Код Безопасности

Средство защиты информации

SECRET NET 7

Руководство администратора

Установка, обновление и удаление

RU.88338853.501410.015 91 2

Почтовый адрес:	**105318, Россия, Москва, а/я 101 ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

Список сокращений ... **5**

Введение ... **6**

Установка ... **7**

Состав устанавливаемых компонентов ... 7
Требования к аппаратному и программному обеспечению ... 7
Клиент ... 7
Компоненты для сетевого режима функционирования ... 8
Серийные номера, их назначение и особенности ... 10
Серийный номер клиента ... 10
Серийный номер подсистемы защиты дисков ... 10
Серийный номер разрешения терминальных подключений ... 10
Серийный номер сервера безопасности ... 10
Серийный номер программ управления ... 11
Установочный компакт-диск системы ... 11
Программа автозапуска ... 11
Установка клиента в автономном режиме функционирования ... 12
Порядок установки для сетевого режима функционирования ... 14
Установка с размещением хранилища объектов ЦУ вне Active Directory ... 14
Установка с размещением хранилища объектов ЦУ в БД Active Directory ... 15
Модификация схемы Active Directory ... 15
Установка сервера безопасности ... 16
Установка клиента в сетевом режиме функционирования ... 20
Установка программы оперативного управления ... 23

Обновление и переустановка ... **25**

Обновление ... 25
Обновление клиента в автономном режиме функционирования ... 25
Порядок обновления для сетевого режима функционирования ... 26
Обновление сервера безопасности ... 27
Обновление клиента в сетевом режиме функционирования ... 28
Обновление программы оперативного управления ... 30
Переустановка (восстановление) ... 30
Переустановка клиента ... 30
Переустановка сервера безопасности ... 31
Переустановка программы оперативного управления ... 33

Настройка системы для автоматической установки клиента ... **34**

Начальное формирование структуры ОУ ... 34
Создание общедоступного сетевого ресурса ... 34
Создание файлов со сценарием установки ... 35
Структура файла сценария ... 36
Пример содержимого файла сценария ... 39
Настройка Active Directory ... 39
Формирование организационных подразделений ... 39
Создание и настройка групповых политик ... 39

Удаление ... **42**

Удаление клиента в автономном режиме функционирования ... 42
Удаление драйвера средства аппаратной поддержки ... 42
Порядок удаления для сетевого режима функционирования ... 42
Удаление программы оперативного управления ... 43
Удаление клиента в сетевом режиме функционирования ... 43
Удаление драйвера средства аппаратной поддержки ... 43
Удаление сервера безопасности ... 44
Удаление средств поддержки клиентов предыдущих версий ... 44

Приложение ... **45**

Программа пакетной установки СУБД Oracle ... 45

Особенности программы пакетной установки ... 45
Подготовка к установке ... 45
Установка сервера Oracle ... 46
Проверка успешности установки ... 47
Сведения об установке и настройке СУБД MS SQL ... 48
Изменения в схеме AD при модификации ... 49
Расстановка прав доступа в ОС Windows XP ... 58
Права доступа на каталоги и файлы ... 58
Каталог установки клиента ... 59
Изменения в реестре при установке клиента ... 59
Изменения в IIS при установке сервера безопасности ... 60
Некоторые рекомендации по обеспечению безопасности в ИС ... 61
О восстановлении регистрации сервера безопасности ... 62
Локальное конфигурирование клиента для работы в структуре ОУ ... 63
Изменение учетных данных для подключения СБ к серверу СУБД ... 65
Резервное копирование хранилища объектов ЦУ, размещенного вне AD ... 66
Создание резервной копии ... 66
Восстановление из резервной копии ... 67
Варианты восстановления при некорректном удалении сервера безопасности 69
Удаление из Active Directory сведений о СБ с хранилищем объектов ЦУ в AD ... 69
Перенос роли мастера схемы LDAP на другой сервер безопасности ... 69
Терминологический справочник ... **71**
Документация ... **72**

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
XML	Extensible Markup Language
БД	База данных
ИС	Информационная система
КЦ	Контроль целостности
НСД	Несанкционированный доступ
ОС	Операционная система
ОСР	Общедоступный сетевой ресурс
ОУ	Оперативное управление
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СБ	Сервер безопасности
СНД	Серийный номер подсистемы защиты дисков
СНК	Серийный номер клиента
СНСб	Серийный номер сервера безопасности
СНТ	Серийный номер разрешения терминальных подключений
СНУ	Серийный номер средств управления
СУБД	Система управления базами данных
ЦУ	Централизованное управление
ЭИ	Электронный идентификатор

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net 7" RU.88338853.501410.015 (далее — система Secret Net, система защиты). В нем содержатся сведения, необходимые администраторам для установки системы защиты, ее обновления, исправления и удаления.

Перед изучением данного руководства необходимо ознакомиться с общими сведениями о системе Secret Net, 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. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://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 на курсах Учебного центра "Информзащита". Перечень курсов и условия обучения представлены на сайте http://www.itsecurity.ru/. Связаться с представителем Учебного центра можно по электронной почте (edu@itsecurity.ru).

Глава 1
Установка

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

Состав устанавливаемых компонентов

Система Secret Net состоит из следующих отдельно устанавливаемых программных средств:

1. Компонент "Secret Net 7" (далее — клиент).
2. Компонент "Модификатор схемы Active Directory" (далее — модификатор AD). Используется только в сетевом режиме функционирования. Применяется в случае использования Active Directory для размещения и хранения сведений об объектах централизованного управления.
3. Компонент "Secret Net 7 — Сервер безопасности" (далее — сервер безопасности или СБ). Используется только в сетевом режиме функционирования.
4. Компонент "Secret Net 7 — Программа управления" (далее — программа оперативного управления). Используется только в сетевом режиме функционирования.

Требования к аппаратному и программному обеспечению

Клиент

Компонент "Secret Net 7" устанавливается на компьютеры, работающие под управлением следующих ОС (поддерживаются 32- и 64-разрядные версии ОС с установленными пакетами обновлений не ниже указанных):

- Windows 8/8.1;
- Windows 7 SP1;
- Windows Vista SP2;
- Windows XP Professional SP3/XP Professional x64 Edition SP2;
- Windows Server 2012/Server 2012 R2;
- Windows Server 2008 SP2/Server 2008 R2 SP1;
- Windows Server 2003 SP2/Server 2003 R2 SP2.

На компьютере должен быть установлен обозреватель Internet Explorer версии 6 или выше. Установка других вспомогательных программ и обновлений выполняется автоматически в процессе установки компонента "Secret Net 7" (после установки дополнительного ПО может потребоваться перезагрузка компьютера).

Минимальные и рекомендуемые аппаратные требования, предъявляемые к компьютеру, аналогичны системным требованиям для соответствующей ОС.

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

Если на компьютере будет использоваться средство аппаратной поддержки (например, программно- аппаратный комплекс "Соболь" или изделие Secret Net Card), рекомендуется подготовить устройство (подключить плату изделия, считыватель, установить ПО) до начала установки Secret Net.

Компоненты для сетевого режима функционирования

Модификатор AD

Для применения компонента "Модификатор схемы Active Directory" компьютер, с которого выполняется модификация схемы, должен быть подключен к сети для установки соединения с контроллером домена. Других специальных требований к программной и аппаратной конфигурации компьютера не предъявляется.

Сервер безопасности

Компонент "Secret Net 7 — Сервер безопасности" устанавливается на компьютеры, работающие под управлением следующих ОС (поддерживаются 32- и 64-разрядные версии ОС с установленными пакетами обновлений не ниже указанных):

- Windows Server 2012/Server 2012 R2;
- Windows Server 2008 SP2/Server 2008 R2 SP1;
- Windows Server 2003 SP2/Server 2003 R2 SP2.

Требования к аппаратной конфигурации компьютера:

Элемент	Минимально	Рекомендуется
Оперативная память	4 ГБ	8 ГБ
Жесткий диск (свободное пространство)	10 ГБ	50 ГБ
Высокопроизводительный жесткий диск (свободное пространство)	100 ГБ	100 ГБ

Для установки сервера безопасности на компьютере под управлением ОС Windows Server 2003 необходимо установить ПО IIS 6.0 (на других ОС установка IIS осуществляется автоматически программой установки сервера безопасности).

Для функционирования компонента требуется наличие системы управления базами данных, реализуемой сервером СУБД Oracle или 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):

- Oracle9i 9.2.0.4e и выше до версии Oracle 11 включительно, в том числе свободно распространяемый вариант Oracle Database 10g Express Edition (установку СУБД Oracle Database 10g Express Edition рекомендуется выполнять с помощью специальной программы пакетной установки, которая автоматически устанавливает компоненты в нужной конфигурации — см. стр.**45**);

  Примечание.
  Корректное взаимодействие сервера безопасности и СУБД Oracle обеспечивается при выполнении следующих условий на компьютере сервера Oracle:
  - включен режим поддержки русского языка для экземпляра базы данных. В варианте Oracle Database 10g Express Edition поддержка русского языка включена по умолчанию, если СУБД установлена с помощью программы пакетной установки;
  - если сервер Oracle установлен на отдельном компьютере — в брандмауэре (если он включен) разрешено использование порта для соединения с СУБД (по умолчанию 1521). При этом на сервере Oracle порт должен быть открыт на входящие соединения, а на сервере безопасности — на исходящие.

- Microsoft SQL Server 2012 SP1, в том числе свободно распространяемый вариант SQL Server 2012 Express (установку СУБД MS SQL Server 2012 SP1 Express в русской редакции можно выполнить с установочного компакт-диска комплекта поставки — см. стр.**48**);

- Microsoft SQL Server 2008 R2 SP1, в том числе свободно распространяемый вариант SQL Server 2008 R2 Express.

Примечание.
Корректное взаимодействие сервера безопасности и СУБД MS SQL обеспечивается при выполнении условий, изложенных в Приложении на стр. 48.

Перед установкой сервера безопасности на компьютере необходимо включить режим "Доверять компьютеру делегирование". Данный режим обеспечивает возможность выполнения служебных запросов сервера к серверам Active Directory от имени пользователя, запустившего программу оперативного управления (администратора безопасности). Включение режима осуществляется в оснастке "Active Directory — пользователи и компьютеры" в диалоговом окне настройки свойств компьютера (по умолчанию режим делегирования отключен).

Если сервер безопасности устанавливается с размещением хранилища объектов централизованного управления вне Active Directory, к компьютеру предъявляются следующие требования:

- на компьютере должны быть свободны (не заняты другими приложениями) TCP-порты 50000–50003;
- перед установкой необходимо отключить на компьютере механизм управления учетными записями (User Account Control — UAC). Данный механизм включен по умолчанию в ОС Windows Server 2008 и выше. После установки ПО механизм можно снова включить.

Программа установки компонента автоматически проверяет и при необходимости устанавливает следующие обновления:

- на компьютере с 32-разрядной версией ОС: Windows Installer 3.1, C/C++ Runtime для платформы x86;
- на компьютере с 64-разрядной версией ОС: C/C++ Runtime для платформ x86 и x64;
- компоненты клиентской части Oracle.

После установки обновлений может потребоваться перезагрузка компьютера.

Программа оперативного управления

Компонент "Secret Net 7 — Программа управления" устанавливается на компьютеры, работающие под управлением следующих ОС (поддерживаются 32- и 64-разрядные версии ОС с установленными пакетами обновлений не ниже указанных):

- Windows 8/8.1;
- Windows 7 SP1;
- Windows Vista SP2;
- Windows XP Professional SP3/XP Professional x64 Edition SP2;
- Windows Server 2012/Server 2012 R2;
- Windows Server 2008 SP2/Server 2008 R2 SP1;
- Windows Server 2003 SP2/Server 2003 R2 SP2.

Требования к аппаратной конфигурации компьютера:

Элемент	Минимально	Рекомендуется
Оперативная память	1 ГБ	2 ГБ
Жесткий диск (свободное пространство)	500 МБ	2 ГБ

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

- Internet Explorer версии 6 или выше;
- компонент "Secret Net 7" в сетевом режиме функционирования.

Программа установки компонента автоматически проверяет и при необходимости устанавливает следующее обновление:

- .NET Framework 3.5 SP1.

Серийные номера, их назначение и особенности

Для эксплуатации системы Secret Net необходимо приобрести и зарегистрировать лицензии на использование компонентов. Лицензии регистрируются посредством ввода серийных номеров при установке компонентов или в процессе эксплуатации системы.

Для лицензирования применяются следующие типы серийных номеров:

- серийный номер клиента (СНК);
- серийный номер подсистемы защиты дисков (СНД);
- серийный номер разрешения терминальных подключений (СНТ);
- серийный номер сервера безопасности (СНСб);
- серийный номер средств управления (СНУ).

Регистрация соответствующего СНК является обязательным условием при установке компонента "Secret Net 7".

Серийный номер клиента

СНК содержит лицензию на использование компонента "Secret Net 7" определенной версии (версий). Лицензия может быть бессрочной или с ограниченным сроком действия (демонстрационная). При регистрации серийного номера с демонстрационной лицензией возможность использования компонента ограничивается сроком действия лицензии. По окончании этого срока защитные функции принудительно отключаются и пользователю выводятся соответствующие сообщения. Для дальнейшего использования компонента необходимо ввести серийный номер с бессрочной лицензией или новый демонстрационный номер (описание процедуры ввода серийного номера см. в документах [**3**] и [**4**]).

СНК определяет разрешенный режим функционирования компонента — сетевой или автономный. Для сетевого режима функционирования дополнительно устанавливается ограничение на количество клиентов, для которых можно использовать данный серийный номер.

Серийный номер подсистемы защиты дисков

Серийный номер подсистемы защиты дисков содержит лицензию на использование механизма защиты дисков в составе программного обеспечения компонента "Secret Net 7". Лицензия относится к определенной версии (версиям) ПО.

В сетевом режиме функционирования лицензия дополнительно определяет ограничение на максимальное количество компьютеров, на которых может использоваться механизм.

Серийный номер разрешения терминальных подключений

Серийный номер разрешения терминальных подключений содержит лицензию на использование терминального доступа к компьютеру. Наличие серийного номера обеспечивает возможность определенного количества терминальных подключений с других компьютеров, на которых не установлено клиентское ПО системы Secret Net. Лицензия относится к определенной версии (версиям) компонента "Secret Net 7" и может использоваться только для одного компьютера в рамках глобального каталога.

Серийный номер сервера безопасности

СНСб содержит лицензию на использование компонента "Secret Net 7 — Сервер безопасности" определенной версии (версий). Лицензия может быть бессрочной или с ограниченным сроком действия (демонстрационная). При регистрации серийного номера с демонстрационной лицензией возможность использования компонента ограничивается сроком действия лицензии. По окончании этого

срока сервер не допускает подключение рабочих станций, а при подключении программ управления выводятся предупреждающие сообщения. Для дальнейшего использования компонента необходимо ввести серийный номер с бессрочной лицензией или новый демонстрационный номер (описание процедуры ввода серийного номера см. в документе [**4**]).

Лицензия дополнительно определяет ограничение на количество одновременно подключенных клиентов к серверу безопасности. То есть сколько клиентов из числа подчиненных серверу безопасности могут открывать сессии доступа к серверу.

Серийный номер программ управления

СНУ содержит лицензию на использование дополнительных подключений компонентов "Secret Net 7 — Программа управления" к серверу безопасности (без СНУ допускается одно подключение). В лицензии заданы ограничения на количество дополнительных компьютеров, с которых возможно одновременное подключение программ оперативного управления к СБ.

Примечание.
При поочередном использовании на разных компьютерах программ оперативного управления СНУ не требуется.

Версия ПО программы оперативного управления, заданная в СНУ, должна быть не выше версии ПО сервера безопасности — в противном случае СНУ считается недействительным.

Установочный компакт-диск системы

Программное обеспечение и эксплуатационная документация системы Secret Net поставляются на установочном компакт-диске. Общая структура каталогов диска представлена в следующей таблице:

Каталог	Содержимое
\Setup\AD\	Программа модификации схемы Active Directory
\Setup\Server\	Дистрибутивы сервера безопасности
\Setup\Console\	Дистрибутивы программы оперативного управления
\Setup\MigrationTools\	Дистрибутивы средств поддержки клиентов предыдущих версий
\Setup\Client\	Дистрибутивы клиента
\Setup\SnTmCard\	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 дисков CD-ROM происходит автоматический запуск программы (далее — программа автозапуска), которая позволяет выполнять следующие действия:

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

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

В окне программы автозапуска представлены команды для выполнения действий. Назначение команд описано в следующей таблице:

Команда	Назначение
Модификатор схемы AD	Запускает программу модификации схемы Active Directory
Клиентское ПО	Запускает программу установки клиента
Сервер безопасности	Запускает программу установки сервера безопасности
Средства управления	Запускает программу установки программы оперативного управления
Дополнительное ПО	Открывает в отдельном окне каталог \Tools\
Документация	Открывает в отдельном окне каталог \Documentation\
Обзор диска	Открывает в отдельном окне корневой каталог диска

Для выполнения нужного действия выберите соответствующую команду. Некоторые команды запуска могут быть заблокированы 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.

