



КОД БЕЗОПАСНОСТИ

Средство защиты информации

# Secret Net Studio

## Руководство администратора

Установка, обновление, удаление



## КОД БЕЗОПАСНОСТИ

**© Компания "Код Безопасности", 2018. Все права защищены.**

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

Почтовый адрес: **115127, Россия, Москва, а/я 66**  
**ООО "Код Безопасности"**

Телефон: **8 495 982-30-20**

E-mail: **info@securitycode.ru**

Web: **http://www.securitycode.ru**

# Оглавление

<b>Список сокращений</b> .....	<b>5</b>
<b>Введение</b> .....	<b>6</b>
<b>Общие сведения о развертывании системы</b> .....	<b>7</b>
Состав устанавливаемых компонентов .....	7
Требования к аппаратному и программному обеспечению .....	7
Клиент .....	7
Сервер безопасности .....	8
Программа управления .....	9
Установочный диск системы .....	9
Программа автозапуска .....	10
Варианты установки компонентов .....	11
Порядок установки для централизованного управления .....	11
Подготовительные действия .....	11
Общий порядок установки компонентов .....	11
Типовой сценарий развертывания .....	11
<b>Локальная установка компонентов</b> .....	<b>13</b>
Установка сервера безопасности .....	13
Создание леса и домена безопасности .....	13
Создание домена безопасности в имеющемся лесу .....	17
Добавление сервера в имеющийся домен безопасности .....	18
Установка программы управления .....	19
Установка клиента .....	19
Установка клиента в интерактивном режиме .....	19
Установка драйвера средства аппаратной поддержки .....	23
<b>Настройка централизованной установки клиента</b> .....	<b>25</b>
Установка под управлением сервера безопасности .....	25
Формирование списка централизованно устанавливаемого ПО .....	25
Формирование заданий развертывания .....	26
<b>Обновление и переустановка компонентов</b> .....	<b>29</b>
Обновление .....	29
Порядок обновления компонентов централизованного управления .....	29
Обновление сервера безопасности .....	29
Обновление программы управления .....	31
Обновление клиента .....	31
Особенности установки клиента в режиме обновления других продуктов .....	32
Переустановка (восстановление) .....	33
Переустановка клиента .....	33
Переустановка программы управления .....	34
<b>Удаление компонентов</b> .....	<b>35</b>
Порядок удаления в сетевом режиме функционирования .....	35
Удаление клиента .....	35
Удаление драйвера средства аппаратной поддержки .....	35
Удаление программы управления .....	36
Удаление сервера безопасности .....	36
Удаление отдельных подсистем клиента .....	36
<b>Приложение</b> .....	<b>38</b>
ПО для использования поддерживаемых USB-ключей и смарт-карт .....	38
Изменения в реестре при установке клиента .....	39
Каталог установки клиента .....	39
Сведения об установке и настройке СУБД MS SQL .....	40
Изменения в IIS при установке сервера безопасности .....	42
Изменение параметров соединения сервера безопасности с БД .....	43
Учетные данные для подключения к базе данных .....	43

Строка соединения с экземпляром БД .....	43
Особенности использования резервного сервера безопасности .....	44
Варианты восстановления некорректно удаленного сервера безопасности .....	45
Перенос роли мастера схемы LDAP на другой сервер безопасности .....	45
<b>Документация .....</b>	<b>46</b>

## Список сокращений

<b>AD</b>	Active Directory
<b>IIS</b>	Internet Information Services
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>NTFS</b>	New Technology File System
<b>OID</b>	Object Identifier
<b>SID</b>	Security Identifier
<b>SP</b>	Service Pack
<b>USB</b>	Universal Serial Bus
<b>VPN</b>	Virtual Private Network
<b>XML</b>	Extensible Markup Language
<b>АПКШ</b>	Аппаратно-программный комплекс шифрования
<b>БД</b>	База данных
<b>ИС</b>	Информационная система
<b>КЦ</b>	Контроль целостности
<b>ОС</b>	Операционная система
<b>ОСР</b>	Общедоступный сетевой ресурс
<b>ОУ</b>	Оперативное управление
<b>ПАК</b>	Программно-аппаратный комплекс
<b>ПО</b>	Программное обеспечение
<b>СБ</b>	Сервер безопасности
<b>СУБД</b>	Система управления базами данных
<b>ЦУ</b>	Централизованное управление
<b>ЭИ</b>	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" (<http://www.securitycode.ru/>) или связаться с представителями компании по электронной почте ([support@securitycode.ru](mailto: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 <http://www.securitycode.ru/company/education/training-courses/>. Связаться с представителем компании по вопросам организации обучения можно по электронной почте ([education@securitycode.ru](mailto: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 8/8.1;
- Windows 7 SP1;
- Windows Server 2012/Server 2012 R2;
- Windows Server 2008 SP2/Server 2008 R2.

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 <sup>1</sup>
Оперативная память	2 ГБ
Жесткий диск (свободное пространство)	4 ГБ

<sup>1</sup> При использовании компонента "Антивирус" (ClamAV) необходим процессор с двумя физическими или логическими (технология hyper-threading) ядрами.

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

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. 38).

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.

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 2013;
- Microsoft .NET Framework 4.5;
- пакеты обновлений Microsoft KB2117917, KB971512 и 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 2012/Server 2012 R2;
- Windows Server 2008 R2.

Требования к аппаратной конфигурации компьютера:

Элемент	Минимально	Рекомендуется
Процессор	В соответствии с требованиями ОС	Intel Core i5/Хеон Е3 и выше
Оперативная память	8 ГБ	16 ГБ <sup>1</sup>
Жесткий диск (свободное место)	150 ГБ Рекомендуется использовать высокоскоростной жесткий диск	

<sup>1</sup> 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 с установленными пакетами обновлений не ниже указанных):

- Microsoft SQL Server 2012 SP1, включая свободно распространяемый вариант SQL Server 2012 Express (установку СУБД MS SQL Server 2012 SP1 Express можно выполнить с установочного диска комплекта поставки — см. стр.40);
- Microsoft SQL Server 2014, включая свободно распространяемый вариант SQL Server 2014 Express;
- Microsoft SQL Server 2008 R2 SP1, включая свободно распространяемый вариант SQL Server 2008 R2 Express.

