Код безопасности
ГК «Информзащита»

Средство защиты информации

# SECRET NET 6

## Руководство администратора

Конфигурирование

RU.88338853.501410.007 91 7




| | |
|---|---|
| Почтовый адрес: | **127018, г. Москва, ул. Сущёвский Вал, дом 47, стр. 2, помещение №1** |
| Телефон: | **(495) 980-23-45** |
| Факс: | **(495) 980-23-45** |
| e-mail: | **info@securitycode.ru** |
| Web: | **http://www.securitycode.ru** |

Версия: 6.5 Последнее обновление: 14-09-10

# Оглавление

**Список сокращений** ..... **4**

**Введение** ..... **5**

Основные задачи конфигурирования ..... 5

Структура оперативного управления ..... 6

Параметры серверов безопасности и защищаемых компьютеров ..... 6

**Глава 1. Начало работы с программой конфигурирования** ..... **7**

Запуск программы ..... 7

Интерфейс программы ..... 7

Элементы интерфейса ..... 8

**Глава 2. Редактирование структуры и настройка параметров** ..... **9**

Редактирование структуры ОУ ..... 9

Операции с серверами безопасности ..... 9

Операции с агентами ОУ ..... 10

Настройка параметров сервера безопасности ..... 12

Общие параметры ..... 12

Параметры передачи журналов агентами ..... 13

Привилегии для работы с программами оперативного управления ..... 15

Параметры лицензий на использование компонентов ..... 16

Параметры архивирования журналов ..... 18

Параметры рассылки почтовых уведомлений ..... 18

Настройка параметров агента ОУ ..... 21

Общие параметры ..... 21

Параметры передачи локальных журналов ..... 21

Параметры лицензии на использование агента ..... 22

Сохранение изменений ..... 22

**Глава 3. Дополнительные средства программы** ..... **23**

Обновление данных ..... 23

Сортировка компьютеров в окне структуры ..... 23

**Приложение** ..... **24**

Настройка элементов интерфейса ..... 24

Навигация при работе со структурами объектов ..... 24

Параметры сетевого взаимодействия ..... 25

Генерация и установка сертификата сервера безопасности ..... 26

**Терминологический справочник** ..... **27**

**Документация** ..... **28**

**Предметный указатель** ..... **29**

# Список сокращений

| | |
|---|---|
| **AD** | Active Directory |
| **DNS** | Domain Name System |
| **IP** | Internet Protocol |
| **RFC** | Request for Comments |
| **БД** | База данных |
| **НСД** | Несанкционированный доступ |
| **ОС** | Операционная система |
| **ОУ** | Оперативное управление |
| **ПО** | Программное обеспечение |
| **РС** | Рабочая станция |
| **СБ** | Сервер безопасности |
| **СНК** | Серийный номер клиента |
| **СНС** | Серийный номер сервера безопасности |
| **СНУ** | Серийный номер средств управления |

# Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net 6" RU.88338853.501410.007 (далее — система Secret Net 6, система защиты). В руководстве содержатся сведения, необходимые для работы с программой конфигурирования, входящей в состав средств оперативного управления в сетевом режиме функционирования системы защиты.

Перед изучением руководства необходимо ознакомиться с документами [ 1 ], [ 2 ], [ 5 ], [ 6 ].

### Условные обозначения

В руководстве для выделения некоторых элементов текста (примечаний и ссылок) 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**. Некоторые примечания могут и не сопровождаться пиктограммами. А на полях, помимо пиктограмм, 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 и hotline@infosec.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@infosec.ru).

## Основные задачи конфигурирования

В сетевом режиме функционирования системы Secret Net 6 реализована возможность централизованного конфигурирования системы защиты. При конфигурировании осуществляется:

- формирование структуры оперативного управления (ОУ);
- настройка параметров серверов безопасности (СБ);
- настройка параметров компьютеров, на которых установлено клиентское ПО системы Secret Net 6 в сетевом режиме функционирования (далее — защищаемые компьютеры или агенты).

Основной объем работ по конфигурированию выполняется на этапе установки компонентов Secret Net 6 на компьютеры автоматизированной системы предприятия.

Для решения задач конфигурирования используется специальное программное средство "Консоль управления" (далее — программа конфигурирования). Эта программа входит в состав компонента "Secret Net 6 – Средства управления".