Установка клиента в автономном режиме функционирования

Установку клиента в автономном режиме функционирования выполняет администратор безопасности, который должен входить в локальную группу администраторов компьютера.

Для установки клиента в автономном режиме функционирования:

1. Вставьте в привод установочный компакт-диск системы Secret Net. Дождитесь появления окна программы автозапуска (см. выше) и запустите установку с помощью команды "Клиентское ПО".

   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 компакт-диска файл \Setup\Client\x64\Setup.exe;
   - при установке на компьютер с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\Win32\Setup.exe.

   Программа установки начнет выполнение подготовительных действий. Перед началом процедуры установки на экране появится диалог для выбора режима работы компонента.
2. Установите отметку в поле "Автономный режим" и затем нажмите кнопку "Далее >".

   По окончании подготовительных действий на экран будет выведен диалог приветствия программы установки.
3. Для продолжения установки нажмите кнопку "Далее >".

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

   На экране появится диалог "Серийный номер".
5. Введите серийный номер клиента с лицензией на использование компонента "Secret Net 7" в автономном режиме функционирования.

   Пояснение.
   Без ввода серийного номера клиента установка невозможна.
6. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог "Защита жесткого диска".

7. Если на данном компьютере будет использоваться механизм защиты дисков, установите отметку в поле "установить защиту жесткого диска" и введите серийный номер лицензии на использование механизма.
8. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог "Серийный номер терминального доступа".
9. Если данный компьютер будет использоваться в качестве терминального сервера для подключений с других компьютеров без установленного клиентского ПО системы Secret Net, введите серийный номер лицензии на разрешение терминальных подключений. В противном случае оставьте пустым поле ввода серийного номера.
10. Для продолжения установки нажмите кнопку "Далее >".

    На экране появится диалог "Папка назначения".
11. Оставьте заданную по умолчанию папку установки ПО или укажите другую папку назначения и нажмите кнопку "Далее >".

    На экране появится диалог "Учетная информация компьютера".
12. Заполните поля диалога учетными данными и нажмите кнопку "Далее >".

    При установке на ОС Windows XP на экране появится диалог "Дополнительные параметры". Если выполняется установка на другой ОС, на экране появится диалог "Готова к установке программы" — в этом случае перейдите к действию **15**.
13. При установке на ОС Windows XP определите необходимость замены установленных по умолчанию прав доступа пользователей к основным ресурсам компьютера. Если требуется заменить права доступа пользователей, оставьте отмеченным поле "выполнить расстановку прав доступа на файлы, каталоги и ключи реестра".

    Пояснения:
    - Замена прав доступа усиливает защищенность операционной системы, однако выполнять ее рекомендуется только в тех случаях, когда после установки ОС администратор не осуществлял специальную расстановку прав доступа. Перечень устанавливаемых прав доступа для соответствующих ОС см. в приложении на стр.58.
    - Права доступа на каталог установки системы Secret Net устанавливаются для любой ОС в обязательном порядке независимо от выбранного режима расстановки прав. Перечень устанавливаемых прав доступа к каталогу установки см. в приложении на стр.59.
14. Для продолжения установки нажмите кнопку "Далее >".

    На экране появится диалог "Готова к установке программы".
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.

    Примечание.
    В процессе установки ПО на экране могут появляться различные запросы системы. Например, в следующих случаях:
    - Если на компьютере установлен брандмауэр, который отслеживает сетевую активность приложений, при первом запуске некоторых подсистем Secret Net может появиться запрос о разрешении сетевых вызовов. Чтобы обеспечить нормальную работу подсистем в дальнейшем, необходимо в таких запросах выбирать вариант разрешения работы соответствующим службам по умолчанию (без подтверждения). Данная рекомендация относится и к случаям, когда брандмауэр начинает функционировать после установки Secret Net.

    Перед завершением установки требуется выполнить окончательную настройку ПО. Действия для окончательной настройки выполняются в диалоговом окне "Управление Secret Net 7", процедуры работы с которым описаны в документе [**3**]. На этапе установки достаточно закрыть диалоговое окно, не внося никаких изменений.
16. После окончательной настройки перезагрузите компьютер.

Внимание!
Дождитесь окончания перезагрузки компьютера. Необходимо иметь в виду, что при первой загрузке текущая аппаратная конфигурация компьютера автоматически принимается в качестве эталонной. Поэтому до начала загрузки проверьте, какие аппаратные устройства подключены к компьютеру, и отключите те устройства, которые должны быть запрещены к использованию.

Порядок установки для сетевого режима функционирования

Установка с размещением хранилища объектов ЦУ вне Active Directory

Если хранилище объектов централизованного управления Secret Net необходимо разместить в отдельной базе данных вне Active Directory, установку следует выполнять в следующем порядке:

1. Если домены безопасности будут формироваться на базе организационных подразделений, подготовьте организационные подразделения и включите в них нужные компьютеры.
2. Создайте группы пользователей, которые будут указаны в качестве групп администраторов леса доменов безопасности при создании лесов доменов безопасности. 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.
4. Для групп администраторов доменов безопасности делегируйте права на управление групповыми политиками. Делегирование обеспечивается назначением следующих прав:
   - для создания новых объектов групповой политики (если требуется) включите группу администраторов домена безопасности в группу Group Policy Creator Owners;
   - для управления ссылками групповой политики делегируйте права CommonTask — Manage Group Policy Links;
   - для редактирования существующей политики предоставьте пользователю разрешения безопасности (Security Permissions) на конкретную политику в оснастке Users and Computers (ОС Windows Server 2003) или Group Policy Management (ОС Windows Server 2012/2008).

   Примечание.
   Данное действие можно пропустить в случае, если настройка параметров Secret Net групповых политик будет осуществляться в программе оперативного управления системы Secret Net (без использования стандартных оснасток управления групповыми политиками ОС Windows).
5. От имени пользователя с правами на изменение конфигурации каталога Active Directory выполните регистрацию конфигурационных данных в разделе конфигурации каталога AD. Регистрация выполняется с помощью командного файла sn7-modify-AD.cmd, который размещается в каталоге \Tools\Infosec\ModifyAD\ на установочном компакт-диске системы Secret Net. По умолчанию права на изменение конфигурации каталога AD предоставлены пользователям группы "Администраторы предприятия" (Enterprise Admins).

   Примечание.
   Данное действие можно пропустить в следующих случаях:
   - если настройка параметров пользователей будет осуществляться в программе управления пользователями из состава ПО клиента системы Secret Net (без использования стандартной оснастки "Active Directory — пользователи и компьютеры");
   - если установку сервера безопасности будет выполнять пользователь с правами на изменение конфигурации каталога AD.

6. На компьютерах, которые будут использоваться в качестве серверов безопасности, 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. При установке необходимо выбирать вариант размещения хранилища объектов централизованного управления "вне Active Directory";
   - установите ПО клиента системы Secret Net с подчинением данному серверу безопасности.
7. На рабочих местах администраторов Secret Net установите:
   - ПО клиента системы Secret Net;
   - средства централизованного управления ОС Windows (при необходимости);
   - программу оперативного управления.
8. Установите ПО клиента системы Secret Net на серверы и контроллеры домена, затем на компьютеры сотрудников.

Совет.
При большом количестве компьютеров целесообразно применить автоматическую установку клиента. Описание настройки системы для автоматической установки см. на стр.34.

Установка с размещением хранилища объектов ЦУ в БД Active Directory

В случае размещения хранилища объектов централизованного управления Secret Net в базе данных доменных служб Active Directory установку следует выполнять в следующем порядке:

1. Включите все контроллеры домена.
2. Выполните модификацию схемы AD (см. ниже) и дождитесь репликации схемы на все контроллеры домена.
3. На компьютерах, которые будут использоваться в качестве серверов безопасности, выполните следующие действия:
   - установите ПО сервера безопасности. При установке необходимо выбирать вариант размещения хранилища объектов централизованного управления "в Active Directory";
   - установите ПО клиента системы Secret Net с подчинением данному серверу безопасности.
4. На рабочих местах администраторов Secret Net установите:
   - ПО клиента системы Secret Net;
   - средства централизованного управления ОС Windows (при необходимости);
   - программу оперативного управления.
5. Установите ПО клиента системы Secret Net на серверы и контроллеры домена, затем на компьютеры сотрудников.

Совет.
При большом количестве компьютеров целесообразно применить автоматическую установку клиента. Описание настройки системы для автоматической установки см. на стр.34.

Модификация схемы Active Directory

Модификацию схемы Active Directory должен выполнять пользователь, которому предоставлены права на изменение конфигурации каталога AD и права для модификации схемы AD. По умолчанию такие права предоставлены пользователям,

включенным, соответственно, в группы "Администраторы предприятия" (Enterprise Admins) и "Администраторы схемы" (Schema Admins). Модификацию AD можно проводить с любого компьютера домена Active Directory (леса доменов).

Подробные сведения об изменениях в AD при модификации схемы см. в приложении на стр.**49**.

Для модификации схемы AD

1. Вставьте в привод установочный компакт-диск системы Secret Net. Дождитесь появления окна программы автозапуска (см. стр.**11**) и выберите команду "Модификатор схемы AD" (или запустите с установочного компакт-диска файл \Setup\AD\SnADMS.exe).

   На экране появится диалог "Модификатор схемы Active Directory". Программа автоматически определит контроллер домена, являющийся мастером схемы AD, и на фоне диалога появится сообщение: "Поиск мастера схемы Active Directory успешно завершен".
2. Нажмите кнопку "OK".
3. В диалоге "Модификатор схемы Active Directory" заполните поля "Пользователь" и "Пароль" учетными данными пользователя, обладающего необходимыми правами.

   Совет.
   Если вход на компьютер выполнен с учетными данными пользователя, которому предоставлены права на изменение конфигурации каталога AD и права для модификации схемы AD, поля "Пользователь" и "Пароль" можно не заполнять.
4. Для запуска процесса модификации AD нажмите кнопку "Применить".

   На экране появится запрос для подтверждения операции.
5. Для начала процесса модификации нажмите кнопку "Да".

   Начнется процесс модификации AD, по окончании которого на экране появится сообщение: "Модификация схемы Active Directory успешно завершена".
6. Нажмите кнопку "OK" и закройте диалог "Модификатор схемы Active Directory".

Установка сервера безопасности

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

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

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 в варианте размещения хранилища объектов централизованного управления вне Active Directory нельзя переименовывать компьютер сервера. Иначе после переименования сервер будет неработоспособен и недоступен для связи с другими компонентами системы Secret Net.

Для установки сервера безопасности:

1. Вставьте в привод установочный компакт-диск системы Secret Net. Дождитесь появления окна программы автозапуска (см. стр.**11**) и запустите установку с помощью команды "Сервер безопасности".

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 компакт-диска файл \Setup\Server\x64\Setup.exe;
- при установке на компьютер с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Server\Win32\Setup.exe.

Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен 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 "Хранилище объектов централизованного управления".

4. Выберите нужный вариант размещения хранилища объектов централизованного управления для сервера безопасности:
- если сервер безопасности будет использовать базу данных альтернативной службы каталогов (не Active Directory) — установите отметку в поле "вне Active Directory";
- если хранилище объектов централизованного управления будет размещаться в БД доменных служб Active Directory — установите отметку в поле "в Active Directory".

5. Для продолжения установки нажмите кнопку "Далее >".

Если был выбран вариант размещения хранилища объектов централизованного управления вне Active Directory, на экране появится диалог "Включение сервера в домен безопасности". При выборе варианта размещения хранилища в AD на экране появится диалог "Родительский сервер" или "Серийные номера".

Примечание.
Диалог "Родительский сервер" не появится на данном этапе, если устанавливается первый сервер в лесу доменов безопасности или лесу AD.

При появлении диалога "Родительский сервер" — перейдите к действию **15**. Если подчинение сервера невозможно, на экране появится диалог "Серийные номера" — в этом случае перейдите к действию **16**.

6. В диалоге "Включение сервера в домен безопасности" выберите нужный вариант включения сервера безопасности в домен безопасности:
- если домен безопасности должен быть сформирован в новом лесу доменов безопасности — установите отметку в поле "создать новый домен в новом лесу доменов безопасности". Данный вариант необходимо выбрать при установке первого сервера безопасности с размещением хранилища объектов централизованного управления вне Active Directory, а также в случаях, когда создается новый лес доменов безопасности;
- если домен безопасности должен быть сформирован в имеющемся лесу доменов безопасности — установите отметку в поле "создать новый домен в существующем лесу доменов безопасности";
- если сервер безопасности должен быть включен в состав имеющегося домена безопасности — установите отметку в поле "добавить сервер в существующий домен безопасности".

7. Для продолжения установки нажмите кнопку "Далее >".

Если был выбран вариант формирования домена в новом лесу доменов безопасности, на экране появится диалог "Контейнер Active Directory". При выборе другого варианта на экране появится диалог "Родительский сервер" — в этом случае перейдите к действию **10**.

8. В диалоге "Контейнер Active Directory" 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 нажмите кнопку "Далее >".

   На экране появится диалог "Группы администраторов домена безопасности".

9. В диалоге "Группы администраторов домена безопасности" 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 оперативного 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. Данная возможность доступна при размещении хранилища объектов ЦУ вне Active Directory (сведения о порядке установки см. на стр. 14).

   На экране появится диалог "Серийные номера". Перейдите к действию **16**.

10. В диалоге "Родительский сервер" 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 оперативного управления.

11. Нажмите кнопку "Далее >".

    Если при выполнении действия **6** был выбран вариант формирования домена в имеющемся лесу доменов безопасности, на экране появится диалог "Контейнер Active Directory". При выборе варианта включения сервера безопасности в состав имеющегося домена безопасности на экране появится диалог "Домен безопасности" — в этом случае перейдите к действию **14**.

12. В диалоге "Контейнер Active Directory" 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 нажмите кнопку "Далее >".

    На экране появится диалог "Группы администраторов домена безопасности".

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

    На экране появится диалог "Серийные номера". Перейдите к действию **16**.

14. В диалоге "Домен безопасности" 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 "Серийные номера". Перейдите к действию **16**.

15. В диалоге "Родительский сервер" выполните следующие действия:

- Определите подчиненность устанавливаемого сервера безопасности:
  - если не требуется подчинять сервер безопасности другим серверам — выберите пункт "не подчинять этот сервер другому серверу безопасности";
  - если требуется установить подчиненность устанавливаемого сервера безопасности — выберите пункт "подчинить этот сервер другому серверу безопасности и настроить параметры подключения" и в раскрывающихся списках выберите имя компьютера, который будет являться родительским сервером безопасности, и 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 оперативного управления.

- Нажмите кнопку "Далее >".

На экране появится диалог "Серийные номера".

16. В диалоге "Серийные номера" введите серийные номера сервера безопасности (СНСб), клиента (СНК), механизма защиты дисков (СНД) и средств управления (СНУ) и нажмите кнопку "Далее >".

Пояснения:
- СНК, СНД и СНУ на установку сервера безопасности не влияют — их можно добавить позже при установке других компонентов системы Secret Net или в программе оперативного управления (см. документ [**4**]). При установке сервера безопасности можно зарегистрировать один или несколько СНК и СНД, что позволит в дальнейшем автоматически регистрировать эти номера на клиентах, подчиняемых данному СБ. СНУ вводится, если к данному серверу безопасности планируется подключение программ оперативного управления с нескольких рабочих мест одновременно.
- Если при выполнении действия **4** был выбран вариант размещения хранилища объектов централизованного управления в Active Directory, дополнительно можно установить средства поддержки клиентов системы Secret Net предыдущих версий (6.X, 5.X). Для этого установите отметку в поле "Установить средства поддержки клиентов прежних версий". Запуск программы установки средств поддержки будет выполнен на завершающем этапе установки ПО сервера безопасности. При наличии на компьютере установленных средств будет возможно подчинение клиентов предыдущих версий серверу безопасности текущей версии. Если в системе не планируется использование клиентов предыдущих версий, удалите отметку из поля.

На экране появится диалог "Папка назначения".

17. Оставьте заданную по умолчанию папку установки сервера безопасности или укажите другую папку назначения и нажмите кнопку "Далее >".

На экране появится диалог "Настройки СУБД".

18. Отметьте тип СУБД для совместной работы с сервером безопасности (Oracle или MS SQL) и 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.
    Формат записи различается в зависимости от типа СУБД. Если используется СУБД Oracle, введите строку в следующем формате:
    <имя_или_IP-адрес_сервера_Oracle>:*<порт>*/*<имя_экземпляра_БД>*
    Если используется СУБД MS SQL, введите:
    *<имя_или_IP-адрес_сервера_MS_SQL>**<имя_экземпляра_БД>*,*<порт>*

    Примечание.
    Порт можно не указывать, если используется номер по умолчанию (для СУБД Oracle порт по умолчанию 1521, для СУБД MS SQL — 1433).