Корректное взаимодействие сервера безопасности и СУБД MS SQL обеспечивается при выполнении условий, изложенных в приложении на стр.40.

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

- для компьютера должна быть включена роль Веб-сервера (IIS).

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

- Microsoft C/C++ Runtime для Visual Studio 2013.

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 8/8.1;
- Windows 7 SP1;
- Windows Server 2012/Server 2012 R2;
- Windows Server 2008 SP2/Server 2008 R2 SP1.

Требования к аппаратной конфигурации компьютера:

Элемент	Минимально
Процессор	В соответствии с требованиями ОС
Оперативная память	2 ГБ <sup>1</sup>
Жесткий диск (свободное пространство)	4 ГБ <sup>2</sup>

<sup>1</sup> 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.

<sup>2</sup> 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.

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

- 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

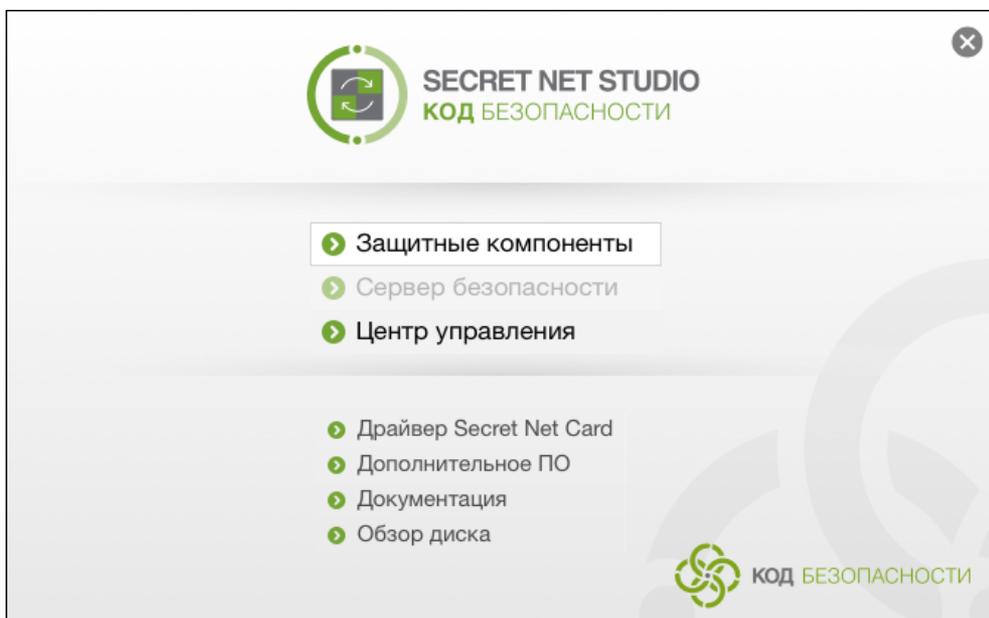
При вставке установочного диска в привод для чтения оптических дисков происходит автоматический запуск программы автозапуска, которая позволяет выполнять следующие действия:

- 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 следующем рисунке.



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

Команда	Назначение
<b>Защитные компоненты</b>	Запускает программу установки клиента
<b>Сервер безопасности</b>	Запускает программу установки сервера безопасности
<b>Центр управления</b>	Запускает программу установки программы управления
<b>Драйвер Secret Net Card</b>	Запускает программу установки драйвера средства аппаратной поддержки Secret Net Card
<b>Дополнительное ПО</b>	Открывает в отдельном окне каталог \Tools\
<b>Документация</b>	Открывает в отдельном окне каталог \Documentation\
<b>Обзор диска</b>	Открывает в отдельном окне корневой каталог диска

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 системы 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 системы 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 системы 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. 13).
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. 19).
4. Установите ПО клиента системы Secret Net Studio в сетевом режиме функционирования (см. стр. 19) 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.

**Примечание.**

В рассматриваемом типовом сценарии вместо двух групп допускается создать одну группу администраторов безопасности. Данную группу можно будет указать и как группу администраторов леса и как группу администраторов домена безопасности. Однако для случая расширения системы до нескольких доменов безопасности рекомендуется создать отдельную группу администраторов леса, и в созданные группы включить различные учетные записи.

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. **13**).

**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. **44**.

4. На компьютере администратора безопасности установите программу управления (см. стр. **19**).
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. **25**).
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 системы 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\i64\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.

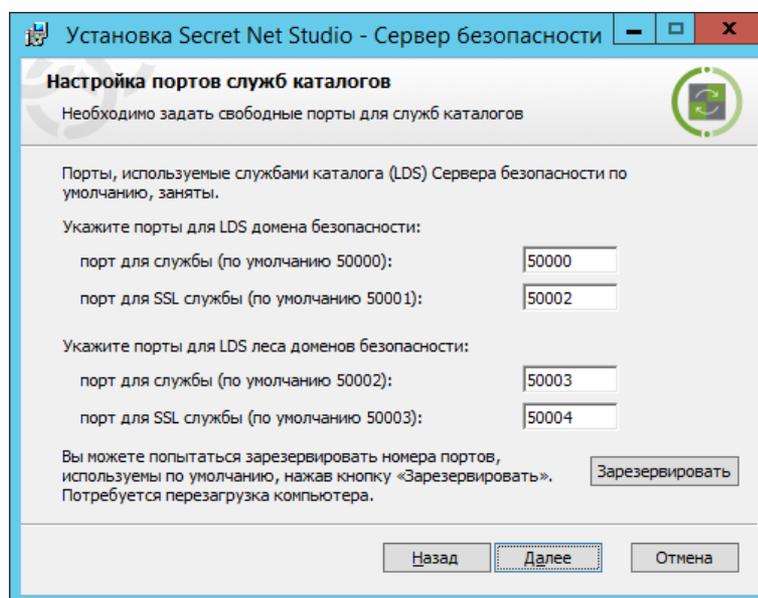
По окончании подготовительных действий на экран будет выведен диалог приветствия программы установки.