## Структура оперативного управления

Структура ОУ представляет собой схему подчиненности компьютеров одного или нескольких доменов в зависимости от их роли в оперативном управлении.

Элементами схемы являются следующие объекты:

- домены;
- серверы безопасности — компьютеры, на которых установлено программное обеспечение "Secret Net 6 — Сервер безопасности";
- агенты — входящие в домен компьютеры, на которых установлено программное обеспечение "Secret Net 6" в сетевом режиме функционирования.

Между объектами в схеме могут быть установлены связи, отражающие отношения включения или подчинения. Описание связей применительно к различным объектам представлено в следующей таблице:

| Связи объектов | Отношения |
|---|---|
| **домен–домен** | Отношение подчинения. Один домен может иметь произвольное количество дочерних доменов. Сведения о связях доменов загружаются из Active Directory (AD) и не могут редактироваться |
| **домен–СБ** | Отношение включения. Домен может включать произвольное количество СБ. Связь определяется при установке СБ и в дальнейшем не редактируется |
| **домен–агент** | Отношение включения. Домен может включать произвольное количество агентов. Связь устанавливается в момент установки агента или после выведения агента из подчинения СБ. Агент, выведенный из подчинения, не управляется ни одним СБ, поэтому таких связей не должно быть в нормальном режиме работы системы защиты |
| **СБ–СБ** | Отношение подчинения. СБ может иметь произвольное количество подчиненных СБ |
| **СБ–агент** | Отношение управления. СБ может управлять произвольным количеством агентов своего домена |

Формирование схемы подчиненности объектов осуществляется по следующим правилам:

- объект "домен" используется только для группировки СБ и агентов;
- в одном домене обязательно должен быть хотя бы один СБ;
- серверы одних доменов могут быть подчинены СБ из других доменов;
- запрещается циклически подчинять серверы безопасности;
- СБ управляет агентами только того домена, в котором он установлен.

Во время эксплуатации системы Secret Net 6 в схему управления вносятся изменения при добавлении и удалении серверов и агентов или при переподчинении компьютеров, уже входящих в схему.

## Параметры серверов безопасности и защищаемых компьютеров

При конфигурировании выполняется настройка следующих параметров:

- параметры сетевого взаимодействия компонентов;
- параметры передачи журналов рабочих станций;
- привилегии для работы с программами оперативного управления;
- лицензии на использование компонентов системы защиты;
- параметры архивирования журналов, хранящихся в базе данных СБ;
- параметры рассылки почтовых уведомлений о событиях НСД.

# Глава 1
# Начало работы с программой конфигурирования

## Запуск программы

Для работы с программой конфигурирования пользователю должны быть предоставлены права на изменение AD. По умолчанию эти права предоставлены пользователям, входящим в группу администраторов домена.

**Для запуска программы:**

1. Активируйте в главном меню Windows команду "Пуск | Все программы | Код безопасности | Secret Net | Консоль управления".

   Если пользователь не имеет прав на изменение AD, на экране появится диалог запроса имени и пароля пользователя, обладающего такими правами.

2. Введите имя и пароль пользователя и нажмите кнопку "ОК".

   Программа загрузит данные из AD.

При загрузке данных программа проверяет наличие заданных значений для ряда параметров серверов безопасности и агентов. Если значения не заданы (например, после установки нового сервера безопасности), на экране появятся сообщения об ошибке загрузки каждого такого параметра.

> В процессе работы с программой рекомендуется в первую очередь корректно настроить параметры, которые указаны в качестве обязательных. Для удобства поиска пиктограммы объектов с незаданными параметрами выделены красным цветом. Перечень других предусмотренных обозначений и пиктограмм, используемых при отображении объектов, приводится на стр. 8.

Дополнительно для каждого сервера безопасности проверяется наличие установленного сертификата, который используется для соединений с сервером. Если найдены сертификаты с истекающим сроком действия, перед запуском программы на экране появляется окно с результатами диагностики сертификатов. В окне отображается список серверов безопасности, для которых требуется замена сертификатов. Генерацию и установку нового сертификата можно выполнить на компьютере с установленным сервером безопасности в программе генерации сертификатов.

