснение.
  Список всех портов, которые должны быть открыты для корректного функционирования Secret Net Studio, приведен на стр.67.

- в качестве языка программ, не поддерживающих стандарт кодирования Юникод, должен быть указан русский язык.

Программа установки автоматически проверяет и при необходимости устанавливает следующий распространяемый пакет компании Microsoft:

- Microsoft C/C++ Runtime для Visual Studio 2017.

После установки обновлений может потребоваться перезагрузка компьютера.

Программа управления

Компонент "Secret Net Studio — Центр управления" устанавливается на компьютеры, включенные в домен Active Directory и работающие под управлением следующих ОС (поддерживаются 32- и 64-разрядные версии ОС с установленными пакетами обновлений не ниже указанных):

- Windows 10;
- Windows 8.1 Rollup Update KB2919355;
- Windows 7 SP1;
- Windows Server 2019;
- Windows Server 2016;
- Windows Server 2012 R2 Rollup Update KB2919355;
- Windows Server 2012;
- Windows Server 2008 R2 SP1.

Требования к аппаратной конфигурации компьютера:

Элемент	Минимально
Процессор	В соответствии с требованиями ОС
Оперативная память	2 ГБ[1]
Жесткий диск (свободное пространство)	4 ГБ[2]

[1] При работе с журналами указанный объем памяти является достаточным для отображения до 1—1,5 млн записей. Чтобы загружать больше данных (например, для просмотра архивов размером более 100 МБ), необходимо либо увеличить объем памяти, либо использовать фильтрацию записей.

[2] При работе с архивами журналов указанный объем памяти является достаточным для распаковки архивов до 80—100 МБ (разархивирование осуществляется в папке временных файлов пользователя). Чтобы загружать более объемные архивы, необходимо увеличить свободное пространство на диске, который используется для временных файлов. Например, для работы с архивами размером 200–300 МБ требуется не менее 10 ГБ свободного пространства.

Для установки программы управления на компьютере должно быть установлено следующее ПО:

- Internet Explorer версии 8 или выше.

Программа установки также проверяет и при необходимости устанавливает в автоматическом режиме пакет Microsoft .NET Framework 4.5.

Установочный диск системы

Программное обеспечение и эксплуатационная документация системы Secret Net Studio поставляются на установочном диске. В корневом каталоге диска размещается исполняемый файл программы для работы с диском (далее — программа автозапуска). Общая структура каталогов диска представлена в следующей таблице.

Каталог	Содержимое
\Setup\Server\	Дистрибутив сервера безопасности
\Setup\Console\	Дистрибутивы программы управления
\Setup\Client\	Дистрибутивы клиента
\Setup\SnCard\	Файлы установки драйвера средства аппаратной поддержки
\Documentation\	Комплект документации
\Tools\	Вспомогательные утилиты, файлы для установки и настройки ПО

Программа автозапуска

При вставке установочного диска в привод для чтения оптических дисков происходит автоматический запуск программы автозапуска, которая позволяет выполнять следующие действия:

- запускать программы установки компонентов системы Secret Net Studio;
- открывать в отдельных окнах каталоги диска.

Примечание.
Если на компьютере отключена функция автозапуска оптических дисков, автоматический запуск программы не выполняется. В этом случае для работы с программой автозапуска запустите файл SnAutoRun.exe в корневом каталоге диска.

Пример содержимого окна программы автозапуска представлен на рисунке ниже.

Окно содержит команды для выполнения действий. Назначение команд описано в следующей таблице.

Команда	Назначение
Защитные компоненты	Запуск программы установки клиента
Сервер безопасности	Запуск программы установки сервера безопасности
Центр управления	Запуск программы установки программы управления
Сервер обновлений	Запуск программы установки сервера обновлений
Драйвер Secret Net Card	Запуск программы установки драйвера средства аппаратной поддержки Secret Net Card
Дополнительное ПО	Открытие каталога \Tools\ в отдельном окне
Документация	Открытие каталога \Documentation\ в отдельном окне
English	Выбор языка для программы автозапуска и устанавливаемого ПО

Для выполнения нужного действия выберите соответствующую команду. Некоторые команды запуска могут быть недоступны из-за невозможности установки компонентов или если установка не требуется. Для просмотра сведений о причине блокировки наведите указатель на команду — через 1–2 секунды на экране появится всплывающее сообщение.

Варианты установки компонентов

Компоненты системы Secret Net Studio можно устанавливать при работе на компьютере локально или в терминальных сессиях.

Кроме того, установка клиента в сетевом режиме функционирования может выполняться централизованно под управлением сервера безопасности.

Порядок установки для централизованного управления

Подготовительные действия

Перед установкой компонентов Secret Net Studio для централизованного управления необходимо выполнить действия по подготовке к созданию доменов безопасности и сетевой структуры. Сведения о доменах безопасности и сетевой структуре Secret Net Studio см. в документе [**1**].

Состав подготовительных действий:

1. Если домены безопасности будут формироваться на базе организационных подразделений, подготовьте организационные подразделения и включите в них нужные компьютеры.
2. Для каждого леса доменов безопасности создайте группу пользователей, которая будет указана в качестве группы администраторов леса. Пользователи, входящие в группу администраторов леса доменов безопасности, будут обладать правами на создание новых доменов безопасности в соответствующем лесу.
3. Создайте группы пользователей, которые будут указаны в качестве групп администраторов доменов безопасности.

Общий порядок установки компонентов

Установка компонентов Secret Net Studio выполняется в следующем порядке:

1. На компьютере, который будет использоваться в качестве корневого сервера безопасности (не подчиненного другим серверам), выполните следующие действия:
   - включите группу администраторов леса доменов безопасности и группу администраторов домена безопасности в локальную группу администраторов компьютера (в соответствии с тем, к какому домену безопасности будет относиться сервер);
   - установите ПО сервера безопасности (см. стр.**14**).
2. На других компьютерах, которые будут использоваться в качестве подчиненных серверов безопасности, выполните действия аналогично п. **1**.
3. На рабочих местах администраторов Secret Net Studio установите программу управления (см. стр.**21**).
4. Установите клиент Secret Net Studio в сетевом режиме функционирования (см. стр. **22**) на компьютерах серверов безопасности, затем на остальных компьютерах.

Типовой сценарий развертывания

Ниже рассматривается типовой сценарий развертывания компонентов системы Secret Net Studio для случая формирования одного домена безопасности на базе организационного подразделения AD. Все защищаемые компьютеры подчиняются одному серверу безопасности.

1. С использованием средств управления объектами Active Directory создайте организационное подразделение и включите в него компьютеры, на которых будет установлено ПО системы Secret Net Studio.
2. Создайте доменные группы пользователей для администраторов леса доменов безопасности и администраторов домена безопасности. Включите в эти группы учетные записи, которые должны обладать соответствующими полномочиями.

3. На компьютере, который будет использоваться в качестве сервера безопасности, выполните следующие действия:
   - включите группу администраторов леса доменов безопасности и группу администраторов домена безопасности в локальную группу администраторов компьютера;
   - установите ПО сервера безопасности (см. стр.14).

   Внимание!
   Чтобы обеспечить бесперебойное функционирование защищаемых компьютеров, следует установить резервный сервер в этом же домене безопасности. Установка резервного сервера выполняется в варианте включения сервера в состав имеющегося домена безопасности. При установке подчините резервный сервер основному серверу домена безопасности. Описание особенностей использования резервного сервера см. в приложении на стр.76.
4. На компьютере администратора безопасности установите программу управления (см. стр.21).
5. Запустите программу управления и установите соединение с сервером безопасности.

   Примечание.
   Сведения о работе с программой управления см. в документе [4].
6. Настройте централизованную установку клиентского ПО Secret Net Studio на компьютерах организационного подразделения. Для этого добавьте комплект установочных файлов клиента в список централизованно устанавливаемого ПО и сформируйте задания развертывания (см. стр.26).
7. Отслеживайте выполнение заданий в программе управления. После установки клиентского ПО и перезагрузки компьютеров они будут появляться в структуре управления в качестве подчиненных объектов сервера безопасности.

Глава 2
Локальная установка компонентов

Установку компонентов Secret Net Studio можно выполнять при работе на компьютере как в локальной сессии, так и в терминальной. Установка любого компонента должна выполняться пользователем, входящим в локальную группу администраторов компьютера.

Для централизованного управления клиентами в сетевом режиме функционирования необходимо установить сервер безопасности и программу управления. Управление клиентами в автономном режиме осуществляется только локально, поэтому установка указанных компонентов не требуется.

Установка сервера безопасности

Перед установкой сервера безопасности необходимо установить ПО сервера СУБД MS SQL (сведения о вариантах установки ПО см. на стр.**8**).

Для выполнения некоторых действий при установке сервера безопасности могут потребоваться особые права доступа. Например, права на администрирование леса доменов безопасности. Если пользователь, выполняющий установку, не обладает нужными правами, программа установки на определенных этапах может запрашивать учетные данные пользователей с правами доступа.

Внимание!
После установки сервера безопасности нельзя изменять имя компьютера сервера. Если компьютер будет переименован, сервер безопасности станет неработоспособен и недоступен для связи с другими компонентами Secret Net Studio.

Установка сервера безопасности может выполняться в одном из следующих вариантов:

- установка с созданием нового леса и домена безопасности;
- установка с созданием нового домена безопасности в имеющемся лесу доменов безопасности;
- установка с включением сервера в состав имеющегося домена безопасности.

Создание леса и домена безопасности

При установке в системе первого сервера безопасности необходимо использовать вариант установки с созданием нового леса доменов безопасности и нового домена безопасности. Данный вариант также применяется для создания отдельного леса доменов безопасности.

Для установки сервера с созданием нового леса и домена безопасности:

1. Вставьте в привод установочный диск системы Secret Net Studio. Дождитесь появления окна программы автозапуска (см. стр.**10**) и запустите установку с помощью команды "Сервер безопасности".

   Примечание.
   Запуск установки можно выполнить вручную без использования программы автозапуска. Для этого запустите с установочного диска файл \Setup\Server\x64\ setup.ru-RU.exe.

   После запуска программы установки выполняется анализ системы на соответствие программным и аппаратным требованиям для установки компонента. При этом проверяется текущее состояние встроенного в ОС механизма управления учетными записями (User Account Control — UAC).

Внимание!
Если механизм UAC включен — на экране появится диалог запроса на его временное отключение. В этом случае нажмите кнопку "Да" для отключения механизма, перезагрузите компьютер и только после этого снова запустите процедуру установки сервера безопасности.

По окончании проверки системы на экран будет выведен диалог с перечнем устанавливаемых компонентов, позволяющий дополнительно выбрать для установки службу синхронизации.

Пояснение.
Служба синхронизации устанавливается на сервере безопасности, чтобы, выполняя функцию шлюза, обеспечить взаимодействие этого сервера с родительским сервером безопасности. Установка данной службы выполняется отдельной программой установки, которая будет автоматически запущена после завершения установки сервера безопасности (см. стр.20).

2. Если требуется установить на данном сервере службу синхронизации, отметьте поле "Служба Синхронизации". Нажмите кнопку "Установить".

   Программа установки сервера начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

3. Для продолжения установки нажмите кнопку "Далее".

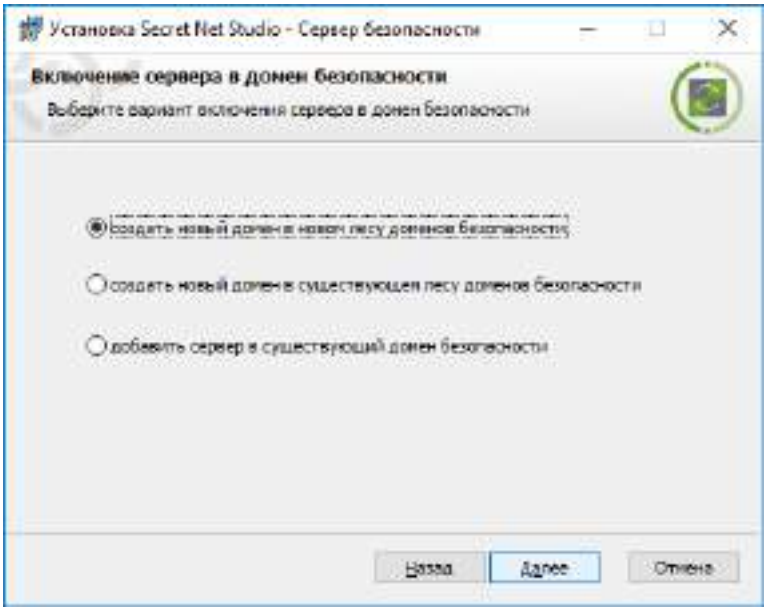
   На экране появится диалог принятия лицензионного соглашения.

4. Ознакомьтесь с содержанием лицензионного соглашения, отметьте пункт о его принятии и нажмите кнопку "Далее".

   Если на компьютере заняты порты для использования службами каталогов (любой порт из диапазона 50000–50003), на экране появится диалог для настройки использования портов.

5. В диалоге "Настройка портов служб каталогов" можно указать номера других портов вместо занятых или выполнить попытку переопределения занятых портов (с помощью кнопки "Зарезервировать") для использования сервером безопасности. Выполните нужные действия и нажмите кнопку "Далее".

   На экране появится диалог "Включение сервера в домен безопасности".



6. Установите отметку в поле "создать новый домен в новом лесу доменов безопасности" и нажмите кнопку "Далее".

   На экране появится диалог "Файл с настройками сервера аутентификации", предназначенный для создания файла с параметрами подключения сервера аутентификации в новом домене безопасности.

7. В диалоге укажите размещение и имя создаваемого файла и нажмите кнопку "Далее".

Внимание!
Файл с параметрами подключения содержит данные для доступа к серверу. Эти данные необходимы при добавлении других серверов безопасности в этот же домен безопасности. Для создаваемого файла необходимо обеспечить условия надежного хранения с защитой от компрометации содержащихся в нем данных.

На экране появится диалог "Настройка домена безопасности".

8. Выберите в раскрывающемся списке контейнер для формирования нового домена безопасности. В качестве контейнера можно выбрать организационное подразделение, в которое входит компьютер, или любое вышестоящее организационное подразделение (включая весь домен AD). После выбора контейнера при необходимости отредактируйте имя создаваемого домена безопасности.
9. Нажмите кнопку "Далее".

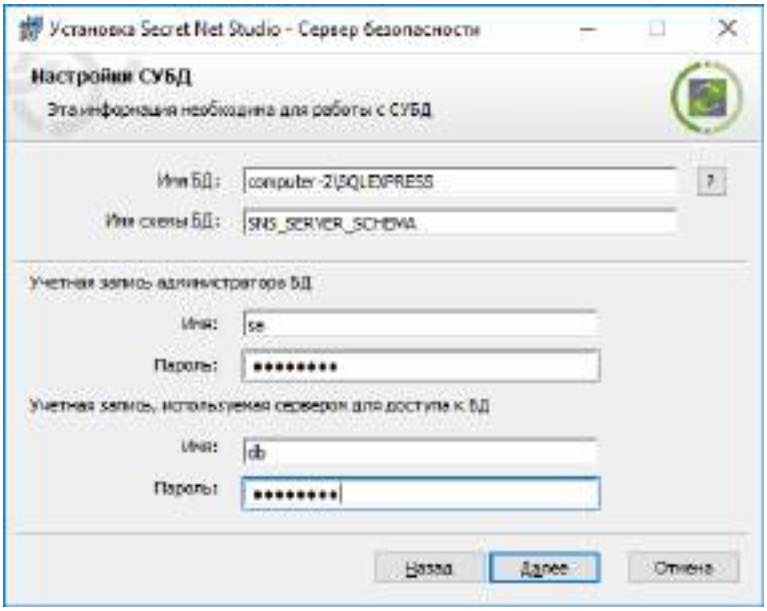
   На экране появится диалог "Группы администраторов безопасности".
10. Укажите группы пользователей, которым будут предоставлены права администрирования домена безопасности и леса доменов безопасности. Нажмите кнопку "Далее".

Совет.
В целях обеспечения безопасности информации разграничьте доступ администраторов, создав отдельную группу пользователей для администраторов домена безопасности. Использовать стандартную доменную группу администраторов (Domain Admins) не рекомендуется.

На экране появится диалог "Настройка каталогов".

11. Оставьте заданные по умолчанию каталоги установки сервера безопасности и размещения служебных файлов или укажите другие пути назначения. Нажмите кнопку "Далее".

    На экране появится диалог "Настройки СУБД". Пример содержимого диалога представлен на следующем рисунке.



12. Для СУБД MS SQL выполните следующие действия:
    - Укажите параметры соединения с тем экземпляром БД, который предназначен для работы с устанавливаемым сервером безопасности:
      - в поле "Имя БД" укажите расположение БД, используя следующий формат строки:

        <имя_или_IP-адрес_сервера_MS_SQL>\<имя_экземпляра_БД>,<порт>

Примечание.
- Если сервер СУБД установлен на компьютере с СБ и используется стандартный экземпляр MSSQLSERVER, то имя или IP-адрес сервера СУБД указывать не нужно.
- Если для подключения используется порт по умолчанию, то порт можно не указывать.

- в поле "Имя схемы БД" введите наименование схемы БД, которая будет создана;

Примечание. Для каждого сервера безопасности создается отдельная схема БД.

- в группу полей "Учетная запись администратора БД" введите учетные данные администратора БД на сервере СУБД;
- в группу полей "Учетная запись, используемая сервером для доступа к БД" введите учетные данные, с которыми сервер безопасности будет выполнять подключение к БД (будет создана учетная запись для подключения).

Примечание.
- Сервер безопасности не поддерживает режим аутентификации Windows при работе с сервером СУБД. Поэтому для соединения с БД необходимо указывать учетные данные пользователя базы данных (не доменного пользователя).
- Для учетных данных используйте латинские символы.

- Нажмите кнопку "Далее".

13. Если база данных уже существует (осталась от предыдущего установленного сервера), на экране появится диалог для выбора варианта дальнейших действий: использовать существующую базу данных или создать новую. В диалоге выберите нужный вариант и нажмите кнопку "Далее".

На экране появится диалог "Название организации".

14. Укажите названия организации и подразделения, которое будет обслуживать устанавливаемый сервер, и нажмите кнопку "Далее".

Примечание.
Эти данные будут использоваться при генерации сертификата сервера безопасности. Названия организации и подразделения могут быть введены позднее или заменены другими при выполнении процедуры "Генерация и установка сертификата сервера безопасности".

На экране появится диалог, сообщающий о готовности к установке.

15. Нажмите кнопку "Установить".

Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса. При выполнении действий на экране могут появляться дополнительные окна, в которых выводятся служебные сведения об отдельных этапах. Окна закрываются автоматически после завершения этапов.

Примечание.
Если пользователь, запустивший процесс установки сервера безопасности, не входит в группу администраторов домена безопасности, то на данном этапе установки будут запрошены учетные данные пользователя.

Если при выполнении действия **2** была выбрана установка службы синхронизации, будет запущена программа установки этой службы. Выполните ее установку так, как это описано на стр.**20**

После успешной установки и настройки на экране появится окно с перечнем операций программы установки. После завершения всех предусмотренных операций появится сообщение о необходимости перезагрузки компьютера.

16. Перезагрузите компьютер.

Внимание!

Объект нового сервера безопасности может появиться в структуре оперативного управления с некоторой задержкой. В программе управления, подключенной к другому серверу безопасности, загрузка обновленной структуры с новым сервером может произойти через несколько минут после установки ПО СБ (порядка 10–15 минут).

При первом запуске сервера безопасности выполняется синхронизация доменных пользователей, имеющихся в Active Directory, с базой данных СБ. В зависимости от количества учетных записей процесс синхронизации может занять от нескольких минут до одного часа. Рекомендуется дождаться завершения синхронизации и до этого времени не выполнять какие-либо действия с учетными записями, включая процедуру первого входа пользователя в систему на защищаемом компьютере. Если пользователь выполнит первый вход до завершения синхронизации, это может привести к сохранению неактуальных сведений о нем в базе данных сервера. В частности, возможна рассинхронизация сведений о пароле пользователя, после чего потребуется сменить пароль в программе управления пользователями Secret Net Studio.

Создание домена безопасности в имеющемся лесу

При наличии леса доменов безопасности (сформированного при установке первого сервера безопасности в этом лесу) можно создать новый домен безопасности и включить его в состав леса. Для этого необходимо выполнить установку нового сервера безопасности в варианте создания домена безопасности в имеющемся лесу.

Для установки сервера безопасности с созданием нового домена безопасности в имеющемся лесу:

1. Выполните действия **1–5** процедуры установки сервера с созданием нового леса и домена безопасности (см. стр.**14**).
2. В диалоге "Включение сервера в домен безопасности" установите отметку в поле "создать новый домен в существующем лесу доменов безопасности" и нажмите кнопку "Далее".

   На экране появится диалог "Файл с настройками сервера аутентификации", предназначенный для создания файла с параметрами подключения сервера аутентификации в новом домене безопасности.
3. В диалоге укажите размещение и имя создаваемого файла и нажмите кнопку "Далее".

   Внимание!

   Файл с параметрами подключения содержит данные для доступа к серверу. Эти данные необходимы при добавлении других серверов безопасности в этот же домен безопасности. Для создаваемого файла необходимо обеспечить условия надежного хранения с защитой от компрометации содержащихся в нем данных.

   На экране появится диалог "Подчинение сервера безопасности".
4. Выберите в раскрывающемся списке поля "Родительский сервер" имя компьютера, который будет являться родительским сервером безопасности. В поле "Настройки подключения" укажите шаблон сетевых параметров взаимодействия с родительским сервером.

   Пояснение.

   Шаблон сетевых параметров взаимодействия определяет значения тайм-аутов в соответствии со скоростными параметрами сети. Значения тайм-аутов могут быть откорректированы позднее при настройке сервера безопасности в программе управления.
5. Нажмите кнопку "Далее".

   Примечание.

   Если пользователь, запустивший процесс установки сервера безопасности, не входит в группу администраторов леса безопасности, то на данном этапе установки будут запрошены учетные данные пользователя.

   На экране появится диалог "Настройка домена безопасности".

6. Выберите в раскрывающемся списке контейнер для формирования нового домена безопасности. В качестве контейнера можно выбрать организационное подразделение, в которое входит компьютер с СБ, или любое вышестоящее организационное подразделение (включая весь домен AD). После выбора контейнера при необходимости отредактируйте имя создаваемого домена безопасности и нажмите кнопку "Далее".

   На экране появится диалог "Группы администраторов безопасности".

7. В диалоге "Группы администраторов безопасности" укажите группу пользователей, которым будут предоставлены права администрирования домена безопасности. Нажмите кнопку "Далее".

   На экране появится диалог "Настройка каталогов". Далее выполните завершающие действия процедуры установки сервера с созданием нового леса и домена безопасности (см. стр.14), начиная с действия **11**.

Добавление сервера в имеющийся домен безопасности

При наличии домена безопасности (сформированного при установке первого сервера безопасности в этом домене) можно включить в его состав дополнительный сервер безопасности. Для этого необходимо выполнить установку нового сервера безопасности в варианте включения в состав имеющегося домена безопасности.

Для установки сервера безопасности с включением сервера в состав имеющегося домена безопасности:

1. Выполните действия **1–5** процедуры установки сервера с созданием нового леса и домена безопасности (см. стр.14).
2. В диалоге "Включение сервера в домен безопасности" установите отметку в поле "добавить сервер в существующий домен безопасности" и нажмите кнопку "Далее".