- в группе полей "Учетная запись администратора БД" — учетные данные администратора базы данных на сервере СУБД;

  Примечание.
  Если используется СУБД Oracle, в качестве администратора БД необходимо указывать учетные данные пользователя с привилегией SYSDBA (по умолчанию такой привилегией обладает пользователь sys, который является встроенным администратором СУБД Oracle).

- 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).

- Оставьте заданный по умолчанию или укажите другой каталог для размещения резервных копий журналов.
- Нажмите кнопку "Далее >".

19. Если база данных уже существует, 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 >".

При успешном соединении с БД на экране появится диалог "Настройки ISAPI-расширения".

20. Оставьте заданный по умолчанию или укажите другой каталог для хранения временных файлов и нажмите кнопку "Далее >".

На экране появится диалог "Название организации".

21. 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 "Готова к установке программы".

22. 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.

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

23. Нажмите кнопку "Готово" и перезагрузите компьютер.

Внимание!
Объект нового сервера безопасности может появиться в структуре оперативного управления с некоторой задержкой. В программе оперативного 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).

Установка клиента в сетевом режиме функционирования

Установка клиента в сетевом режиме функционирования выполняется пользователем, входящим в локальную группу администраторов компьютера.

Для выполнения некоторых действий при установке клиента могут потребоваться особые права доступа. Например, права на администрирование домена безопасности. Если пользователь, выполняющий установку, не обладает

нужными правами, программа установки на определенных этапах может запрашивать учетные данные пользователей с правами доступа.

Для установки клиента в сетевом режиме функционирования:

1. Вставьте в привод установочный компакт-диск системы Secret Net. Дождитесь появления окна программы автозапуска (см. стр.**11**) и запустите установку с помощью команды "Клиентское ПО".

   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 компакт-диска файл \Setup\Client\x64\Setup.exe;
   - при установке на компьютер с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\Win32\Setup.exe.

   Программа установки начнет выполнение подготовительных действий. Перед началом процедуры установки на экране появится диалог для выбора режима работы компонента.

2. Установите отметку в поле "Сетевой режим" и нажмите кнопку "Далее >".

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

3. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог принятия лицензионного соглашения.

4. Ознакомьтесь с содержанием лицензионного соглашения, отметьте соответствующий принятию соглашения пункт и нажмите кнопку "Далее >".

   На экране появится диалог "Настройка подключения к серверу безопасности".

5. Выберите вариант продолжения процедуры (при наличии в домене хотя бы одного сервера безопасности):
   - с подключением к серверу безопасности — отметьте пункт "связать этот компьютер с сервером и настроить параметры подключения" и заполните поля данными, необходимыми для установления связи данного компьютера с сервером безопасности:
     - в поле "Имя сервера" из раскрывающегося списка выберите имя компьютера, на котором установлен нужный сервер безопасности;
     - в поле "Скорость подключения" из раскрывающегося списка выберите название шаблона сетевых настроек, который соответствует скоростным параметрам используемой сети;

     Примечание.
     При установке клиента с подключением к серверу безопасности программа установки дополнительно может выдать запрос на использование лицензии продукта. Если на сервере безопасности зарегистрирован подходящий СНК с доступными для использования лицензиями, можно выбрать вариант использования зарегистрированной лицензии либо ввести другой СНК вручную.

   - без подключения к серверу безопасности — отметьте пункт "не связывать этот компьютер с сервером". При такой установке подключить компьютер к серверу безопасности можно позже с помощью программы оперативного управления (см. документ [**4**]) или с помощью программы для локального конфигурирования клиента (см. стр.**63**).

   Примечание.
   Поля диалога заблокированы для редактирования, если в домене отсутствует компьютер с установленным ПО сервера безопасности.

6. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог "Серийный номер".

7. Введите серийный номер клиента.

Пояснения:
- Без ввода СНК установка клиента невозможна.
- Если на шаге **5** выбран сервер безопасности, поле ввода будет автоматически заполнено серийным номером, для которого есть свободные лицензии на данном сервере.

8. При установке клиента на компьютер, который будет использоваться администратором для централизованной настройки параметров механизмов КЦ и ЗПС, а также параметров доменных пользователей, оставьте отмеченным поле "установить средства централизованного управления". Если на компьютере будут работать только рядовые пользователи — удалите отметку из поля.

9. Для продолжения установки нажмите кнопку "Далее >".

На экране появится диалог "Защита жесткого диска".

10. Если на данном компьютере будет использоваться механизм защиты дисков, установите отметку в поле "установить защиту жесткого диска" и введите серийный номер лицензии на использование механизма.

Пояснение:
- Если на шаге **5** выбран сервер безопасности, поле ввода будет автоматически заполнено серийным номером, для которого есть свободные лицензии на данном сервере.

11. Для продолжения установки нажмите кнопку "Далее >".

На экране появится диалог "Серийный номер терминального доступа".

12. Если данный компьютер будет использоваться в качестве терминального сервера для подключений с других компьютеров без установленного клиентского ПО системы Secret Net, введите серийный номер лицензии на разрешение терминальных подключений. В противном случае оставьте пустым поле ввода серийного номера.

13. Для продолжения установки нажмите кнопку "Далее >".

На экране появится диалог "Папка назначения".

14. Оставьте заданную по умолчанию папку установки клиента или укажите другую папку назначения и нажмите кнопку "Далее >".

На экране появится диалог "Учетная информация компьютера".

15. Заполните поля диалога учетными данными и нажмите кнопку "Далее >".

При установке на ОС Windows XP на экране появится диалог "Дополнительные параметры". Если выполняется установка на другой ОС, на экране появится диалог "Готова к установке программы" — в этом случае пропустите действия **16–17**.

16. При установке на ОС Windows XP определите необходимость замены установленных по умолчанию прав доступа пользователей к основным ресурсам компьютера. Если требуется заменить права доступа пользователей, оставьте отмеченным поле "выполнить расстановку прав доступа на файлы, каталоги и ключи реестра".

Пояснения:
- Замена прав доступа усиливает защищенность операционной системы, однако выполнять ее рекомендуется только в тех случаях, когда после установки ОС администратор не осуществлял специальную расстановку прав доступа. Перечень устанавливаемых прав доступа для соответствующих ОС см. в приложении на стр. 58.
- Права доступа на каталог установки системы Secret Net устанавливаются для любой ОС в обязательном порядке независимо от выбранного режима расстановки прав. Перечень устанавливаемых прав доступа к каталогу установки см. в приложении на стр. 59.

17. Для продолжения установки нажмите кнопку "Далее >".

На экране появится диалог "Готова к установке программы".

18. 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.

Примечание.

В процессе установки ПО на экране могут появляться различные запросы системы. Например, в следующем случае:

- Если на компьютере установлен брандмауэр, который отслеживает сетевую активность приложений, при первом запуске некоторых подсистем Secret Net может появиться запрос о разрешении сетевых вызовов. Чтобы обеспечить нормальную работу подсистем в дальнейшем, необходимо в таких запросах выбирать вариант разрешения работы соответствующим службам по умолчанию (без подтверждения). Данная рекомендация относится и к случаям, когда брандмауэр начинает функционировать после установки Secret Net.

Перед завершением установки требуется выполнить окончательную настройку ПО. Действия для окончательной настройки выполняются в диалоговом окне "Управление Secret Net 7", процедуры работы с которым описаны в документе [**3**]. На этапе установки достаточно закрыть диалоговое окно, не внося никаких изменений.

19. После окончательной настройки перезагрузите компьютер.

Внимание!

Дождитесь окончания перезагрузки компьютера. Необходимо иметь в виду, что при первой загрузке текущая аппаратная конфигурация компьютера автоматически принимается в качестве эталонной. Поэтому до начала загрузки проверьте, какие аппаратные устройства подключены к компьютеру, и отключите те устройства, которые должны быть запрещены к использованию.

Установка программы оперативного управления

Установка программы оперативного управления выполняется пользователем, входящим в локальную группу администраторов компьютера.

Для установки программы оперативного управления:

1. Вставьте в привод установочный компакт-диск системы Secret Net. Дождитесь появления окна программы автозапуска (см. стр.**11**) и запустите установку с помощью команды "Средства управления".

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 компакт-диска файл \Setup\Console\x64\Setup.exe;
- при установке на компьютер с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Console\Win32\Setup.exe.

Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен 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 "Папка назначения".

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

На экране появится диалог "Готова к установке программы".

5. 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.

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

6. Нажмите кнопку "Готово" и перезагрузите компьютер.

Глава 2
Обновление и переустановка

Обновление

В системе Secret Net реализована возможность обновления программного обеспечения предыдущих версий на текущую версию. Обновление поддерживается для следующих компонентов:

- Клиент — с версии 5.0.180.4 и выше.
- Сервер безопасности — с версии 7.0 и выше.
- Программа оперативного управления — с версии 7.0 и выше.

При обновлении сохраняются заданные параметры настройки системы (для некоторых параметров могут быть выставлены значения по умолчанию, если сохранение прежних значений технически невозможно).

Для функционирования компонентов текущей версии системы Secret Net требуются соответствующие серийные номера лицензий. Поэтому для обновления необходимо приобрести нужное количество лицензий на использование компонентов текущей версии. Компоненты предыдущих версий могут продолжать функционировать в системе с ранее приобретенными лицензиями.

Обновление компонентов на компьютерах системы осуществляется по отдельности с помощью программ установки компонентов. Имеется возможность автоматического обновления клиента на компьютерах системы.

Обновление клиента в автономном режиме функционирования

Обновление клиента в автономном режиме функционирования выполняет администратор безопасности, который должен входить в локальную группу администраторов компьютера.

Предупреждение.
Если на компьютере имеются файлы, зашифрованные средствами системы Secret Net предыдущей версии, перед обновлением системы обязательно расшифруйте их. Иначе после обновления доступ к содержимому этих файлов будет невозможен.

Для обновления клиента в автономном режиме функционирования:

1. Вставьте в привод установочный компакт-диск системы Secret Net. Дождитесь появления окна программы автозапуска (см. стр.11) и запустите обновление с помощью команды "Клиентское ПО".

   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 компакт-диска файл \Setup\Client\x64\Setup.exe;
   - при установке на компьютер с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\Win32\Setup.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 "Далее >".

   На экране появится диалог "Серийный номер".

3. Введите серийный номер клиента для автономного режима функционирования и нажмите кнопку "Далее >".

Пояснение.
Без ввода СНК установка клиента невозможна.

На экране появится диалог "Защита жесткого диска".

4. Если на данном компьютере будет использоваться механизм защиты дисков, установите отметку в поле "установить защиту жесткого диска" и введите серийный номер лицензии на использование механизма.
5. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог "Серийный номер терминального доступа" (кроме случая обновления с версии 7.0 и выше).
6. Если данный компьютер будет использоваться в качестве терминального сервера для подключений с других компьютеров без установленного клиентского ПО системы Secret Net, введите серийный номер лицензии на разрешение терминальных подключений. В противном случае оставьте пустым поле ввода серийного номера.
7. Для продолжения установки нажмите кнопку "Далее >".

   Программа установки выполнит анализ установленных компонентов, после чего на экране появится диалог "Программа готова к обновлению".
8. Нажмите кнопку "Обновить".

   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.

Примечание.
В процессе установки ПО на экране могут появляться различные запросы системы. Например, в следующих случаях:

- Если не завершена работа программы автозапуска (см. действие **1**), в процессе обновления на экране может появиться диалог "Используются файлы", в котором сообщается о необходимости закрыть приложение. В этом случае завершите работу программы автозапуска, после чего нажмите кнопку "Повторить" в диалоге "Используются файлы".
- Если на компьютере установлен брандмауэр, который отслеживает сетевую активность приложений, при первом запуске некоторых подсистем Secret Net может появиться запрос о разрешении сетевых вызовов. Чтобы обеспечить нормальную работу подсистем в дальнейшем, необходимо в таких запросах выбирать вариант разрешения работы соответствующим службам по умолчанию (без подтверждения). Данная рекомендация относится и к случаям, когда брандмауэр начинает функционировать после установки Secret Net.

По окончании обновления появится диалог "Программа установки завершена".

9. Нажмите кнопку "Готово" и перезагрузите компьютер.

Внимание!
Дождитесь окончания перезагрузки компьютера. Необходимо иметь в виду, что при первой загрузке текущая аппаратная конфигурация компьютера автоматически принимается в качестве эталонной. Поэтому до начала загрузки проверьте, какие аппаратные устройства подключены к компьютеру, и отключите те устройства, которые должны быть запрещены к использованию.

Порядок обновления для сетевого режима функционирования

Обновление компонентов в сетевом режиме функционирования системы осуществляется в следующей последовательности:

1. Включите все контроллеры домена.
2. Выполните модификацию AD (см. стр.**16**) и дождитесь репликации схемы AD на все контроллеры домена.

Примечание.
Данное действие можно пропустить, если выполняется обновление с версии 7.0 и выше и при этом хранилище объектов централизованного управления Secret Net размещается вне AD.

3. Обновите ПО серверов безопасности на текущую версию (см. стр. 27). Если в системе была развернута иерархия серверов безопасности, обновление рекомендуется выполнить последовательно по иерархии, начиная с корневого сервера. При этом при обновлении ПО подчиненных серверов корневой сервер должен быть включен и доступен по сети.
4. Обновите ПО клиента (см. стр. 28) на серверах безопасности и рабочих местах администраторов.
5. Обновите программу оперативного управления (см. стр. 30) на рабочих местах администраторов.
6. Обновите ПО клиента (см. стр. 28) в порядке:
   - контроллеры домена;
   - компьютеры сотрудников.

Совет.
При большом количестве компьютеров целесообразно применить автоматическое обновление клиента. Описание настройки системы для автоматической установки см. на стр. 34.

7. В программе оперативного 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.

Для обновления сервера безопасности:

1. Вставьте в привод установочный компакт-диск системы Secret Net. Дождитесь появления окна программы автозапуска (см. стр. 11) и запустите обновление с помощью команды "Сервер безопасности".

   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 компакт-диска файл \Setup\Server\x64\Setup.exe;
   - при установке на компьютер с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Server\Win32\Setup.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. Для продолжения установки нажмите кнопку "Далее >".

   Если сервер безопасности предыдущей версии установлен в варианте размещения хранилища объектов централизованного управления вне Active Directory, на экране появится диалог "Учетные данные администратора безопасности". Для варианта размещения хранилища в AD на экране появится диалог "Серийные номера". При появлении диалога "Серийные номера" перейдите к действию **5**.

3. В диалоге "Учетные данные администратора безопасности" оставьте отмеченным поле "использовать учетные данные текущего пользователя", если пользователь, выполняющий установку, входит в группы администраторов леса доменов безопасности и администраторов домена безопасности. В противном случае установите отметку в поле "использовать следующие имена и пароли" и укажите нужные учетные данные в соответствующих полях.
4. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог "Серийные номера".
5. В диалоге "Серийные номера" введите серийные номера сервера безопасности (СНСб), клиента (СНК), механизма защиты дисков (СНД) и средств управления (СНУ) и нажмите кнопку "Далее >".

   Пояснения:
   - СНК, СНД и СНУ на установку сервера безопасности не влияют — их можно добавить позже при установке других компонентов системы Secret Net или в программе оперативного управления (см. документ [**4**]). При установке сервера безопасности можно зарегистрировать один или несколько СНК и СНД, что позволит в дальнейшем автоматически регистрировать эти номера на клиентах, подчиняемых данному СБ. СНУ вводится, если к данному серверу безопасности планируется подключение программ оперативного управления с нескольких рабочих мест одновременно.

   На экране появится диалог "Обновление БД".
6. В полях "Имя пользователя" и "Пароль" укажите учетные данные администратора базы данных на сервере СУБД и нажмите кнопку "Далее >".

   Примечание.
   Если используется СУБД Oracle, в качестве администратора БД необходимо указывать учетные данные пользователя с привилегией SYSDBA (по умолчанию такой привилегией обладает пользователь sys, который является встроенным администратором СУБД Oracle).

   На экране появится диалог "Программа готова к обновлению".
7. Нажмите кнопку "Обновить".

   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 компонентов на экране появится диалог "Программа установки завершена".
8. Нажмите кнопку "Готово" и перезагрузите компьютер.

Внимание!
Объект нового сервера безопасности может появиться в структуре оперативного управления с некоторой задержкой. В программе оперативного 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 клиента в сетевом режиме функционирования

Обновление клиента в сетевом режиме функционирования 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 пользователь, выполняющий установку, не обладает нужными правами, программа установки на определенных этапах может запрашивать учетные данные пользователей с правами доступа.

Предупреждение.
Если на компьютере имеются файлы, зашифрованные средствами системы Secret Net предыдущей версии, перед обновлением системы обязательно расшифруйте их. Иначе после обновления доступ к содержимому этих файлов будет невозможен.

Для обновления клиента в сетевом режиме функционирования:

1. Вставьте в привод установочный компакт-диск системы Secret Net. Дождитесь появления окна программы автозапуска (см. стр.**11**) и запустите обновление с помощью команды "Клиентское ПО".

   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 компакт-диска файл \Setup\Client\x64\Setup.exe;
   - при установке на компьютер с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\Win32\Setup.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 "Далее >".