2. Для продолжения установки нажмите кнопку "Далее".

На экране появится диалог принятия лицензионного соглашения.

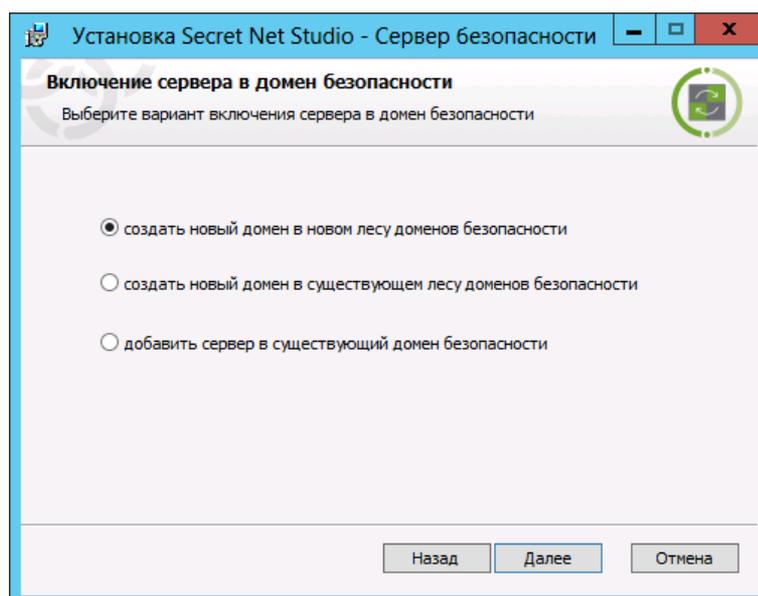
3. Ознакомьтесь с содержанием лицензионного соглашения, отметьте пункт о его принятии и нажмите кнопку "Далее".

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



4. 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".



5. 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.

6. 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".

7. 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.

8. Нажмите кнопку "Далее".

На экране появится диалог "Группы администраторов безопасности".

9. Укажите группы пользователей, которым будут предоставлены права администрирования домена безопасности и леса доменов безопасности. Нажмите кнопку "Далее".

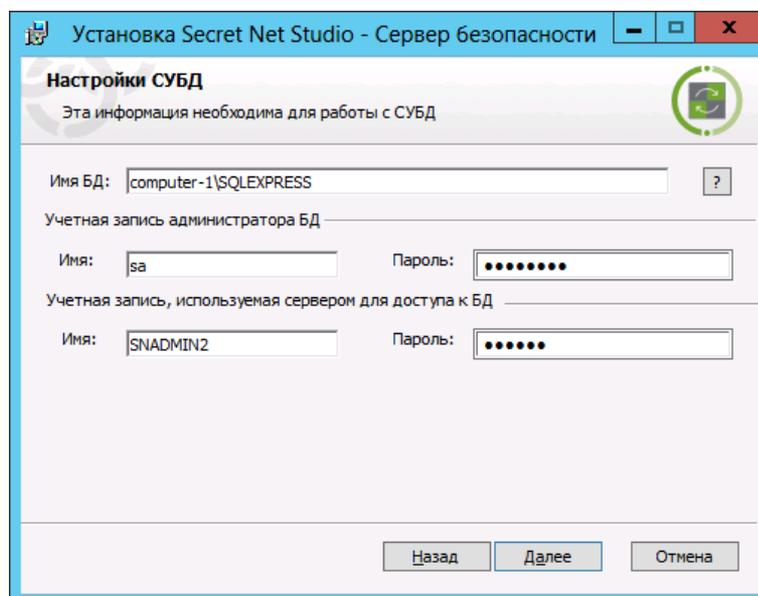
**Примечание.**

В качестве группы администраторов домена безопасности не рекомендуется использовать стандартную доменную группу администраторов (Domain Admins). Иначе при подключении к серверу программы управления, установленной на этом же компьютере, может возникать ошибка из-за недостаточных привилегий пользователя, если включен механизм управления учетными записями (User Account Control — UAC). В этих условиях подключение будет разрешено только для первичной учетной записи администратора домена Windows. Чтобы начать сеанс работы с программой с нужными правами, можно использовать команду "Запуск от имени администратора" ("Run As Administrator") в контекстном меню ярлыка программы управления. Для администраторов домена безопасности рекомендуется использовать специально созданную группу пользователей.

На экране появится диалог "Настройка каталогов".

10. 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.



**11.** 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 строку соединения с экземпляром БД: `<имя_или_IP-адрес_сервера_MS_SQL>\<имя_экземпляра_БД>,<порт>`

**Примечание.**

Номер порта можно не указывать, если используется порт по умолчанию.

- в группе полей "Учетная запись администратора БД" — учетные данные администратора базы данных на сервере СУБД;
- в группе полей "Учетная запись, используемая сервером для доступа к БД" — учетные данные, с которыми сервер безопасности будет выполнять подключение к базе данных (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).

- Нажмите кнопку "Далее".

**12.** 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".

**13.** 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.

**14.** 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.

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

#### 15. Нажмите кнопку "Готово".

На экране появится окно с перечнем операций программы установки. После завершения всех предусмотренных операций будет выведено предупреждение 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, имеющих в Active Directory, с базой данных СБ. В зависимости от количества учетных записей процесс синхронизации может занять от нескольких минут до одного часа. Во время синхронизации подключение к этому серверу программы управления невозможно (в программе выдается сообщение о выполнении синхронизации). Рекомендуется дождаться завершения синхронизации (когда подключение программы к серверу станет возможным) 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 **1–4** процедуры установки сервера с созданием нового леса и домена безопасности (см. стр. **13**).
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".

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. **13**), начиная с действия **10**.

## 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 **1–4** процедуры установки сервера с созданием нового леса и домена безопасности (см. стр. **13**).
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 диалог "Домен безопасности".