   На экране появится диалог "Файл с настройками сервера аутентификации", предназначенный для выбора файла с параметрами подключения сервера аутентификации в целевом домене безопасности.
3. В диалоге укажите размещение и имя файла, созданного при установке первого сервера в этом домене безопасности, и нажмите кнопку "Далее".

Внимание!
Для файла с параметрами подключения необходимо обеспечить безопасную передачу на компьютер, чтобы не допустить компрометации содержимого файла.

   На экране появится диалог "Подчинение сервера безопасности".
4. Выберите в раскрывающемся списке поля "Родительский сервер" имя компьютера, который будет являться родительским сервером безопасности. В поле "Настройки подключения" укажите шаблон сетевых параметров взаимодействия с родительским сервером.

Пояснение.
Шаблон сетевых параметров взаимодействия определяет значения тайм-аутов в соответствии со скоростными параметрами сети. Значения тайм-аутов могут быть откорректированы позднее при настройке сервера безопасности в программе управления.

5. Нажмите кнопку "Далее".

   На экране появится окно с информацией о домене безопасности родительского сервера.
6. Нажмите кнопку "Далее".

Примечание.
Если пользователь, запустивший процесс установки сервера безопасности, не входит в группу администраторов леса и домена безопасности, то на данном этапе установки будут запрошены учетные данные пользователя.

На экране появится диалог "Настройка каталогов". Далее выполните завершающие действия процедуры установки сервера с созданием нового леса и домена безопасности (см. стр.14), начиная с действия **11**.

Установка ПО шлюза

Программное обеспечение шлюза — служба синхронизации — входит в состав сервера безопасности и может устанавливаться в процессе его установки либо отдельно. Программа установки службы синхронизации запускается программой установки сервера безопасности после выбора этого компонента при выполнении следующих операций:

- установка нового сервера безопасности;
- обновление существующего сервера безопасности до новой версии;
- повторный запуск программы установки для существующего сервера безопасности той же версии — используйте этот вариант для установки ПО шлюза на уже имеющийся и функционирующий сервер безопасности.

Внимание!

При выборе к установке службы синхронизации для успешного ее завершения необходимо соблюдать следующие условия:

- На родительском сервере безопасности в программе управления должен быть зарегистрирован соответствующий шлюз;
- Дочерний сервер безопасности должен иметь в наличие специальный файл (pav) с параметрами данного шлюза;
- На момент установки компьютер с дочерним сервером безопасности должен иметь возможность устанавливать сетевое соединение с компьютером, на котором функционирует родительский сервер безопасности, по полному DNS-имени этого компьютера.

Для установки службы синхронизации:

1. После выполнения подготовительных действий и появления на экране диалога приветствия программы установки службы синхронизации нажмите кнопку "Далее".

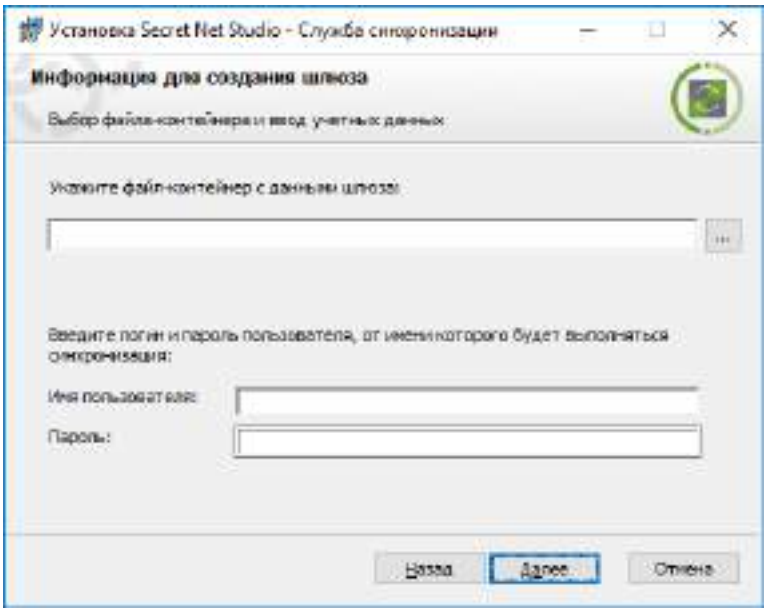
   На экране появится диалог принятия лицензионного соглашения.

2. Ознакомьтесь с содержанием лицензионного соглашения, отметьте пункт о его принятии и нажмите кнопку "Далее".

   На экране появится диалог "Конечная папка".

3. Оставьте заданную по умолчанию папку установки ПО или укажите другую папку назначения и нажмите кнопку "Далее".

   На экране появится следующий диалог.



4. Введите в полях диалога информацию, необходимую для создания шлюза.
   - Укажите путь к специальному файлу с параметрами шлюза. Для этого нажмите кнопку справа от поля и выберите нужный файл в появившемся стандартном диалоге.
   - Введите имя пользователя и его пароль, которые были заданы при регистрации данного шлюза в корневом (родительском) лесу безопасности.
   - Нажмите кнопку "Далее".

   Если все сведения указаны верно, на экране появится диалог с информацией о создаваемом шлюзе.
5. Нажмите кнопку "Далее".

   При успешной проверке доступности нужного сервера безопасности на экране появится диалог, сообщающий о готовности к установке.
6. Нажмите кнопку "Установить".

   Начнется процесс установки службы синхронизации, ход которого отображается в информационном окне в виде полосы прогресса. При его успешном завершении на экране появится диалог с сообщением об этом.
7. Нажмите кнопку "Готово".

   На завершающем этапе управление будет передано программе установки сервера безопасности. Выполните все предлагаемые ею действия, включая перезагрузку компьютера.

Установка программы управления

Для установки программы управления:

1. Вставьте в привод установочный диск системы Secret Net Studio. Дождитесь появления окна программы автозапуска (см. стр.10) и нажмите в нем кнопку "Центр управления".

   Совет.

   Для запуска установки без использования программы автозапуска:
   - на компьютере с 64-разрядной версией Windows — запустите с установочного диска файл \Setup\Console\x64\setup.ru-RU.exe;
   - на компьютере с 32-разрядной версией Windows — запустите с установочного диска файл \Setup\Console\Win32\setup.ru-RU.exe.

   Программа установки выполнит подготовительные действия, по окончании которых на экране появится диалог приветствия.
2. Для продолжения установки нажмите кнопку "Далее".

   На экране появится диалог принятия лицензионного соглашения.
3. Ознакомьтесь с содержанием лицензионного соглашения, отметьте соответствующий принятию соглашения пункт и нажмите кнопку "Далее".

   На экране появится диалог "Конечная папка".
4. Оставьте заданную по умолчанию папку установки ПО или укажите другую папку назначения и нажмите кнопку "Далее".

   На экране появится диалог, сообщающий о готовности к установке.
5. Нажмите кнопку "Установить".

   Начнется процесс установки, ход которого отображается в информационном окне в виде полосы прогресса. После успешной установки на экране появится диалог "Установка завершена".
6. Нажмите кнопку "Готово", а затем нажмите кнопку "Закрыть" в еще одном появившемся на экране диалоге.

Установка клиента

Локальная установка компонента "Secret Net Studio" выполняется при невозможности или нецелесообразности применения централизованной установки клиента (см. стр. **26**). В частности, для установки в автономном режиме функционирования.

Установка клиента в интерактивном режиме

Для установки клиента:

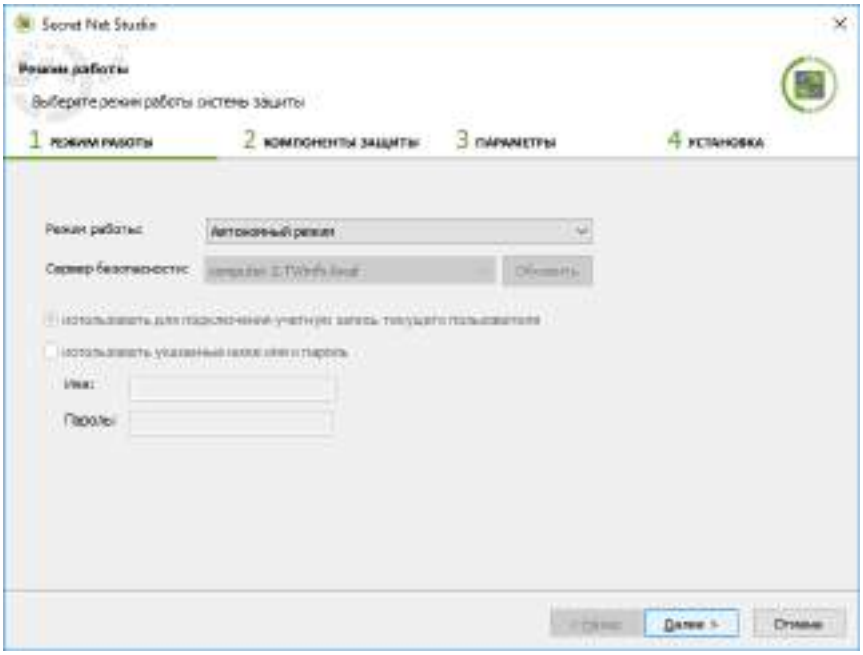
1. Вставьте в привод установочный диск системы Secret Net Studio. Дождитесь появления окна программы автозапуска (см. стр. **10**) и запустите установку с помощью команды "Защитные компоненты".

   Примечание.
   Запуск установки можно выполнить вручную без использования программы автозапуска. Для этого в зависимости от операционной системы компьютера выполните следующее действие:
   - при установке на компьютер с 64-разрядной версией Windows — запустите с установочного диска файл \Setup\Client\x64\SnSetup.ru-RU.exe;
   - при установке на компьютер с 32-разрядной версией Windows — запустите с установочного диска файл \Setup\Client\Win32\SnSetup.ru-RU.exe.

   На экране появится диалог принятия лицензионного соглашения.

2. Ознакомьтесь с содержанием лицензионного соглашения и нажмите кнопку "Принимаю".

   На экране появится диалог для выбора режима работы компонента.

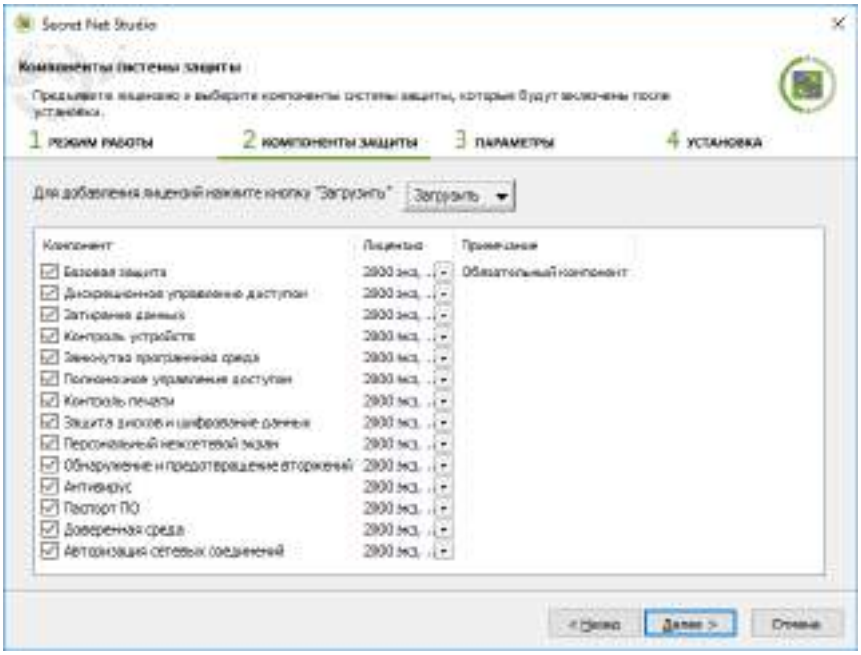


3. В поле "Режим работы" укажите нужный режим функционирования клиента — автономный ("Автономный режим") или сетевой ("Под управлением сервера безопасности"). Для сетевого режима функционирования настройте параметры подчинения серверу безопасности:
   - Выберите имя компьютера сервера безопасности, которому будет подчинен данный компьютер (если в раскрывающемся списке отсутствует имя нужного сервера, нажмите кнопку "Обновить").

- Для подчинения компьютера необходимы права на администрирование домена безопасности, к которому относится сервер. Если пользователь, выполняющий установку, обладает такими правами, оставьте отмеченным поле "использовать для подключения учетную запись текущего пользователя". В противном случае установите отметку в поле "использовать указанные ниже имя и пароль" и введите учетные данные пользователя из группы администраторов домена безопасности.

4. Нажмите кнопку "Далее >".

На экране появится диалог для выбора лицензий и формирования списка устанавливаемых защитных подсистем.



5. Нажмите кнопку "Загрузить" и выберите из раскрывающегося списка метод получения лицензий:

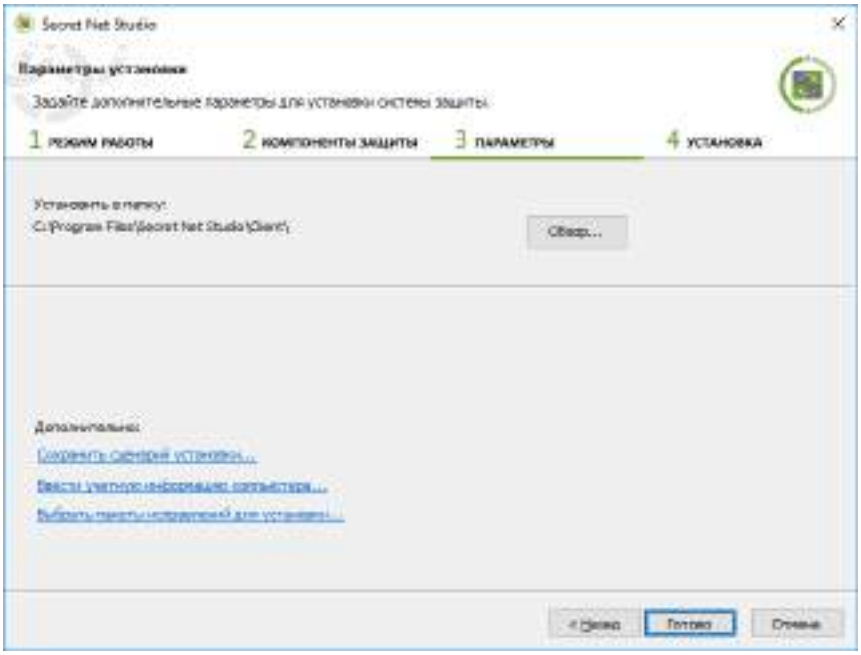
- чтобы загрузить лицензии с сервера безопасности, который был выбран для подчинения — укажите "С сервера безопасности";
- чтобы загрузить лицензии из файла (в частности, при установке клиента в автономном режиме функционирования) — укажите "Из файла", а затем выберите нужный файл в появившемся диалоге.

После загрузки данных в диалоге появятся сведения о лицензиях.

6. Отметьте в списке устанавливаемые подсистемы, для которых имеются свободные лицензии (установку компонента "Базовая защита" отключить нельзя). При наличии нескольких групп лицензий для компонента можно выбрать нужную группу в раскрывающемся списке.

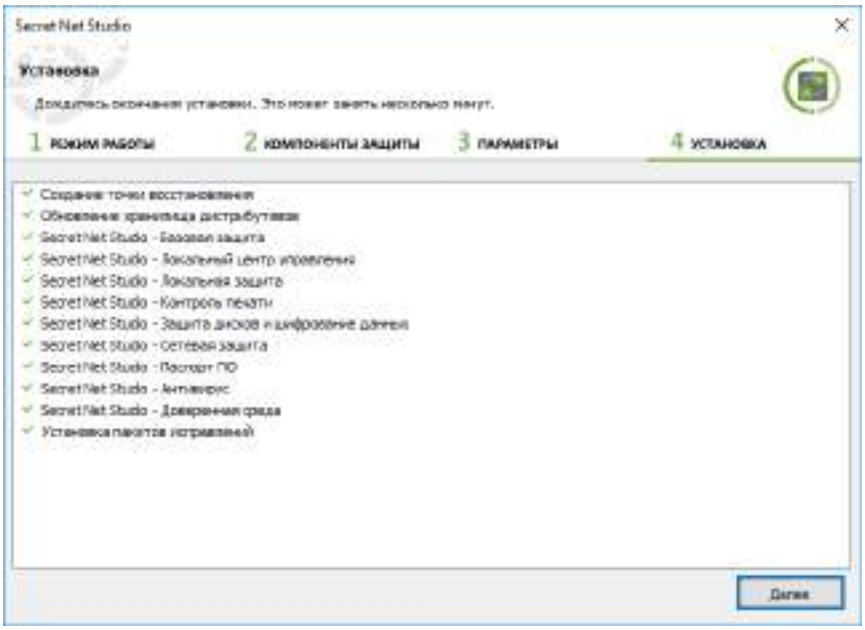
7. Нажмите кнопку "Далее >".

На экране появится диалог для выбора папки установки клиента и настройки параметров подключений.



8. В поле "Установить в папку" оставьте заданную по умолчанию папку установки клиента или укажите другую папку назначения.
9. При необходимости используйте ссылки в разделе "Дополнительно" для выполнения следующих действий:
   - чтобы сохранить заданные параметры установки в файле — выберите ссылку "Сохранить сценарий установки". Файл сценария установки можно использовать для автоматизации процесса установки клиентского ПО на других компьютерах;
   - чтобы ввести сведения о компьютере для учета — выберите ссылку "Ввести учетную информацию компьютера";
   - чтобы просмотреть и выбрать пакеты исправлений, которые будут применены при установке, — выберите ссылку "Выбрать пакеты исправлений для установки".
10. По окончании настройки параметров нажмите кнопку "Готово".

    Начнется процесс установки защитных подсистем в соответствии с заданными параметрами.



11. После завершения всех операций установки нажмите кнопку "Далее".

    На экране появится завершающий диалог со сведениями о выполненных операциях.

12. Проверьте состав подключенных к компьютеру устройств. Если подключены устройства, которые в дальнейшем должны быть запрещены к использованию, — отключите их.

Внимание!

При первой загрузке компьютера после установки клиентского ПО текущая аппаратная конфигурация автоматически принимается в качестве эталонной. Поэтому до перезагрузки необходимо отключить те устройства, которые должны быть запрещены к использованию на данном компьютере.

Совет.

При необходимости используйте ссылки в разделе "Информация" для выполнения следующих действий:

- чтобы посмотреть записи журнала трассировки — выберите ссылку "отчет об установке";
- чтобы собрать все необходимые для диагоностики Secret Net Studio файлы и данные, в случае возникновения проблем при установке — выберите ссылку "диагностическую информацию".

13. Перезагрузите компьютер и дождитесь загрузки системы.

Установка драйвера средства аппаратной поддержки

При наличии средства аппаратной поддержки Secret Net Card для его использования необходимо установить специальный драйвер дополнительно к ПО клиента.

Для установки драйвера средства Secret Net Card:

1. Вставьте в привод установочный диск системы Secret Net Studio. Дождитесь появления окна программы автозапуска (см. стр.**10**) и запустите установку с помощью команды "Драйвер Secret Net Card".

Примечание.

Запуск установки можно выполнить вручную без использования программы автозапуска. Для этого в зависимости от операционной системы компьютера выполните следующее действие:

- при установке на компьютер с 64-разрядной версией Windows — запустите с установочного диска файл \Setup\SnCard\x64\SnCard.msi;
- при установке на компьютер с 32-разрядной версией Windows — запустите с установочного диска файл \Setup\SnCard\Win32\SnCard.msi.

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

2. Для продолжения установки нажмите кнопку "Далее".

   Начнется установка и регистрация драйвера. Ход выполнения операций отображается в информационном окне в виде полосы прогресса.

   После успешной установки на экране появится диалог "Установка завершена".

3. Нажмите кнопку "Готово".

Глава 3
Настройка централизованной установки клиента

Установка под управлением сервера безопасности

Централизованная установка ПО клиента под управлением сервера безопасности инициируется средствами программы управления (сведения о запуске программы и работе с ней см. в документе [**4**]). В программе управления формируется список устанавливаемого ПО и создаются задания развертывания.

На клиентских компьютерах установка ПО выполняется автоматически в фоновом режиме. Пользователь оповещается о начале и завершении процесса установки. В ходе этого процесса, в зависимости от настройки параметров задания развертывания, пользователю будет предложено самостоятельно перезагрузить компьютер или перезагрузка произойдет автоматически.

Внимание!

Для централизованного развертывания ПО компьютеры должны удовлетворять требованиям к аппаратному и программному обеспечению для установки клиента (см. стр.7). В частности, необходимо разрешить использование портов для доступа к общим ресурсам: 137, 138, 139, 445. Данные порты по умолчанию закрыты брандмауэром при отсутствии на компьютере сетевых папок общего доступа.

Формирование списка централизованно устанавливаемого ПО

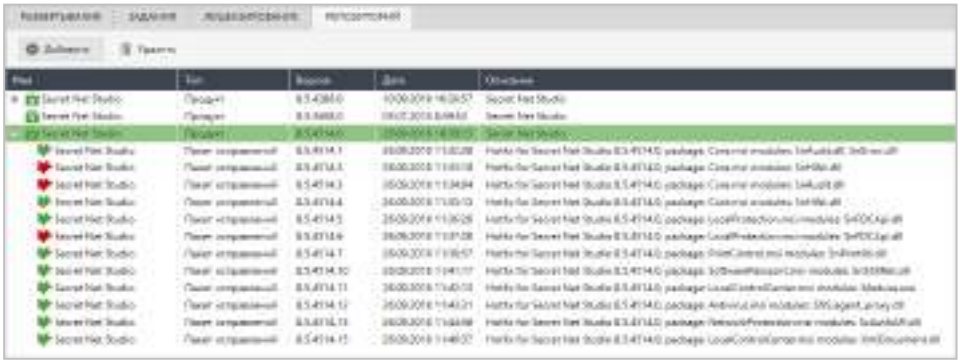
По умолчанию список централизованно устанавливаемого ПО не заполнен. Для настройки развертывания необходимо добавить в список комплект (комплекты) установочных файлов. Комплект может быть создан на основе установочного диска системы Secret Net Studio или пакета обновлений ("патч").

Внимание!

Комплекты установочных файлов помещаются в каталог Repository. Этот каталог создается при установке сервера безопасности в каталоге установки сервера и ему назначаются нужные права общего доступа. Не меняйте права доступа к данному каталогу, иначе централизованная установка ПО станет невозможна.

Для добавления комплекта установочных файлов:

1. В панели "Развертывание" перейдите на вкладку "Репозиторий".



Пояснение.

Пиктограммы пакетов исправлений, отмеченные красным цветом, являются обязательными обновлениями.

2. Нажмите кнопку "Добавить", которая расположена под вкладкой "Развертывание".

На экране появится диалог для добавления комплекта установочных файлов.

3. В появившемся диалоге нажмите кнопку "Добавить".

   На экране появится диалог для выбора папки, содержащей комплект установочных файлов.