## Интерфейс программы

По умолчанию основное окно программы конфигурирования имеет вид:

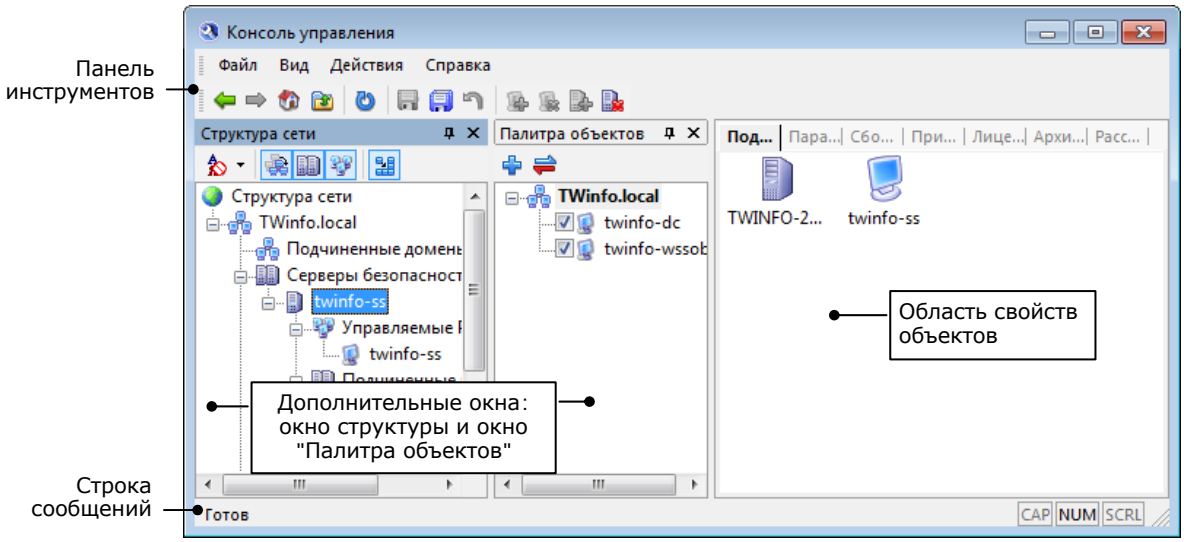



**Рис. 1. Основное окно программы**

Пользователь может изменять состав отображаемых элементов и их расположение на экране (см. стр. 24). Параметры внешнего вида основного окна сохраняются в системном реестре компьютера и используются в следующих сеансах работы пользователя с программой.

При большом количестве отображаемых элементов в окне структуры могут использоваться средства навигации (см. стр. 24).

## Элементы интерфейса

Основное окно программы может содержать следующие элементы интерфейса:

| |
|---|
| **Меню** |
| Содержит команды управления программой |
| **Панель инструментов основного окна** |
| Содержит кнопки быстрого вызова команд управления и программных средств |
| **Строка сообщений** |
| Отображает служебные сообщения программы, а также краткие подсказки к командам и кнопкам панели инструментов |
| **Информационный заголовок** |
| Отображает название программы и имя выбранного элемента структуры (сервера безопасности, защищаемого компьютера или папки структуры) |
| **Окно структуры** |
| Предназначено для управления объектами в иерархическом списке структуры сети. Кнопки панели инструментов окна позволяют включить или отключить отображение:<br>• доменов;<br>• серверов безопасности и ссылок на подчиненные серверы в других доменах;<br>• агентов (защищаемых компьютеров);<br>• папок, группирующих объекты.<br>Кроме того, панель инструментов окна содержит кнопку для сортировки списков компьютеров в иерархии.<br>При обнаружении конфигурационных несоответствий элементы структуры обозначаются следующим образом:<br>• красным цветом выделяются пиктограммы серверов безопасности, если значения параметров заданы некорректно или истек срок действия сертификата сервера безопасности;<br>• восклицательным знаком отмечаются серверы безопасности с отсутствующими или некорректными лицензиями на использование компонентов;<br>• красным крестом отмечаются серверы безопасности или агенты, не найденные в домене, но присутствующие в структуре AD. Например, если эти компоненты были некорректно удалены. Такие объекты следует удалить вручную — см. стр. 10, 11;<br>• пиктограмма  обозначает сервер безопасности, не выведенный из подчинения удаленного сервера безопасности другого домена. Сервер, обозначенный такой пиктограммой, необходимо сделать корневым — см. стр. 9. |
| **Окно "Палитра объектов"** |
| Предназначено для отображения списка объектов, доступных для подчинения серверу безопасности, который выбран в окне структуры (описание процедур подчинения объектов содержится на стр. 9 и стр. 10).<br>Для поиска объекта в структуре сети вызовите в окне "Палитра объектов" контекстное меню нужного объекта и активируйте команду "Синхронизировать". Программа выделит искомый объект в окне структуры |
| **Область свойств объектов** |
| Область предназначена для отображения списка подчиненных объектов и настройки параметров объекта, выбранного в окне структуры.<br>Параметры группируются в диалогах, переключение между которыми осуществляется с помощью закладок в верхней части области. Порядок следования диалогов можно изменить путем перемещения отдельных закладок с помощью мыши |