   На экране появится диалог "Серийный номер".

3. Введите серийный номер клиента.

   Пояснение:
   - Без ввода СНК установка клиента невозможна.

4. При установке клиента на компьютер, который будет использоваться администратором для централизованной настройки параметров механизмов КЦ и ЗПС, а также параметров доменных пользователей, оставьте отмеченным поле "установить средства централизованного управления". Если на компьютере будут работать только рядовые пользователи — удалите отметку из поля.

5. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог "Защита жесткого диска".

6. Если на данном компьютере будет использоваться механизм защиты дисков, установите отметку в поле "установить защиту жесткого диска" и введите серийный номер лицензии на использование механизма.

7. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог "Серийный номер терминального доступа" (кроме случая обновления с версии 7.0 и выше).

8. Если данный компьютер будет использоваться в качестве терминального сервера для подключений с других компьютеров без установленного клиентского ПО системы Secret Net, введите серийный номер лицензии на разрешение терминальных подключений. В противном случае оставьте пустым поле ввода серийного номера.

9. Для продолжения установки нажмите кнопку "Далее >".

   Программа установки выполнит анализ установленных компонентов, после чего на экране появится диалог "Программа готова к обновлению".

10. Нажмите кнопку "Обновить".

    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.

Примечание.
В процессе установки ПО на экране могут появляться различные запросы системы. Например, в следующих случаях:

- Если не завершена работа программы автозапуска (см. действие **1**), в процессе обновления на экране может появиться диалог "Используются файлы", в котором сообщается о необходимости закрыть приложение. В этом случае завершите работу программы автозапуска, после чего нажмите кнопку "Повторить" в диалоге "Используются файлы".
- Если на компьютере установлен брандмауэр, который отслеживает сетевую активность приложений, при первом запуске некоторых подсистем Secret Net может появиться запрос о разрешении сетевых вызовов. Чтобы обеспечить нормальную работу подсистем в дальнейшем, необходимо в таких запросах выбирать вариант разрешения работы соответствующим службам по умолчанию (без подтверждения). Данная рекомендация относится и к случаям, когда брандмауэр начинает функционировать после установки Secret Net.

По окончании обновления появится диалог "Программа установки завершена".

11. Нажмите кнопку "Готово" и перезагрузите компьютер.

Внимание!
Дождитесь окончания перезагрузки компьютера. Необходимо иметь в виду, что при первой загрузке текущая аппаратная конфигурация компьютера автоматически принимается в качестве эталонной. Поэтому до начала загрузки проверьте, какие аппаратные устройства подключены к компьютеру, и отключите те устройства, которые должны быть запрещены к использованию.

Обновление программы оперативного управления

Обновление программы оперативного управления выполняется пользователем, входящим в локальную группу администраторов компьютера. Для запуска процедуры обновления компонента используйте установочный компакт-диск (см. стр.**23**). Процедура обновления выполняется без особенностей.

Переустановка (восстановление)

При необходимости можно осуществлять переустановку ПО компонентов системы Secret Net. Переустановка применяется для восстановления нарушенной работоспособности системы. Для переустановки следует использовать дистрибутив установленной на компьютере версии компонента.

Переустановка клиента

Переустановка клиента выполняется пользователем, входящим в локальную группу администраторов компьютера.

При переустановке клиента в сетевом режиме функционирования для выполнения некоторых действий могут потребоваться особые права доступа. Например, права на администрирование домена безопасности. Если пользователь, выполняющий установку, не обладает нужными правами, программа установки на определенных этапах может запрашивать учетные данные пользователей с правами доступа.

Для переустановки клиента:

1. Вставьте в привод установочный компакт-диск системы Secret Net. Дождитесь появления окна программы автозапуска (см. стр.**11**) и запустите переустановку с помощью команды "Клиентское ПО".

Примечание.
Запуск процедуры переустановки компонента можно также выполнить стандартным способом в окне ОС Windows "Программы и компоненты" ("Установка и удаление программ") или путем запуска соответствующего файла:
- если переустановка выполняется на компьютере с 64-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\x64\Setup.exe;
- если переустановка выполняется на компьютере с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Client\Win32\Setup.exe.

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

2. Для продолжения нажмите кнопку "Далее >".

   На экране появится диалог "Обслуживание программ".

3. Выберите вариант "Исправить" и нажмите кнопку "Далее >".

   На экране появится диалог "Готова к исправлению программы".

4. 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.

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

5. Нажмите кнопку "Готово" и перезагрузите компьютер.

Внимание!
Дождитесь окончания перезагрузки компьютера. Необходимо иметь в виду, что при первой загрузке текущая аппаратная конфигурация компьютера автоматически принимается в качестве эталонной. Поэтому до начала загрузки проверьте, какие аппаратные устройства подключены к компьютеру, и отключите те устройства, которые должны быть запрещены к использованию.

Переустановка сервера безопасности

Переустановка сервера безопасности позволяет:
- заменить поврежденные файлы компонента;
- создать новый каталог для размещения резервных копий журналов;
- создать новый каталог для хранения временных файлов;
- восстановить регистрацию компонентов сервера безопасности в хранилище объектов централизованного управления.

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

Для выполнения некоторых действий при переустановке 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.

Для переустановки сервера безопасности:

1. Вставьте в привод установочный компакт-диск системы Secret Net. Дождитесь появления окна программы автозапуска (см. стр.11) и запустите переустановку с помощью команды "Сервер безопасности".

Примечание.
Запуск процедуры переустановки можно также выполнить стандартным способом в окне ОС Windows "Программы и компоненты" ("Установка и удаление программ") или вручную. Для запуска процедуры вручную в зависимости от операционной системы компьютера выполните следующее действие:
- если переустановка выполняется на компьютере с 64-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Server\x64\Setup.exe;
- если переустановка выполняется на компьютере с 32-разрядной версией Windows — запустите с установочного компакт-диска файл \Setup\Server\Win32\Setup.exe.

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

2. Нажмите кнопку "Далее >".

На экране появится диалог "Обслуживание программ".

3. Выберите вариант "Исправить" и нажмите кнопку "Далее >".

На экране появится диалог "Настройки СУБД".

4. Отметьте тип СУБД для совместной работы с сервером безопасности (Oracle или MS SQL) и выполните следующие действия:
- Укажите параметры соединения с тем экземпляром БД, который предназначен для работы с сервером безопасности:
  - в поле "Имя БД" укажите строку соединения с экземпляром БД. Формат записи различается в зависимости от типа СУБД. Если используется СУБД Oracle, введите строку в следующем формате: *<имя_или_IP-адрес_сервера_Oracle>:<порт>/<имя_экземпляра_БД>* Если используется СУБД MS SQL, введите: *<имя_или_IP-адрес_сервера_MS_SQL>\<имя_экземпляра_БД>,<порт>*

    Примечание.
    Порт можно не указывать, если используется номер по умолчанию (для СУБД Oracle порт по умолчанию 1521, для СУБД MS SQL — 1433).
  - в группе полей "Учетная запись администратора БД" — учетные данные администратора базы данных на сервере СУБД;

    Примечание.
    Если используется СУБД Oracle, в качестве администратора БД необходимо указывать учетные данные пользователя с привилегией SYSDBA (по умолчанию такой привилегией обладает пользователь sys, который является встроенным администратором СУБД Oracle).
  - в группе полей "Учетная запись, используемая сервером для доступа к БД" — учетные данные, с которыми сервер безопасности выполняет подключение к базе данных.

    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).
- При необходимости укажите другой каталог для размещения резервных копий журналов Secret Net.
- Нажмите кнопку "Далее >".

На экране появится диалог "Настройки ISAPI-расширения".

5. Оставьте прежним или создайте новый каталог для хранения временных файлов и нажмите кнопку "Далее >".

На экране появится диалог "Регистрация в хранилище централизованного управления".

6. Выполните следующие действия:

- Для сохранения в хранилище объектов централизованного управления имеющейся информации (рекомендуется) — удалите отметку в поле "восстановить регистрацию компонентов программы в хранилище" и нажмите кнопку "Далее >".

  На экране появится диалог "Готова к исправлению программы".

  Перейдите к выполнению действия **7**.

- Для восстановления начальной регистрационной информации сервера в хранилище — выполните действия, описанные в приложении на стр.**62**.

  Предупреждение.
  Режим восстановления регистрации сервера безопасности в хранилище объектов централизованного управления следует использовать только в крайнем случае, когда другими способами восстановить сервер не удалось. При восстановлении потребуется заново ввести все серийные номера, используя программу оперативного управления.

7. 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.

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

8. Нажмите кнопку "Готово" и перезагрузите компьютер.

Переустановка программы оперативного управления

Переустановка программы оперативного управления выполняется пользователем, входящим в локальную группу администраторов компьютера. Запуск процедуры переустановки компонента можно выполнить с установочного компакт-диска (см. стр. **23**) или стандартным способом в окне ОС Windows "Программы и компоненты" ("Установка и удаление программ"). Процедура переустановки выполняется без особенностей.

Глава 3
Настройка системы для автоматической установки клиента

Если система состоит из большого количества компьютеров, обычный способ установки ПО клиента локально на каждом компьютере может оказаться затруднительным для администратора. Чтобы упростить процесс развертывания системы, администратор может централизованно настроить автоматическую установку и обновление компонента "Secret Net 7".

Реализация автоматической установки и обновления основана на применении специально настроенных групповых политик на компьютерах определенных организационных подразделений. На каждом компьютере запуск процесса установки или обновления происходит автоматически при завершении работы операционной системы. Если на компьютере ПО клиента не установлено — запускается процесс установки. При наличии установленного компонента предыдущей версии — выполняется обновление на текущую версию.

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

1. Начальное формирование структуры ОУ.
2. Создание общедоступного сетевого ресурса.
3. Создание файлов со сценарием установки.
4. Создание организационных подразделений и включение в них компьютеров.
5. Создание и настройка групповых политик для организационных подразделений.

Начальное формирование структуры ОУ

Компьютеры, на которых будет выполняться автоматическая установка ПО, следует включить в структуру оперативного управления и подчинить каждый компьютер серверу безопасности. Для этого в системе должна быть развернута соответствующая структура серверов безопасности и подготовлено рабочее место администратора Secret Net. При отсутствии серверов безопасности необходимо выполнить установку компонентов системы Secret Net в соответствии с порядком установки для сетевого режима функционирования (см. стр.14).

Подчинение серверам безопасности компьютеров без установленного клиентского ПО осуществляется при работе с программой оперативного управления в режиме конфигурирования. Для этого на сервере безопасности должно быть зарегистрировано достаточное число лицензий на запланированное количество клиентов. Подробные сведения о работе с программой оперативного управления см. в документе [**4**].

Создание общедоступного сетевого ресурса

В домене необходимо создать общедоступный сетевой ресурс (ОСР), содержащий файлы для установки ПО клиента.

Для создания ОСР:

1. На одном из компьютеров домена создайте папку и откройте общий доступ к этой папке. Дополнительно предоставьте права доступа к папке всем учетным записям компьютеров, на которые планируется устанавливать ПО клиента, или для группы "Прошедшие проверку" ("Authenticated Users"). Необходимые права обеспечиваются установленными разрешениями на чтение, чтение и выполнение и просмотр содержимого.

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

2. С установочного компакт-диска системы Secret Net скопируйте в папку содержимое следующих каталогов (сохраняя их структурную вложенность):

Имя каталога	Назначение
\Setup\Client\	Содержит дистрибутивы для установки ПО клиента на 32- и 64-разрядных версиях ОС Windows
\Setup\SnTmCard\	Содержит файлы для установки драйвера средства аппаратной поддержки Secret Net Card на 32- и 64-разрядных версиях ОС Windows. Добавляется в каталог при необходимости автоматической установки драйвера на компьютерах
\Tools\Microsoft\	Содержит файлы установки необходимых обновлений ОС Windows. Если файлы отсутствуют, автоматическая установка клиента на компьютерах не будет выполняться

Создание файлов со сценарием установки

Сценарии предназначены для автоматизации процесса установки клиентского программного обеспечения. Они позволяют частично или полностью автоматизировать ввод информации, запрашиваемой программой установки клиента.

Файлы со сценарием установки создаются в XML-формате (кодировка "windows-1251"). Созданные файлы необходимо поместить в общедоступном сетевом ресурсе в каталогах \Setup\Client\Win32 и \Setup\Client\x64.

Создать файл сценария можно с использованием программы установки клиента или вручную.

Для создания файла сценария с помощью программы установки:

1. На компьютере без установленного ПО клиента создайте на локальном диске папку для временного размещения дистрибутивных файлов.
2. С установочного компакт-диска системы Secret Net скопируйте в папку содержимое следующих каталогов (сохраняя их структурную вложенность):

Имя каталога	Назначение
\Setup\Client\	Содержит дистрибутивы для установки ПО клиента на 32- и 64-разрядных версиях ОС Windows
\Tools\Microsoft\	Содержит файлы установки необходимых обновлений ОС Windows. Если файлы отсутствуют, автоматическая установка клиента на компьютерах не будет выполняться

3. Запустите консоль командной строки (cmd.exe).
4. Введите команду для запуска программы установки клиента в режиме создания файла сценария:
   - на компьютере под управлением 32-разрядной версии Windows: start <*имя_папки*>\Setup\Client\Win32\Setup.exe /script:3
   - на компьютере под управлением 64-разрядной версии Windows: start <*имя_папки*>\Setup\Client\x64\Setup.exe /script:3

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.
5. Нажмите кнопку "Далее >" и выполните предлагаемые программой действия до появления диалога "Готова к установке программы".

Пояснение.
Программа установки функционирует как в обычном режиме, при этом полученные программой данные протоколируются и на определенном этапе сохраняются в файле сценария. Файл сценария создается программой до начала непосредственной установки ПО на компьютер, поэтому после создания файла работу программы установки можно завершить.

6. В диалоге "Готова к установке программы" нажмите кнопку "Отмена" и подтвердите решение о прекращении установки в появившемся диалоге запроса.

   На экране появится диалог "Программа установки завершена".

7. Нажмите кнопку "Готово" и проверьте наличие в папке файла сценария SnInstall.script. Скопируйте файл в подкаталоги \Setup\Client\Win32 и \Setup\Client\x64 папки OCP.

Для создания файла сценария вручную:

1. В текстовом редакторе создайте файл SnInstall.script, сформируйте содержимое документа по правилам языка XML и сохраните файл в подкаталогах \Setup\Client\Win32 и \Setup\Client\x64 папки OCP.

Структура файла сценария

Файл сценария имеет следующую структуру:

```
<?xml version="1.0" encoding="windows-1251"?>
<SnInstallScript>
<DB>
    <Property>
        <параметр_1>значение_параметра</параметр_1>
        <параметр_2>значение_параметра</параметр_2>
        ...
        <параметр_N>значение_параметра</параметр_N>
    </Property>
</DB>
</SnInstallScript>
```

В группе Property указываются параметры и их значения, необходимые программе установки ПО клиента. Перечень основных параметров, предусмотренных для редактирования, представлен в таблице.

Параметр	Значение по умолчанию	Описание
INSTALLDIR	[ProgramFilesFolder]Secret Net\Client	Путь установки ПО клиента
REBOOT	Force	Определяет необходимость перезагрузки компьютера после установки: • "Force" – перезагрузка должна выполняться; • "ReallySuppres" – перезагрузка не выполняется, даже если она нужна для работы ПО
SNPRODUCTKIND	Client	Определяет режим работы устанавливаемого ПО: • "Client" – сетевой режим функционирования; • "Local" – локальный режим функционирования

Параметр	Значение по умолчанию	Описание
SNSETPERMISSIONS	1 — для Windows XP; 0 — для других ОС	Определяет необходимость замены прав доступа пользователей к основным ресурсам компьютера: • "0" — замена прав не выполняется; • "1" — замена прав будет выполняться
SNADMANAGERACCOUNTNAME	Отсутствует	Имя учетной записи для доступа к AD
SNADMANAGERPASSWORD	Отсутствует	Пароль учетной записи для доступа в AD
SNSERIALNUMBER	Отсутствует	Серийный номер клиента
SNINSTALLADMINISTRATIVETOOLS	Отсутствует	Определяет необходимость установки средств централизованной настройки (параметров механизмов КЦ, ЗПС и параметров доменных пользователей): • "0" — средства не устанавливаются; • "1" — средства устанавливаются
SNOMSLIST	Отсутствует	Определяет имя компьютера сервера безопасности, которому будет подчинен устанавливаемый клиент. Параметр не устанавливает связь компьютера с сервером безопасности и используется для обеспечения возможности загрузки параметров. Указывается только в случае размещения объектов централизованного управления вне AD
SNDIVISION	Отсутствует	Учетная информация компьютера: название подразделения
SNAUTOSYSTEMNAME	Отсутствует	Учетная информация компьютера: название автоматизированной системы
SNPCLOCATION	Отсутствует	Учетная информация компьютера: рабочее место
SNPCSERIAL	Отсутствует	Учетная информация компьютера: номер системного блока
SNINSTALLTBL	Отсутствует	Определяет необходимость включения механизма защиты дисков: • "0" — механизм не включается; • "1" — механизм включается
TBLSERIALNUMBER	Отсутствует	Серийный номер подсистемы защиты дисков
SNTSERIALNUMBER	Отсутствует	Серийный номер разрешения терминальных подключений
KEYFILEPATH	C:\	Путь для сохранения файла с ключом аварийного восстановления механизма защиты дисков
TURNOFFDACS	0	Определяет необходимость отключения механизма контроля устройств после установки: • "0" — механизм остается включенным; • "1" — механизм отключается
TURNOFFERASER	0	Определяет необходимость отключения механизма затирания данных после установки: • "0" — механизм остается включенным; • "1" — механизм отключается

Параметр	Значение по умолчанию	Описание
TURNOFFEXEQUOTA	0	Определяет необходимость отключения механизма замкнутой программной среды после установки: • "0" — механизм остается включенным; • "1" — механизм отключается
TURNOFFPRNCTRL	0	Определяет необходимость отключения механизма контроля печати после установки: • "0" — механизм остается включенным; • "1" — механизм отключается
TURNOFFSNMC	0	Определяет необходимость отключения механизма полномочного управления доступом после установки: • "0" — механизм остается включенным; • "1" — механизм отключается

Если параметру не присвоено значение, будет использоваться значение, заданное по умолчанию. Для установки клиента обязательно должны быть указаны значения для следующих параметров: INSTALLDIR, SNSERIALNUMBER и SNINSTALLADMINISTRATIVETOOLS.