4. В поле "Папка" укажите каталог с файлами для создания установочного комплекта и нажмите кнопку "Выбор папки". Например, если комплект нужно создать на основе установочного диска системы Secret Net Studio и пакета обновлений — укажите корневой каталог установочного диска. Если комплект нужно создать только на основе пакета обновлений — укажите корневой каталог пакета обновлений, который находится на установочном диске в каталоге \Tools\SecurityCode\Patches. Пакет обновлений добавится в список централизованно устанавливаемого ПО только при наличии добавленного ранее в репозитории установочного диска системы Secret Net Studio.

   Внимание!
   Версии установочного комплекта системы Secret Net Studio и пакета обновлений должны быть одинаковы.

   В диалоге для добавления комплекта установочных файлов появится новый элемент списка, содержащий сведения о загруженном комплекте.

5. Нажмите кнопку "Применить".

   На экране появится диалог процесса добавления файлов. Дождитесь окончания процедуры создания комплекта (процесс отправки файлов на сервер безопасности может занять продолжительное время).

6. Нажмите кнопку "Закрыть".

   По окончании процесса в списке появится новый элемент, содержащий сведения о загруженном комплекте.

Формирование заданий развертывания

После формирования списка централизованно устанавливаемого ПО необходимо добавить задания развертывания. Задания определяют списки компьютеров, на которых в автоматическом режиме будут выполняться нужные действия.

Для добавления задания развертывания:

1. В панели "Развертывание" перейдите на вкладку "Развертывание".

2. При наличии нескольких лесов настройте отображение структуры управления с помощью раскрывающегося списка "Лес".

3. Выберите компьютеры, для которых нужно сформировать задание. При необходимости используйте возможности фильтрации, сортировки и вывода сведений о компьютерах.

   Список компьютеров можно фильтровать по наличию или отсутствию установленного ПО клиента (кнопки "SNS", "Без SNS"), по принадлежности контейнерам Active Directory (отображаются компьютеры тех контейнеров, которые отмечены в структуре управления слева), а также по наличию в названии заданной строки символов (поля для поиска расположены над списком контейнеров AD и над таблицей со списком компьютеров).

   Сортировка списка компьютеров выполняется стандартными методами с помощью заголовков колонок.

Компьютеры, подчиненные серверу безопасности, отмечены в списке зеленой пиктограммой и полужирным шрифтом.

Для просмотра подробных сведений о компьютере выберите строку с ним двойным щелчком мыши или воспользуйтесь кнопкой с изображением стрелки в правой части строки под списком компьютеров.

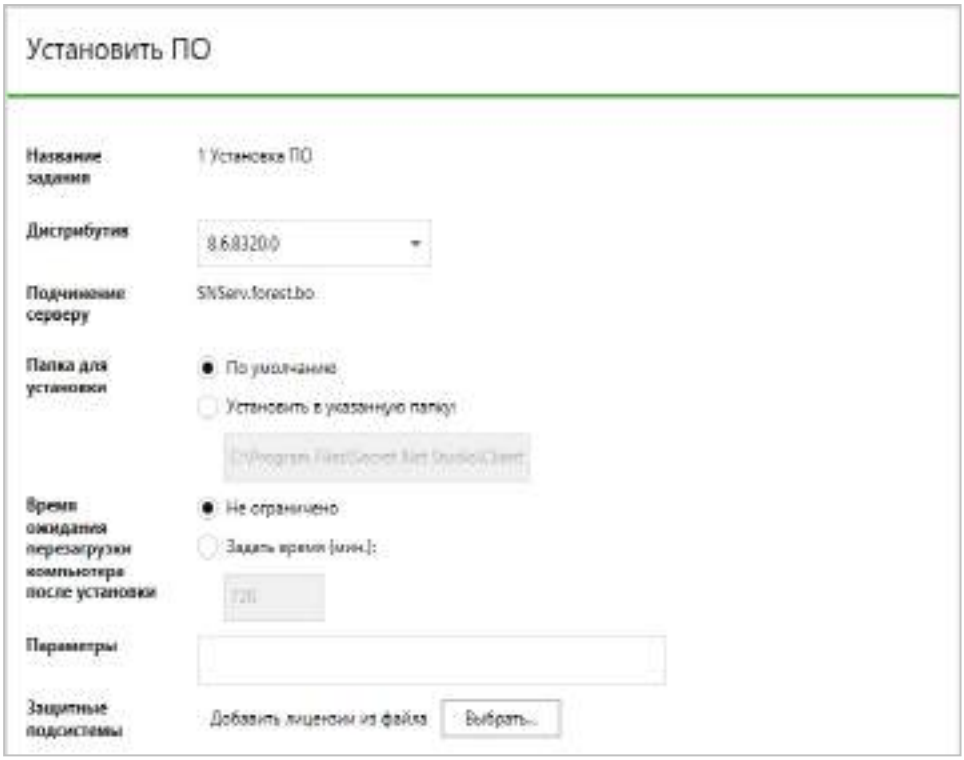
В таблице можно изменять состав отображаемых колонок и порядок их следования. Чтобы настроить колонки, вызовите контекстное меню в строке заголовков, выберите команду "Настройка колонок" и в появившемся диалоге сформируйте список отображаемых колонок.

Примечание.
Если на компьютере установлено ПО клиента, полные сведения о его версии и установленных защитных подсистемах выводятся при подключении программы управления к серверу безопасности, которому непосредственно подчинен данный компьютер. В случае подключения к другому серверу в том же домене безопасности для этого компьютера отображается только признак наличия ПО клиента. Сведения о составе установленных защитных подсистем в этом случае недоступны.

4. Вызовите контекстное меню одного из выбранных компьютеров и выберите нужную команду. Перечень предусмотренных команд представлен в таблице.

Команда	Описание
Установить ПО	Выполняется установка программного обеспечения клиента (подробное описание настройки параметров задания см. ниже)
Обновить ПО	Выполняется обновление установленной ранее версии программного обеспечения клиента на новую. В этом случае для задания настраивается параметр "Время ожидания перезагрузки ..." и указывается версия клиента для обновления. Запуск процесса обновления программного обеспечения на выбранных компьютерах происходит при выходе пользователя из системы
Исправить ПО	Выполняется исправление установленного ранее программного обеспечения клиента. При выборе этой команды на экране появится сообщение о сформированном задании. Запуск процесса исправления программного обеспечения на выбранных компьютерах происходит при их перезагрузке
Удалить ПО	Выполняется удаление установленного программного обеспечения клиента. При выборе этой команды на экране появится сообщение о сформированном задании. Запуск процесса удаления программного обеспечения на выбранных компьютерах происходит автоматически
Установить пакет исправлений	Выполняется установка пакетов обновлений. В этом случае в параметрах задания можно выбрать один или несколько пакетов обновлений, ранее загруженных в репозиторий. Запуск процесса установки пакетов обновлений на выбранных компьютерах происходит при их перезагрузке
Удалить все пакеты исправлений	Удаляет все установленные ранее пакеты обновлений. При выборе этой команды на экране появится сообщение о сформированном задании. Запуск процесса удаления обновлений на выбранных компьютерах происходит при их перезагрузке

В правой части окна появится панель настройки параметров задания.



5. Настройте параметры задания и нажмите кнопку "Установить" в нижней части панели. Для задания на установку ПО клиента выполняется настройка следующих параметров:
   - версия устанавливаемого ПО;
   - папка для установки ПО;
   - время ожидания перезагрузки компьютера после установки — если выбран вариант "Не ограничено", автоматическая перезагрузка компьютера после установки ПО не выполняется. Для включения режима автоматической перезагрузки выберите вариант "Задать время" и в поле ввода укажите, через сколько минут после завершения установки следует выполнить автоматическую перезагрузку;

     Пояснение.
     При настройке параметров задания для обновления ПО данный параметр определяет, через сколько минут после получения задания компьютер автоматически перезагрузится. Обновление ПО будет выполнено во время перезагрузки компьютера.

   - параметры — определяет параметры командной строки, с которыми будет запущена программа установки (опционально);
   - лицензии на использование компонентов;
   - пакеты обновлений;
   - учетные данные локального администратора (доменного пользователя, входящего в локальные группы администраторов на выбранных компьютерах, а также обладающего привилегией интерактивного входа в систему).
6. После создания задания перейдите к списку заданий на вкладке "Задания" для проверки добавления нового элемента.

Установка с использованием групповых политик

Реализация автоматической установки и обновления ПО клиента с использованием групповых политик основана на применении специально настроенных групповых политик на компьютерах определенных организационных подразделений. На каждом компьютере запуск процесса установки или обновления происходит автоматически при его перезагрузке. Если ПО клиента на компьютере не установлено — запускается процесс установки. При наличии ПО клиента — выполняется обновление на текущую версию.

Процедура настройки системы для автоматической установки и обновления состоит из следующих этапов:

1. Начальное формирование структуры ОУ (см. стр.**30**).
2. Создание файлов со сценарием установки (см. стр.**30**).
3. Создание общедоступного сетевого ресурса (см. стр.**36**).
4. Создание организационных подразделений и включение в них компьютеров (см. стр.**37**).
5. Создание и настройка групповых политик для нужных организационных подразделений (см. стр.**37**).

Начальное формирование структуры ОУ

Компьютеры, на которых будет выполняться автоматическая установка ПО клиента (сетевой режим работы), следует включить в структуру оперативного управления (ОУ), подчинив каждый компьютер серверу безопасности. Для этого в системе должна быть развернута соответствующая структура серверов безопасности и подготовлено рабочее место администратора Secret Net Studio.

Подчинение серверам безопасности компьютеров без установленного клиентского ПО осуществляется средствами программы управления. Сведения о работе с программой управления см. в документе [**4**].

Примечание.
Не требуется подчинять серверу безопасности компьютеры, на которых предполагается использовать клиент Secret Net Studio в автономном режиме работы.

Создание файлов со сценарием установки

Сценарий предназначен для автоматизации процесса установки клиентского ПО и позволяет полностью автоматизировать ввод информации, запрашиваемой программой установки клиента.

Файлы со сценарием установки создаются в INI-формате и являются файлами конфигурации, которые содержат данные по настройке клиентского ПО Secret Net Studio. Созданные файлы необходимо поместить в корневые папки созданных ОСР (см. стр.**36**).

Создать файл сценария можно средствами программы установки клиента (см. стр.**22**) или вручную.

Совет.
В качестве шаблона сценария можно использовать файл сценария, созданный с помощью программы установки клиента, или использовать пример сценария, приведенный ниже.

Для создания файла сценария вручную:

- В текстовом редакторе создайте файл SnInst.rsp, сформируйте его содержимое и сохраните файл.

Структура файла сценария

Файл сценария имеет следующую структуру:

[Section_1]
параметр_1 = значение_параметра_1
параметр_2 = значение_параметра_2
...
параметр_N = значение_параметра_N
[Section_2]
параметр_1 = значение_параметра_1
параметр_2 = значение_параметра_2
...
параметр_N = значение_параметра_N
[Section_N]
параметр_1 = значение_параметра_1
параметр_2 = значение_параметра_2
...
параметр_N = значение_параметра_N

В секциях [Section...] указываются параметры и их значения, необходимые программе установки ПО клиента. Перечень основных секций и параметров представлен в следующей таблице.

Параметр	Значение по умолчанию	Описание
Секция [Core]		
Action	install	Определяет состояние компонента "Базовая защита": • "install" – компонент установлен; • "none" – компонент не установлен
Секция [Console]		
Action	install	Определяет состояние программы управления в локальном режиме: • "install" – программа установлена; • "none" – программа не установлена
Секция [Local]		
Action	none	Определяет состояние компонента локальной защиты: • "install" – компонент установлен; • "none" – компонент не установлен
ERASER	0	Определяет состояние компонента "Затирание данных": • "1" — компонент включен; • "0" — компонент отключен
DC	0	Определяет состояние компонента "Контроль устройств": • "1" — компонент включен; • "0" — компонент отключен
FDC	0	Определяет состояние компонента "Дискреционное управление доступом": • "1" — компонент включен; • "0" — компонент отключен

Параметр	Значение по умолчанию	Описание
EXEQUOTA	0	Определяет состояние компонента "Замкнутая программная среда": • "1" — компонент включен; • "0" — компонент отключен
MC	0	Определяет состояние компонента "Полномочное управление доступом": • "1" — компонент включен; • "0" — компонент отключен
Секция [Pc]		
Action	none	Определяет состояние компонента "Контроль печати": • "install" – компонент включен; • "none" – компонент отключен
Секция [Disk]		
Action	none	Определяет состояние компонента "Защита дисков и шифрование данных": • "install" – компонент включен; • "none" – компонент отключен
TBL	0	Определяет состояние компонента защиты дисков: • "1" — компонент установлен; • "0" — компонент не установлен
CRCONT	0	Определяет состояние компонента защиты криптоконтейнеров: • "1" — компонент установлен; • "0" — компонент не установлен
Секция [Ta]		
Action	none	Определяет состояние компонента сетевой защиты: • "install" – компонент установлен; • "none" – компонент не установлен
TA_Firewall	0	Определяет состояние компонента "Персональный межсетевой экран": • "1" — компонент включен; • "0" — компонент отключен
TA_IPSEC	0	Определяет состояние компонента "Авторизация сетевых соединений": • "1" — компонент включен; • "0" — компонент отключен
TA_IDS	0	Определяет состояние компонента "Обнаружение и предотвращение вторжений": • "1" — компонент включен; • "0" — компонент отключен
Секция [Antivirus]		
Action	none	Определяет состояние компонента "Антивирус": • "install" – компонент включен; • "none" – компонент отключен
Секция [Common]		
Installdir	[ProgramFilesFolder]Secret Net Studio\Client	Папка установки ПО клиента
User	Отсутствует	Имя пользователя из группы администраторов домена безопасности

Параметр	Значение по умолчанию	Описание
Password	Отсутствует	Пароль пользователя
Server	Отсутствует	Идентификатор безопасности сервера безопасности: • присутствует – сетевой режим функционирования клиента; • отсутствует – автономный режим функционирования клиента
Source *	Отсутствует	Источник установочного файла клиента
Division	Отсутствует	Учетная информация компьютера: название подразделения
SysName	Отсутствует	Учетная информация компьютера: название автоматизированной системы
Workplace	Отсутствует	Учетная информация компьютера: рабочее место
Id	Отсутствует	Учетная информация компьютера: номер системного блока
LicenseFilePath *	Отсутствует	Имя файла лицензии
Servername	Отсутствует	DNS-имя сервера безопасности
locale **	Отсутствует	Определяет язык системы: • "ru-RU" – русский; • "en-US" – английский
RebootTimeOut	Отсутствует	Время в минутах до перезагрузки компьютера и начала установки
Секция [Softpspt]		
Action	none	Определяет состояние компонента "Паспорт ПО": • "install" – компонент включен; • "none" – компонент отключен
Секция [Patches]		
Count	Отсутствует	Количество необязательных (Normal) пакетов исправлений для установки
PatchN	Отсутствует	Путь к необязательному пакету исправлений, где "N" – порядковый номер пакета
Секция [Te]		
Action	none	Определяет состояние компонента "Доверенная среда": • "install" – компонент включен; • "none" – компонент отключен

* Обязательный параметр.

** Обязательный и регистрозависимый параметр.

Для задания пути допускается использование переменных среды. Имя переменной среды задается в квадратных скобках и должно находиться в начале значения параметра. Перечень поддерживаемых переменных среды представлен в таблице.

Переменная среды	Пример значения
WindowsVolume	C:\
WindowsFolder	C:\WINDOWS\
USERPROFILE	C:\Documents and Settings\Ivanov\

Переменная среды	Пример значения
TemplateFolder	C:\Documents and Settings\All Users\Templates\
TempFolder	C:\Documents and Settings\Ivanov\Local Settings\Temp
SystemFolder	C:\WINDOWS\system32\
StartupFolder	C:\Documents and Settings\All Users\Start Menu\Programs\Startup\
StartMenuFolder	C:\Documents and Settings\All Users\Start Menu
SendToFolder	C:\Documents and Settings\Ivanov\SendTo\
ProgramMenuFolder	C:\Documents and Settings\All Users\Start Menu\Programs\
PrimaryVolumePath	C:\
PersonalFolder	C:\Documents and Settings\Ivanov\My Documents\
MyPicturesFolder	C:\Documents and Settings\Ivanov\My Documents\My Pictures\
LocalAppDataFolder	C:\Documents and Settings\Ivanov\Local Settings\Application Data\
FontsFolder	C:\WINDOWS\Fonts\
FavoritesFolder	C:\Documents and Settings\Ivanov\Favorites\
CommonFilesFolder	C:\Program Files\Common Files\
CommonAppDataFolder	C:\Documents and Settings\All Users\Application Data\
ProgramFilesFolder	C:\Program Files\
AppDataFolder	C:\Documents and Settings\Ivanov\Application Data
AdminToolsFolder	C:\Documents and Settings\All Users\Start Menu\Programs\Administrative Tools\
ALLUSERSPROFILE	C:\Documents and Settings\All Users

Пример содержимого файла сценария

Ниже представлен пример содержимого файла сценария для установки клиента, который будет функционировать в автономном режиме.

```
[core]
Action=install
[console]
Action=install
[local]
Action=install
ERASER=1
DC=1
FDC=1
EXEQUOTA=1
MC=1
[pc]
Action=none
[disk]
Action=install
TBL=1
CRCONT=1
[ta]
Action=install
TA_Firewall=1
TA_IPSEC=1
TA_IDS=1
```

```
[antivirus]
Action=install
[Common]
Installdir=C:\Program Files\Secret Net Studio\Client\
server=
Source=\\computer.TWinfo.local\OSR
LicenseFilePath=full_new
locale=ru-RU
[softpspt]
Action=none
[patches]
count=2
patch0=\\computer.TWinfo.local\OSR\tools\SecurityCode\Patches\8_ 5_ 5329_ 8_ Inc72574_Build5\
patch1=\\computer.TWinfo.local\OSR\tools\SecurityCode\Patches\8_ 5_ 5329_ 9_ Inc72994_Build6\
```

В приведенном примере предписывается:

1. Установить компонент "Базовая защита".
2. Установить программу управления в локальном режиме.
3. Установить компонент локальной защиты.
   - Включить компонент "Затирание данных".
   - Включить компонент "Контроль устройств".
   - Включить компонент "Дискреционное управление доступом".
   - Включить компонент "Замкнутая программная среда".
   - Включить компонент "Полномочное управление доступом".
4. Отключить компонент "Контроль печати".
5. Включить компонент "Защита дисков и шифрование данных".
   - Установить компонент защиты дисков.
   - Установить компонент защиты криптоконтейнеров.
6. Установить компонент сетевой защиты.
   - Включить компонент "Персональный межсетевой экран".
   - Включить компонент "Авторизация сетевых соединений".
   - Включить компонент "Обнаружение и предотвращение вторжений".
7. Включить компонент "Антивирус".
8. Установить продукт в папку программ на системном диске в папке \Secret Net Studio\Client.
   - Идентификатор безопасности сервера безопасности отсутствует.
   - Источник установочного файла клиента:\\computer.TWinfo.local\OSR.
   - Имя файла используемой лицензии "full_new".
   - Установить русский язык для системы защиты.
9. Отключить компонент "Паспорт ПО".
10. Установить два необязательных (Normal) пакета исправлений. Все обязательные (Critical) пакеты исправлений устанавливаются автоматически.
    - Два пакета исправлений с указанием их месторасположения.

Примечание.
В сценарии может быть использован только один тип антивируса согласно выбранной лицензии: антивирус, антивирус (технология ESET) или антивирус (технология Касперского).

Создание общедоступного сетевого ресурса

В домене AD необходимо создать общедоступный сетевой ресурс (ОСР), содержащий файлы для установки ПО клиента, файл с лицензиями и файл со сценарием установки.

Внимание!
Если в домене AD имеется несколько серверов безопасности, то для каждого из них требуется создать отдельный ОСР со своим набором данных.

Для создания ОСР:

1. На одном из компьютеров домена создайте папку и откройте к ней общий доступ.

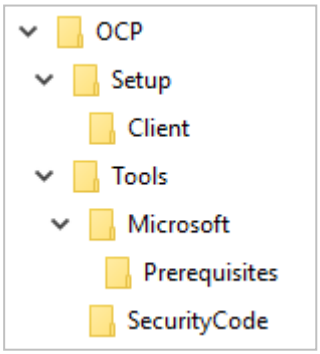
Внимание!
Дополнительно предоставьте права доступа на чтение содержимого этой папки всем учетным записям компьютеров, на которые планируется устанавливать ПО клиента, или группе "Domain Computers".

Примечание.
Во время проведения автоматической установки ПО этот компьютер должен быть доступен для сетевых обращений. Рекомендуется создать ОСР на одном из файловых серверов домена.

2. С установочного диска Secret Net Studio скопируйте в созданную папку содержимое следующих папок (сохраняя их структурную вложенность):

Имя папки	Назначение
\Setup\Client\	Содержит дистрибутивы для установки ПО клиента на 32- и 64-разрядных версиях ОС Windows
\Tools\Microsoft\ Prerequisites	Содержит файлы установки необходимых обновлений ОС Windows. Если файлы отсутствуют, автоматическая установка клиента на компьютерах не будет выполняться
\Tools\SecurityCode\	Содержит вспомогательные утилиты и файлы настройки, необходимые для работы с Secret Net Studio

Структура папки ОСР представлена на следующем рисунке.



3. В созданную папку скопируйте файл с лицензиями на использование компонентов Secret Net Studio.

Совет.
Если предполагается использовать клиент в сетевом режиме работы, также добавьте на сервер безопасности лицензии, содержащиеся в данном файле.

4. В созданную папку скопируйте файл со сценарием установки.

Настройка Active Directory

Формирование организационных подразделений

Чтобы выделить компьютеры домена, на которых будет выполняться автоматическая установка или обновление ПО, необходимо создать организационные подразделения (Organizational Units) и включить в них нужные компьютеры. Также можно использовать имеющиеся организационные подразделения.

Создание организационных подразделений и добавление объектов осуществляется стандартными средствами управления.

Создание и настройка групповых политик

Для подготовленных организационных подразделений необходимо создать групповые политики автоматической установки ПО. Групповые политики создаются отдельно для 32- и 64-разрядных версий ОС Windows.

После того как автоматическая установка ПО будет выполнена на всех компьютерах, созданные групповые политики можно удалить стандартными способами.

Для создания групповой политики на контроллере домена:

1. Вызовите консоль "Управление групповой политикой".
2. Вызовите контекстное меню организационного подразделения, на компьютерах которого будет проводиться автоматическая установка, и выберите команду "Создать объект групповой политики в этом домене и связать его".
3. В появившемся диалоге введите имя создаваемой политики и нажмите кнопку "OK".

   Новая политика появится в иерархическом списке в качестве подчиненного объекта организационного подразделения.
4. Вызовите контекстное меню политики и выберите команду "Изменить".

   На экране появится окно редактора групповых политик.
5. В дереве объектов политики перейдите к разделу "Конфигурация компьютера\ Политики\Конфигурация программ\Установка программ", вызовите контекстное меню подраздела и выберите команду "Создать\Пакет".

   На экране появится диалог "Открытие".
6. В поле "Имя файла" введите нужное значение:
   - для применения политики на компьютерах с 32-разрядной ОС Windows: <*сетевой_путь_к_папке_ОСР*>\Setup\Client\Win32\InstAgent.msi;
   - для применения политики на компьютерах с 64-разрядной ОС Windows: <*сетевой_путь_к_папке_ОСР*>\Setup\Client\x64\InstAgent.msi.
7. В диалоговом окне нажмите кнопку "Открыть".