6. Выберите в раскрывающемся списке контейнер для включения сервера безопасности в состав домена безопасности, сформированного на базе контейнера. В списке представлены контейнеры, для которых уже сформированы домены безопасности. После выбора контейнера 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. **13**), начиная с действия **10**.

## 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 "Заккрыть" 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. **25**). 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.**

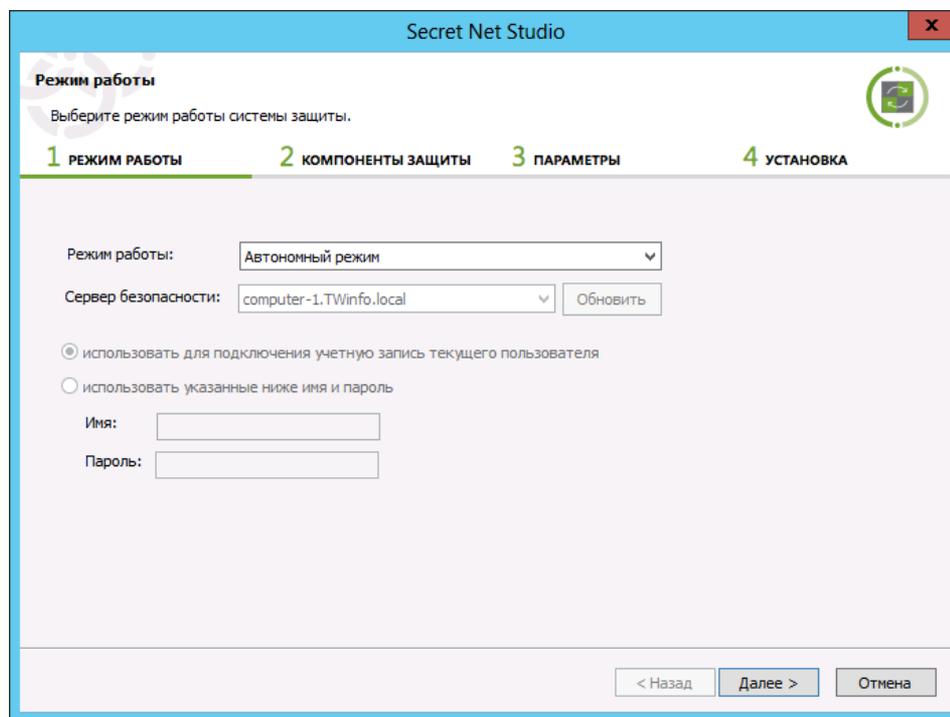
Запуск установки можно выполнить вручную без использования программы автозапуска. Для этого в зависимости от операционной системы компьютера выполните следующее действие:

- 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.

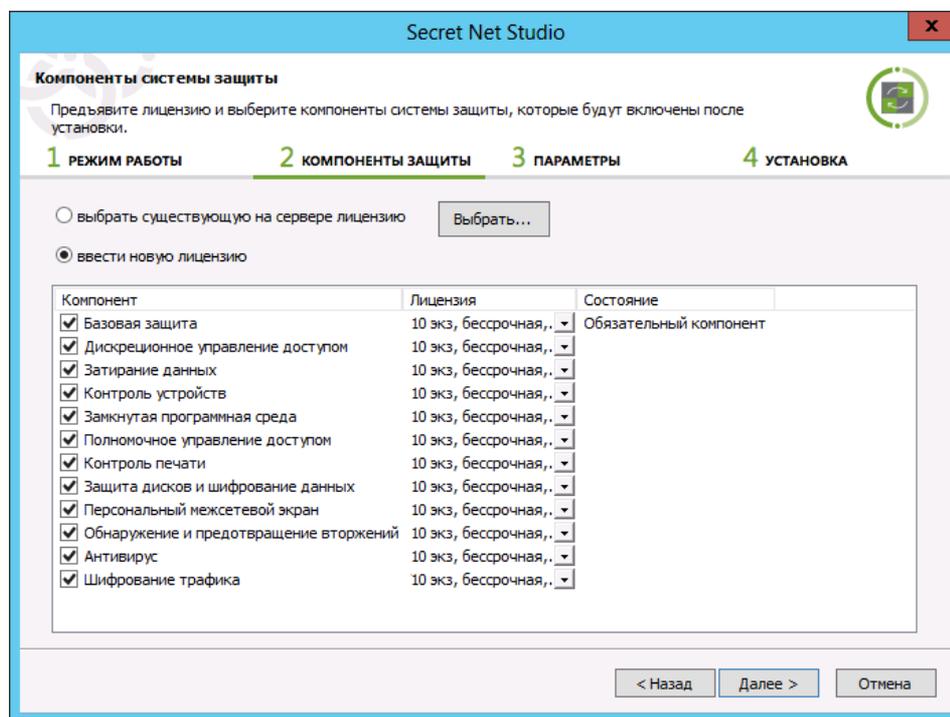


3. В поле "Режим работы" укажите нужный режим функционирования клиента — автономный ("Автономный режим") или сетевой ("Под управлением сервера безопасности"). Для сетевого режима функционирования настройте параметры подчинения серверу безопасности:

- Выберите имя компьютера сервера безопасности, которому будет подчинен данный компьютер (если в раскрывающемся списке отсутствует имя нужного сервера, нажмите кнопку "Обновить" для повторной загрузки).
- 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.** В диалоге укажите метод получения лицензий:

- чтобы загрузить лицензии с сервера безопасности, который был выбран для подчинения, — установите отметку в поле "выбрать существующую на сервере лицензию";
- чтобы загрузить лицензии из файла (в частности, при установке клиента в автономном режиме функционирования) — установите отметку в поле "вести новую лицензию".