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

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

```
<?xmlversion="1.0" encoding="windows-1251"?>
<SnInstallScript>
<DB>
    <Property>
        <INSTALLDIR>
        [ProgramFilesFolder]Secret Net\Client
        </INSTALLDIR>
        <REBOOT>Force</REBOOT>
        <SNSETPERMISSIONS></SNSETPERMISSIONS>
        <SNADMANAGERACCOUNTNAME>
        domainname\V_Ivanov
        </SNADMANAGERACCOUNTNAME>
        <SNADMANAGERPASSWORD>
        12345678
        </SNADMANAGERPASSWORD>
        <SNSERIALNUMBER>
        1234-5678-9123-4567-8901-2345-6789
        </SNSERIALNUMBER>
        <SNINSTALLADMINISTRATIVETOOLS>
        0
        </SNINSTALLADMINISTRATIVETOOLS>
    </Property>
</DB>
</SnInstallScript>
```

В приведенном примере предписывается:

1. Установить продукт в папку программ на системном диске в каталоге \Secret Net\Client.
2. Перезагрузить компьютер после установки.
3. Для доступа к AD использовать учетную запись "domainname\V_Ivanov" с паролем "12345678".
4. Для установки продукта использовать серийный номер: "1234-5678-9123-4567-8901-2345-6789".
5. Не устанавливать средства централизованной настройки системы Secret Net.

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 способами.

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 отключить или удалить стандартными способами.

Для создания групповой политики на контроллере домена под управлением ОС Windows Server 2012/2008:

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" (вариант англоязычного названия: "Create a GPO in this domain, and Link it here") .
3. В появившемся диалоге введите имя создаваемой политики и нажмите кнопку "ОК".

   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\Административные шаблоны:...\Система\Сценарии" и вызовите диалоговое окно настройки свойств параметра "Указать максимальное время выполнения сценариев групповой политики" (вариант англоязычного названия: "Maximum wait time for Group Policy scripts").
6. Установите отметку в поле "Включено", укажите значение "7200" и нажмите кнопку "ОК".
7. Вызовите диалоговое окно настройки свойств параметра "Отображать команды сценариев завершения работы во время их выполнения" ("Display instructions in shutdown scripts as they run") для ОС Windows Server 2012 или "Выполнять сценарии завершения работы с отображением команд" ("Run shutdown scripts visible") для ОС Windows Server 2008.
8. Установите отметку в поле "Включено" и нажмите кнопку "ОК".
9. В дереве объектов политики перейдите к разделу "Конфигурация компьютера\Политики\Конфигурация Windows\Сценарии" и вызовите диалоговое окно настройки свойств параметра "Завершение работы".
10. В диалоговом окне нажмите кнопку "Добавить".

    На экране появится диалог "Добавление сценария".
11. В поле "Имя сценария" введите нужное значение:
    - для применения политики на компьютерах с 32-разрядной ОС Windows: *<сетевой_путь_к_папке_ОСР>*\Setup\Client\Win32\Setup.exe
    - для применения политики на компьютерах с 64-разрядной ОС Windows: *<сетевой_путь_к_папке_ОСР>*\Setup\Client\x64\Setup.exe
12. В поле "Параметры сценария" введите значение /autoinstall.

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 создания групповой политики на контроллере домена под управлением ОС Windows Server 2003:

1. Откройте оснастку "Active Directory — Пользователи и Компьютеры", выберите организационное подразделение, на компьютерах которого будет проводиться автоматическая установка, и вызовите диалоговое окно настройки свойств организационного подразделения.
2. Перейдите на вкладку "Групповая политика" и нажмите кнопку "Создать".

3. Введите имя создаваемой политики и нажмите клавишу <Enter>.
4. Нажмите кнопку "Изменить".

   На экране появится окно редактора групповых политик.
5. В дереве объектов политики перейдите к разделу "Конфигурация компьютера\Административные шаблоны\Система\Сценарии" и вызовите диалоговое окно настройки свойств параметра "Maximum wait time for Group Policy scripts".
6. Установите отметку в поле "Включен", укажите значение "7200" и нажмите кнопку "OK".
7. Вызовите диалоговое окно настройки свойств параметра "Выполнять сценарии завершения работы с отображением команд" ("Run shutdown scripts visible").
8. Установите отметку в поле "Включен" и нажмите кнопку "OK".
9. В дереве объектов политики перейдите к разделу "Конфигурация компьютера\Конфигурация Windows\Сценарии" и вызовите диалоговое окно настройки свойств параметра "Завершение работы".
10. В диалоговом окне нажмите кнопку "Добавить".

    На экране появится диалог "Добавление сценария".
11. В поле "Имя сценария" введите нужное значение:
    - для применения политики на компьютерах с 32-разрядной ОС Windows: *<сетевой_путь_к_папке_ОСР>*\Setup\Client\Win32\Setup.exe
    - для применения политики на компьютерах с 64-разрядной ОС Windows: *<сетевой_путь_к_папке_ОСР>*\Setup\Client\x64\Setup.exe
12. В поле "Параметры сценария" введите значение /autoinstall.

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 (для этого используйте кнопку "Добавить" на вкладке "Групповая политика" в окне настройки свойств организационного подразделения).

Глава 4
Удаление

Предупреждение.
Если на защищаемых компьютерах имеется конфиденциальная информация, следует принять меры по ее защите после удаления системы Secret Net.

Удаление клиента в автономном режиме функционирования

Удаление клиента в автономном режиме функционирования выполняет администратор безопасности, который должен входить в локальную группу администраторов компьютера.

Для удаления клиента в автономном режиме функционирования:

1. В окне ОС Windows "Программы и компоненты" ("Установка и удаление программ") выберите в списке компонент "Secret Net 7" и нажмите кнопку "Изменить".

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.
2. Для продолжения нажмите кнопку "Далее >".

   На экране появится диалог "Обслуживание программ".
3. Выберите вариант "Удалить" и нажмите кнопку "Далее >".

   На экране появится диалог "Удаление программы".
4. Нажмите кнопку "Удалить".

   Начнется процесс удаления программного обеспечения, завершающийся появлением диалога "Программа установки завершена".
5. Нажмите кнопку "Готово" и перезагрузите компьютер.

Удаление драйвера средства аппаратной поддержки

Если на компьютере установлен драйвер средства аппаратной поддержки Secret Net Card или Secret Net Touch Memory Card (регистрируется в качестве самостоятельного компонента при установке клиента), удаление драйвера осуществляется отдельно. Запуск процедуры удаления драйвера выполняется стандартным способом в окне ОС Windows "Программы и компоненты" ("Установка и удаление программ").

Порядок удаления для сетевого режима функционирования

Компоненты системы Secret Net в сетевом режиме функционирования, установленные на компьютерах, удаляются по отдельности. Процедуры удаления предусмотрены для следующих компонентов:

- "Secret Net 7";
- "Secret Net 7 — Сервер безопасности";
- "Secret Net 7 — Программа управления".

Для компонента "Модификатор схемы Active Directory" процедура удаления не предусмотрена.

При удалении компонентов системы Secret Net рекомендуется придерживаться следующей последовательности действий:

1. Удалите программу оперативного управления на рабочих местах администраторов.
2. Удалите ПО клиентов на всех компьютерах.
3. Удалите ПО серверов безопасности.
4. Удалите (если требуется) компоненты СУБД.

Удаление программы оперативного управления

Удаление программы оперативного управления выполняется без особенностей. Запуск процедуры удаления компонента "Secret Net 7 — Программа управления" можно выполнить стандартным способом в окне ОС Windows "Программы и компоненты" ("Установка и удаление программ").

Удаление клиента в сетевом режиме функционирования

Удаление клиента в сетевом режиме функционирования выполняется пользователем, входящим в локальную группу администраторов компьютера.

Для удаления клиента:

1. В окне ОС Windows "Программы и компоненты" ("Установка и удаление программ") выберите компонент "Secret Net 7" и нажмите кнопку "Изменить".

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.
2. Для продолжения нажмите кнопку "Далее >".

   На экране появится диалог "Обслуживание программ".
3. Выберите вариант "Удалить" и нажмите кнопку "Далее >".

   На экране появится диалог "Запись данных...".
4. Укажите учетные данные пользователя с правами администратора домена безопасности и нажмите кнопку "Далее >".

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

   Если процедура удаления клиента выполняется на контроллере домена, на экране появится диалог "Дополнительные параметры". При удалении клиента на другом компьютере перейдите к действию **7**.
5. Определите необходимость сохранения параметров системы Secret Net в групповых политиках домена. Для удаления параметров из всех групповых политик установите отметку в поле "удалить групповые политики Secret Net". При необходимости сохранить централизованно заданные параметры удалите отметку из поля.

   Пояснение.
   Если выбран вариант без удаления, централизованно заданные параметры групповых политик Secret Net продолжают применяться на компьютерах домена с установленным клиентским ПО системы защиты.
6. Нажмите кнопку "Далее >".

   На экране появится диалог "Удаление программы".
7. Нажмите кнопку "Удалить".

   Начнется процесс удаления программного обеспечения, завершающийся появлением диалога "Программа установки завершена".
8. Нажмите кнопку "Готово" и перезагрузите компьютер.

Удаление драйвера средства аппаратной поддержки

Если на компьютере установлен драйвер средства аппаратной поддержки Secret Net Card или Secret Net Touch Memory Card (регистрируется в качестве самостоятельного компонента при установке клиента), удаление драйвера осуществляется отдельно. Запуск процедуры удаления драйвера выполняется стандартным способом в окне ОС Windows "Программы и компоненты" ("Установка и удаление программ").

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.

Удаление сервера безопасности выполняется пользователем, входящим в группу администраторов домена безопасности. Пользователь должен иметь права администратора БД.

Для выполнения некоторых действий при удалении сервера безопасности могут потребоваться особые права доступа. 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" ("Установка и удаление программ") выберите в списке компонент "Secret Net 7 — Сервер безопасности" и нажмите кнопку "Изменить".

   Программа установки начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия.
2. Нажмите кнопку "Далее >".

   На экране появится диалог "Обслуживание программ".
3. Выберите вариант "Удалить" и нажмите кнопку "Далее >".

   На экране появится диалог "Удаление базы данных".
4. Выполните нужное действие:
   - для сохранения БД — выберите "не удалять базу данных";
   - для удаления БД — выберите "удалить базу данных" и заполните поля "Имя пользователя" и "Пароль" учетными данными администратора базы данных на сервере СУБД.
5. Нажмите кнопку "Далее >".

   На экране появится диалог "Дополнительно".
6. При необходимости сохранить сертификат сервера безопасности в IIS удалите отметку из поля "удалить сертификат из Internet Information Server" и нажмите кнопку "Далее >".

   На экране появится диалог "Удаление программы".
7. Нажмите кнопку "Удалить".

   Начнется процесс удаления сервера безопасности, завершающийся появлением диалога "Программа установки завершена".

   Примечание.
   В процессе удаления ПО на экране могут появляться различные запросы системы. Например, если службы сервера безопасности продолжают функционировать, может появиться диалог "Используются файлы", в котором сообщается о необходимости закрыть приложение. В этом случае не обязательно останавливать работу служб — достаточно нажать в диалоге кнопку "Пропустить".
8. Нажмите кнопку "Готово" и перезагрузите компьютер.

Удаление средств поддержки клиентов предыдущих версий

Если на компьютере установлены средства поддержки клиентов системы Secret Net предыдущих версий (устанавливаются в качестве самостоятельного компонента при установке сервера безопасности), удаление средств осуществляется отдельно. Запуск процедуры удаления средств поддержки выполняется стандартным способом в окне ОС Windows "Программы и компоненты" ("Установка и удаление программ").

Приложение

Программа пакетной установки СУБД Oracle

Для обеспечения функционирования сервера безопасности может применяться СУБД Oracle Database 10g Express Edition.

В соответствии с лицензионным соглашением СУБД Oracle Database 10g Express Edition распространяется бесплатно.

Установку компонентов Oracle Database 10g Express Edition следует выполнять с помощью программы пакетной установки Oracle (далее — программа пакетной установки), разработанной компанией "Код Безопасности". Программа пакетной установки в автоматическом режиме осуществляет компоновку и настройку СУБД в объеме, необходимом для функционирования сервера безопасности.

Описание работы с программой пакетной установки дано на примере операционной системы Microsoft Windows Server 2008.

Особенности программы пакетной установки

Программа пакетной установки не поддерживает следующие функции:

- установка компонентов на контроллере домена;
- установка компонентов в корневую папку диска;
- удаление установленных компонентов;
- обновление, переустановка и изменение установленных компонентов;
- выбор номера порта связи (значение задается автоматически — 1521).

Примечание.
Изменить номер порта можно штатными средствами Oracle после установки компонентов Oracle программой пакетной установки.

Требования к программному обеспечению

Программа пакетной установки предназначена для использования на компьютерах, на которых установлены следующие операционные системы:

- Windows Server 2008/Server 2008 R2;
- Windows Server 2003/Server 2003 R2.

Внимание!
Существует ограничение на размер файла подкачки MS Windows, требующийся для установки Oracle. Размер файла подкачки необходимо задать явно и не менее 1,5 ГБ.

Повторное использование

Если требуется повторная установка компонентов Oracle средствами программы пакетной установки, предварительно следует удалить ПО Oracle. Запуск процедуры удаления ПО выполняется стандартным способом удаления программ в ОС Windows.

Подготовка к установке

Установка компонентов Oracle может выполняться как с установочного компакт-диска, так и из сетевых ресурсов (далее — установочный ресурс Oracle). Сетевой ресурс должен полностью соответствовать структуре папки \Tools\Oracle\OracleDataBase установочного компакт-диска.

Предупреждение!
В путях копирования и установки компонентов Oracle не должно быть кириллических символов — наличие таких символов приводит к ошибкам установки.

Перед началом установки компонентов Oracle на компьютер следует убедиться в том, что на этом компьютере отсутствуют установленные ранее компоненты Oracle. Если такие компоненты имеются, их необходимо удалить (см. выше).

Установку СУБД Oracle должен выполнять локальный пользователь, входящий в локальную группу администраторов компьютера. В процессе установки назначаются права доступа к СУБД, поэтому учетной записи пользователя, под которой выполняется установка, будут предоставлены права на администрирование СУБД.

Внимание!
Запуск программы пакетной установки необходимо осуществлять только под учетной записью локального пользователя. Если вход в систему выполнен с учетными данными доменного пользователя, установка запрещается.

Выбор варианта размещения сервера Oracle

Возможны следующие варианты размещения сервера Oracle и сервера безопасности:

- совместная установка — сервер безопасности и сервер Oracle функционируют на одном компьютере;
- раздельная установка — сервер безопасности и сервер Oracle функционируют на разных компьютерах.

Внимание!
При любом варианте ПО сервера Oracle устанавливается до установки ПО сервера безопасности.

Установка сервера Oracle

Для установки сервера Oracle:

1. Выполните вход в систему с учетными данными локального пользователя.
2. Запустите на исполнение файл \Tools\Oracle\OracleDataBase\Setup.exe с установочного ресурса Oracle.

   На экране появится диалог приветствия программы пакетной установки.
3. Для продолжения установки нажмите кнопку "Далее >".

   На экране появится диалог "Компоненты СУБД".
4. Удалите отметку из поля "Клиентская часть СУБД", оставьте отмеченным поле "Серверная часть СУБД" и нажмите кнопку "Далее >".

   Примечание.
   Установка клиентской части Oracle выполняется автоматически при установке сервера безопасности.