   На экране появится окно развертывания программ.
8. Нажмите кнопку "OK".

Совет.

Для созданного пакета с 32-разрядной версией дистрибутива рекомендуется удалить отметку из поля "Сделать это 32-разрядное X86 приложение доступным для компьютеров с архитектурой Win64". Для этого в свойствах пакета перейдите на вкладку "Развертывание " и нажмите кнопку "Дополнительно".

Совет.

Если используются несколько организационных подразделений для автоматической установки ПО, создавать отдельные групповые политики для каждого подразделения необязательно. В остальных подразделениях можно добавить ссылку на созданные групповые политики (с помощью команды контекстного меню "Связать существующий объект групповой политики").

Для применения созданной групповой политики:

1. Перезагрузите компьютер, на котором выполняется установка ПО клиента.
2. Войдите в систему под учетной записью пользователя.

   После успешного входа пользователя в систему над пиктограммой Secret Net Studio, находящейся на панели задач Windows, появится сообщение об установке. После запуска перезагрузки компьютера начнется установка компонентов Secret Net Studio.

Установка с использованием SCCM

Реализация централизованного запуска процессов для клиентов Secret Net Studio осуществляется с помощью продукта для управления ИТ-инфраструктурой на основе Microsoft Windows и смежных устройств —System Center Configuration Manager (SCCM).

Средствами SCCM может происходить запуск процессов:

- установки, обновления, исправления или удаления клиентского ПО;
- установки или удаления пакетов обновления.

Процедура настройки системы состоит из следующих этапов:

1. Начальное формирование структуры ОУ (см. стр.**38**).
2. Создание файлов со сценарием установки (см. стр.**38**).
3. Создание общедоступного сетевого ресурса SCCM (см. стр.**40**).
4. Настройка SCCM (см. стр.**41**).

Начальное формирование структуры ОУ

Компьютеры, на которых будет выполняться запуск процессов, следует подчинить серверу безопасности. Для этого в системе должна быть развернута соответствующая структура серверов безопасности и подготовлено рабочее место администратора Secret Net Studio.

Подчинение серверам безопасности компьютеров без установленного клиентского ПО осуществляется средствами программы управления. Сведения о работе с программой управления см. в документе [**4**].

Примечание.
Не требуется подчинять серверу безопасности компьютеры, на которых предполагается использовать клиента Secret Net Studio в автономном режиме работы.

Создание файлов со сценарием установки

Описание процесса создания файлов со сценарием для процесса установки ПО клиента и структура файла сценария соответствует описанию групповых политик (стр.**30**).

Пример содержимого файла сценария

Ниже представлен пример содержимого файла сценария для установки клиента, который будет функционировать в сетевом режиме.

```
[core]
Action=install
[console]
Action=install
[local]
Action=install
ERASER=1
DC=1
FDC=1
```

```
EXEQUOTA=1
MC=1
[pc]
Action=install
[disk]
Action=install
TBL=1
CRCONT=1
[Common]
Action=install
Installdir=C:\Program Files\Secret Net Studio\Client\
server=S-1-5-21-3534210826-639358159-2414785253-3826
Source=\\MSS2012\OSR\
LicenseFilePath=lic
servername=WIN-ATC89VIN2B9.testsn7.ru
locale=ru-RU
[ta]
Action=install
TA_Firewall=1
TA_IPSEC=1
TA_IDS=1
[softpspt]
Action=none
[te]
Action=none
[antivirus]
Action=install
[patches]
count=3
patch0=\\MSS2012\OSR\tools\SecurityCode\Patches\8_6_6186_11_IncidentTest_
LocalControlCentre_Client\
patch1=\\MSS2012\OSR\tools\SecurityCode\Patches\8_6_6186_14_IncidentTest_
AuthServer_Server\
patch2=\\MSS2012\OSR\tools\SecurityCode\Patches\8_ 6_ 6186_ 16_
IncidentTest5_Core_Client\
```

В приведенном примере предписывается:

1. Установить компонент "Базовая защита".
2. Установить программу управления в локальном режиме.
3. Установить компонент локальной защиты.
   - Включить компонент "Затирание данных".
   - Включить компонент "Контроль устройств".
   - Включить компонент "Дискреционное управление доступом".
   - Включить компонент "Замкнутая программная среда".
   - Включить компонент "Полномочное управление доступом".
4. Включить компонент "Контроль печати".
5. Включить компонент "Защита дисков и шифрование данных".
   - Установить компонент защиты дисков.
   - Установить компонент защиты криптоконтейнеров.

6. Установить продукт в папку программ на системном диске в папке \Secret Net Studio\Client.
   - Идентификатор безопасности сервера безопасности S- 1- 5- 21-3534210826-639358159-2414785253-3826.
   - Источник установочного файла клиента:\\MSS2012\OSR.
   - Имя файла используемой лицензии "lic".
   - DNS-Имя сервера безопасности WIN-ATC89VIN2B9.testsn7.ru.
   - Установить русский язык для системы защиты.
7. Установить компонент сетевой защиты.
   - Включить компонент "Персональный межсетевой экран".
   - Включить компонент "Авторизация сетевых соединений".
   - Включить компонент "Обнаружение и предотвращение вторжений".
8. Отключить компонент "Паспорт ПО".
9. Отключить компонент "Доверенная среда".
10. Включить компонент "Антивирус".
11. Установить три необязательных (Normal) пакета исправлений. Все обязательные (Critical) пакеты исправлений устанавливаются автоматически.
    - Три пакета исправлений с указанием их месторасположения.

Примечание.
В сценарии может быть использован только один тип антивируса согласно выбранной лицензии: антивирус, антивирус (технология ESET) или антивирус (технология Касперского).

Создание общедоступного сетевого ресурса SCCM

В домене AD необходимо создать общедоступный сетевой ресурс (ОСР), содержащий файлы для установки ПО клиента, файл с лицензиями и файл со сценарием установки.

Внимание!
Если в домене AD имеется несколько серверов безопасности, то для каждого из них требуется создать отдельный ОСР со своим набором данных.

Для создания ОСР:

1. На одном из компьютеров домена создайте папку и откройте общий доступ к ней и к диску, на котором расположена эта папка. Дополнительно предоставьте все права доступа на содержимое этой папки всем учетным записям компьютеров, на которые планируется устанавливать ПО клиента.

   Примечание.
   Во время проведения автоматической установки ПО этот компьютер должен быть доступен для сетевых обращений. Рекомендуется создать ОСР на одном из файловых серверов домена.

2. В созданную папку скопируйте файл с лицензиями на использование компонентов Secret Net Studio.

   Совет.
   Если предполагается использовать клиента в сетевом режиме работы, также добавьте на сервер безопасности лицензии, содержащиеся в данном файле.

3. В созданную папку скопируйте файл со сценарием установки.

   Примечание.
   Для обновления, исправления, удаления клиентского ПО и удаления пакетов обновления, наличие файла с лицензиями на использование компонентов и файла со сценарием установки не требуется в ОСР.

Настройка SCCM

Возможны следующие варианты развертывания ПО на клиентском компьютере:

- пакет установки;
- приложение.

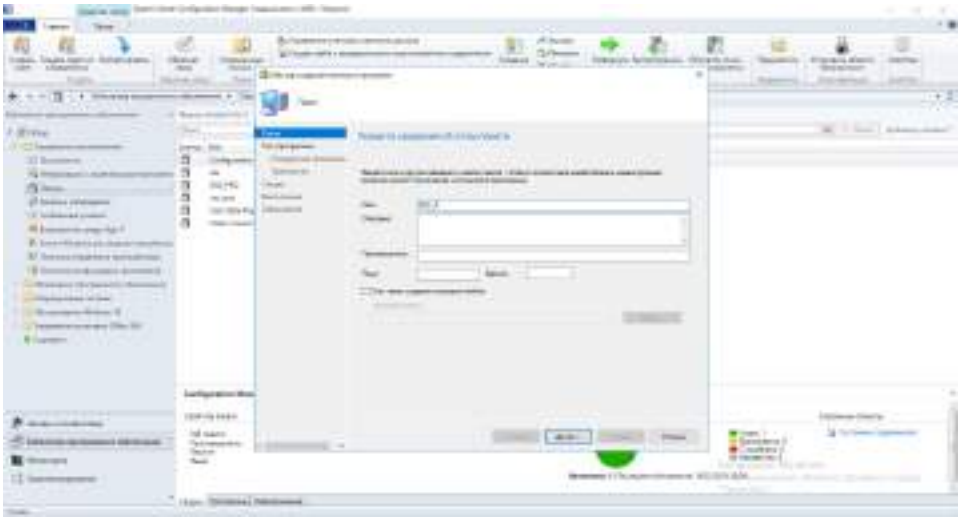
Развертывание пакета установки через SCCM

Для централизованного развертывания клиентов необходимо создать и установить пакет установки.

Для создания пакета установки:

1. Откройте System Center Configuration Manager.
2. В нижней части панели навигации выберите "Библиотека программного обеспечения" (слева в основном окне).
3. В верхней части панели навигации в окне структуры раскройте ветвь "Управление приложениями" (слева в основном окне).
4. Вызовите контекстное меню объекта "Пакеты" и выберите команду "Создать пакет".

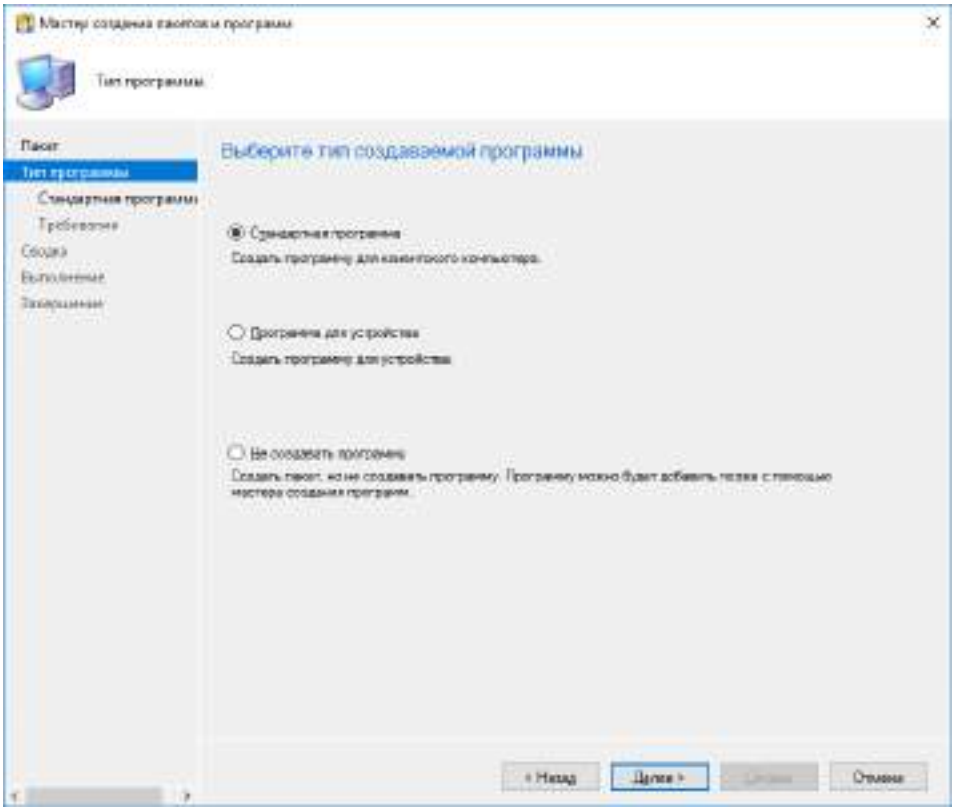
   На экране появится диалог, подобный следующему.



5. В поле "Имя" укажите название пакета и нажмите кнопку "Далее >".

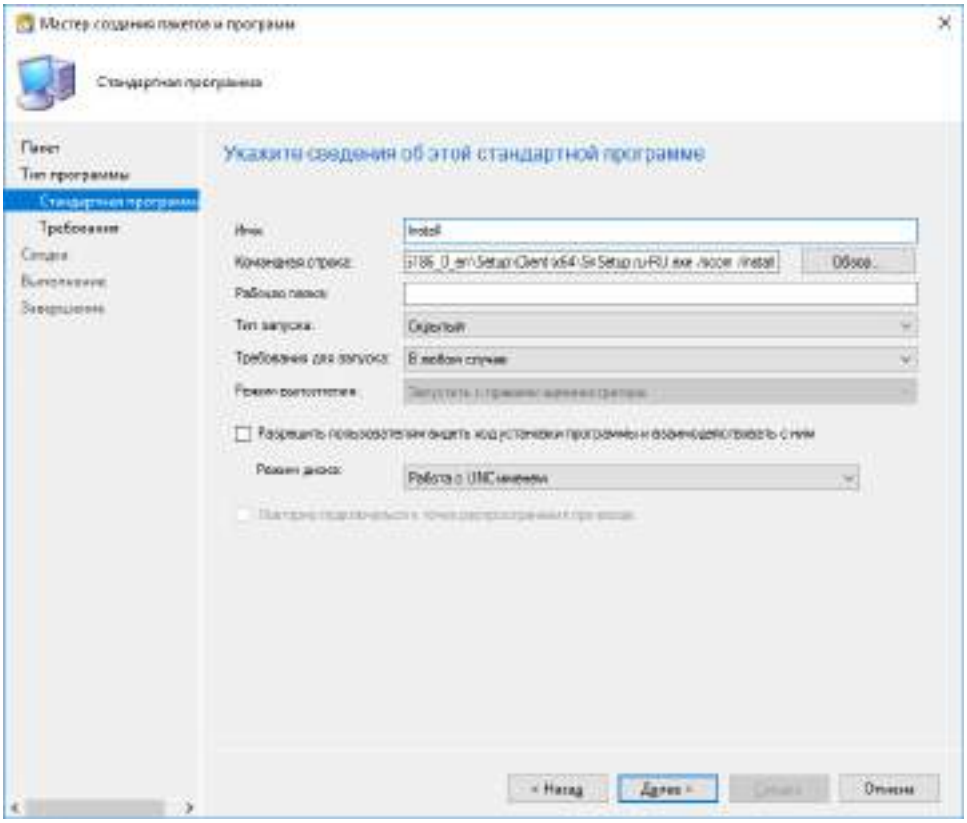
   Примечание
   Если дистрибутив находится на ОСР, то не требуется устанавливать отметку в поле "Этот пакет содержит исодные файлы".

   На экране появится диалог, подобный следующему.



6. В диалоге установите отметку в поле "Стандартная программа" и нажмите кнопку "Далее >".

На экране появится диалог, подобный следующему.



7. Для стандартной программы выполните следующие действия:

- Укажите информацию:
  - в поле "Имя" укажите название стандартной программы;

- в поле "Командная строка" укажите в соответствующем формате путь к дистрибутиву и команду (см. ниже);
- в поле "Тип запуска" выберите параметр "Скрытый";
- в поле "Требования для запуска" выберите параметр "В любом случае".

- Нажмите кнопку "Далее >".

На экране появится диалог требований для стандартной программы.

Поле "Командная строка" имеет следующий формат ввода:

```
<путь к дистрибутиву> /sccm /<команда>
```

Описание команд представлено в следующей таблице.

Команда	Описание
install	Выполняется установка программного обеспечения клиента
upgrade	Выполняется обновление установленной ранее версии программного обеспечения клиента на новую
repair	Выполняется исправление установленного ранее программного обеспечения клиента
uninstall	Выполняется удаление установленного программного обеспечения клиента
applypatch "путь к папке с пакетом обновлений"	Выполняется установка пакетов обновления
removeallpatches	Удаляет все установленные ранее пакеты обновления

8. Нажмите кнопку "Далее >".

   На экране появится диалог подтверждения параметров.

9. В диалоге проверьте содержимое и нажмите кнопку "Далее >".

   Начнется процесс создания пакета установки.

10. После завершения нажмите кнопку "Закрыть".

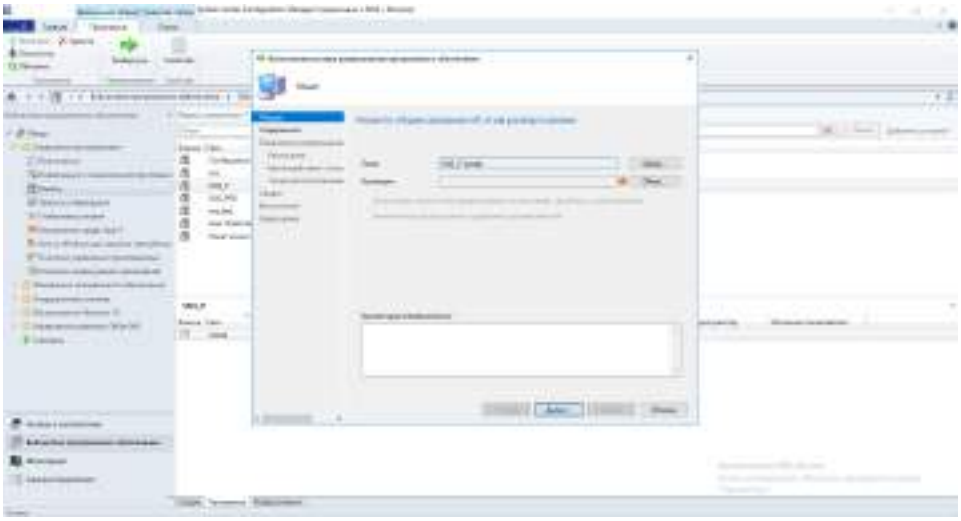
    По окончании процесса в списке пакетов установок появится новый пакет, содержащий сведения о созданных программах.

Примечание.
Добавление новых стандартных программ в пакет установки осуществляется после его создания. Для добавления новой стандартной программы вызовите контекстное меню созданного пакета установки и выберите команду "Создать программу", а затем выполните действия **6–10**.

Для установки стандартной программы созданного пакета установки:

1. Откройте System Center Configuration Manager.
2. В нижней части панели навигации выберите "Библиотека программного обеспечения" (слева в основном окне).
3. В верхней части панели навигации в окне структуры раскройте ветвь "Управление приложениями" (слева в основном окне).
4. Выберите объект "Пакеты".
5. В списке пакетов установок выберите созданный ранее пакет.
6. Перейдите на вкладку "Программы" (снизу в основном окне) и выберите стандартную программу, созданную ранее.
7. Вызовите контекстное меню стандартной программы и выберите команду "Развернуть".

   На экране появится диалог, подобный следующему.

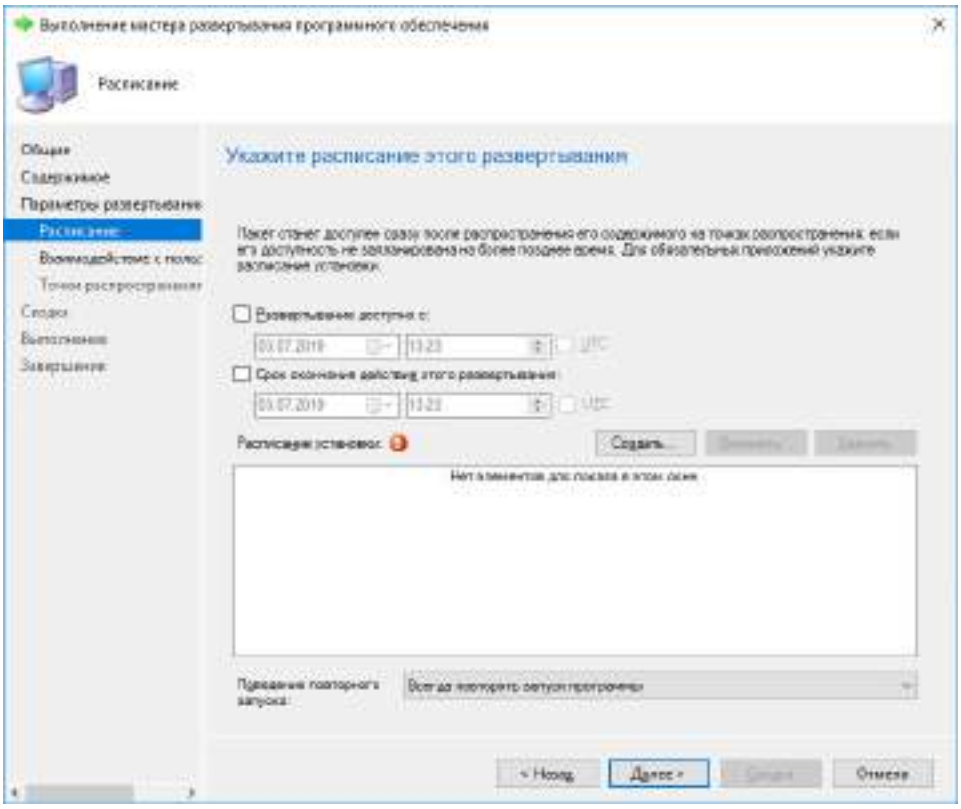


8. Напротив поля "Коллекция" нажмите на кнопку "Обзор" и в появившемся списке выберите необходимую коллекцию компьютеров на которую требуется установить пакет установки, а затем нажмите кнопку "ОК".
9. Нажмите кнопку "Далее >".

   На экране появится диалог места распространения содержимого.
10. Нажмите кнопку "Далее >".

    На экране появится диалог параметров управления процессом развертывания этого программного обеспечения.
11. В поле "Намерение" укажите "Обязательная установка" и нажмите кнопку "Далее >".

    На экране появится диалог расписания этого развертывания программного обеспечения.



12. Выполните следующие действия:
    - Нажмите кнопку "Создать":
      - Установите отметку в поле "Назначить сразу после этого события";

- В выпадающем меню выберите "Как можно скорее".
- Нажмите кнопку "ОК".

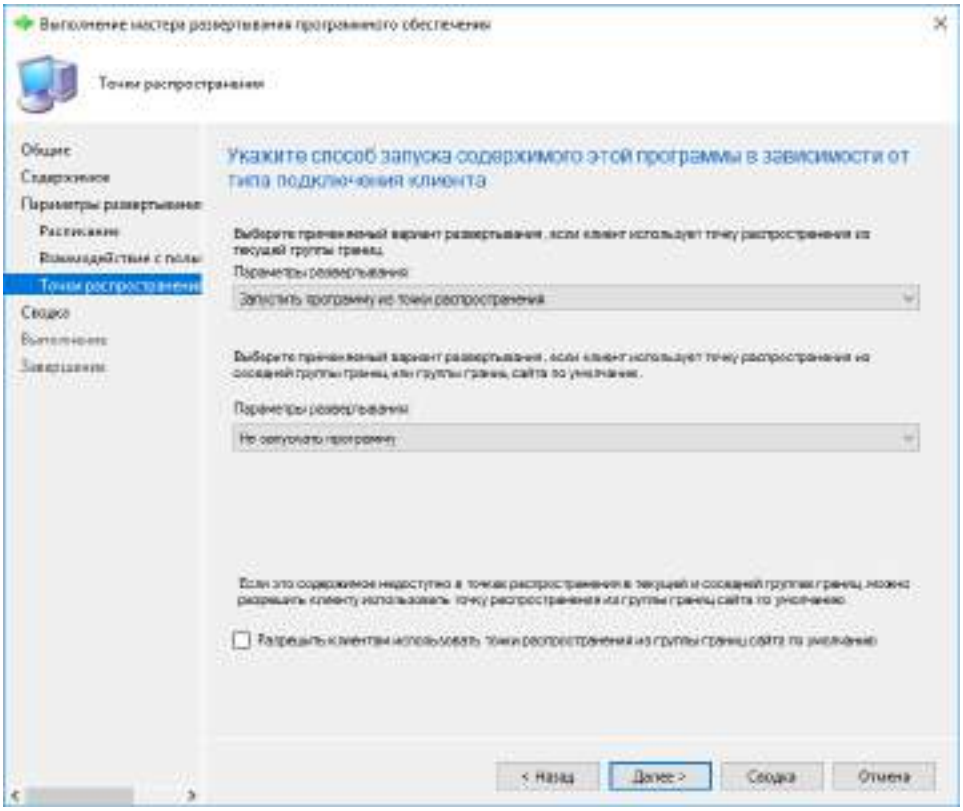
В списке расписания заданий появится новая запись.