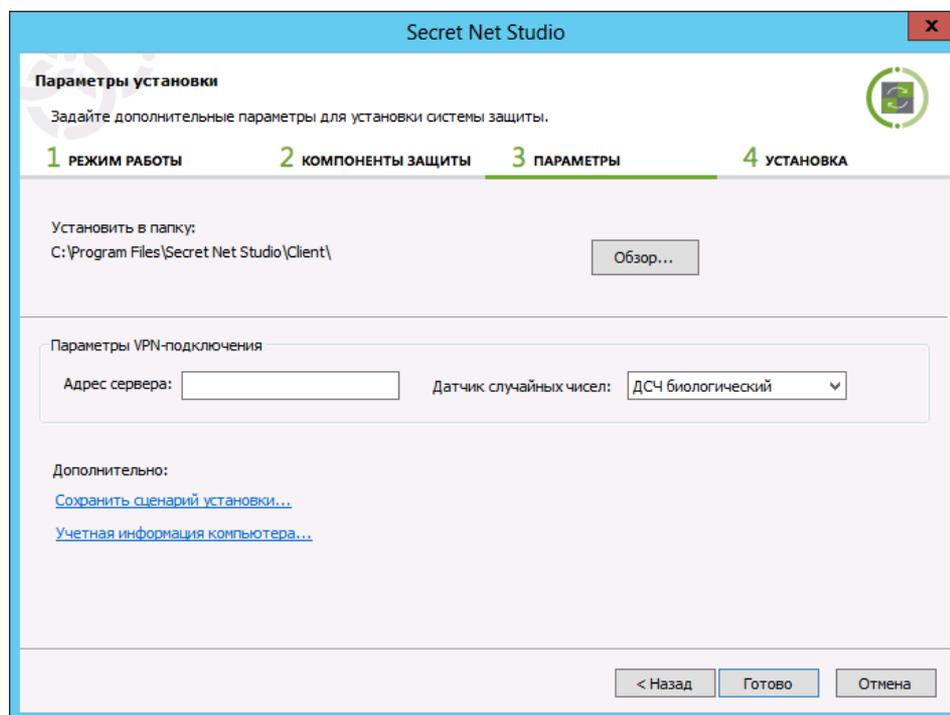
**6.** Нажмите кнопку "Выбрать". Если указан метод получения лицензий из файла, выберите нужный файл в появившемся диалоге.

После загрузки данных в диалоге появятся сведения о лицензиях.

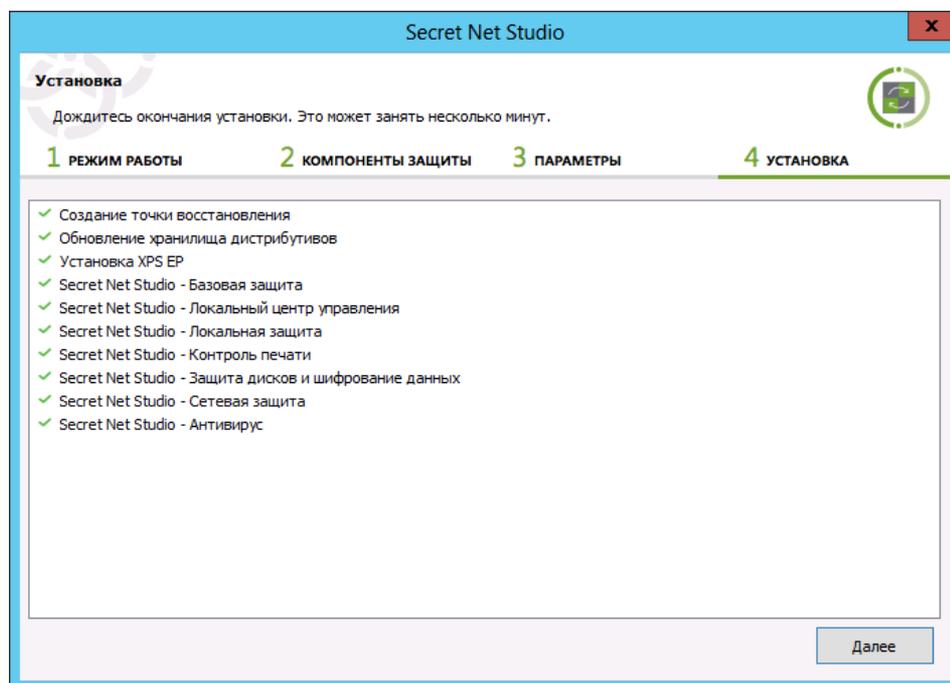
**7.** Отметьте в списке устанавливаемые подсистемы, для которых имеются свободные лицензии (установку компонента "Базовая защита" отключить нельзя). При наличии нескольких групп лицензий для компонента, можно выбрать нужную группу в раскрывающемся списке.

**8.** Нажмите кнопку "Далее >".

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



9. В поле "Установить в папку" оставьте заданную по умолчанию папку установки клиента или укажите другую папку назначения.
10. Если на компьютере будет использоваться подсистема шифрования трафика (VPN клиент), настройте параметры подключения и установки в группе полей "Параметры VPN-подключения":
  - в поле "Адрес сервера" укажите адрес сервера доступа АПКШ "Континент", к которому будет выполняться подключение;
  - в поле "Датчик случайных чисел" выберите средство для генерации случайных чисел — программный модуль генерации ("ДСЧ биологический") или, при наличии ПАК "Соболь", физический датчик устройства ("ДСЧ ПАК "Соболь").
11. 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 "Учетная информация компьютера".
12. По окончании настройки параметров нажмите кнопку "Готово". Начнется процесс установки защитных подсистем в соответствии с заданными параметрами.



**13.** После завершения всех операций установки нажмите кнопку "Далее".

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

**14.** 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.

**15.** 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. По окончании 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 специального пакета исправлений ("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".

РАЗВЕРТЫВАНИЕ		ЗАДАНИЯ		ЛИЦЕНЗИРОВАНИЕ		РЕПОЗИТОРИЙ	
Добавить            Удалить		действия					
Имя	Тип	Версия	Дата	Описание			
Secret Net Studio	Обновление	8.1.685.4	10-09-2016 00:46:19	Дистрибутив продукта Secret Net Studio			

2. Вызовите контекстное меню в любом месте списка и выберите команду "Добавить".