   На экране появится диалог "Папка назначения".
5. Укажите папку для установки программного обеспечения и нажмите кнопку "Далее >".

   На экране появится диалог "Пароль администратора базы данных".
6. Введите пароль и нажмите кнопку "Далее >".

   Внимание!
   Пароль должен содержать только буквы латинского алфавита и цифры, при этом цифра не может быть указана на первой позиции.

   На экране появится следующий диалог программы пакетной установки.
7. Нажмите кнопку "Установить".

   Начнется процесс установки компонентов Oracle, сопровождаемый индикатором прогресса.

   Процесс установки завершается появлением на экране отчета, в котором содержатся следующие сведения:

   - наименование и полный путь к каталогу установленного программного обеспечения (файл отчета находится в этом же каталоге);

- наименование и полный путь к каталогу базы данных;
- наименование экземпляра базы данных;
- пароли встроенных учетных записей пользователей SYS и SYSTEM.

Примечание.
В случае возникновения ошибок при установке в отчете будут приведены имена файлов, содержащих сведения о ходе установки. Если причины ошибок выяснить не удается, обратитесь в отдел технической поддержки компании "Код Безопасности". Для рассмотрения причин ошибок нужно предоставить файлы, указанные в отчете.

8. Примите меры по учету и защите информации, содержащейся в отчете, и закройте файл отчета.

   На экране появится диалог "Программа установки завершена".

9. Для завершения работы и перезагрузки компьютера нажмите кнопку "Готово".

Проверка успешности установки

Признаки успешной установки компонентов Oracle:

- системные журналы компьютера, на котором выполнена установка Oracle, не должны содержать сообщений об ошибках установки или неработоспособности системы или приложений;
- должны быть созданы соответствующие службы Oracle. Перечень служб, необходимых для работы с СУБД:
  - OracleServiceXE;
  - OracleXETNSListener.

  Эти службы должны быть запущены, иметь тип запуска "Авто" и выполнять вход в систему от имени системной учетной записи;
- в главном меню Windows должно присутствовать меню "Oracle Database 10g Express Edition".

Сведения об установке и настройке СУБД MS SQL

При использовании для сервера безопасности системы управления базами данных, реализуемой сервером 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.aspx — для SQL Server 2012 и http://technet.microsoft.com/ru-ru/library/ms143506%28v=sql.105%29.aspx — для SQL Server 2008. 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 компакт-диск комплекта поставки содержит средства установки бесплатно распространяемого варианта СУБД версии MS SQL Server 2012 SP1 Express в русской редакции. 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 4.0. Для этого запустите файл dotNetFx40_Full_x86_x64.exe из каталога \Tools\Microsoft\MS SQL Server 2012 SP1 Express.
3. Установить языковой пакет к .NET Framework 4.0. Для этого запустите файл dotNetFx40LP_Full_x86_x64ru.exe из каталога \Tools\Microsoft\MS SQL Server 2012 SP1 Express.
4. Установить сервер MS SQL. Для этого запустите файл SQLEXPRWT_x64_RUS.exe или SQLEXPRWT_x86_RUS.exe (в зависимости от разрядности ОС) из каталога \Tools\Microsoft\MS 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;
- 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) — включен режим поддержки протокола TCP/IP. Режим по умолчанию отключен при использовании свободно распространяемого варианта SQL Server Express. Управление режимом осуществляется с помощью утилиты 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, соответственно, пустое значение и значение "1433";
- если сервер MS SQL установлен на отдельном компьютере — в брандмауэре (если он включен) разрешено использование порта 1433 для соединения с СУБД. При этом на сервере MS SQL порт должен быть открыт на входящие соединения, а на сервере безопасности — на исходящие.

Изменения в схеме AD при модификации

Модификатор AD осуществляет:

1. Добавление атрибутов к стандартным классам

Атрибуты, добавляемые к стандартным классам "User", "Computer", "DomainDNS" и "OrganizationalUnit", представлены в таблицах ниже.

Табл.1 Добавляемые атрибуты класса "User"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-User-AccessLevel. Назначение: хранение полномочного уровня допуска к конфиденциальной информации. OID: 1.2.840.113556.1.8000.1620.1.1.1
2	Наименование атрибута: Infosec-SN-User-fPrintSecretPriv. Назначение: хранение привилегии на печать конфиденциальной информации. OID: 1.2.840.113556.1.8000.1620.1.1.2
3	Наименование атрибута: Infosec-SN-User-fOutputSecret. Назначение: хранение привилегии на вывод конфиденциальной информации. OID: 1.2.840.113556.1.8000.1620.1.1.3
4	Наименование атрибута: Infosec-SN-User-fControlLabels. Назначение: хранение привилегии на управление категориями конфиденциальности. OID: 1.2.840.113556.1.8000.1620.1.1.4
5	Наименование атрибута: Infosec-SN-User-EffectivePublicKey. Назначение: хранение текущего открытого криптографического ключа. OID: 1.2.840.113556.1.8000.1620.1.1.14
6	Наименование атрибута: Infosec-SN-User-PreviousPublicKey. Назначение: хранение предыдущего открытого криптографического ключа. OID: 1.2.840.113556.1.8000.1620.1.1.15
7	Наименование атрибута: Infosec-SN-User-EffectiveKeyTimeGenerated. Назначение: хранение времени генерации текущего криптографического ключа. OID: 1.2.840.113556.1.8000.1620.1.1.16
8	Наименование атрибута: Infosec-SN-User-PreviousKeyTimeGenerated. Назначение: хранение времени генерации предыдущего криптографического ключа. OID: 1.2.840.113556.1.8000.1620.1.1.17
9	Наименование атрибута: Infosec-SN-User-DBMS-Access-Privilege. Назначение: хранение дополнительных флагов. OID: 1.2.840.113556.1.8000.1620.1.1.35
10	Наименование атрибута: Infosec-SN-User-ImitSableCompList. Назначение: хранение имитовставки списка компьютеров, хранящегося в атрибуте Infosec-SN-User-SableCompList (см. ниже). OID: 1.2.840.113556.1.8000.1620.1.1.41
11	Наименование атрибута: Infosec-SN-User-SableCompList. Назначение: хранение списка компьютеров с ПАК "Соболь", доступных данному пользователю. OID: 1.2.840.113556.1.8000.1620.1.1.46
12	Наименование атрибута: Infosec-SN-User-AccessCheck. Назначение: для проверки маски доступа пользователя к объектам. OID: 1.2.840.113556.1.8000.1620.1.1.64
13	Наименование атрибута: Infosec-SS-User-AccessLevel64. Назначение: хранение неиерархической метки доступа (64 бита). OID: 1.2.840.113556.1.8000.1620.1.1.65

№ п/п	Атрибут
14	Наименование атрибута: Infosec-SS-User-Privileges. Назначение: хранение привилегий пользователя (все в одном). OID: 1.2.840.113556.1.8000.1620.1.1.66
15	Наименование атрибута: Infosec-SN-User-Is-TrustAccess-Synchronized. Назначение: признак синхронизации пользователя с TrustAccess. OID: 1.2.840.113556.1.8000.1620.1.1.84
16	Наименование атрибута: Infosec-SN-User-PasswordHash. Назначение: хранение свертки пароля пользователя. OID: 1.2.840.113556.1.8000.1620.1.1.85
17	Наименование атрибута: Infosec-SN-User-PasswordTimeGenerated. Назначение: хранение времени генерации пароля пользователя. OID: 1.2.840.113556.1.8000.1620.1.1.86

Табл.2 Добавляемые атрибуты класса "Computer"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-Computer-OMS-SID. Назначение: хранение SID того СБ, которому подчинен данный компьютер. OID: 1.2.840.113556.1.8000.1620.1.1.6
2	Наименование атрибута: Infosec-SN-Computer-fAgent. Назначение: хранение флага, отображающего наличие Агента на компьютере. OID: 1.2.840.113556.1.8000.1620.1.1.19
3	Наименование атрибута: Infosec-SN-Computer-Shedule. Назначение: хранение расписания сбора журналов для данного компьютера. OID: 1.2.840.113556.1.8000.1620.1.1.22
4	Наименование атрибута: Infosec-SN-Computer-fLogLogon. Назначение: хранение флага сбора журналов для данного компьютера при его подключении к СБ. OID: 1.2.840.113556.1.8000.1620.1.1.26
5	Наименование атрибута: Infosec-SN-Computer-HttpTransportSettings. Назначение: хранение настроек транспортной подсистемы для данного компьютера. OID: 1.2.840.113556.1.8000.1620.1.1.34
6	Наименование атрибута: Infosec-SN-Computer-SablePublicKey. Назначение: хранение открытого ключа компьютера. OID: 1.2.840.113556.1.8000.1620.1.1.42
7	Наименование атрибута: Infosec-SN-Computer-SableVK. Назначение: хранение дополнительных данных для расчета ключа SComp. OID: 1.2.840.113556.1.8000.1620.1.1.43
8	Наименование атрибута: Infosec-SN-Computer-SableKeyInfoImit. Назначение: хранение имитовставки от блоба CompKeyInfo (PKk + VK). OID: 1.2.840.113556.1.8000.1620.1.1.44
9	Наименование атрибута: Infosec-SN-Computer-SableSyncData. Назначение: хранение данных синхронизации ПАК "Соболь". OID: 1.2.840.113556.1.8000.1620.1.1.45
10	Наименование атрибута: Infosec-SN-Computer-AgentFlags. Назначение: хранение управляющих флагов Агента. OID: 1.2.840.113556.1.8000.1620.1.1.50
11	Наименование атрибута: Infosec-SN-Computer-SablePlantNumber. Назначение: хранение заводского номера платы ПАК "Соболь". OID: 1.2.840.113556.1.8000.1620.1.1.59

№ п/п	Атрибут
12	Наименование атрибута: Infosec-SN-Computer-RegWSDepartement. Назначение: хранение учетной информации компьютера (название подразделения). OID: 1.2.840.113556.1.8000.1620.1.1.60
13	Наименование атрибута: Infosec-SN-Computer- RegWSSystem. Назначение: хранение учетной информации компьютера (название автоматизированной системы). OID: 1.2.840.113556.1.8000.1620.1.1.61
14	Наименование атрибута: Infosec-SN-Computer-RegWSLocation. Назначение: хранение учетной информации компьютера (расположение компьютера). OID: 1.2.840.113556.1.8000.1620.1.1.62
15	Наименование атрибута: Infosec-SN-Computer-RegWSNumber. Назначение: хранение учетной информации компьютера (номер системного блока). OID: 1.2.840.113556.1.8000.1620.1.1.63
16	Наименование атрибута: Infosec-SS-Computer-SnProductInfo. Назначение: хранение информации об установленном продукте. OID: 1.2.840.113556.1.8000.1620.1.1.67
17	Наименование атрибута: Infosec-SN-Computer-ClientSN-Item. Назначение: хранение серийного номера текущего клиента. OID: 1.2.840.113556.1.8000.1620.1.1.69
18	Наименование атрибута: Infosec-SN-Computer-ServiceSN. Назначение: хранение списка серийных номеров служб (лицензирование SS 1.0). OID: 1.2.840.113556.1.8000.1620.1.1.70
19	Наименование атрибута: Infosec-SN-Computer-ClientSN61. Назначение: хранение серийного номера текущего клиента (лицензирование SN 6.1). OID: 1.2.840.113556.1.8000.1620.1.1.74
20	Наименование атрибута: Infosec-SN-Computer-ClientSN70. Назначение: хранение серийного номера клиента СНК (лицензирование SN 7). OID: 1.2.840.113556.1.8000.1620.1.1.88
21	Наименование атрибута: Infosec-SN-Computer-TrustedBootSN70. Назначение: хранение серийного номера защиты диска СНД (лицензирование SN 7). OID: 1.2.840.113556.1.8000.1620.1.1.89
22	Наименование атрибута: Infosec-SN-Computer-TerminalServerSN70. Назначение: хранение серийного номера терминального сервера СНТ (лицензирование SN 7). OID: 1.2.840.113556.1.8000.1620.1.1.90
23	Наименование атрибута: Infosec-SN-Computer-UAFilter. Назначение: хранение настроек фильтра НСД для компьютера. OID: 1.2.840.113556.1.8000.1620.1.1.95
24	Наименование атрибута: Infosec-SN-Product-Version-Major. Назначение: хранение основного номера текущей версии ПО клиента. OID: 1.2.840.113556.1.8000.1620.1.1.97
25	Наименование атрибута: Infosec-SN-Product-Version-Minor. Назначение: хранение основного номера текущей версии ПО клиента. OID: 1.2.840.113556.1.8000.1620.1.1.98

Табл.3 Добавляемые атрибуты класса "DomainDNS"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-Policy-Link. Назначение: ссылка на политику Secret Net, которая привязана к этому домену. OID: 1.2.840.113556.1.8000.1620.1.1.99

Табл.4 Добавляемые атрибуты класса "OrganizationalUnit"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-Policy-Link. Назначение: ссылка на политику Secret Net, которая привязана к этому организационному подразделению. OID: 1.2.840.113556.1.8000.1620.1.1.99

2. Добавление новых классов с соответствующими атрибутами

- **Класс "Infosec-SN-ADSchema"**

  Класс предназначен для хранения информации о текущей схеме AD и имеет OID 1.2.840.113556.1.8000.1620.1.2.1 (атрибуты см. в таблице ниже).

Табл.5 Добавляемые атрибуты класса "Infosec-SN-Schema"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-ADSchema-Version. Назначение: хранение основного номера текущей версии схемы AD. OID: 1.2.840.113556.1.8000.1620.1.1.5
2	Наименование атрибута: Infosec-SN-ADSchema-VersionExtended. Назначение: хранение расширенного номера текущей версии схемы AD. OID: 1.2.840.113556.1.8000.1620.1.1.54

- **Класс "Infosec-SN-OMS"**

  Класс предназначен для хранения информации о серверах безопасности и имеет OID: 1.2.840.113556.1.8000.1620.1.2.2 (атрибуты см. в таблице ниже).

Табл.6 Добавляемые атрибуты класса "Infosec-SN-OMS"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-OMS-SID. Назначение: хранение SID данного СБ. OID: 1.2.840.113556.1.8000.1620.1.1.7
2	Наименование атрибута: Infosec-SN-OMS-ParentSID. Назначение: хранение SID родительского СБ в иерархии СБ (родительского для СБ, SID которого хранится в предыдущем атрибуте). OID: 1.2.840.113556.1.8000.1620.1.1.8
3	Наименование атрибута: Infosec-SN-OMS-Certificate. Назначение: хранение X.509 сертификата СБ. OID: 1.2.840.113556.1.8000.1620.1.1.9
4	Наименование атрибута: Infosec-SN-OMS-Shedule. Назначение: хранение расписания сбора журналов для подчиненных данному СБ рабочих станций. OID: 1.2.840.113556.1.8000.1620.1.1.25

№ п/п	Атрибут
5	Наименование атрибута: Infosec-SN-OMS-fLogLogon. Назначение: хранение флага сбора журналов для подчиненных данному СБ рабочих станций при их подключении к СБ. OID: 1.2.840.113556.1.8000.1620.1.1.27
6	Наименование атрибута: Infosec-SN-OMS-SecurityDescriptor. Назначение: хранение дескриптора безопасности для СБ. OID: 1.2.840.113556.1.8000.1620.1.1.32
7	Наименование атрибута: Infosec-SN-OMS-HttpTransportSettings. Назначение: хранение настроек транспорта для СБ. OID: 1.2.840.113556.1.8000.1620.1.1.33
8	Наименование атрибута: Infosec-SN-OMS-MailSettings. Назначение: хранение правил почтовой рассылки уведомлений о событиях НСД для данного СБ. OID: 1.2.840.113556.1.8000.1620.1.1.36
9	Наименование атрибута: Infosec-SN-OMS-ClientSN. Назначение: хранение серийных номеров клиентов (лицензирование SN 5.0). OID: 1.2.840.113556.1.8000.1620.1.1.37
10	Наименование атрибута: Infosec-SN-OMS-ManagementSN. Назначение: хранение серийных номеров программ управления (лицензирование SN 5.0). OID: 1.2.840.113556.1.8000.1620.1.1.38
11	Наименование атрибута: Infosec-SN-OMS-ADQueryTimeOut. Назначение: хранение тайм-аута, задающего периодичность опроса AD данным СБ для считывания настроек. OID: 1.2.840.113556.1.8000.1620.1.1.51
12	Наименование атрибута: Infosec-SN-OMS-ArchiveJournalSchedule. Назначение: хранение расписания архивирования журналов. OID: 1.2.840.113556.1.8000.1620.1.1.52
13	Наименование атрибута: Infosec-SN-OMS-Config. Назначение: хранение настроек для данного СБ. OID: 1.2.840.113556.1.8000.1620.1.1.53
14	Наименование атрибута: Infosec-SN-OMS-Flags. Назначение: хранение управляющих флагов СБ. OID: 1.2.840.113556.1.8000.1620.1.1.55
15	Наименование атрибута: Infosec-SN-OMS-ClientSNEx. Назначение: хранение серийных ключей клиентов (лицензирование SN 5.1). OID: 1.2.840.113556.1.8000.1620.1.1.71
16	Наименование атрибута: Infosec-SN-OMS- ManagementSNEx. Назначение: хранение серийных ключей программ управления (лицензирование SN 5.1). OID: 1.2.840.113556.1.8000.1620.1.1.72
17	Наименование атрибута: Infosec-SN-OMS-ServerSN. Назначение: хранение серийного номера сервера безопасности (лицензирование SN 5.1). OID: 1.2.840.113556.1.8000.1620.1.1.73
18	Наименование атрибута: Infosec-SN-OMS-ClientSN61. Назначение: хранение серийных ключей клиентов (лицензирование SN 6.1). OID: 1.2.840.113556.1.8000.1620.1.1.75
19	Наименование атрибута: Infosec-SN-OMS-ManagementSN61. Назначение: хранение серийных ключей программ управления (лицензирование SN 6.1). OID: 1.2.840.113556.1.8000.1620.1.1.76