# Глава 2
# Редактирование структуры и настройка параметров

## Редактирование структуры ОУ

Для редактирования структуры оперативного управления программа предоставляет следующие возможности:

- изменение списка объектов, подчиненных серверу безопасности;
- добавление и удаление объектов структуры ОУ.

Все изменения структуры ОУ применяются непосредственно при выполнении операций. Дополнительные действия по сохранению изменений не требуются, и эти изменения отменить нельзя.

Изменения структуры ОУ сохраняются в Active Directory от имени пользователя, открывшего сеанс работы с программой. Если пользователю не предоставлены права на изменение AD, для сохранения изменений программа предложит ввести учетные данные пользователя, имеющего необходимые права.

### Операции с серверами безопасности

Серверы безопасности обозначаются пиктограммой, показанной слева. При выполнении операций с серверами безопасности объекты изменяют свое положение в структуре ОУ.

#### Подчинение и вывод из подчинения

Операцию подчинения серверов можно выполнять в окне "Палитра объектов" или в дереве структуры ОУ стандартным методом Drag-and-Drop.

**Для подчинения сервера безопасности:**

1. В дереве структуры ОУ выберите сервер безопасности, которому нужно подчинить другие серверы безопасности.

   В окне "Палитра объектов" отобразится список свободных серверов и агентов в доменах.

2. Отметьте нужные серверы безопасности и нажмите кнопку "Добавить" на панели инструментов в верхней части окна "Палитра объектов".

Программа переместит сервер (серверы) в папку "Подчиненные СБ" родительского сервера безопасности. Если подчиненный сервер находится в другом домене, перемещение не осуществляется, а в папке "Подчиненные СБ" будет создана ссылка на подчиненный сервер.

Ссылка на подчиненный сервер другого домена обозначается специальной пиктограммой и используется для переходов между подчиненным и родительским серверами в структуре объектов. Для перехода от родительского сервера к подчиненному выберите нужную ссылку и активируйте команду "Действия | Перейти к серверу". Чтобы перейти от подчиненного сервера к родительскому, выберите нужный СБ и активируйте команду "Действия | Перейти к прокси".

**Для вывода сервера безопасности из подчинения:**

1. В дереве структуры ОУ выберите подчиненный сервер безопасности:
   - если родительский и подчиненный серверы находятся в одном домене — в папке "Подчиненные СБ" родительского сервера;
   - если родительский и подчиненный серверы находятся в разных доменах — в папке "Серверы безопасности" того домена, в котором находится подчиненный сервер.
2. Активируйте команду "Действия | Сделать корневым".

В случае если родительский и подчиненный серверы находятся в одном домене, программа переместит сервер в папку "Серверы безопасности" домена.

### Добавление и удаление сервера безопасности

При установке в системе нового сервера безопасности соответствующий ему объект добавляется в структуру оперативного управления автоматически и также автоматически удаляется из структуры ОУ после штатного удаления программного обеспечения этого сервера. В тех случаях, когда добавление или удаление объекта СБ не было выполнено автоматически, эти действия выполняются вручную.

**Для добавления сервера безопасности в структуру ОУ:**

1. В дереве структуры ОУ перейдите к домену, на компьютере которого установлен СБ, и выберите папку "Серверы безопасности".
2. Активируйте команду "Действия | Добавить сервер безопасности".

   На экране появится стандартный диалог ОС Windows для выбора компьютера.
3. Выберите нужный компьютер и нажмите кнопку "ОК".