На экране появится диалог для добавления.

3. В поле "Путь к дистрибутиву" укажите путь к каталогу с файлами для создания установочного комплекта. Например, если комплект нужно создать на основе установочного диска системы Secret Net Studio — укажите корневой каталог установочного диска.

После считывания содержимого указанного каталога автоматически будут заполнены остальные поля в диалоге для добавления.

4. Нажмите кнопку "Добавить" и дождитесь окончания процедуры создания комплекта (процесс отправки файлов на сервер безопасности может занять продолжительное время).

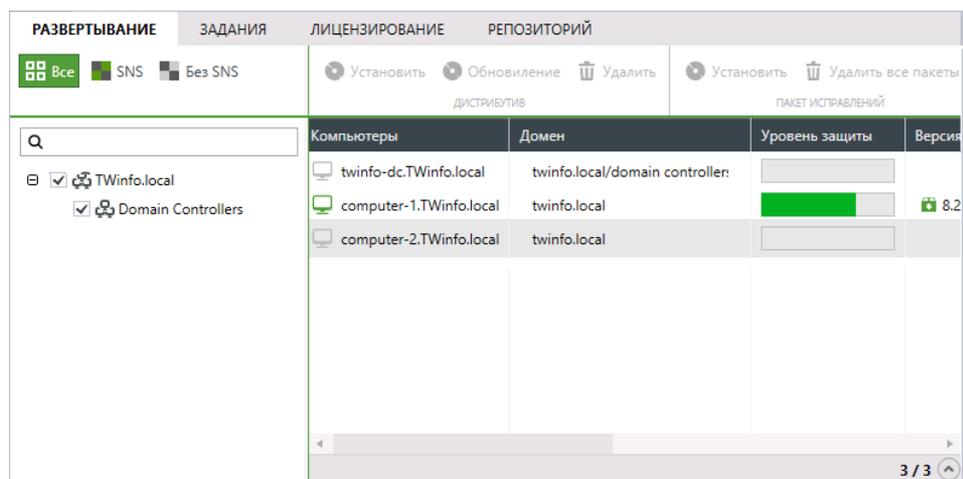
По окончании процесса в списке появится новый элемент, содержащий сведения о загруженном комплекте.

## 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. 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.

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.

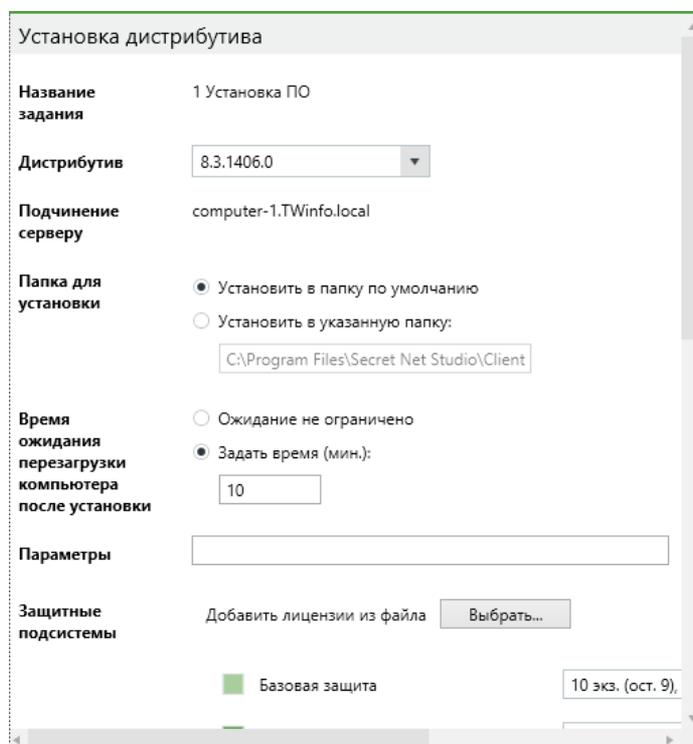
Для просмотра подробных сведений о компьютерах можно включить отображение области сведений с помощью кнопки, которая расположена в правой части строки под списком компьютеров.

**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.

3. Вызовите контекстное меню одного из выбранных компьютеров и выберите нужную команду. Например, для установки ПО клиента используйте команду "Установить ПО".

В правой части окна появится панель настройки параметров задания.



Установка дистрибутива

Название задания: 1 Установка ПО

Дистрибутив: 8.3.1406.0

Подчинение серверу: computer-1.TWinfo.local

Папка для установки:
 

- Установить в папку по умолчанию
- Установить в указанную папку: C:\Program Files\Secret Net Studio\Client

Время ожидания перезагрузки компьютера после установки:
 

- Ожидание не ограничено
- Задать время (мин.): 10

Параметры: [Empty text box]

Защитные подсистемы:
 

- Добавить лицензии из файла [Выбрать...]
- Базовая защита (10 экз. (ост. 9))

4. 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 "Ожидание 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;
  - параметры — определяет параметры командной строки, с которыми будет запущена программа установки;
  - лицензии на использование компонентов;
  - учетные данные локального администратора (доменного пользователя, входящего в локальные группы администраторов на выбранных компьютерах).
5. После создания задания перейдите к списку заданий на вкладке "Задания" для проверки добавления нового элемента.

РАЗВЕРТЫВАНИЕ    **ЗАДАНИЯ**    ЛИЦЕНЗИРОВАНИЕ    РЕПОЗИТОРИЙ

Отменить    Удалить  
ЗАДАНИЕ

Отменить  
КОМПЬЮТЕР

Компьютеры	Начало выполнения	Конец выполнения	Статус
compute	24.10.2016 20:01:0		Установ

**00 Установка ПО**    Выполнение

Время запуска: 24.10.2016 20:00:26 [подробнее](#)

1/1

## 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 обновления 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. [29](#)). 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. [31](#)) на рабочих местах администраторов.
4. Обновите ПО клиента (см. стр. [31](#)) в порядке:
  - серверы безопасности;
  - компьютеры сотрудников.