№ п/п	Атрибут
20	Наименование атрибута: Infosec-SN-OMS-ServerSN61. Назначение: хранение серийного номера сервера безопасности (лицензирование SN 6.1). OID: 1.2.840.113556.1.8000.1620.1.1.77
21	Наименование атрибута: Infosec-SN-OMS-ClientSN70. Назначение: хранение серийных ключей клиентов (лицензирование SN 7). OID: 1.2.840.113556.1.8000.1620.1.1.91
22	Наименование атрибута: Infosec-SN-OMS-ManagementSN70. Назначение: хранение серийных ключей программ управления (лицензирование SN 7). OID: 1.2.840.113556.1.8000.1620.1.1.92
23	Наименование атрибута: Infosec-SN-OMS-ServerSN70. Назначение: хранение серийного номера сервера безопасности (лицензирование SN 7). OID: 1.2.840.113556.1.8000.1620.1.1.93
24	Наименование атрибута: Infosec-SN-OMS-UAFilter. Назначение: хранение настроек фильтра НСД для данного СБ. OID: 1.2.840.113556.1.8000.1620.1.1.94
25	Наименование атрибута: Infosec-SN-OMS-TrustedBootSN70. Назначение: хранение серийных ключей защиты диска (лицензирование SN 7). OID: 1.2.840.113556.1.8000.1620.1.1.96
26	Наименование атрибута: Infosec-SN-Product-Version-Major. Назначение: хранение основного номера текущей версии ПО сервера. OID: 1.2.840.113556.1.8000.1620.1.1.97
27	Наименование атрибута: Infosec-SN-Product-Version-Minor. Назначение: хранение основного номера текущей версии ПО сервера. OID: 1.2.840.113556.1.8000.1620.1.1.98
28	Наименование атрибута: Infosec-SN-Policy-Link. Назначение: ссылка на политику Secret Net, которая привязана к этому домену. OID: 1.2.840.113556.1.8000.1620.1.1.99

- **Класс "Infosec-SN-UEI"**

  Класс предназначен для хранения информации об ЭИ пользователя и имеет OID: 1.2.840.113556.1.8000.1620.1.2.3 (атрибуты см. в таблице ниже).

Табл.7 Добавляемые атрибуты класса "Infosec-SN-UEI"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-UEI-UserSID. Назначение: хранение SID пользователя. OID: 1.2.840.113556.1.8000.1620.1.1.10
2	Наименование атрибута: Infosec-SN-UEI-Type. Назначение: хранение типа электронного идентификатора. OID: 1.2.840.113556.1.8000.1620.1.1.11
3	Наименование атрибута: Infosec-SN-UEI-Size. Назначение: хранение размера ID ЭИ, хранимого в следующем атрибуте. OID: 1.2.840.113556.1.8000.1620.1.1.12
4	Наименование атрибута: Infosec-SN-UEI-Id. Назначение: хранение ID электронного идентификатора. OID: 1.2.840.113556.1.8000.1620.1.1.13
5	Наименование атрибута: Infosec-SN-UEI-Flags. Назначение: хранение флагов электронного идентификатора. OID: 1.2.840.113556.1.8000.1620.1.1.18

№ п/п	Атрибут
6	Наименование атрибута: Infosec-SN-UEI-AuthInfo. Назначение: хранение информации об аутентификаторе. OID: 1.2.840.113556.1.8000.1620.1.1.39

- **Класс "Infosec-SN-GSableData"**

  Класс предназначен для хранения глобальной информации о проверке ключей ЦУ ПАК "Соболь" и имеет OID 1.2.840.113556.1.8000.1620.1.2.4 (атрибуты см. в таблице ниже).

Табл.8 Добавляемые атрибуты класса "Infosec-SN-GSableData"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-GSableData-KeysCheckData. Назначение: хранение случайной последовательности для проверки ключей ЦУ ПАК "Соболь". OID: 1.2.840.113556.1.8000.1620.1.1.47
2	Наименование атрибута: Infosec-SN-GSableData-KaCheckImit. Назначение: хранение имитовставки случайной последовательности на ключе Ka. OID: 1.2.840.113556.1.8000.1620.1.1.48
3	Наименование атрибута: Infosec-SN-GSableData-SKaCheckImit. Назначение: хранение имитовставки случайной последовательности на ключе SKa. OID: 1.2.840.113556.1.8000.1620.1.1.49

- **Классы "Infosec-SN-ICheckObj" и "Infosec-SN-ICheckObj64"**

  Классы предназначены для хранения информации об объектах ЦУ КЦ ЗПС и имеют OID 1.2.840.113556.1.8000.1620.1.2.5 и 1.2.840.113556.1.8000.1620.1.2.7 (атрибуты см. в таблице ниже).

Табл.9 Добавляемые атрибуты классов "Infosec-SN-ICheckObj" и "Infosec-SN-ICheckObj64"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-ICheckObj-ID. Назначение: хранение идентификатора объекта ЦУ КЦ ЗПС. OID: 1.2.840.113556.1.8000.1620.1.1.56
2	Наименование атрибута: Infosec-SN-ICheckObj-Type. Назначение: хранение типа объекта ЦУ КЦ ЗПС. OID: 1.2.840.113556.1.8000.1620.1.1.57
3	Наименование атрибута: Infosec-SN-ICheckObj-Data. Назначение: хранение данных объекта ЦУ КЦ ЗПС. OID: 1.2.840.113556.1.8000.1620.1.1.58

- **Класс "Infosec-SS-GClientInfo"**

  Класс предназначен для хранения глобальной информации об установленных в системе продуктах Secret Net и имеет OID 1.2.840.113556.1.8000.1620.1.2.6 (атрибуты см. в таблице ниже).

Табл.10 Добавляемые атрибуты класса "Infosec-SS-GClientInfo"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SS-GClientInfo-ProductTypes. Назначение: хранение информации об установленных типах продуктов. OID: 1.2.840.113556.1.8000.1620.1.1.68

- **Класс "Infosec-SN-GTrustAccessInfo"**

  Класс предназначен для хранения параметров интеграции с СЗИ TrustAccess и имеет OID 1.2.840.113556.1.8000.1620.1.2.8 (атрибуты см. в таблице ниже).

Табл.11 Добавляемые атрибуты класса "Infosec-SN-GTrustAccessInfo"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-TrustAccess-Is-Integrated. Назначение: признак включения интеграции с СЗИ TrustAccess. OID: 1.2.840.113556.1.8000.1620.1.1.80
2	Наименование атрибута: Infosec-SN-TrustAccess-Is-User-Locked. Назначение: признак блокировки пользователя при неуспешном входе в TrustAccess. OID: 1.2.840.113556.1.8000.1620.1.1.81
3	Наименование атрибута: Infosec-SN-TrustAccess-KDC-Host. Назначение: хост сервера управления TrustAccess. OID: 1.2.840.113556.1.8000.1620.1.1.82
4	Наименование атрибута: Infosec-SN-TrustAccess-Kerberos-Realm. Назначение: домен TrustAccess. OID: 1.2.840.113556.1.8000.1620.1.1.83

- **Класс "Infosec-SN-PolicyObject"**

  Класс предназначен для хранения объекта групповой политики и имеет OID 1.2.840.113556.1.8000.1620.1.2.9 (атрибуты см. в таблице ниже).

Табл.12 Добавляемые атрибуты класса "Infosec-SN-PolicyObject"

№ п/п	Атрибут
1	Наименование атрибута: Infosec-SN-Policy-Revision. Назначение: ревизия политики (инкрементируется при модификации модели данных). OID: 1.2.840.113556.1.8000.1620.1.1.100
2	Наименование атрибута: Infosec-SN-Policy-Version. Назначение: версия объекта политики (инкрементируется при изменении данных). OID: 1.2.840.113556.1.8000.1620.1.1.101
3	Наименование атрибута: Infosec-SN-Policy-Base. Назначение: базовые политики Secret Net. OID: 1.2.840.113556.1.8000.1620.1.1.102
4	Наименование атрибута: Infosec-SN-Policy-Devices. Назначение: политика устройств Secret Net. OID: 1.2.840.113556.1.8000.1620.1.1.103

3. Создание конфигурационной информации

Конфигурационная информация для установленного продукта создается в разделе конфигурации каталога AD.

В этом разделе создаются следующие объекты:

- В контейнере "Services" создается служебный контейнер "SecretNet 5.0 Configuration".
- В контейнере "SecretNet 5.0 Configuration" создается объект ADSchema (класс Infosec-SN-ADSchema), хранящий текущую версию схемы AD.

После проведения модификации текущая версия схемы AD хранится в разделе конфигурации, что позволяет после проведения очередной репликации иметь доступ к этой информации в рамках всего леса.

- В контейнерах "CN=409, CN=DisplaySpecifiers" и "CN=419, CN=DisplaySpecifiers" создаются конфигурационные данные для поддержки управляющих модулей системы:
  - в атрибут adminContextMenu объектов user-Display и inetOrgPerson-Display добавляется GUID {26DFFB2F-9AA6-4219-8287-88489C3E55F0} для обработки операций смены пароля пользователя в контекстном меню;
  - в атрибут adminPropertyPages объектов user-Display и inetOrgPerson-Display добавляется GUID {2F01C0A1-E5DD-496c-AA30-196A26D3B1C2} для отображения дополнительной страницы свойств при управлении параметрами пользователей;
  - в атрибут dSUIAdminNotification объекта DS-UI-Default-Settings добавляется GUID {26DFFB2F-9AA6-4219-8287-88489C3E55F0} для получения уведомления при удалении пользователя;
  - в атрибут dSUIAdminNotification объекта DS-UI-Default-Settings добавляется GUID {CDB5CE54-B162-48bd-968F-A9CA4E81F31E}, обеспечивающий пункт "Загрузить ключи ЦУ" в контекстном меню объекта "User" (при выборе этого пункта запускается загрузка ключей ЦУ ПАК "Соболь");
  - в атрибут dSUIAdminNotification объекта DS-UI-Default-Settings добавляется GUID {17BBFB57-491A-4BCE-AF8B-93ADA4F2A387} для получения уведомления при удалении пользователя в части TrustAccess.

Расстановка прав доступа в ОС Windows XP

Права доступа на каталоги и файлы

Имя объекта	Права доступа
%SystemDrive%\	Administrators: FullControl CREATOR OWNER: FullControl (Subfolders & files) SYSTEM: FullControl Users: Read, Execute
%SystemDrive%\Documents and Settings	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute Power Users: Read, Execute
%AllUsersProfile%	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%AllUsersProfile%\Application Data\Microsoft	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute Power Users: Travers Folder, Execute File List Folder, Read Data, Read Attributes, Read Extended Attributes, Create Files, Write Data, Create Folders, Append Data, Write Attributes, Write Extended Attributes, Delete Subfolders and Files, Delete, Read Permissions
%AllUsersProfile%\Application Data\Microsoft\Crypto\DSS\MachineKeys	Administrators: FullControl SYSTEM: FullControl Users: List folder, Read attributes, Read extended attributes, Create files, Create folders, Write attributes, Write extended attributes, Read permissions (Folder Only)
%AllUsersProfile%\Application Data\ Microsoft\HTML Help	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute Power Users: Modify
%AllUsersProfile%\Application Data\ Microsoft\Media Index	Administrators: FullControl SYSTEM: FullControl Users: Create files, Create folders, Write attributes, Write extended attributes, Read permissions (Folder only) Users: Write (Subfolders & files) Users: Read, Execute Power Users: Traverse Folder, Execute File List Folder, Read Data, Read Attributes, Read Extended Attributes, Create Files, Write Data, Create Folders, Append Data, Write Attributes, Write Extended Attributes, Delete Subfolders and Files, Delete, Read Permissions
%SystemDrive%\Documents and Settings\ Default User	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute Power Users: Read, Execute
%SystemRoot%\Installer	Administrators: FullControl SYSTEM: FullControl Users: Read, Execute
%SystemRoot%\Registration	Administrators: FullControl (Folder & files) SYSTEM: FullControl (Folder & files) Users: Read (Folder & files)

Каталог установки клиента

При установке клиентского ПО системы Secret Net 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

Изменения в реестре при установке клиента

Программа установки компонента "Secret Net 7" вносит следующие изменения в стандартные параметры реестра:

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

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 общих параметрах сайта (Default Web Site) выполняется:

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

Некоторые рекомендации по обеспечению безопасности в ИС

Ниже приведены некоторые рекомендации Microsoft по обеспечению информационной безопасности в информационной системе (ИС) предприятия:

1. Для предотвращения атак домена переименуйте или отключите встроенную учетную запись администратора (а также учетную запись гостя) в каждом домене.
2. Держите все контроллеры домена в закрытой комнате для обеспечения физической безопасности.
3. Для обеспечения дополнительной защиты схемы Active Directory контролируйте состав группы "Администраторы схемы" и добавляйте пользователей в эту группу только при необходимости.
4. Ограничьте для пользователей, групп и компьютеров доступ к общим ресурсам и параметрам фильтра групповой политики.
5. Избегайте отключения подписывания и шифрования трафика LDAP для средств администрирования Active Directory.
6. Некоторые права пользователей по умолчанию, присвоенные определенным группам по умолчанию, позволяют членам этих групп получить дополнительные, в том числе административные, права в домене. Поэтому организация должна в равной степени доверять всем сотрудникам, являющимся членами групп "Администраторы предприятия", "Администраторы домена", "Операторы учета", "Операторы сервера", "Опытные пользователи", "Операторы печати" и "Операторы архива".

Источник: Microsoft TechNet.

О восстановлении регистрации сервера безопасности

В результате восстановления регистрации сервера безопасности в хранилище объектов централизованного управления все настройки сервера, включая лицензионную информацию, возвращаются в значения по умолчанию. При возвращении настроек сервера в значения по умолчанию происходит восстановление целостности параметров сервера и удаляются серийные номера, хранимые на сервере.

В результате удаления серийных номеров подчиненные серверу безопасности компьютеры становятся свободными и перестают управляться системой Secret Net, а при загрузке сервера появляется сообщение о нарушении лицензионной политики.

Для восстановления регистрации сервера безопасности в хранилище объектов централизованного управления

1. В процедуре переустановки сервера безопасности при выполнении действия **6** (см. стр. **31**) в диалоге "Регистрация в хранилище централизованного управления" установите отметку в поле "восстановить регистрацию компонентов программы в хранилище" и нажмите кнопку "Далее >".

   На экране появится диалог "Учетные данные администратора безопасности".

2. Укажите учетные данные пользователя с правами администратора домена безопасности и нажмите кнопку "Далее >".

   Пояснение.
   Если текущий пользователь имеет необходимые права — оставьте отмеченным поле "Использовать учетную запись текущего пользователя". Если права не предоставлены — выберите пункт "Использовать указанные ниже имя пользователя и пароль" и введите данные соответствующей учетной записи.

   Далее в диалогах программы установки выполняйте действия аналогично процедуре установки сервера безопасности.

Для восстановления подчинения компьютеров серверу безопасности:

1. Запустите программу оперативного управления в режиме конфигурирования и выполните следующие действия:
   - введите для данного сервера безопасности все серийные номера, которые должны храниться на нем;
   - добавьте свободные компьютеры (ранее подчиненные данному серверу безопасности) в структуру оперативного управления и подчините их серверу.
2. Перезагрузите компьютер с сервером безопасности.
3. Вернитесь к программе оперативного управления и проверьте значения параметров сервера безопасности, при необходимости откорректируйте их.
4. Запустите программу в режиме мониторинга и убедитесь в работоспособности сервера безопасности.

Локальное конфигурирование клиента для работы в структуре ОУ

Конфигурирование клиента системы Secret Net для работы в структуре оперативного управления осуществляется при установке ПО клиента. Большинство возможностей конфигурирования доступны также и после установки клиента — они реализуются централизованно в программе оперативного управления (см. документ [**4**]).

При необходимости внесения изменений локально может использоваться специальная программа из состава клиентского ПО системы Secret Net (далее — программа локального конфигурирования клиента). Программа предоставляет следующие возможности:

- отображение сведений о текущей конфигурации;
- вывод списка доступных серверов безопасности;
- регистрация компьютера в структуре ОУ;
- подчинение серверу безопасности;
- регистрация серийного номера клиента.