> **Примечание**. Для добавляемого сервера безопасности должны быть зарегистрированы корректные лицензии и установлен действительный сертификат для соединений с сервером. При нарушении указанных условий на экране появляются соответствующие сообщения.

Новый сервер безопасности будет добавлен в папку "Серверы безопасности".

**Для удаления сервера безопасности из структуры ОУ:**

1. В дереве структуры ОУ выберите сервер, который требуется удалить.
2. Активируйте команду "Действия | Удалить сервер безопасности" и подтвердите удаление в появившемся диалоге запроса.

## Операции с агентами ОУ

Агенты оперативного управления обозначаются пиктограммой, показанной слева. При выполнении операций с агентами объекты изменяют свое положение в структуре ОУ.

### Подчинение и вывод из подчинения

Все агенты (защищаемые компьютеры), представленные в структуре ОУ, должны быть подчинены серверам безопасности. Агенты, подчиненные серверу безопасности, отображаются в папке "Управляемые РС". Если агент не подчинен какому-либо СБ, выполнение задач оперативного управления и аудита для него невозможно.

Количество подчиненных серверу безопасности агентов ограничивается лицензиями. Не допускается подчинение агента серверу, если на сервере отсутствует или исчерпана соответствующая лицензия. При выводе агента из подчинения лицензия высвобождается на сервере.

> Сведения о лицензиях сервера безопасности можно получить в диалоге "Лицензии" (см. стр. 16).

Операцию подчинения агентов можно выполнять в окне "Палитра объектов" или в дереве структуры ОУ стандартным методом Drag-and-Drop.

**Для подчинения агента серверу безопасности:**

1. В дереве структуры ОУ выберите сервер безопасности, которому необходимо подчинить агентов.

   В окне "Палитра объектов" отобразится список свободных серверов и агентов из того же домена, в котором находится выбранный сервер.
2. Отметьте нужных агентов и нажмите кнопку "Добавить" на панели инструментов в верхней части окна "Палитра объектов".

Программа переместит агента (агентов) в папку "Управляемые РС" выбранного сервера безопасности.

**Для вывода агента из подчинения серверу безопасности:**

1. В дереве структуры ОУ перейдите к папке "Управляемые РС" нужного сервера безопасности и выберите в ней нужного агента.
2. Активируйте команду "Действия | Сделать свободным".

### Добавление и удаление агентов

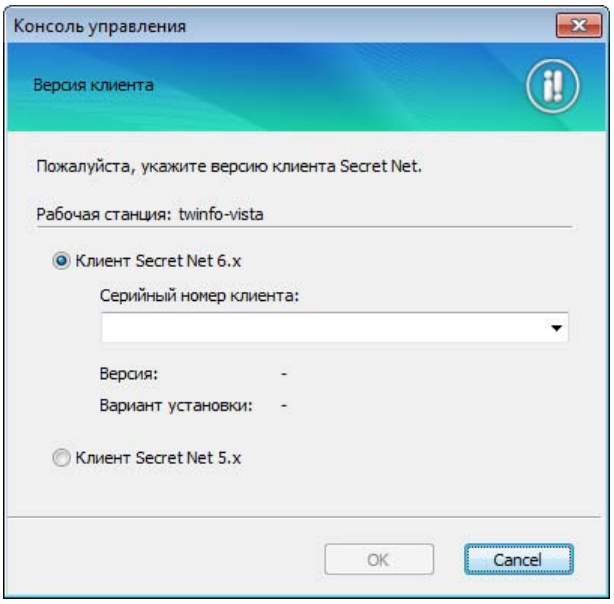
При установке или удалении программного обеспечения клиента системы Secret Net 6 структура оперативного управления корректируется автоматически. Программа конфигурирования предоставляет возможность добавлять и удалять агентов вручную. Эти процедуры используются в случаях, если корректировка структуры не была выполнена автоматически.

**Для добавления агента в структуру ОУ:**

1. В дереве структуры ОУ перейдите к домену, на компьютере которого установлено ПО клиента, и выберите папку "Свободные PC".
2. Активируйте команду "Действия | Добавить свободную рабочую станцию".

   На экране появится стандартный диалог ОС Windows для выбора компьютера.
3. Выберите нужный компьютер и нажмите кнопку "ОК".