#### Совет.

При большом количестве компьютеров целесообразно применить автоматическое обновление клиента путем централизованной установки под управлением сервера безопасности (см. стр. [25](#)).

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.

**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.

2. Нажмите кнопку "Обновить".

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

**Примечание.**

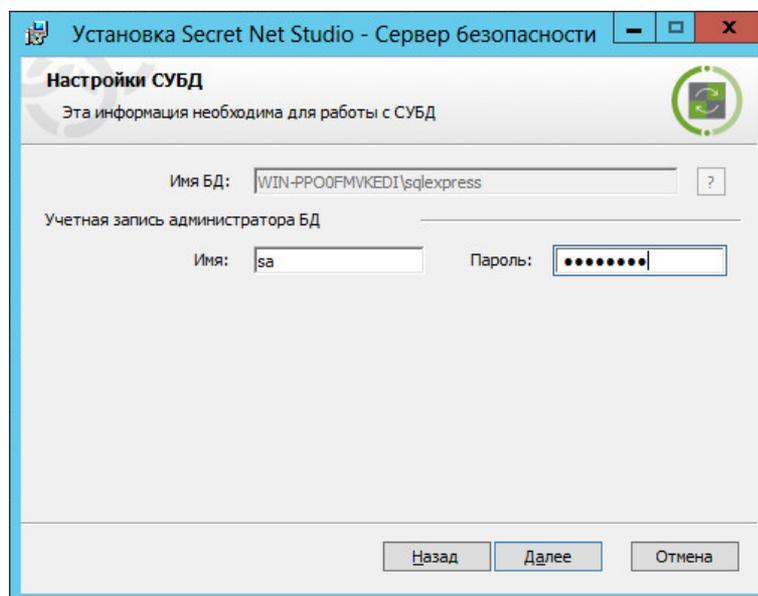
Перед выполнением дальнейших действий рекомендуется завершить работу программы автозапуска, нажав кнопку "Выход" в окне программы.

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 сервере СУБД и нажмите кнопку "Далее".  
На экране появится диалог "Все готово к обновлению".
6. Нажмите кнопку "Обновить".  
Начнется процесс обновления программных модулей.  
После завершения всех операций появится сообщение с предложением перезагрузить компьютер.
7. Перезагрузите компьютер и дождитесь загрузки системы.



#### **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).

## **Обновление программы управления**

Обновление программы управления выполняется пользователем, входящим в локальную группу администраторов компьютера. Для запуска процедуры обновления компонента используйте установочный диск (см. стр. 19). Процедура обновления выполняется без особенностей.

## **Обновление клиента**

Обновление клиента выполняется пользователем, входящим 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 завершить работу программы автозапуска, нажав кнопку "Выход" в окне программы.

2. Нажмите кнопку "Готово".

Начнется процесс обновления защитных подсистем.

3. После завершения всех операций нажмите кнопку "Далее".

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

4. 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.

5. Перезагрузите компьютер и дождитесь загрузки системы.

## 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;
- СКЗИ "Континент-АП".

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, если в списке устанавливаемых подсистем выбран антивирус.

#### 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.

### Установка при наличии СКЗИ "Континент-АП"

При наличии ПО СКЗИ "Континент-АП" (до версии 4.0) сохраняется имеющаяся версия продукта, которая будет функционировать без интеграции с системой Secret Net Studio. В этом случае не выполняется установка подсистемы шифрования трафика (VPN клиента) из состава клиента Secret Net Studio.

## 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. 19), 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 для выбора варианта действий установите отметку в поле "исправить" и нажмите кнопку "Готово".  
Начнется процесс установки защитных подсистем. Ход выполнения операций отображается в информационном окне в виде полосы прогресса.
2. После завершения всех операций установки нажмите кнопку "Далее".  
На экране появится сообщение, содержащее отчет о выполнении операций.
3. Перезагрузите компьютер.

## Переустановка программы управления

При переустановке программы управления выполняется восстановление компонента.

Запуск процедуры переустановки осуществляется так же, как и запуск установки программы (см. стр. 19). 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.  
После успешной установки и настройки на экране появится диалог "Установка завершена".
3. Нажмите кнопку "Готово".

## 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

При удалении клиентов Secret Net Studio в сетевом режиме функционирования и компонентов для централизованного управления рекомендуется придерживаться следующей последовательности действий:

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. 26).

Ниже рассматриваются процедуры локального удаления клиента.

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

### Для удаления клиента:

1. Выполните запуск процедуры установки клиента в интерактивном режиме (см. стр. 19 ) 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".  
Начнется процесс удаления защитных подсистем.
4. После завершения всех операций удаления нажмите кнопку "Далее".  
На экране появится сообщение, содержащее отчет о выполнении операций.
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 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:

- антивирус;
- подсистема шифрования трафика (VPN клиент);
- 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. 19) 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".

На экране появится диалог для выбора удаляемых подсистем.

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

Начнется процесс удаления защитных подсистем.

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

На экране появится сообщение, содержащее отчет о выполнении операций.

5. Перезагрузите компьютер.

# Приложение

## 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 или с сертификатами для подключения к серверу доступа АПКШ "Континент" необходимо дополнительно установить набор драйверов и утилит SafeNet Authentication Client, предоставляемый производителем устройств.

## Изменения в реестре при установке клиента

Программа установки компонента "Secret Net Studio" вносит следующие изменения в стандартные параметры реестра:

Имя параметра	Тип	Значение
Раздел HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\		
NoDriveTypeAutoRun	DWORD	0xFF

## Каталог установки клиента

При установке клиентского ПО системы Secret Net Studio создается системная переменная окружения SNINSTALLDIR, в которую записывается путь к каталогу установки клиента. Также для каталога установки определяются права доступа, перечисленные в следующей таблице.