13. В поле "Поведение повторного запуска" выберите "Всегда повторять запуск программы" и нажмите кнопку "Далее >".

На экране появится диалог параметров взаимодействия с пользователем при установке этого программного обеспечения.

14. Нажмите кнопку "Далее >".

На экране появится диалог, подобный следующему.



15. В поле "Параметры развертывания" укажите "Запустить программу из точки распространения" и нажмите кнопку "Далее >".

На экране появится диалог подтверждения параметров развертывания.

16. В диалоге проверьте содержимое и нажмите кнопку "Далее >".

Начнется процесс установки стандартной программы.

17. После завершения нажмите кнопку "Закрыть".

Примечание.
Для установки созданных ранее стандартных программ из пакета установки выполните действия **6–17**.

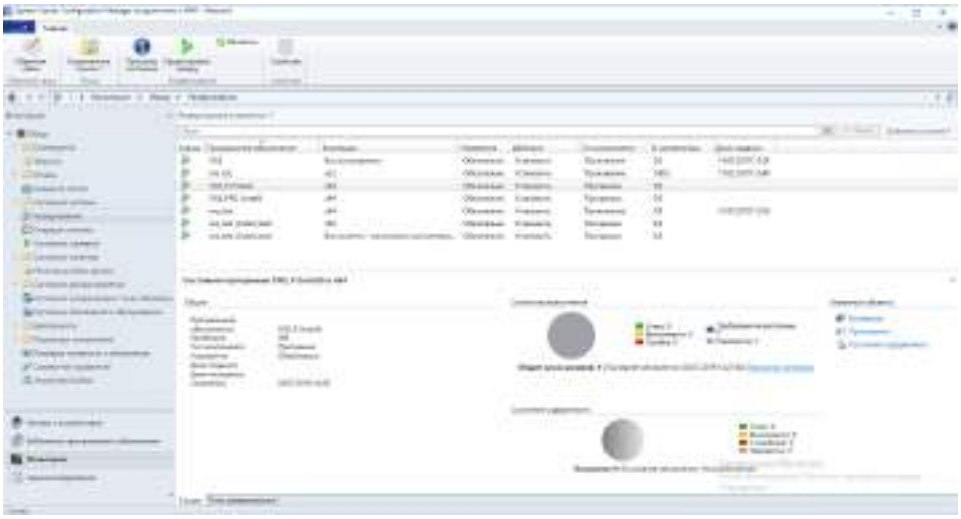
Для отслеживания процесса выполнения стандартной программы:

1. Откройте System Center Configuration Manager.

2. В нижней части панели навигации выберите "Мониторинг" (снизу в основном окне).

3. В верхней части панели навигации в окне структуры выберите "Развертывания".

На экране появится диалог, подобный следующему.



4. В списке программного обеспечения выберите требуемую стандарнтую программу и посмотрите ее состояние.

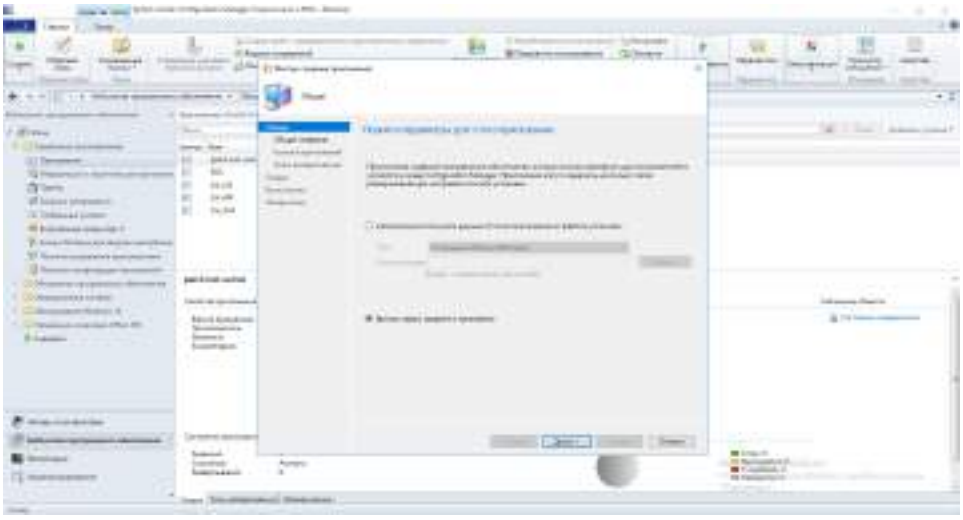
Развертывание приложения через SCCM

Для централизованного развертывания клиентов необходимо создать и установить приложение.

Для создания приложения:

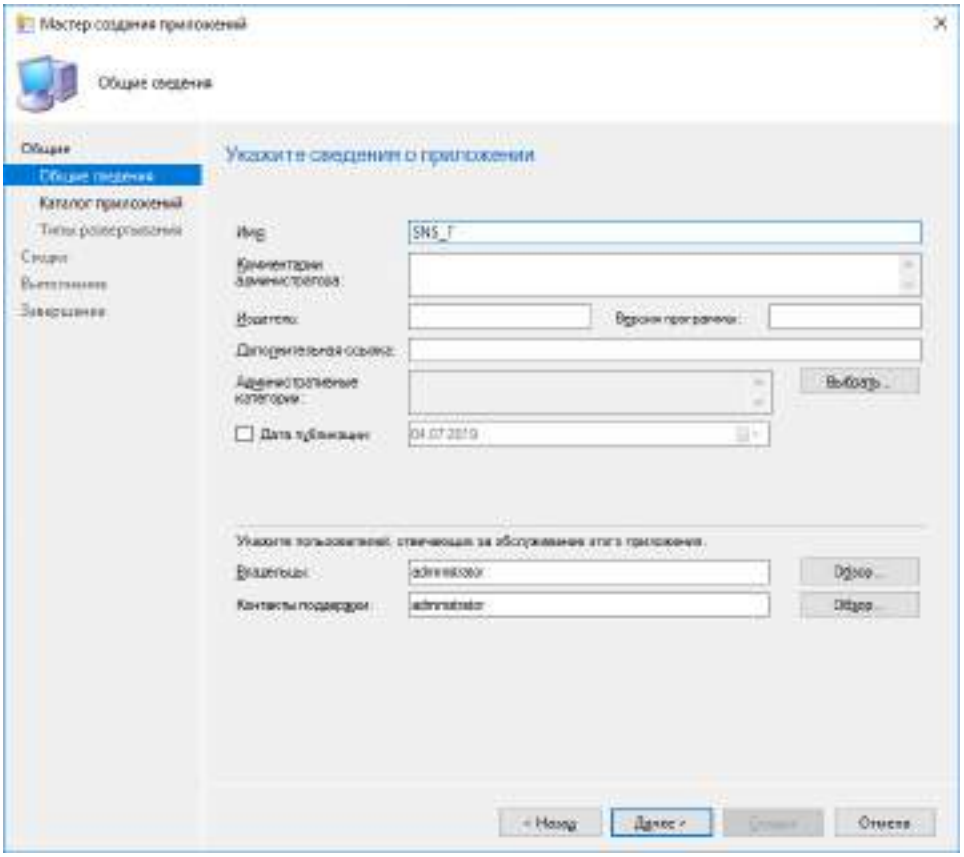
1. Откройте System Center Configuration Manager.
2. В нижней части панели навигации выберите "Библиотека программного обеспечения" (слева в основном окне).
3. В верхней части панели навигации в окне структуры раскройте ветвь "Управление приложениями" (слева в основном окне).
4. Вызовите контекстное меню объекта "Приложения" и выберите команду "Создать приложение".

   На экране появится диалог, подобный следующему.

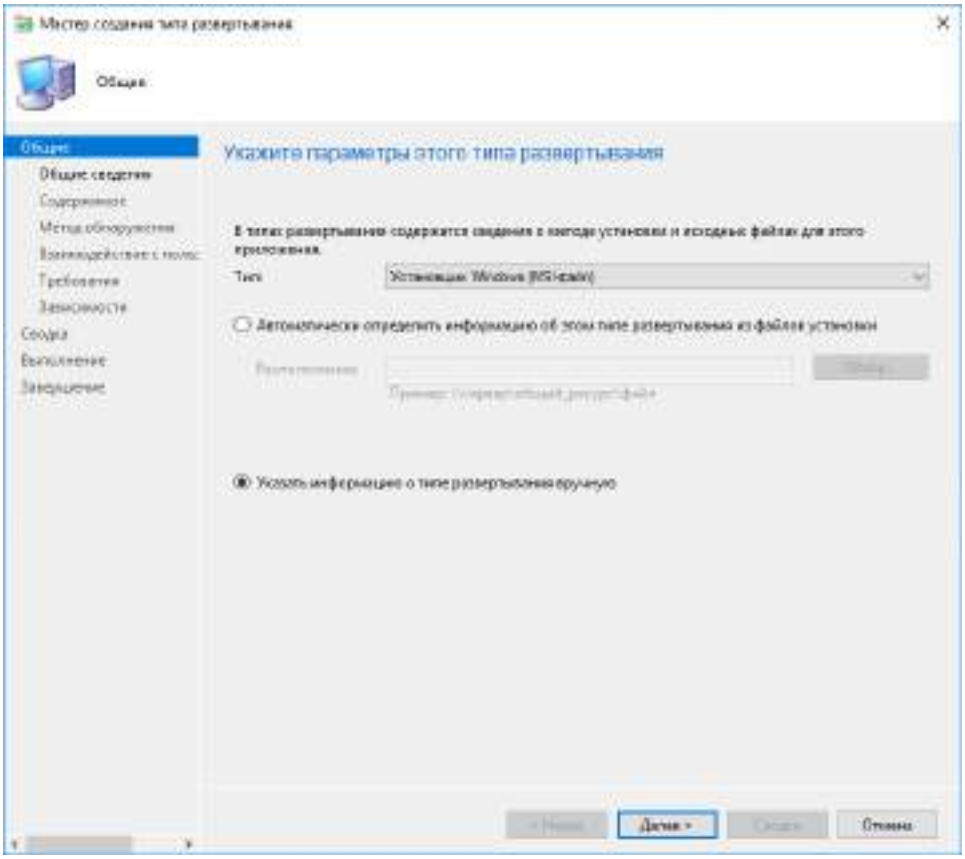


5. В диалоге установите отметку в поле "Вручную задать сведения о приложении" и нажмите кнопку "Далее >".

   На экране появится диалог, подобный следующему.

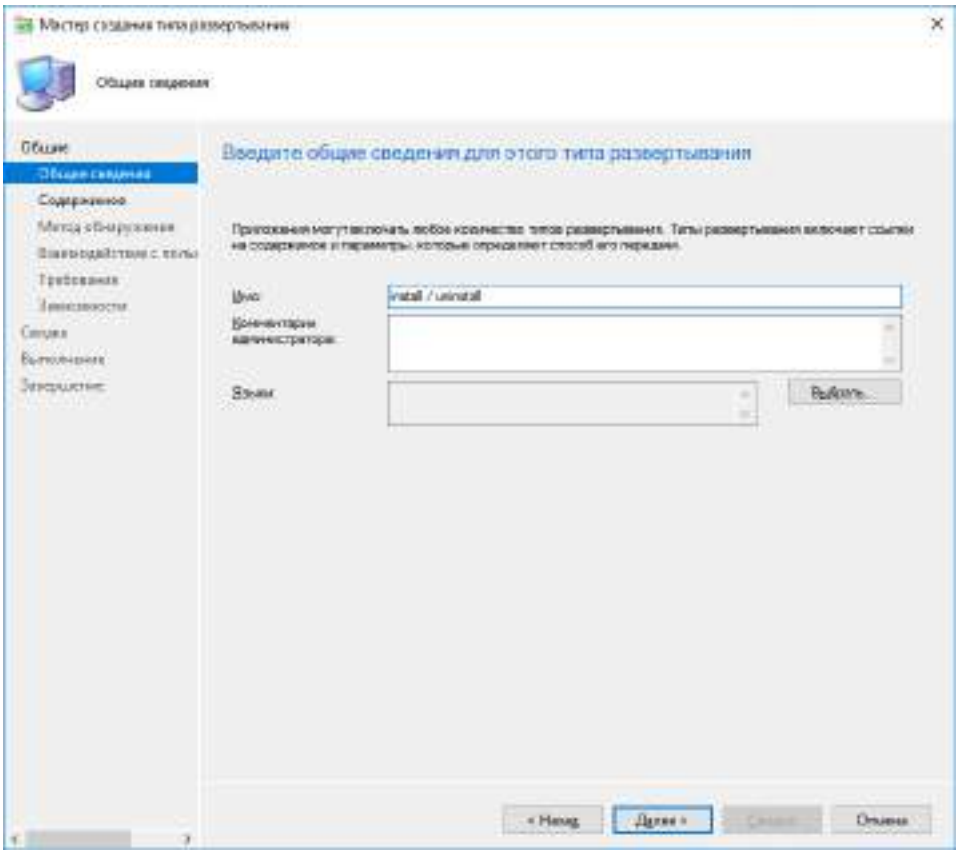


6. В поле "Имя" укажите название приложения и нажмите кнопку "Далее >".
   На экране появится диалог каталог приложений.
7. Нажмите кнопку "Далее >".
   На экране появится диалог типы развертывания.
8. Нажмите кнопку "Добавить".
   На экране появится диалог создания типа развертывания.



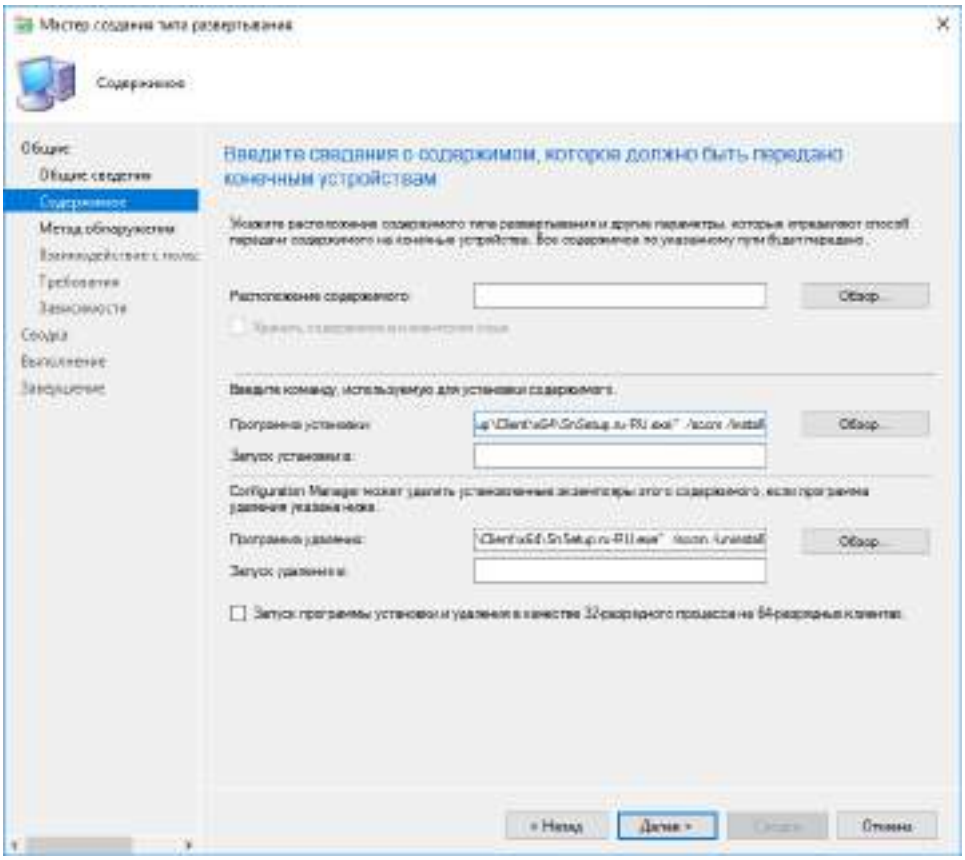
9. В поле "Тип" укажите "Установщик Windows (MSI-файл)", установите отметку в поле "Указать информацию о типе развертывания вручную" и нажмите кнопку "Далее >".

На экране появится диалог, подобный следующему.



10. В поле "Имя" укажите название типа развертывания и нажмите кнопку "Далее >".

На экране появится диалог содержимого.



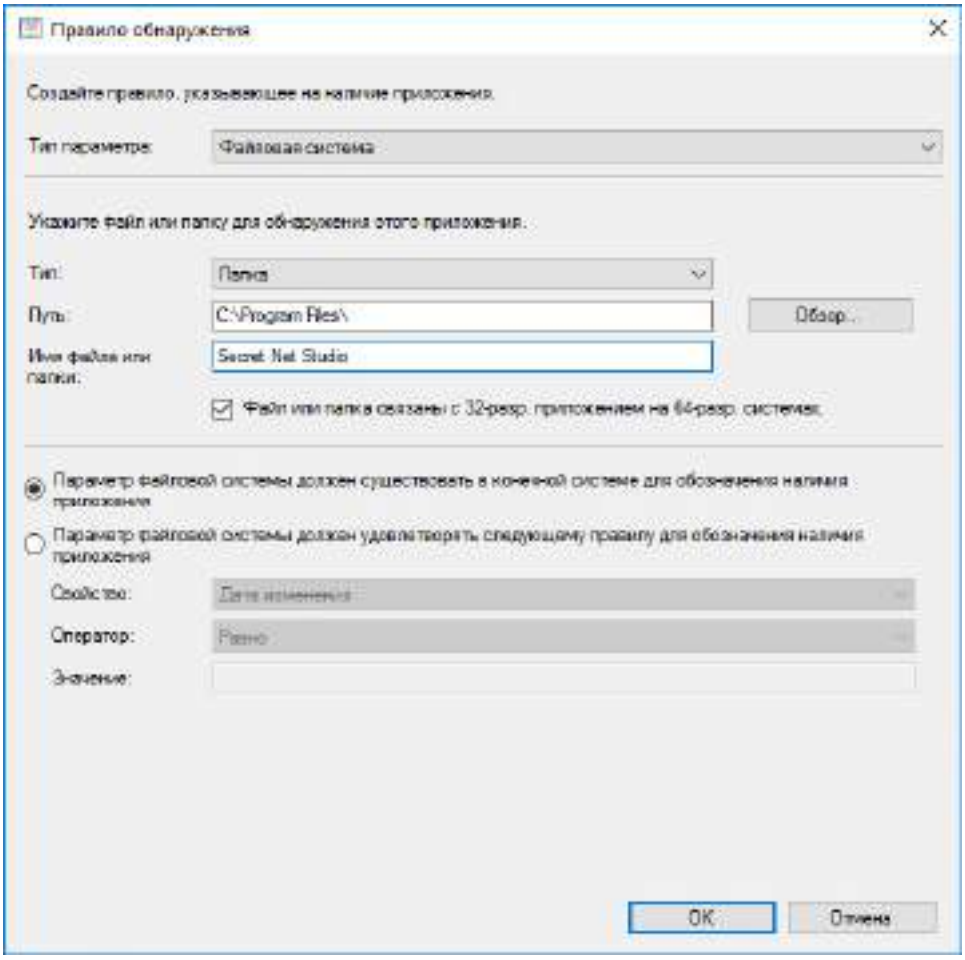
11. Для типа развертывания выполните следующие действия:

- Укажите информацию:
  - в поле "Программа установки" укажите в соответствующем формате путь к дистрибутиву и команду (см. стр.**43**);
  - в поле "Программа удаления" укажите в соответствующем формате путь к дистрибутиву и команду (см. стр.**43**).
- Нажмите кнопку "Далее >".

На экране появится диалог "Метод обнаружения".

12. Нажмите кнопку "Добавить".

На экране появится диалог создания правил обнаружения.



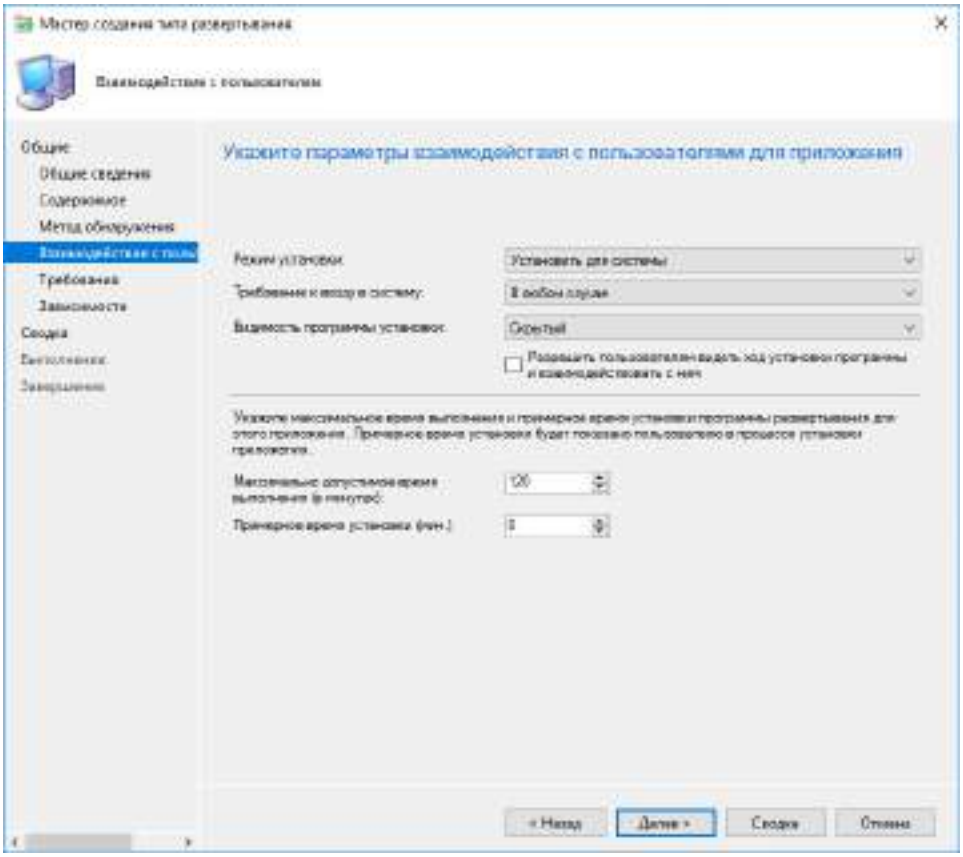
13. Для настройки правила обнаружения выполните следующие действия:

- Укажите следующее условие для правила обнаружения:
  - в поле "Путь" укажите путь к папке \Program Files;
  - в поле "Имя файла или папки" укажите имя папки \Secret Net Studio.
- Нажмите кнопку "OK".