С помощью программы локального конфигурирования клиента также могут выполняться некоторые специфические действия, связанные с подчинением агентов серверам других доменов безопасности без переустановки клиентского ПО. Например, данная программа позволяет подчинить компьютер серверу безопасности с хранилищем объектов централизованного управления вне Active Directory, если клиент был установлен без подчинения СБ или ранее был подчинен серверу с хранилищем объектов ЦУ в AD. Или если требуется выполнить перенос агента из одного домена безопасности в другой (когда компьютер нужно переместить в контейнер Active Directory, соответствующий другому домену безопасности).

Внимание!

В случае переноса агента из одного домена безопасности в другой действия необходимо выполнить в следующей последовательности: в программе оперативного управления (см. документ [**4**]) удалить агента из структуры ОУ предыдущего домена безопасности; в оснастке ОС Windows "Active Directory — пользователи и компьютеры" переместить компьютер в другой контейнер; добавить агента в структуру ОУ нового домена безопасности; на компьютере агента с помощью программы локального конфигурирования подчинить агента серверу в новом домене безопасности.

Для локального конфигурирования клиента:

1. Выполните вход в систему с учетными данными пользователя, входящего в локальную группу администраторов.
2. С использованием стандартных средств ОС Windows остановите работу службы "Secret Net Agent".
3. В каталоге установки клиента запустите на исполнение файл SnLDAPConfig.exe.

   На экране появится диалог программы локального конфигурирования клиента. После получения данных в диалоге появятся сведения о текущей конфигурации клиента и список доступных серверов безопасности.
4. Выберите сервер безопасности, в хранилище объектов которого требуется поместить сведения о компьютере, и установите отметку в соответствующем поле:
   - для регистрации компьютера в структуре ОУ в качестве свободного агента — отметьте поле "внести информацию о компьютере в хранилище";
   - для регистрации компьютера в структуре ОУ с подчинением выбранному серверу — отметьте поле "подчинить компьютер серверу безопасности".
5. Чтобы зарегистрировать серийный номер клиента, установите отметку в поле "внести в хранилище данные о лицензии" и выберите нужный вариант действий:

- для получения СНК со свободной лицензией с сервера безопасности и регистрации в локальном хранилище — отметьте поле "запросить лицензию у сервера безопасности";
- для регистрации в централизованном хранилище СНК из локального хранилища — отметьте поле "использовать лицензию, имеющуюся на этом компьютере";
- для регистрации нового СНК — отметьте поле "использовать новый лицензионный ключ" и укажите серийный номер в поле ввода.

6. При необходимости укажите учетные данные пользователя с правами на конфигурирование каталога LDAP в группе полей "Учетные данные".

Пояснение.
Если текущий пользователь имеет необходимые права — оставьте отмеченным поле "использовать учетные данные текущего пользователя". Если права не предоставлены — отметьте поле "использовать указанные ниже имя и пароль" и введите данные соответствующей учетной записи.

7. Нажмите кнопку "Выполнить".

После выполнения действий на экране появится соответствующее сообщение программы.

8. После завершения конфигурирования закройте программу и снова запустите службу "Secret Net Agent".

Использование программы в режиме командной строки

Для программы локального конфигурирования клиента предусмотрена возможность использования в режиме командной строки. Формат команды запуска: SnLDAPConfig.exe /server:< *DNS- имя_ сервера* > [/nosubordinate] [/noadd] [/license:local | /license:server | /license:<*серийный_номер*>] [/user:<*имя_пользователя*> /password:<*пароль*>]

Описание параметров команды:

- /server:< *DNS- имя_ сервера* > — выполняет подключение к указанному серверу безопасности. Обязательный параметр для режима командной строки. Если другие параметры не указаны, выполняется подчинение компьютера указанному серверу, получение от этого сервера серийного номера и сохранение его в локальном хранилище;
- /nosubordinate — отменяет подчинение серверу безопасности и считывание серийного номера;
- /noadd — отменяет все другие параметры, происходит только запись в системный реестр данных для подключения к указанному серверу;
- /license — выполняет регистрацию серийного номера. Предусмотрены следующие варианты:
  - /license:local — регистрация в централизованном хранилище СНК, имеющегося на этом компьютере;
  - /license:server — получение СНК с сервера;
  - /license:<*серийный_номер*> — регистрация нового СНК;
- /user и /password — учетные данные пользователя с правами на конфигурирование каталога LDAP.

Примеры команд:
- SnLDAPConfig.exe /server:SnLDSServer1.SnDomain.ru — выполняется подчинение серверу безопасности на компьютере с именем SnLDSServer1.SnDomain.ru, получение серийного номера клиента с сервера и сохранение СНК в локальном хранилище;
- SnLDAPConfig.exe /server:SnADServer.SnDomain.ru /license:local — выполняется подчинение серверу безопасности на компьютере с именем SnADServer.SnDomain.ru и регистрация в централизованном хранилище серийного номера клиента, сохраненного локально.

Изменение учетных данных для подключения СБ к серверу СУБД

Сервер безопасности выполняет подключение к базе данных на сервере СУБД с использованием учетных данных, указанных при установке СБ. Если имя и/или пароль этой учетной записи были изменены средствами СУБД, для обеспечения доступа к базе данных необходимо синхронизировать новые учетные данные в конфигурационном файле сервера безопасности. Процедура ввода новых учетных данных выполняется на компьютере сервера безопасности с использованием специальной программы.

Для изменения учетных данных, используемых сервером безопасности:

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.

Резервное копирование хранилища объектов ЦУ, размещенного вне AD

При размещении хранилища объектов централизованного управления вне Active Directory сервер безопасности использует базу данных альтернативной службы каталогов. В зависимости от операционной системы компьютера сервера безопасности вместо доменных служб AD обработку данных осуществляют службы облегченного доступа к каталогам Active Directory (Active Directory Lightweight Directory Services, AD LDS) или компонент режима приложений Active Directory (Active Directory Application Mode, ADAM).

Хранилище объектов централизованного управления содержит информацию о лесе доменов безопасности и о конкретном домене безопасности, к которому относится сервер. При резервном копировании этой информации сохраняются файлы данных AD LDS/ADAM и конфигурационный файл сервера безопасности.

Примечание.
Для резервного копирования и восстановления базы данных КЦ-ЗПС используются средства экспорта и импорта модели данных в программе "Контроль программ и данных". Описание процедур экспорта и импорта см. в документе [3].

Создание резервной копии

Процедуры создания резервной копии хранилища объектов централизованного управления различаются в зависимости от операционной системы компьютера сервера безопасности.

Для создания резервной копии на компьютере под управлением ОС Windows Server 2012/2008:

1. Если резервную копию необходимо записать в новый каталог, создайте его.
2. Запустите VBS-скрипт BackupServerData2008_2012.vbs, который размещается в каталоге \Tools\Infosec\BackupServerData\ на установочном компакт-диске системы Secret Net. Синтаксис запуска:

   CScript.exe BackupServerData2008_2012.vbs <*каталог_резервной_копии*>

После выполнения скрипта в указанном каталоге создается вложенный каталог с именем в виде даты и времени создания. Каталог содержит резервные копии следующих данных:

- экземпляр AD LDS с данными домена безопасности (файл adamntds.dit в подкаталоге \SecretNet\);
- экземпляр AD LDS с данными глобального каталога (файл adamntds.dit в подкаталоге \SecretNet-GC\);
- конфигурационный файл сервера безопасности (файл ServerConfig.xml).

Для создания резервной копии на компьютере под управлением ОС Windows Server 2003:

- Запустите VBS-скрипт BackupServerData2003.vbs, который размещается в каталоге \Tools\Infosec\BackupServerData\ на установочном компакт-диске системы Secret Net. Синтаксис запуска:

  CScript.exe BackupServerData2003.vbs <*каталог_резервной_копии*>

  Для работы с резервной копией используется утилита ntbackup, входящая в состав ОС.

После выполнения скрипта в указанном каталоге создается файл резервной копии с именем в виде даты и времени создания. Файл содержит данные:

- экземпляр ADAM с данными домена безопасности (все файлы и каталоги, расположенные в %ProgramFiles%\Microsoft ADAM\SecretNet\);
- экземпляр ADAM с данными глобального каталога (все файлы и каталоги, расположенные в %ProgramFiles%\Microsoft ADAM\SecretNet-GC\);
- конфигурационный файл сервера безопасности (файл ServerConfig.xml).

Восстановление из резервной копии

Восстановление из резервной копии целесообразно применять в следующих случаях:

- если все серверы в лесу доменов безопасности вышли из строя — необходимо восстановить первый сервер, а на остальных серверах выполнить переустановку ПО с отключенным параметром "восстановить регистрацию компонентов программы в хранилище" (см. стр.**31**);
- если произошла замена оборудования, в результате которой компьютер сервера безопасности имеет новый SID, — можно выполнить восстановление из резервной копии, после чего необходимо переподчинить агентов данного сервера в программе оперативного управления (см. документ [**4**]).

Примечание.
При наличии в лесу доменов безопасности хотя бы одного работоспособного сервера процедуру восстановления из резервной копии на других серверах выполнять не следует, поскольку при следующей репликации данные с работоспособного сервера автоматически заменят данные восстановленного сервера как более актуальные. В этом случае при выходе из строя какого-либо сервера безопасности выполните на этом компьютере переустановку ПО с отключенным параметром "восстановить регистрацию компонентов программы в хранилище" (см. стр.**31**).

Процедуру восстановления из резервной копии необходимо выполнять на компьютере под управлением операционной системы из того же семейства, к которому относилась ОС компьютера при создании резервной копии.

Для восстановления из резервной копии на компьютере под управлением ОС Windows Server 2012/2008:

1. Установите ПО сервера безопасности на компьютер, включенный в состав домена Active Directory и организационного подразделения, к которым относился сервер созданной резервной копии. При установке необходимо выбирать вариант размещения хранилища объектов централизованного управления "вне Active Directory" и вариант включения в домен безопасности "создать новый домен в новом лесу доменов безопасности". На данном этапе не требуется вводить все серийные номера лицензий.
2. Последовательно остановите работу следующих служб:
   - World Wide Web Publishing Service;
   - Secret Net Security Server;
   - SecretNet;
   - SecretNet-GC.
3. Удалите содержимое каталогов %ProgramFiles%\Microsoft ADAM\SecretNet\data\ и %ProgramFiles%\Microsoft ADAM\SecretNet\logs\.
4. Скопируйте файл adamntds.dit из подкаталога \SecretNet\ резервной копии в каталог %ProgramFiles%\Microsoft ADAM\SecretNet\data\.
5. Удалите содержимое каталогов %ProgramFiles%\Microsoft ADAM\SecretNet-GC\data\ и %ProgramFiles%\Microsoft ADAM\SecretNet-GC\logs\.
6. Скопируйте файл adamntds.dit из подкаталога \SecretNet-GC\ резервной копии в каталог %ProgramFiles%\Microsoft ADAM\SecretNet-GC\data\.
7. Скопируйте файл ServerConfig.xml из каталога резервной копии в каталог установки сервера безопасности.

   Примечание.
   Будьте внимательны при восстановлении файлов из резервной копии. Указанные файлы должны быть размещены в корректных каталогах. Необходимо учитывать, что пути для размещения файлов могут отличаться от тех, которые были при создании резервной копии.
8. В конфигурационном файле сервера безопасности обновите учетные данные для подключения СБ к серверу СУБД с помощью программы OmsDBPasswordChange.exe (см. стр.**65**).
9. Последовательно запустите следующие службы:

- SecretNet;
- SecretNet-GC;
- World Wide Web Publishing Service.

10. Выполните действия для восстановления регистрации сервера безопасности (см. стр.**62**).

Для восстановления из резервной копии на компьютере под управлением ОС Windows Server 2003:

1. Установите ПО сервера безопасности на компьютер, включенный в состав домена Active Directory и организационного подразделения, к которым относился сервер созданной резервной копии. При установке необходимо выбирать вариант размещения хранилища объектов централизованного управления "вне Active Directory" и вариант включения в домен безопасности "создать новый домен в новом лесу доменов безопасности". На данном этапе не требуется вводить все серийные номера лицензий.
2. Последовательно остановите работу следующих служб:
   - World Wide Web Publishing Service;
   - Secret Net Security Server;
   - SecretNet;
   - SecretNet-GC.
3. Удалите содержимое каталогов %ProgramFiles%\Microsoft ADAM\SecretNet\data\ и %ProgramFiles%\Microsoft ADAM\SecretNet\logs\.
4. Удалите содержимое каталогов %ProgramFiles%\Microsoft ADAM\SecretNet-GC\data\ и %ProgramFiles%\Microsoft ADAM\SecretNet-GC\logs\.
5. Запустите утилиту ntbackup (входит в состав ОС) и восстановите с ее помощью все файлы из резервной копии.

   Примечание.
   Будьте внимательны при восстановлении файлов из резервной копии. Указанные файлы должны быть размещены в корректных каталогах. Необходимо учитывать, что пути для размещения файлов могут отличаться от тех, которые были при создании резервной копии.

6. В конфигурационном файле сервера безопасности обновите учетные данные для подключения СБ к серверу СУБД с помощью программы OmsDBPasswordChange.exe (см. стр.**65**).
7. Последовательно запустите следующие службы:
   - SecretNet;
   - SecretNet-GC;
   - World Wide Web Publishing Service.
8. Выполните действия для восстановления регистрации сервера безопасности (см. стр.**62**).

Варианты восстановления при некорректном удалении 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.

Удаление из Active Directory сведений о СБ с хранилищем объектов ЦУ в AD

Если сервер безопасности был установлен с размещением хранилища объектов централизованного управления в Active Directory, при некорректном удалении сервера в AD могут остаться сведения о нем. Из-за этого установка нового сервера с тем же серийным номером будет невозможна по причине конфликта лицензий.

Для исправления ситуации необходимо очистить AD от сведений о некорректно удаленном сервере. Очистку AD можно выполнить следующими способами:

- Переустановите сервер безопасности с восстановлением регистрации сервера (см. стр.62). Данный способ применим не во всех случаях.
- Подключите программу оперативного управления в режиме конфигурирования к другому серверу безопасности, который установлен в том же домене. В программе удалите объект, соответствующий некорректно удаленному серверу.

Примечание.
Если в домене отсутствует второй сервер безопасности, его можно установить без ввода серийного номера сервера (СНСб). В этом технологическом режиме сервер безопасности допускает подключение одной программы оперативного управления для выполнения конфигурационных действий.

Перенос роли мастера схемы LDAP на другой сервер безопасности

При размещении хранилища объектов централизованного управления вне Active Directory сервер безопасности использует базу данных альтернативной службы каталогов. В этом случае, как и в схеме AD, одному из серверов должна быть присвоена роль мастера схемы LDAP для службы каталогов. По умолчанию эта роль присваивается первому серверу безопасности, установленному с размещением хранилища объектов ЦУ вне Active Directory.

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.

Терминологический справочник

A	
AD	Active Directory — служба каталога для операционных систем MS Windows 2000 Server и выше. Active Directory Schema (схема Active Directory или схема каталога AD) — набор правил, описывающих структуру каталога (классы объектов домена и их атрибуты). Схема каталога AD гарантирует, что все добавления или изменения каталога соответствуют правилам
L	
LDAP	Lightweight Directory Access Protocol — протокол, работающий в домене поверх TCP/IP и обеспечивающий доступ к данным в AD
А	
Администратор безопасности	Лицо или группа лиц, ответственных за обеспечение безопасности системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты
Аутентификация	Проверка регистрационной информации пользователя
Г	
Глобальный каталог	Глобальный каталог (Global Catalog — GC) хранит полную копию всех объектов AD для того домена, в который входит сервер GC, и частичную копию объектов других доменов, образующих лес (хранятся только те свойства объектов, которые представляют интерес с точки зрения "масштабов" леса). С помощью оснастки Active Directory Schema администраторы могут указывать свои атрибуты (свойства объектов) для хранения в GC
Ж	
Журнал регистрации событий	Хранилище с информацией о событиях, зарегистрированных в системе защиты, например, попытках входа в систему
М	
Модификатор AD	Модификатор AD (или Модификатор схемы) — программа, которая вносит в схему каталога Active Directory классы и атрибуты, описывающие объекты Secret Net

Документация

1. Средство защиты информации Secret Net 7. Руководство администратора. Принципы построения	RU.88338853.501410.015 91 1
2. Средство защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление	RU.88338853.501410.015 91 2
3. Средство защиты информации Secret Net 7. Руководство администратора. Настройка механизмов защиты	RU.88338853.501410.015 91 3
4. Средство защиты информации Secret Net 7. Руководство администратора. Работа с программой оперативного управления	RU.88338853.501410.015 91 4
5. Средство защиты информации Secret Net 7. Руководство администратора. Локальная работа с журналами регистрации	RU.88338853.501410.015 91 5
6. Средство защиты информации Secret Net 7. Руководство пользователя	RU.88338853.501410.015 92