Имя объекта	Права доступа
%SNINSTALLDIR%	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Read, Execute
%SNINSTALLDIR%\icheck	Administrators: FullControl SYSTEM: FullControl

## 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:

- <http://technet.microsoft.com/ru-ru/library/ms143506%28v=sql.120%29.aspx> (для SQL Server 2014);
- <http://technet.microsoft.com/ru-ru/library/ms143506%28v=sql.110%29.aspx> (для SQL Server 2012);
- <http://technet.microsoft.com/ru-ru/library/ms143506%28v=sql.105%29.aspx> (для SQL Server 2008 R2).

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 SQLEXPRT\_x64\_ENU.exe или SQLEXPRT\_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.



## 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, развёрнутых на компьютере. В связи с этим может быть нарушена работоспособность других сайтов и приложений, использующих в IIS порт 443.

В дополнительных параметрах пула приложений SecretNetAppPool 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 сервера безопасности с БД

Сервер безопасности выполняет подключение к базе данных на сервере СУБД с использованием параметров, указанных при установке СБ. В случае необходимости параметры можно изменить без переустановки ПО сервера безопасности.

### Учетные данные для подключения к базе данных

Если средствами СУБД были изменены имя и/или пароль учетной записи, используемой для подключения к базе данных, необходимо синхронизировать новые учетные данные в конфигурационном файле сервера безопасности. Процедура ввода учетных данных выполняется на компьютере сервера безопасности.

#### Для изменения учетных данных в конфигурационном файле:

1. В каталоге установки сервера безопасности запустите на исполнение файл OmsDBPasswordChange.exe.  
На экране появится диалог программы изменения учетных данных.  
Программа автоматически определит размещение основного конфигурационного файла, используемого сервером безопасности, и выведет полный путь к этому файлу.
2. При необходимости укажите другое размещение конфигурационного файла (например, чтобы внести изменения в резервную копию основного файла). Для этого нажмите кнопку, которая расположена справа от строки со значением текущего пути, и укажите файл в диалоге выбора файлов ОС Windows.
3. Введите измененные учетные данные пользователя в соответствующих полях: "Имя пользователя" (по умолчанию содержит имя, полученное из конфигурационного файла), "Пароль" и "Подтверждение пароля".
4. Нажмите кнопку "Сохранить изменения".
5. После обновления основного конфигурационного файла, используемого сервером безопасности, перезагрузите компьютер.

### Строка соединения с экземпляром БД

Строка соединения с экземпляром БД определяет имя или IP-адрес компьютера, который является сервером СУБД, имя экземпляра базы данных на этом сервере и порт для подключения. При необходимости можно изменить параметры соединения в конфигурационном файле сервера безопасности. Например, если база данных перенесена на другой сервер СУБД.



#### Примечание.

В случае переноса базы данных на другой сервер СУБД необходимо средствами СУБД создать на новом сервере учетную запись для подключения сервера безопасности к БД. После создания учетной записи, если ее имя и/или пароль отличаются от предыдущей учетной записи, нужно выполнить процедуру изменения учетных данных, с которыми сервер безопасности выполняет подключение к БД (см. выше).

#### Для изменения параметров соединения:

1. В каталоге установки сервера безопасности откройте для редактирования конфигурационный файл ServerConfig.xml.
2. Найдите элемент DB, содержащий атрибут dataSource.
3. Отредактируйте значение атрибута dataSource. Формат строки:  
dataSource="*<имя\_или\_IP-адрес\_сервера\_MS\_SQL>\<имя\_экземпляра\_БД>*,*<порт>*"

#### Примечание.

Номер порта можно не указывать, если используется порт по умолчанию.

4. Закройте конфигурационный файл с сохранением сделанных изменений и перезагрузите компьютер сервера безопасности.

## 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

Если сервер безопасности был некорректно удален, установка нового сервера в штатном порядке может оказаться невозможной из-за ошибок. Также возможны ошибки при изменении конфигурации структуры оперативного управления.

Причины некорректного удаления сервера могут быть различными — например, из-за сбоя во время работы программы установки в режиме удаления или при выходе из строя жесткого диска на компьютере сервера безопасности. Чтобы обеспечить возможность нормального функционирования, необходимо выполнить дополнительные действия для восстановления нужного состояния системы.

### Перенос роли мастера схемы LDAP на другой сервер безопасности

Одному из серверов должна быть присвоена роль мастера схемы LDAP для службы каталогов. По умолчанию эта роль присваивается первому установленному серверу безопасности.

Если мастер схемы был некорректно удален, в системе будет невозможно установить новые серверы безопасности, а также выполнять другие конфигурационные действия, требующие синхронизации между серверами.

Для исправления ситуации необходимо восстановить доступность сервера или выполнить перенос роли мастера схемы LDAP на другой сервер безопасности. Перенос роли выполняется с помощью утилиты Dsmgmt из состава ОС Windows.



#### Внимание!

После переноса роли мастера схемы на другой компьютер будет утрачена возможность использования в этом качестве для предыдущего компьютера. Поэтому перенос роли необходимо выполнять только в случае невозможности восстановления функционирования этого сервера.

#### Для переноса роли мастера схемы LDAP:

1. На компьютере сервера безопасности, который будет использоваться в качестве мастера схемы, запустите консоль командной строки (cmd.exe) от имени администратора.
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 50002.
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. После присвоения роли мастера схемы завершите работу с утилитой с помощью команды quit.

## Документация

<b>1.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Принципы построения	RU.88338853.501400.001 91 1
<b>2.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Установка, обновление, удаление	RU.88338853.501400.001 91 2
<b>3.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация	RU.88338853.501400.001 91 3
<b>4.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Централизованное управление, мониторинг и аудит	RU.88338853.501400.001 91 4
<b>5.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Локальная защита	RU.88338853.501400.001 91 5
<b>6.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Сетевая защита	RU.88338853.501400.001 91 6
<b>7.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Антивирус и средство обнаружения вторжений	RU.88338853.501400.001 91 7
<b>8.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Шифрование сетевого трафика	RU.88338853.501400.001 91 8
<b>9.</b> Средство защиты информации Secret Net Studio. Руководство пользователя	RU.88338853.501400.001 92