В списке появится новое правило обнаружения.

14. Нажмите кнопку "Далее >".

На экране появится диалог взаимодействие с пользователями.



15. Для настройки взаимодействия с пользователями выполните следующие действия:

- Укажите информацию:
  - в поле "Режим установки" укажите "Установить для системы";
  - в поле "Требование к входу в систему" укажите "В любом случае";
  - в поле "Видимость программы установки" укажите "Скрытый".
- Нажмите кнопку "Далее >".

На экране появится диалог требований.

16. Нажмите кнопку "Далее >".

На экране появится диалог зависимости.

17. Нажмите кнопку "Далее >".

На экране появится диалог подтверждения параметров развертывания.

18. В диалоге проверьте содержимое и нажмите кнопку "Далее >".

Начнется процесс содания типа развертывания.

19. После завершения нажмите кнопку "Закрыть".

На экране в диалоге типы развертывания появится новый элемент.

20. Нажмите кнопку "Далее >".

На экране появится диалог подтверждения параметров приложения.

21. В диалоге проверьте содержимое и нажмите кнопку "Далее >".

Начнется процесс содания приложения.

22. После завершения нажмите кнопку "Закрыть".

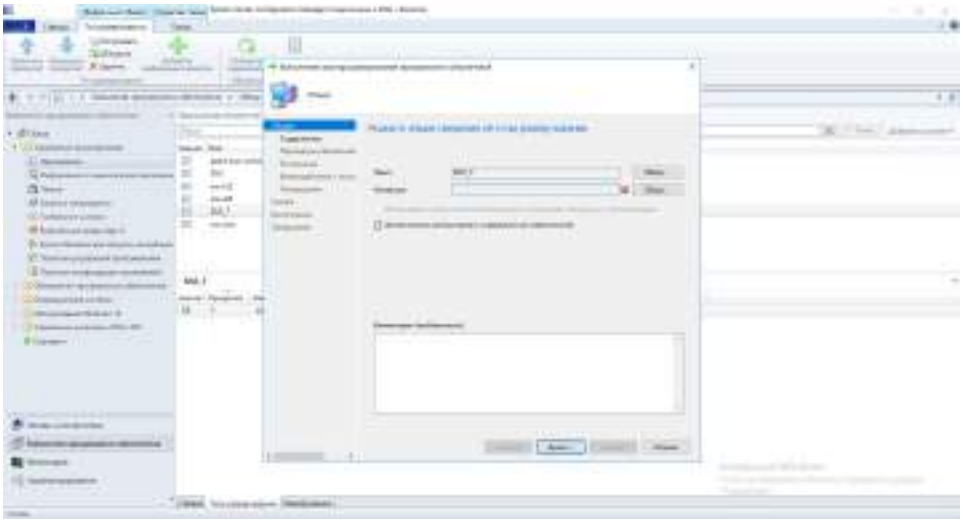
По окончании процесса в списке появится новый элемент, содержащий сведения о созданном приложении.

Примечание.
Для создания приложений по установке и удалению пакетов исправлений используется аналогичный алгоритм.

Для установки созданного приложения:

1. Откройте System Center Configuration Manager.
2. В нижней части панели навигации выберите "Библиотека программного обеспечения" (слева в основном окне).
3. В верхней части панели навигации в окне структуры раскройте ветвь "Управление приложениями" (слева в основном окне).
4. Выберите объект "Приложения".
5. В списке созданных приложений выберите созданное ранее приложение.
6. Вызовите контекстное меню приложения и выберите команду "Развернуть".

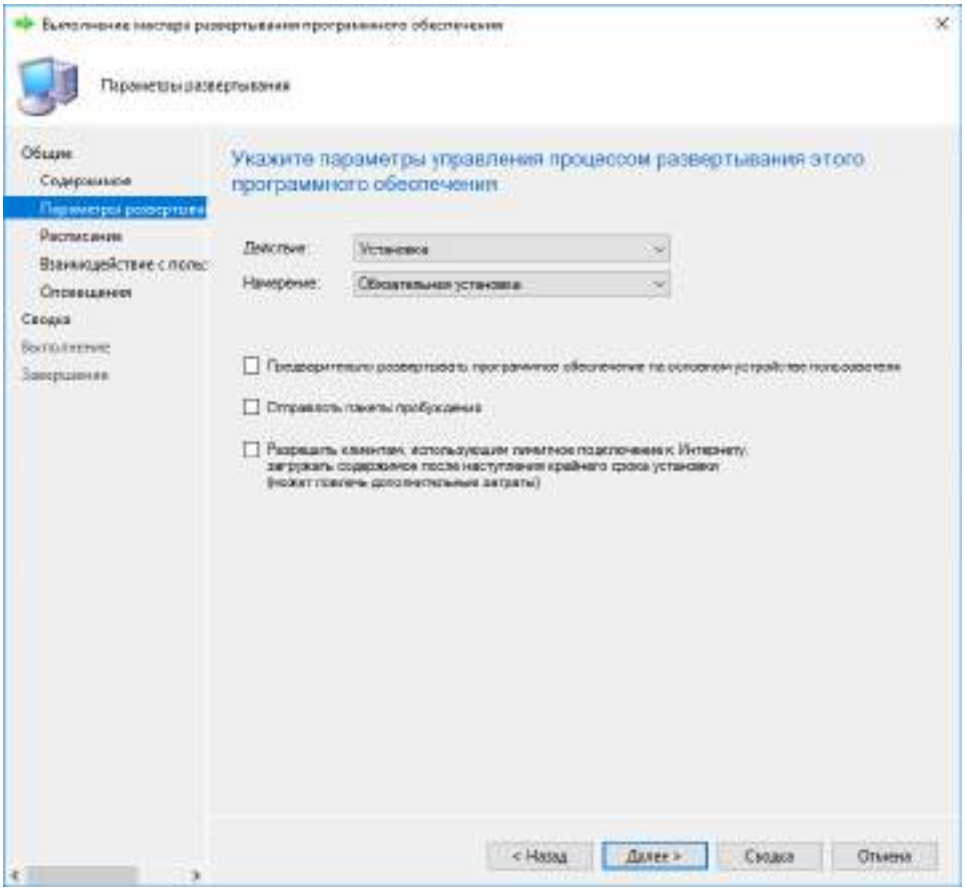
   На экране появится диалог, подобный следующему.



7. Напротив поля "Коллекция" нажмите на кнопку "Обзор" и в появившемся списке выберите необходимую коллекцию компьютеров на которую требуется установить пакет установки, а затем нажмите кнопку "ОК".
8. Нажмите кнопку "Далее >".

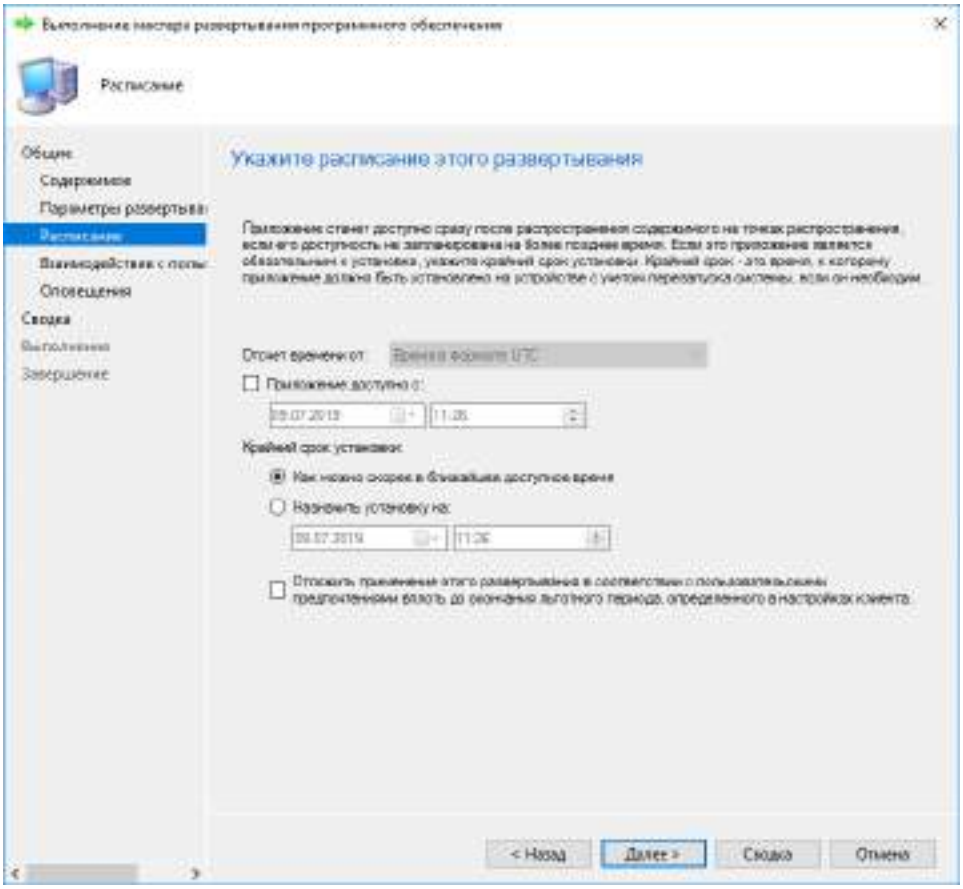
   На экране появится диалог места распространения содержимого.
9. Нажмите кнопку "Далее >".

   На экране появится диалог параметров управления процессом развертывания этого программного обеспечения.



10. В поле "Намерение" укажите "Обязательная установка" и нажмите кнопку "Далее >".

На экране появится диалог расписания этого развертывания программного обеспечения."



Примечание.
Если требуется выполнить удаление, то в поле "Действие" укажите "Удаление", параметр "Обязательная установка" в поле "Намерение" будет установлен автоматически.

11. Нажмите кнопку "Далее >".

На экране появится диалог параметров взаимодействия с пользователем при установке этого программного обеспечения.

12. Нажмите кнопку "Далее >".

На экране появится диалог параметров оповещений.

13. Нажмите кнопку "Далее >".

На экране появится диалог подтверждения параметров этого развертывания.

14. В диалоге проверьте содержимое и нажмите кнопку "Далее >".

Начнется процесс установки приложения.

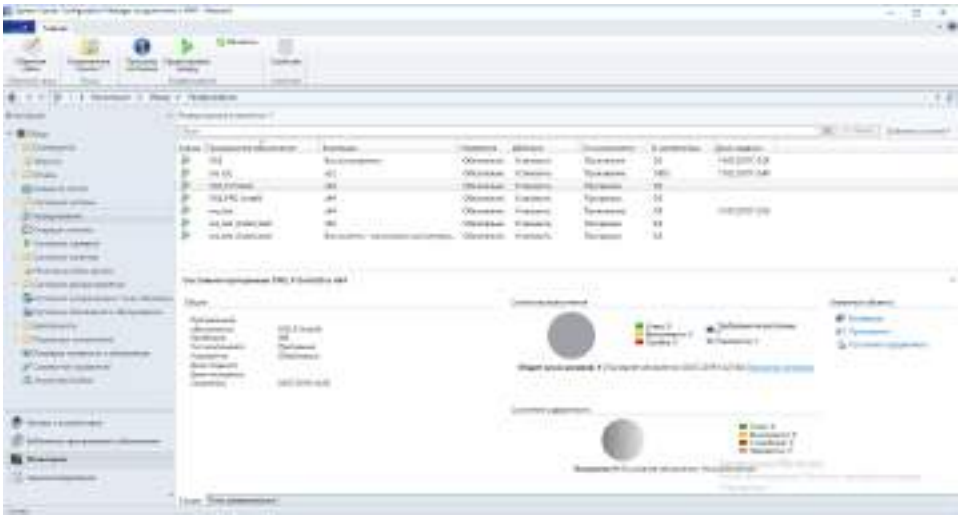
15. После завершения нажмите кнопку "Закрыть".

Примечание.
Для команд обновления и исправления ПО приложение не используется.

Для отслеживания процесса выполнения приложения:

1. Откройте System Center Configuration Manager.
2. В нижней части панели навигации выберите "Мониторинг" (снизу в основном окне).
3. В верхней части панели навигации в окне структуры выберите "Развертывания".

   На экране появится диалог, подобный следующему.



4. В списке программного обеспечения выберите требуемое приложение и посмотрите его состояние.

Глава 4
Обновление и переустановка компонентов

Обновление

В системе Secret Net Studio реализована возможность обновления программного обеспечения предыдущих версий на текущую версию. При обновлении сохраняются заданные параметры настройки системы (для некоторых параметров могут быть выставлены значения по умолчанию, если сохранение прежних значений технически невозможно).

Обновление компонентов на компьютерах системы осуществляется по отдельности с помощью программ установки компонентов. При этом для клиента Secret Net Studio в сетевом режиме функционирования обновление может выполняться централизованно под управлением сервера безопасности.

Порядок обновления компонентов централизованного управления

Обновление компонентов Secret Net Studio, реализующих централизованное управление, осуществляется в следующей последовательности:

1. Включите все контроллеры домена.
2. Обновите ПО серверов безопасности на текущую версию (см. стр.**56**). Если в домене безопасности имеется несколько серверов, процедуру обновления нужно начать с сервера, которому присвоена роль мастера схемы LDS домена безопасности. Обычно роль мастера схемы присвоена первому установленному серверу.
3. Обновите программу управления (см. стр. **58**) на рабочих местах администраторов.
4. Обновите ПО клиента (см. стр.**59**) в следующем порядке:
   - серверы безопасности;
   - компьютеры сотрудников.

   Совет.
   При большом количестве компьютеров целесообразно применить автоматическое обновление клиента путем централизованной установки под управлением сервера безопасности (см. стр.**26**).
5. В программе управления проверьте и при необходимости отредактируйте структуру оперативного управления (см. документ [**4**]).

Обновление сервера безопасности

Обновление сервера безопасности выполняется пользователем, входящим в локальную группу администраторов компьютера.

Для выполнения некоторых действий при обновлении сервера безопасности могут потребоваться особые права доступа. Например, права на администрирование леса доменов безопасности и домена безопасности. Если пользователь, выполняющий установку, не обладает нужными правами, программа установки на определенных этапах может запрашивать учетные данные пользователей с правами доступа.

Внимание!
При обновлении сервера безопасности процесс обновления нельзя прерывать и нужно довести до завершения. Если при замене модулей и модификации структур баз данных возникнут ошибки (например, по причинам недостаточных прав доступа или недоступности сервисов), будет выполнен возврат к предыдущему состоянию сервера (до обновления). Минимально необходимые условия для успешного обновления:
- работоспособное состояние сервера безопасности предыдущей версии;
- наличие прав администратора леса доменов безопасности — при первом обновлении в лесу доменов;
- наличие прав администратора домена безопасности.

В Secret Net Studio версий 8.0-8.5 и Secret Net версий 7.x при установке сервера безопасности на контроллерах домена AD программа установки создавала служебную учетную запись доменного пользователя SecretNetLDS$ или SecretNetLDS (в зависимости от версии ОС), используемую для запуска служб AD LDS. Эта учетная запись в текущей версии Secret Net Studio не требуется.

Внимание!
После обновления ПО всех серверов безопасности до текущей версии данную учетную запись необходимо в обязательном порядке удалить. Перед выполнением удаления необходимо вначале обновить ПО сервера безопасности на всех без исключения контроллерах домена AD, на которых он функционирует. Затем на одном из контроллеров домена следует запустить на выполнение под учетной записью администратора домена AD утилиту lds_dc_patch.exe с параметром del — lds_dc_patch.exe /del. Утилита размещается на установочном диске Secret Net Studio в каталоге Tools\SecurityCode\LdsPasswordChange\.

Для обновления сервера безопасности:

1. Вставьте в привод установочный диск системы Secret Net Studio. Дождитесь появления окна программы автозапуска (см. стр.**10**) и запустите обновление с помощью команды "Сервер безопасности".

   Примечание.
   Запуск обновления можно выполнить вручную без использования программы автозапуска. Для этого запустите с установочного диска файл \Setup\Server\x64\setup.ru-RU.exe.

   После запуска программы установки выполняется анализ системы на соответствие программным и аппаратным требованиям для установки компонента. При этом проверяется текущее состояние встроенного в ОС механизма управления учетными записями (User Account Control — UAC).

   Внимание!
   Если механизм UAC включен — на экране появится диалог запроса на его временное отключение. В этом случае нажмите кнопку "Да" для отключения механизма, перезагрузите компьютер и только после этого снова запустите процедуру обновления сервера безопасности.

   По окончании проверки системы на экран будет выведен диалог с сообщением о готовности к началу обновления и позволяющий также дополнительно выбрать для установки службу синхронизации.

   Пояснение.
   Служба синхронизации устанавливается на сервере безопасности, чтобы, выполняя функцию шлюза, обеспечить взаимодействие этого сервера с родительским сервером безопасности. Установка данной службы выполняется отдельной программой установки, которая будет автоматически запущена после завершения обновления сервера безопасности (см. стр.**20**).

2. Нажмите кнопку "Обновить" или отметьте поле "Служба Синхронизации" и нажмите кнопку "Изменить".

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

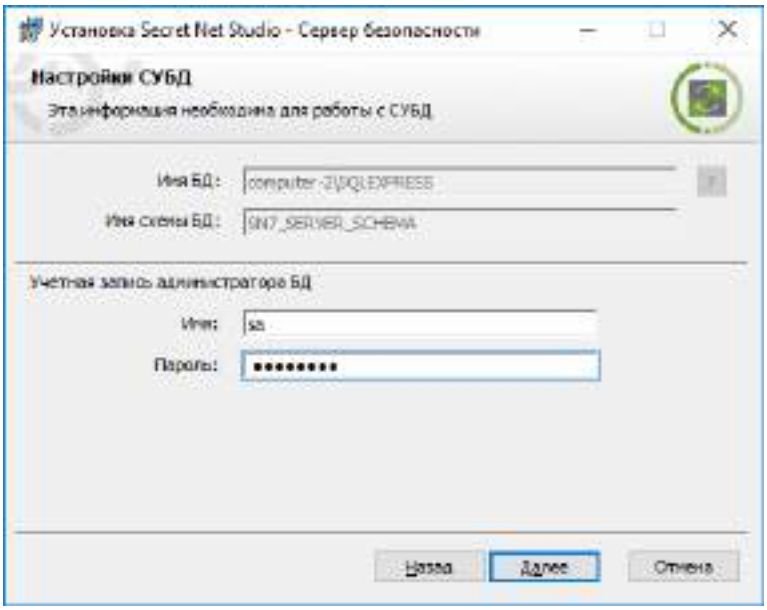
   Примечание.
   Перед выполнением дальнейших действий рекомендуется закрыть программу автозапуска.

3. Нажмите кнопку "Далее".

На экране появится диалог принятия лицензионного соглашения.

4. Ознакомьтесь с содержанием лицензионного соглашения, отметьте пункт о его принятии и нажмите кнопку "Далее".

   На экране появится диалог "Настройки СУБД". Пример содержимого диалога представлен на следующем рисунке.



5. В группе полей "Учетная запись администратора БД" укажите учетные данные администратора базы данных на СУБД и нажмите кнопку "Далее".

   На экране появится диалог "Все готово к обновлению".

6. Нажмите кнопку "Обновить".

   Начнется процесс обновления программных модулей.

   Внимание!
   Если некоторые программные модули в данный момент используются, на экране появится диалог запроса на обновление файлов или служб, которые невозможно обновить. В этом случае нажмите кнопку "ОК" для начала процесса обновления.

   Если при выполнении действия **2** была выбрана установка службы синхронизации, будет запущена программа установки этой службы. Выполните ее установку так, как это описано на стр.**20**

   После завершения всех операций появится сообщение с предложением перезагрузить компьютер.

7. Перезагрузите компьютер и дождитесь загрузки системы.

   Пояснение.
   Информация о сервере безопасности в структуре оперативного управления может обновиться с некоторой задержкой. В программе управления, подключенной к другому серверу безопасности, загрузка обновленной структуры с новыми данными может произойти через несколько минут после обновления ПО СБ (порядка 10–15 минут).

Обновление программы управления

Обновление программы управления выполняется пользователем, входящим в локальную группу администраторов компьютера. Для запуска процедуры обновления компонента используйте установочный диск (см. стр.**21**). Процедура обновления выполняется без особенностей.

Обновление клиента

Обновление клиента выполняет пользователь, входящий в локальную группу администраторов компьютера.

Для выполнения некоторых действий при обновлении клиента могут потребоваться особые права доступа. Например, права на администрирование домена безопасности, если клиент подчинен серверу безопасности. Если пользователь, выполняющий установку, не обладает нужными правами, программа установки на определенных этапах может запрашивать учетные данные пользователей с правами доступа.

Для обновления клиента:

1. Вставьте в привод установочный диск системы Secret Net Studio. Дождитесь появления окна программы автозапуска (см. стр.10) и запустите обновление с помощью команды "Защитные компоненты".

   Примечание.
   Запуск обновления можно выполнить вручную без использования программы автозапуска. Для этого в зависимости от операционной системы компьютера выполните следующее действие:
   - при установке на компьютер с 64-разрядной версией Windows — запустите с установочного диска файл \Setup\Client\x64\SnSetup.ru-RU.exe;
   - при установке на компьютер с 32-разрядной версией Windows — запустите с установочного диска файл \Setup\Client\Win32\SnSetup.ru-RU.exe.

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.

   Примечание.
   Перед выполнением дальнейших действий рекомендуется закрыть программу автозапуска.

2. Нажмите ссылку "Пакеты исправлений..." для просмотра и выбора пакетов исправлений, которые будут применены при обновлении ПО.

   Примечание.
   Пакеты исправлений можно установить отдельно от обновления системы защиты. Для этого запустите требуемый файл пакета исправлений на установочном диске в папке Tools\SecurityCode\Patches\<название_пакета_исправлений>.

3. Нажмите кнопку "Готово".

   На экране появится окно запроса с предложением перезагрузить компьютер.

4. Нажмите кнопку "Да" в окне запроса.

   Начнется перезагрузка компьютера, во время которой выполняется обновление компонентов Secret Net Studio. После успешного входа пользователя в систему над пиктограммой Secret Net Studio, находящейся на панели задач Windows, появится сообщение об успешном завершении обновления.

Особенности установки клиента в режиме обновления других продуктов

При установке клиента Secret Net Studio проверяется наличие установленного ПО следующих продуктов компании "Код Безопасности":

- СЗИ Secret Net (клиентское ПО);
- СЗИ Security Studio Endpoint Protection;
- СЗИ TrustAccess.

Функциональные возможности перечисленных продуктов могут быть реализованы частично или полностью механизмами защиты клиента Secret Net Studio.

Если обнаружен какой-либо из указанных продуктов, в зависимости от ситуации возможны следующие варианты:

- обновление (замена) имеющейся версии продукта с применением ранее заданных параметров в соответствующих подсистемах клиента Secret Net Studio, если для этого имеется техническая возможность;
- установка клиента Secret Net Studio с сохранением имеющейся версии продукта для самостоятельного функционирования (без интеграции);
- отмена установки клиента.

Установка при наличии СЗИ Secret Net (клиентское ПО)

При наличии клиентского ПО СЗИ Secret Net выполняется обновление этого ПО на устанавливаемую версию клиента Secret Net Studio. После обновления будут действовать защитные подсистемы клиента Secret Net Studio, которые были указаны для установки.

Установка при наличии СЗИ Security Studio Endpoint Protection

При наличии ПО СЗИ Security Studio Endpoint Protection выполняется удаление этого ПО.

Примечание.
Если в СЗИ Security Studio Endpoint Protection задан пароль защиты, отличающийся от пароля по умолчанию, удаление будет возможно только при установке клиента в интерактивном режиме. В этом случае при установке можно указать текущий пароль. Для выполнения централизованной установки клиента необходимо предварительно либо вернуть пароль по умолчанию (securitycode), либо вручную удалить данное ПО.

Установка при наличии СЗИ TrustAccess

При наличии ПО СЗИ TrustAccess возможны следующие варианты:

- для версий 1.3.x — выполняется обновление, если в списке устанавливаемых защитных подсистем указан хотя бы один из компонентов сетевой защиты. В противном случае сохраняется имеющаяся версия продукта;
- для остальных версий — в процессе установки выводится сообщение об ошибке из-за неподдерживаемой версии продукта. В этом случае необходимо вручную выполнить процедуру удаления ПО.

Переустановка (восстановление)

Для восстановления нарушенной работоспособности компонентов системы Secret Net Studio может применяться процедура переустановки ПО. Переустановка выполняется с использованием дистрибутива той же версии, которая установлена на компьютере.

Переустановку должен выполнять пользователь, входящий в локальную группу администраторов компьютера.

Примечание.
В текущей реализации не предусмотрена процедура переустановки ПО сервера безопасности.

Переустановка клиента

Запуск процедуры переустановки клиента можно выполнить так же, как и запуск установки в интерактивном режиме (см. стр. 22), или использовать стандартный способ переустановки для компонента "Secret Net Studio" в окне ОС Windows "Программы и компоненты". После запуска программы установки на экран будет выведен диалог для выбора варианта действий.

Для переустановки клиента с восстановлением ПО:

1. В диалоге выбора варианта действий установите отметку в поле "исправить" и нажмите кнопку "Готово".

   На экране появится окно запроса с предложением перезагрузить компьютер.
2. Нажмите кнопку "Да" в окне запроса.

Начнется перезагрузка компьютера, во время которой будет выполнена повторная установка компонентов Secret Net Studio. После успешного входа пользователя в систему над пиктограммой Secret Net Studio, находящейся на панели задач Windows, появится сообщение об успешном завершении данной процедуры.

Переустановка программы управления

При переустановке программы управления выполняется ее восстановление.

Запуск процедуры переустановки осуществляется так же, как и запуск установки программы (см. стр. 21). После диалога приветствия на экран будет выведен диалог для выбора варианта действий.

Для переустановки программы управления:

1. В диалоге для выбора варианта действий нажмите кнопку "Восстановить".

   На экране появится диалог, сообщающий о готовности к установке.

2. Нажмите кнопку "Восстановить".

   Начнется копирование файлов на жесткий диск и регистрация компонентов в системном реестре ОС Windows. Ход процессов копирования и настройки отображается в информационном окне в виде полосы прогресса. При их завершении на экране появится диалог "Установка завершена".

3. Нажмите кнопку "Готово", а затем нажмите кнопку "Закрыть" в еще одном появившемся на экране диалоге.

Глава 5
Удаление компонентов

Предупреждение.
Если на защищаемых компьютерах имеется конфиденциальная или зашифрованная информация, следует принять меры для ее защиты и сохранения до удаления системы Secret Net Studio.

Порядок удаления в сетевом режиме функционирования

Удаление клиентов Secret Net Studio в сетевом режиме функционирования и компонентов для централизованного управления рекомендуется выполнять в следующем порядке:

1. Удалите ПО клиентов на всех компьютерах.
2. Удалите программу управления на рабочих местах администраторов.
3. Удалите ПО серверов безопасности.

Удаление клиента

ПО клиента можно удалить при работе на компьютере локально или в терминальной сессии. Для сетевого режима функционирования также предусмотрен метод централизованного удаления под управлением сервера безопасности. Централизованное удаление реализуется с помощью программы управления (см. документ [**4**]). Для этого в программе необходимо сформировать задания на удаление ПО, аналогичные заданиям развертывания (см. стр.**27**).

Ниже рассматривается процедура локального удаления клиента.

Процедуру удаления должен выполнять пользователь, входящий в локальную группу администраторов компьютера.

Для удаления клиента:

1. Выполните запуск процедуры установки клиента в интерактивном режиме (см. стр. **22**) или используйте стандартный способ запуска удаления для компонента "Secret Net Studio" в окне ОС Windows "Программы и компоненты".

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог для выбора варианта продолжения.
2. В диалоге установите отметку в поле "удалить" и укажите учетные данные пользователя с правами администратора домена безопасности.

   Пояснение.
   Если текущий пользователь имеет права на запись в хранилище объектов централизованного управления — оставьте отмеченным поле "использовать для подключения учетную запись текущего пользователя". Если права не предоставлены — выберите пункт "использовать указанные ниже имя и пароль" и введите данные соответствующей учетной записи.
3. Нажмите кнопку "Готово".

   Если на компьютере включена функция "Контроль административных привилегий", на экране появится диалоговое окно ввода PIN администратора. Для продолжения процедуры удаления введите PIN и нажмите кнопку "OK".

   Начнется процесс удаления защитных подсистем.
4. После завершения всех операций удаления нажмите кнопку "Далее".

   На экране появится завершающий диалог со сведениями о выполненных операциях и предложением перезагрузить компьютер.

Совет.
При необходимости используйте ссылки в разделе "Информация" для выполнения следующих действий:
- чтобы посмотреть записи журнала трассировки — выберите ссылку "отчет об установке";
- чтобы собрать все необходимые для диагностики Secret Net Studio файлы и данные, в случае возникновения проблем при установке — выберите ссылку "диагностическую информацию".

5. Перезагрузите компьютер.

Удаление драйвера средства аппаратной поддержки

Если на компьютере установлен драйвер средства аппаратной поддержки Secret Net Card, его удаление осуществляется отдельно. Запуск процедуры удаления драйвера выполняется стандартным способом в окне ОС Windows "Программы и компоненты".

Удаление программы управления

Процедура удаления программы управления выполняется без особенностей. Запуск удаления компонента "Secret Net Studio — Центр управления" можно выполнить стандартным способом в окне ОС Windows "Программы и компоненты".

Удаление сервера безопасности

При удалении сервера безопасности следует иметь в виду, что все компьютеры, подчиненные данному серверу, станут свободными — то есть не подчиненными какому-либо серверу безопасности.

Для выполнения некоторых действий при удалении сервера безопасности могут потребоваться особые права доступа. Например, права, предоставленные группе администраторов домена безопасности. Если пользователь, выполняющий удаление, не обладает нужными правами, программа установки на определенных этапах может запрашивать учетные данные пользователей с правами доступа.

Для удаления сервера безопасности:

1. В окне ОС Windows "Программы и компоненты" выберите в списке компонент "Secret Net Studio — Сервер безопасности" и нажмите кнопку "Удалить".

   На экране появится диалог запроса на удаление компонента.

2. Нажмите кнопку "Да" в диалоге запроса.

   Программа установки проверит текущее состояние встроенного в ОС механизма управления учетными записями (User Account Control — UAC). Возможны следующие варианты:

   - если механизм UAC включен — на экране появится диалог запроса на его временное отключение. В этом случае нажмите кнопку "Да" для отключения механизма, перезагрузите компьютер и после этого снова запустите процедуру удаления сервера безопасности (см. действие **1**);
   - если механизм UAC отключен — процедура удаления будет продолжена, и на экране появится диалог программы установки, содержащий сведения о ходе выполнения операций. На этапе выбора действий с базой данных сервера на экране появится диалог "Удаление базы данных".

3. Выполните нужное действие:

   - для сохранения БД — нажмите кнопку "Отмена";
   - для удаления БД — введите учетные данные администратора базы данных на сервере СУБД в полях "Имя администратора" и "Пароль администратора" и нажмите кнопку "ОК".

   Процедура удаления будет продолжена. На этапе выбора действий с сертификатом сервера на экране появится запрос об удалении сертификата.

4. Чтобы удалить сертификат сервера безопасности из IIS, нажмите кнопку "Да" в диалоге запроса. При необходимости сохранить сертификат в IIS нажмите кнопку "Нет".

   После завершения всех операций удаления в диалоге программы установки появится предупреждение о необходимости перезагрузки компьютера.

5. Перезагрузите компьютер.

Удаление шлюза

Если на сервере безопасности установлено и используется ПО шлюза, его можно удалить отдельно от сервера, предварительно удалив шлюз из структуры ОУ.

Внимание!

При удалении настроенного и функционирующего шлюза необходимо учитывать, что взаимодействие между родительским и дочерним лесами безопасности будет прекращено. В результате управление защищаемыми компьютерами дочернего леса средствами корневого сервера безопасности станет невозможно.

Рекомендуется выполнять данную операцию в указанном ниже порядке.

Для удаления шлюза:

Шаг 1. Удалите шлюз из структуры ОУ:

1. Запустите программу управления и подключитесь к родительскому серверу безопасности, на котором зарегистрирован шлюз.
2. В программе управления в нижней части панели навигации нажмите кнопку "Настройки" и в появившейся панели нажмите ссылку "Конфигурирование".

   На экране появится диалог выбора режима работы этой программы.
3. Выберите вариант "Редактирование иерархии лесов безопасности".

   На экране появится диалог редактирования списка шлюзов.
4. Выберите нужный шлюз, нажмите кнопку "Удалить" и подтвердите свое решение в появившемся окне запроса.

   Начнется процесс удаления шлюза, занимающий некоторое время. Информация о ходе этого процесса отображается в виде сообщений в панели событий системы. Дождитесь его завершения и удаления из списка выбранного шлюза. После этого из иерархической структуры ОУ также будет удален соответствующий данному шлюзу лес безопасности.
5. Нажмите кнопу "Закрыть.

Подробные сведения о конфигурировании структуры ОУ содержатся в документе [**4**].

Шаг 2. Удалите ПО шлюза:

1. На компьютере, на котором установлено ПО шлюза, запустите программу установки сервера безопасности той же версии, что и установленный здесь сервер.

   Программа установки проверит текущее состояние встроенного в ОС механизма управления учетными записями (User Account Control — UAC). Возможны следующие варианты:

   - если механизм UAC включен — на экране появится диалог запроса на его временное отключение. В этом случае нажмите кнопку "Да" для отключения механизма, перезагрузите компьютер и после этого снова запустите программу установки сервера безопасности;
   - если механизм UAC отключен — процедура будет продолжена, и на экране появится диалог программы установки, содержащий сведения об установленных компонентах.
2. Удалите отметку из поля "Служба Синхронизации" и нажмите кнопку "Изменить".

   Начнется процесс удаления службы синхронизации, по окончании которого в информационном окне появится сообщение об этом.

3. Нажмите кнопку "Закрыть".

Удаление отдельных подсистем клиента

Если на компьютере не используются некоторые из установленных защитных подсистем клиента Secret Net Studio, эти подсистемы можно удалить локально или в терминальной сессии. С учетом особенностей модульных взаимосвязей функциональных компонентов клиента, удаление может выполняться для следующих отдельных подсистем и групп:

- доверенная среда;
- антивирус;
- паспорт ПО;
- подсистемы группы сетевой защиты и средство обнаружения вторжений;
- подсистемы защиты информации на локальных дисках и шифрования данных в криптоконтейнерах;
- подсистема контроля печати;
- подсистемы группы локальной защиты (кроме вышеуказанных подсистем).

Кроме того, предусмотрена возможность удаления программы управления, установленной для работы в локальном режиме (при установке клиента).

Процедура удаления подсистем клиента должна выполняться пользователем, входящим в локальную группу администраторов компьютера.

Для удаления отдельных подсистем клиента:

1. Выполните запуск процедуры установки клиента в интерактивном режиме (см. стр. 22) или используйте стандартный способ запуска удаления для компонента "Secret Net Studio" в окне ОС Windows "Программы и компоненты".

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог для выбора варианта продолжения.

2. В диалоге установите отметку в поле "удалить компоненты" и нажмите кнопку "Далее".

   Если на компьютере включена функция "Контроль административных привилегий", на экране появится диалоговое окно ввода PIN администратора.

3. Для продолжения процедуры удаления введите PIN и нажмите кнопку "ОК".

   На экране появится диалог для выбора удаляемых подсистем.

4. Отметьте элементы, которые нужно удалить, и нажмите кнопку "Готово".

   Начнется процесс удаления защитных подсистем.

5. После завершения всех операций удаления нажмите кнопку "Далее".

   На экране появится завершающий диалог со сведениями о выполненных операциях и предложением перезагрузить компьютер.

   Совет.
   При необходимости используйте ссылки в разделе "Информация" для выполнения следующих действий:
   - чтобы посмотреть записи журнала трассировки — выберите ссылку "отчет об установке";
   - чтобы собрать все необходимые для диагностики Secret Net Studio файлы и данные, в случае возникновения проблем при установке — выберите ссылку "диагностическую информацию".

6. Перезагрузите компьютер.

Удаление всех пакетов исправлений

Запуск процедуры удаления всех пакетов исправлений клиента можно выполнить так же, как и запуск установки в интерактивном режиме (см. стр. 22), или использовать стандартный способ удаления для компонента "Secret Net Studio" в окне ОС Windows "Программы и компоненты". После запуска программы установки на экран будет выведен диалог для выбора варианта действий.

Для удаления всех пакетов исправлений:

1. В диалоге выбора варианта действий установите отметку в поле "удалить все пакеты исправлений" и нажмите кнопку "Готово".

   Если на компьютере включена функция "Контроль административных привилегий", на экране появится диалоговое окно ввода PIN администратора. Для продолжения процедуры удаления введите PIN и нажмите кнопку "ОК".

   На экране появится окно запроса с предложением перезагрузить компьютер.

2. Нажмите кнопку "Да" в окне запроса.

   Начнется перезагрузка компьютера, во время которой будет выполнено удаление всех ранее установленных пакетов исправлений Secret Net Studio. После успешного входа пользователя в систему над пиктограммой Secret Net Studio, находящейся на панели задач Windows, появится сообщение об успешном завершении данной процедуры.

Приложение

Открытые порты для работы Secret Net Studio

Для корректного функционирования Secret Net Studio на оборудовании должны быть открыты порты, приведенные в таблицах ниже.

На всех компьютерах и серверах необходимо открыть порты, приведенные в первой таблице данного раздела.

Дополнительно необходимо открыть порты из остальных таблиц данного раздела на оборудовании, выполняющем соответствующие функции.

Табл.1 Открытые порты для всех компьютеров и серверов (общесистемные разрешения для работы с AD)

Назначение	TCP	UDP
Взаимодействие с AD	49152-65535	49152-65535
Взаимодействие с DNS-сервером	49152-65535	53 49152-65535
NetBIOS name resolution	-	137
NetBIOS datagram service	-	138
NTP-синхронизация времени	-	123

Табл.2 Открытые порты для контроллера домена

Назначение	TCP	UDP
Доступ к LDAP	389	389
Доступ к LDAPS	636	-
Мезанизм GPO, другие взаимодействия с AD	445	-
Служба сеанса NetBIOS	139	-
Kerberos аутентификация пользователя	88	-
RPC-взаимодействия	135	-
Доступ к Global Catalog	3268	-
Доступ к Global Catalog по SSL (если настроен)	3269	-

Табл.3 Открытые порты для других серверов

Назначение	TCP	UDP
DNS-сервер	53	53
SQL-сервер	1433	1434

Табл.4 Открытые порты для сетевого оборудования

Назначение	TCP	UDP
Network broadcast	-	137 138
Обновление антивируса и СОВ	43444	43444

Табл.5 Открытые порты для работы всех СБ Secret Net Studio

Назначение	TCP	UDP
Интерфейс управления сервера аутентификации	42100	-
Центр распространения ключей Kerberos	42088	42088
Смена пароля пользователя Kerberos	42464	42464
Взаимодействие с программой управления	443	-
Взаимодействие с Secret Net LDS	50000*	-
Взаимодействие с Secret Net LDS по SSL	50001*	-
Взаимодействие с Secret Net-GC LDS	50002*	-
Взаимодействие с Secret Net-GC LDS по SSL	50003*	-

***** Порт используется по умолчанию, если при установке СБ не указан другой порт.

Табл.6 Открытые порты для работы родительского и подчиненного СБ Secret Net Studio

Назначение	TCP	UDP
RPC-взаимодействия	135	-
Взаимодействие между СБ по HTTP	443	-

Табл.7 Открытые порты для работы СБ, которому подчинен клиент Secret Net Studio

Назначение	TCP	UDP
RPC-взаимодействия	135	-
Взаимодействие СБ и клиента по HTTP	443	-
Автоматическая установка клиента	139	137

Табл.8 Открытые порты для работы сервера обновлений Secret Net Studio

Назначение	TCP	UDP
Обновление антивируса и СОВ	43444	43444

Табл.9 Открытые порты для работы клиента Secret Net Studio

Назначение	TCP	UDP
Автоматическая установка клиента с СБ	445	137
RPC-взаимодействие с СБ при централизованной установке клиента	135	-
Аппаратная поддержка	21326	-
Синхронизация настроек механизмов КЦ, ЗПС	21327	-
Согласование ключей ipsec, протокол ISAKMP согласования параметров безопасности	-	42200
Обновление антивируса и СОВ	43444	43444

ПО для использования поддерживаемых USB-ключей и смарт-карт

Для использования в системе Secret Net Studio поддерживаемых USB-ключей и смарт-карт на компьютере должно быть установлено дополнительное ПО соответствующих производителей устройств. Установку необходимого ПО можно выполнить с установочного диска системы Secret Net Studio. Каталоги с файлами для установки ПО перечислены в следующей таблице.

Тип средства	**Каталоги с файлами для установки**
USB-ключи и смарт-карты	
Rutoken S, Rutoken ЭЦП, Rutoken Lite	\Tools\Tokens\RuToken\
JaCarta PKI, JaCarta PKI Flash, JaCarta ГОСТ, JaCarta ГОСТ Flash	\Tools\Tokens\Aladdin\JaCartaUC\
eToken PRO (Java)*	\Tools\Tokens\Aladdin\JaCartaUC\ + \Tools\Tokens\Aladdin\eToken\
ESMART Token, ESMART Token ГОСТ	\Tools\Tokens\eSmart\
Считыватели смарт-карт	
Athena ASEDrive	\Tools\Tokens\Aladdin\Acedrv\

* При использовании идентификаторов eToken для работы со стандартными сертификатами Microsoft необходимо дополнительно установить набор драйверов и утилит SafeNet Authentication Client, предоставляемый производителем устройств.

Каталоги установки клиента

При установке клиентского ПО Secret Net Studio создаются четыре системные переменные окружения LocalProtectionDir, NetworkProtectionDir, AntivirusDir и LocalControlCenterDir, в которые записываются пути к каталогам установки клиента и его основных подсистем.

Права доступа на каталог установки клиента наследуются от родительского объекта.

Сведения об установке и настройке СУБД MS SQL

Установку сервера MS SQL необходимо выполнить в соответствии с требованиями производителя. Перечень требований приводится на сайте компании Microsoft.

В частности, перед установкой сервера MS SQL должна быть выполнена установка компонента .NET Framework соответствующей версии и языкового пакета для этого компонента (при использовании русской редакции СУБД).

Установочный диск комплекта поставки содержит средства установки бесплатно распространяемого варианта СУБД версии MS SQL Server 2012 SP1 Express. Общий порядок действий для установки сервера MS SQL с использованием указанных средств (на примере ОС Windows Server 2008 R2):

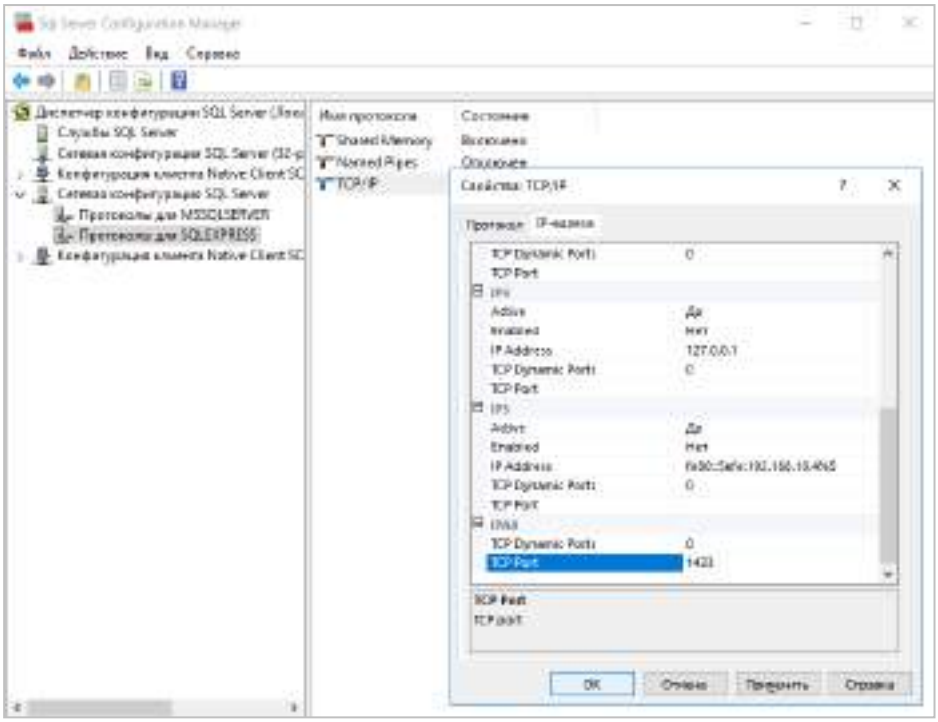
1. Включить в ОС компонент .NET Framework 3.5.
2. Установить .NET Framework 4.5. Для этого запустите на исполнение файл dotNetFx45_Full_x86_x64.exe из каталога \Tools\Microsoft\Prerequisites.
3. Установить языковой пакет к .NET Framework 4.5. Для этого в том же каталоге запустите на исполнение файл dotNetFx45LP_Full_x86_x64ru.exe.
4. Установить сервер MS SQL. Для этого запустите на исполнение файл SQLEXPRWT_x64_ENU.exe или SQLEXPRWT_x86_ENU.exe (в зависимости от разрядности ОС) из каталога \Tools\Microsoft\SQL Server 2012 SP1 Express.

Корректное взаимодействие сервера безопасности и СУБД MS SQL обеспечивается при выполнении следующих условий на компьютере сервера MS SQL:

- включен режим поддержки сортировки кириллицы для экземпляра базы данных — для этого при установке экземпляра необходимо в параметрах сортировки для компонента Database Engine указать значение Cyrillic_General_CI_AS (в разделе "Server Configuration", вкладка "Collation");
- включен режим аутентификации, обеспечивающий проверку подлинности SQL Server и Windows, — для этого на сервере MS SQL необходимо включить смешанный режим аутентификации (mixed mode).

Если сервер MS SQL установлен на отдельном компьютере (не на компьютере сервера безопасности), дополнительно требуется выполнить следующие действия:

- в брандмауэре (если он включен) разрешить использование порта для соединения с СУБД (по умолчанию порт 1433). При этом на сервере MS SQL порт должен быть открыт на входящие соединения, а на сервере безопасности — на исходящие;
- включить режим поддержки протокола TCP/IP. Режим по умолчанию отключен при использовании свободно распространяемого варианта SQL Server Express. Управление режимом осуществляется с помощью компонента SQL Server Configuration Manager из состава ПО MS SQL Server. Для включения режима перейдите к разделу "SQL Server Network Configuration / Protocols for <*имя_экземпляра_БД*>" и вызовите окно настройки свойств элемента "TCP/IP". В диалоге "Protocol" укажите значение "Yes" для параметра "Enabled" и затем в диалоге "IP Addresses" проверьте значения параметров "TCP Dynamic Ports" и "TCP Ports" для всех IP-адресов: параметрам должны быть присвоены пустое значение и значение "1433" соответственно. Пример диалога с параметрами настройки представлен на следующем рисунке.



Примечание.

При включенной трассировке сведения о взаимодействии с СУБД сохраняются на сервере безопасности в log-файлах SnTrace.log и SB.txt (размещаются в каталоге трассировки C:\logs). Данные в указанных файлах могут использоваться для диагностики проблем соединения.

Изменения в IIS при установке сервера безопасности

При установке сервера безопасности изменяются некоторые параметры компонентов IIS. Параметрам присваиваются значения, необходимые для корректного функционирования сервера.

В IIS формируется специальный сайт SecretNetStudioSite. Для сайта выполняется:

- установка доступа по SSL;
- привязка (binding) протокола "https" по адресам "*:443:" .

Примечание.

Привязка протокола "https" для сайта SecretNetStudioSite добавляется во время установки сервера безопасности, а также при генерации нового сертификата для сервера.

Порт 443 необходим для функционирования сервера безопасности, поэтому для исключения конфликтов при добавлении привязки одновременно удаляются привязки для этого порта на остальных сайтах IIS, развернутых на компьютере. В связи с этим может быть нарушена работоспособность других сайтов и приложений, использующих в IIS порт 443.

В дополнительных параметрах пула приложений SecretNetStudioPool устанавливаются значения для следующих параметров:

Имя параметра	Значение
Раздел (General)	
queueLength	10000
Раздел processModel	
identityType	ApplicationPoolIdentity
idleTimeout	0.00:00:00
pingingEnabled	false
Раздел recycling	
periodicRestart.memory	0
periodicRestart.privateMemory	0
periodicRestart.time	0.00:00:00
periodicRestart.requests	0
periodicRestart.schedule	отключена

В секциях сайтов устанавливаются значения для следующих параметров:

Имя параметра	Значение
Секция сайта system.webServer/serverRuntime	
appConcurrentRequestLimit	100000
uploadReadAheadSize	104857600
Секция сайта windowsAuthentication	
enabled	true
Секция сайта anonymousAuthentication	
enabled	false
Секция сайта handlers	
accessPolicy	Read,Execute

Изменение параметров соединения СБ с БД

Сервер безопасности подключается к базе данных, указанной при установке СБ. При необходимости можно создать новую БД и изменить параметры соединения СБ с БД без переустановки ПО сервера безопасности.

Изменение учетных данных для подключения к БД

Если средствами СУБД были изменены имя и/или пароль учетной записи, используемой для подключения к БД, необходимо внести новые учетные данные в конфигурационный файл СБ. Процедура выполняется на компьютере СБ.

Для изменения учетных данных:

1. В каталоге установленного сервера безопасности запустите утилиту OmsDBPasswordChange.exe.

   На экране появится окно, представленное на рисунке ниже.

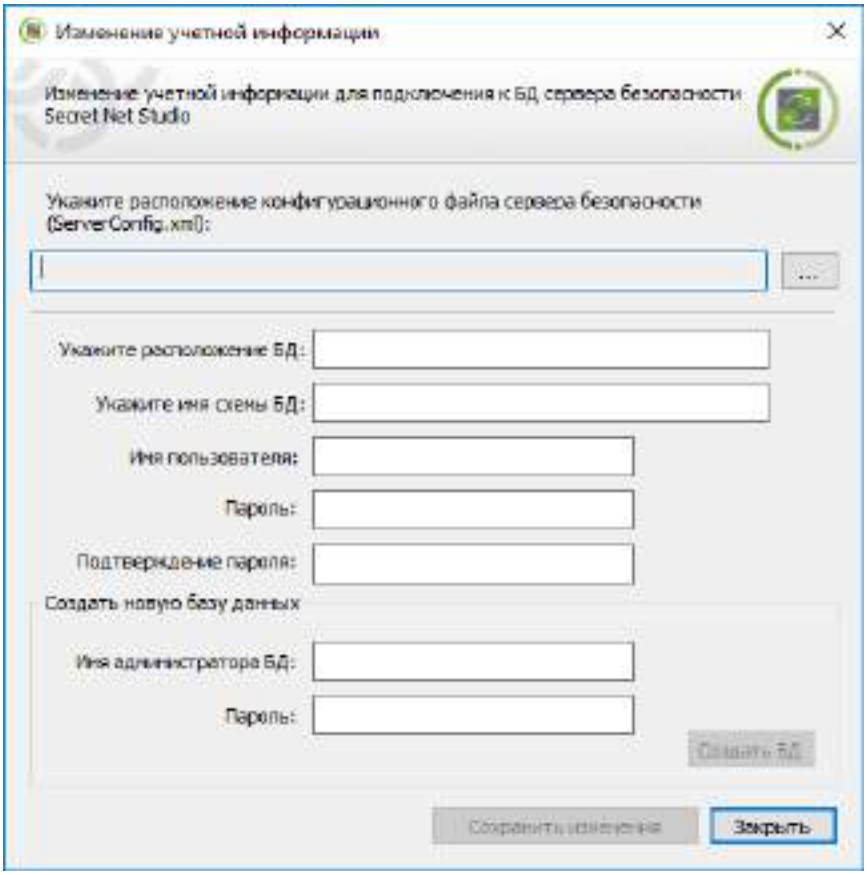


Рис.1 Окно утилиты OmsDBPasswordChange.exe

2. В окне утилиты укажите размещение конфигурационного файла ServerConfig.xml. Для этого нажмите кнопку справа от строки для указания пути и выберите файл в стандартном диалоге ОС Windows.

   Поля с расположением БД, именем схемы БД и именем пользователя для доступа к БД заполнятся автоматически.

3. Введите новые учетные данные пользователя в поля "Имя пользователя", "Пароль" и "Подтверждение пароля".
4. Нажмите кнопку "Сохранить изменения".
5. Перезагрузите компьютер.

Изменение параметров подключения к БД

При необходимости можно изменить параметры подключения СБ к БД:

- имя или IP-адрес компьютера, который является сервером СУБД;
- имя экземпляра БД на этом сервере;
- порт для подключения СБ к БД.

Примечание.
Изменение параметров может понадобиться, например, если БД перенесена на другой сервер СУБД. В данном случае необходимо средствами СУБД создать на новом сервере учетную запись для подключения СБ к БД. После создания учетной записи, если ее имя и/или пароль отличаются от предыдущей учетной записи, нужно изменить учетные данные, с которыми СБ выполняет подключение к БД (см. выше).

Для изменения параметров подключения:

1. В каталоге установленного сервера безопасности запустите утилиту OmsDBPasswordChange.exe.

   На экране появится окно утилиты (см. Рис.1 на стр.**73**)

2. Укажите размещение конфигурационного файла ServerConfig.xml. Для этого нажмите кнопку справа от строки для указания пути и выберите файл в стандартном диалоге ОС Windows.

   Поля с расположением БД, именем схемы БД и именем пользователя для доступа к БД заполнятся автоматически.

3. Измените значение поля с расположением БД, используя следующий формат строки:

   <имя_или_IP-адрес_сервера_MS_SQL>\<имя_экземпляра_БД>,<порт>

   Примечание.
   - Если сервер СУБД установлен на компьютере с СБ и используется стандартное имя экземпляра MSSQLSERVER, то имя или IP-адрес сервера СУБД указывать не нужно.
   - Если для подключения используется порт по умолчанию, то порт можно не указывать.

4. Введите пароль и подтверждение пароля учетной записи, используемой для подключения к БД.
5. Нажмите кнопку "Сохранить изменения".
6. Перезагрузите компьютер.

Создание новой БД

С помощью утилиты OmsDBPasswordChange.exe можно создать новую БД для Secret Net Studio на основе любой БД, имеющейся на сервере СУБД.

Для создания БД:

1. В каталоге установленного сервера безопасности запустите утилиту OmsDBPasswordChange.exe.

   На экране появится окно утилиты (см. Рис.1 на стр.**73**).

2. Укажите размещение конфигурационного файла ServerConfig.xml. Для этого нажмите кнопку справа от строки для указания пути и выберите файл в стандартном диалоге ОС Windows.

   Поля с расположением БД, именем схемы БД и именем пользователя для доступа к БД заполнятся автоматически.

3. Укажите расположение БД, имеющейся на сервере СУБД, используя следующий формат:

   <имя_или_IP-адрес_сервера_MS_SQL>\<имя_экземпляра_БД>,<порт>

Примечание.
- Если сервер СУБД установлен на компьютере с СБ и используется стандартный экземпляр MSSQLSERVER, то имя или IP-адрес сервера СУБД указывать не нужно.
- Если для подключения используется порт по умолчанию, то порт можно не указывать.

4. Введите имя схемы БД Secret Net Studio, которая будет создана.
5. Введите имя, пароль и подтверждение пароля учетной записи, которая будет использоваться для подключения СБ к БД.
6. В области "Создать новую базу данных" введите учетные данные администратора БД, имеющейся на сервере СУБД.
7. Нажмите кнопку "Создать БД".

   В указанной БД будет создана схема БД Secret Net Studio и учетная запись для подключения СБ к БД.
8. Нажмите кнопку "Сохранить изменения".
9. Перезагрузите компьютер.

Обновление БД

Обновление БД может понадобиться при обновлении Secret Net Studio с версии 8.4 и ниже до актуальной версии.

Внимание!
Перед обновлением рекомендуется сделать резервную копию БД средствами СУБД.

Для обновления БД:

1. В каталоге установленного сервера безопасности запустите программу OmsDBPasswordChange.exe.

   На экране появится окно программы (см. Рис.1 на стр.**73**).
2. Укажите размещение конфигурационного файла ServerConfig.xml. Для этого нажмите кнопку справа от строки для указания пути и выберите файл в стандартном диалоге ОС Windows.

   Поля с расположением БД, именем схемы БД и именем пользователя для доступа к БД заполнятся автоматически.
3. Введите имя, пароль и подтверждение пароля учетной записи, используемой для подключения СБ к БД.

   Примечание. На данном этапе можно создать новую учетную запись для подключения СБ к БД.
4. В области "Создать новую базу данных" введите учетные данные администратора имеющейся БД.
5. Нажмите кнопку "Создать БД".

   На экране появится сообщение "База данных будет обновлена до актуальной версии. Перед процедурой рекомендуется сделать резервную копию.".
6. Нажмите кнопку "ОК".

   База данных будет обновлена. Будет создан новый пользователь для подключения СБ к БД.
7. Перезагрузите компьютер.

Особенности использования резервного сервера безопасности

Чтобы обеспечить бесперебойное функционирование защищаемых компьютеров, подчиненных серверу безопасности, следует предусмотреть наличие резервного сервера в этом же домене безопасности. Резервный сервер безопасности должен находиться в постоянной доступности для регулярной синхронизации с основным сервером.

При выходе из строя основного сервера безопасности не происходит автоматического переподчинения компьютеров резервному серверу. Подчинение резервному серверу можно выполнить в программе оперативного управления (см. документ [**4**]). Для этого выведите компьютеры из подчинения предыдущему серверу и затем подчините их резервному серверу.

При этом возможны ситуации, когда после переподчинения на компьютерах возникает сбой при определении нового сервера безопасности. Это может происходить из-за недоступности сервера или отсутствия информации о нем в локальном хранилище. Например, если резервный сервер был установлен, а основной сервер вышел из строя в то время, когда компьютер клиента был отключен. В этом случае агент на компьютере не сможет обнаружить новый сервер и из-за этого будет функционировать некорректно. В частности, могут возникнуть проблемы входа в систему в режиме усиленной аутентификации и в других механизмах защиты.

Варианты восстановления некорректно удаленного сервера безопасности

Для функционирования сервера безопасности используется два каталога LDAP: глобальный и доменный. Между этими каталогами выполняется синхронизация, однако в остальном они независимы друг от друга.

Глобальный каталог является единственным для всего леса безопасности, в то же время, для каждого домена безопасности в лесу создаётся свой доменный каталог. Каждый сервер безопасности в лесу относится к единственному глобальному каталогу и к некоторому доменному каталогу, в зависимости от того, в какой домен безопасности он входит.

Перенос ролей мастера схемы и мастера именования LDAP на другой сервер безопасности

В каждом каталоге LDAP (глобальном или локальном) существуют сервера, которым присвоены специальные роли, а именно, роль мастера схемы и роль мастера именования, позволяющие выполнять различные операции внутри каталога. По умолчанию обе роли присваиваются первому серверу в каталоге (в случае глобального каталога это первый сервер в лесу безопасности, в случае доменного каталога – первый сервер в домене).

Если по какой-либо причине компьютер, которому присвоены роли, недоступен, то некоторые операции внутри каталога буду невозможны.

Для исправления ситуации необходимо восстановить доступность сервера или выполнить перенос ролей мастера схемы и мастера именования на другой сервер безопасности.

Примечание.
В общем случае в каталоге LDAP разные роли могут быть присвоены разным серверам – мастером схемы может являться один сервер, а мастером именования другой. Однако для корректного функционирования серверов безопасности необходимо, чтобы обе роли принадлежали одному серверу безопасности как в глобальном, так и в доменном каталоге. При переносе ролей необходимо следить за тем, чтобы в рамках леса в глобальном каталоге один сервер являлся как мастером схемы, так и мастером именования. Также в рамках каждого домена некоторый сервер безопасности должен являться и мастеров схемы, и мастером именования доменного каталога.

Дальнейшие операции описаны с учетом того, что обе роли присвоены одному серверу.

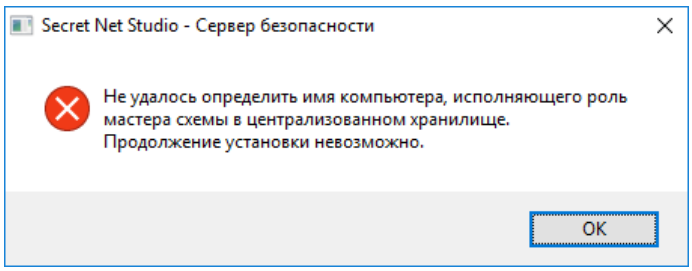
Причины недоступности мастера схемы

Выделяют две основные причины, по которым мастер схемы может оказаться недоступен в глобальном или локальном каталогах:

1. Сервер безопасности, выполняющий роль мастера схемы был удален из леса или домена безопасности. По умолчанию, мастером схемы в глобальном каталоге является первый сервер в лесу. Аналогично, мастером схемы в локальном каталоге является первый сервер в домене безопасности. Если удалить первый сервер в лесу, то такой лес потеряет мастера схемы глобального каталога. Если в некотором домене удалить первый сервер в домене, то такой домен потеряет мастера схемы доменного каталога.
2. Сервер безопасности, выполняющий роль мастера схемы был потерян (например, машина была физически отключена от сети, и больше никогда не включалась), или некорректно удален (без ввода паролей администраторов домена и леса безопасности, в результате чего информация о сервере осталась в каталоге). В этом случае, каталог через некоторое время диагностирует, что мастер схемы длительное время не выходил на связь, и будет считать, что мастер схемы отсутствует.

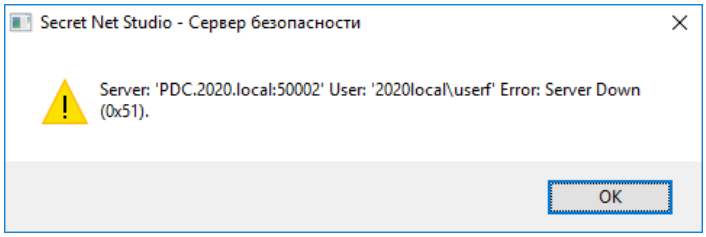
Проблемы, возникающие при отсутствии мастера схемы

Если мастер схемы глобального каталога был удален, то при установке новых серверов безопасности в данный лес может появляться следующая ошибка:



Аналогично, если в некотором домене безопасности в его доменном каталоге удален мастер схемы, то при попытке установить новый сервер безопасности в данный домен, может появляться вышеуказанная ошибка.

Если сервер мастер схемы глобального или доменного каталога был потерян по какой-либо причине (не существует, был некорректно удален), то в процессе установки нового сервера появится следующая ошибка:



Просмотр ролей в глобальном и доменном каталогах

Для того, чтобы выяснить, какой сервер является мастером схемы и мастером именования можно воспользоваться утилитой Dsmgmt, входящей в состав ОС Windows:

1. На компьютере, на котором установлена серверная версия ОС Windows, запустите консоль командной строки (cmd.exe) от имени администратора леса (если планируется просмотр ролей в глобальном каталоге) или от имени администратора домена (если планируется просмотр ролей в доменном каталоге)
2. Введите команду запуска утилиты:
   ```
   dsmgmt
   ```
3. В появившейся строке **dsmgmt:** введите команду управления:
   ```
   roles
   ```
4. В появившейся строке **fsmo maintenance:** введите команду управления:
   ```
   connections
   ```
5. В появившейся строке **server connections:** введите команду управления:
   ```
   connect to server <имя_компьютера>:<номер_порта>
   ```
6. В параметрах команды укажите полное DNS-имя компьютера сервера безопасности, принадлежащего лесу, если хотим просмотреть роли в лесу (или принадлежащего интересующему домену безопасности, если хотим просмотреть роли в конкретном доменном каталоге) и номер порта (значение порта по умолчанию для глобального каталога равно 50002, для доменного каталога - 50000).
7. После соединения с указанным компьютером в строке **server connections:** введите команду:
   ```
   quit
   ```
8. В строке **fsmo maintenance:** введите команду управления:

```
select operation target
```

9. В строке **select operation target:** введите команду управления:

```
list roles for connected server
```

В результате выполнения вышеуказанной команды, на экран будет выведено сообщение примерно следующего содержания:

```
Server "pdc:50002" knows about 2 roles
Schema - CN=NTDS Settings\0ADEL:98e3bb5c-8645-400f-8436-
8905e8c53b54,CN=2016FD$SecretNet-GC\0ADEL:8098b33f-16ec-44fa-
85d9-ff74aacea953,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,CN={00D201E5-F194-489D-9A9C-
6B28E33C2ADE}
Naming Master - CN=NTDS Settings\0ADEL:98e3bb5c-8645-400f-
8436-8905e8c53b54,CN=2016FD$SecretNet-GC\0ADEL:8098b33f-16ec-
44fa-85d9-ff74aacea953,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,CN={00D201E5-F194-489D-9A9C-
6B28E33C2ADE}
```

Данное сообщение содержит приставку DEL и имя сервера. Это значит, что сервер удален.

В системном журнале службы ADAM (Secretnet-GC) будет зарегистрировано следующее событие:

```
Event ID 2091: Ownership of the following FSMO role is set to
a server which is deleted or does not exist. Operations which
require contacting a FSMO operation master will fail until
this condition is corrected.
```

В случае, если мастер схемы не был удалён, или же он был потерян (вся информация о сервере осталась в системе) результат вывода команды **list roles for connected server** будет примерно следующим:

```
Server "pdc:50002" knows about 2 roles
Schema - CN=NTDS Settings,CN=BOSS$SecretNet-
GC,CN=Servers,CN=Default-First-Site-N
ame,CN=Sites,CN=Configuration,CN={20256F81-63B0-46B4-991C-
74AC57F17622}
Naming Master - CN=NTDS Settings,CN=BOSS$SecretNet-
GC,CN=Servers,CN=Default-
First-Site-Name,CN=Sites,CN=Configuration,CN={20256F81-63B0-
46B4-991C-74AC57F176
22}
```

Данное сообщение не содержит пометок DEL напротив имен серверов, исполняющих роли мастера схемы и мастера именования.

Перенос ролей

Перенос ролей выполняется с помощью утилиты Dsmgmt из состава ОС Windows.

Внимание!

После переноса ролей мастера схемы и мастера именования на другой компьютер будет утрачена возможность использования в этом качестве для предыдущего компьютера. Поэтому перенос ролей необходимо выполнять только в случае невозможности восстановления функционирования этого сервера. Если сервер безопасности, с которого были перенесены роли (пока он был недоступен) снова появится в лесу (или домене безопасности), это приведет к нарушению работоспособности, так как в каталоге LDAP будет более одного сервера с данными ролями

Для переноса ролей мастера схемы и мастера именования LDAP:

1. На компьютере сервера безопасности, который будет использоваться в качестве мастера схемы и мастера именования, запустите консоль командной строки (cmd.exe) от имени администратора леса (если планируется перенос ролей в глобальном каталоге) или от имени администратора домена (если планируется перенос ролей в доменном каталоге).
2. Введите команду запуска утилиты:

   ```
   dsmgmt
   ```

3. В появившейся строке **dsmgmt:** введите команду управления:

   ```
   roles
   ```

4. В появившейся строке **fsmo maintenance:** введите команду управления:

   ```
   connections
   ```

5. В появившейся строке **server connections:** введите команду управления:

   ```
   connect to server <имя_компьютера>:<номер_порта>
   ```

   В параметрах команды укажите полное DNS-имя компьютера сервера безопасности, который будет использоваться в качестве мастера схемы (или значение **localhost**), и номер порта (значение порта по умолчанию для глобального каталога равно 50002, для доменного каталога - 50000).
6. После соединения с указанным компьютером в строке **server connections:** введите команду:

   ```
   quit
   ```

7. В строке **fsmo maintenance:** введите команду управления:

   ```
   seize schema master
   ```

8. По появившейся информации о результате выполнения команды убедитесь, что роль мастера схем присвоена нужному серверу безопасности.
9. В строке **fsmo maintenance:** введите команду управления:

   ```
   seize naming master
   ```

10. По появившейся информации о результате выполнения команды убедитесь, что роль мастера именования присвоена нужному серверу безопасности.
11. После присвоения ролей мастера схемы и мастера именования завершите работу с утилитой с помощью команды **quit**.

Документация

1. Средство защиты информации Secret Net Studio. Руководство администратора. Принципы построения	RU.88338853.501400.001 91 1
2. Средство защиты информации Secret Net Studio. Руководство администратора. Установка, обновление, удаление	RU.88338853.501400.001 91 2
3. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Основы и базовая защита	RU.88338853.501400.001 91 3
4. Средство защиты информации Secret Net Studio. Руководство администратора. Централизованное управление, мониторинг и аудит	RU.88338853.501400.001 91 4
5. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Локальная защита	RU.88338853.501400.001 91 5
6. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Сетевая защита	RU.88338853.501400.001 91 6
7. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Антивирус и средство обнаружения вторжений	RU.88338853.501400.001 91 7
8. Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Доверенная среда	RU.88338853.501400.001 91 8
9. Средство защиты информации Secret Net Studio. Руководство администратора. Сервер обновлений. Установка и настройка	
10. Средство защиты информации Secret Net Studio. Руководство пользователя	RU.88338853.501400.001 92