   На экране появится следующий диалог:




4. В зависимости от установленной (или планируемой для установки) на компьютере версии клиентского ПО системы защиты выполните соответствующие действия:
   - для клиентского ПО версий 6.1 и выше — отметьте поле "Клиент Secret Net 6.x" и введите серийный номер клиента, содержащий лицензию на использование ПО текущей версии;
   - для клиентского ПО версий 5.0 или 5.1 — отметьте поле "Клиент Secret Net 5.x".
5. Нажмите кнопку "ОК".

Новый агент будет добавлен в папку "Свободные PC".

**Для удаления агента из структуры ОУ:**

1. В дереве структуры ОУ выберите агента, которого требуется удалить.
2. Активируйте команду "Действия | Удалить рабочую станцию" и подтвердите удаление в окне запроса.

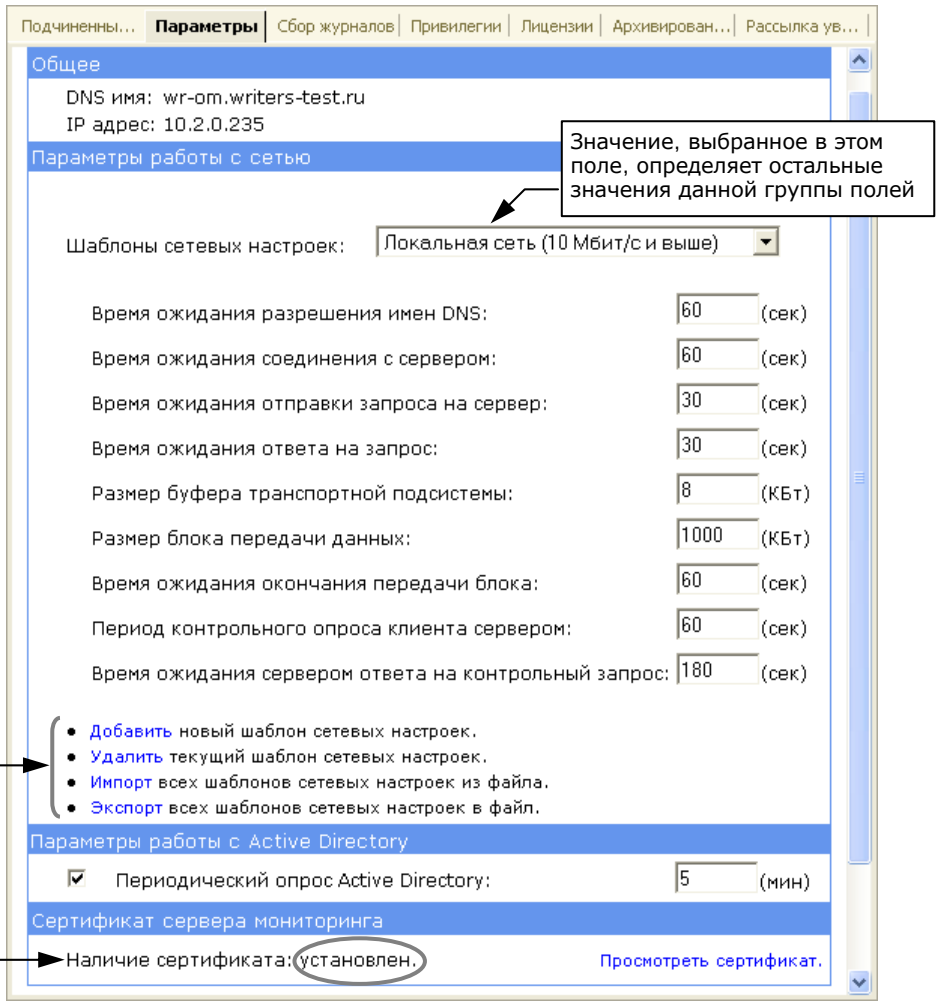
# Настройка параметров сервера безопасности

Настройка параметров осуществляется в соответствующих диалогах области свойств объектов.

## Общие параметры

**Для настройки общих параметров:**

1. Выберите сервер безопасности и в окне свойств выберите диалог "Параметры".




Диалог содержит общие сведения о компьютере сервера безопасности (имя и IP-адрес компьютера) и настраиваемые параметры СБ.

2. Укажите необходимые значения параметров:

| **Шаблоны сетевых настроек** |
|---|
| Выберите нужный шаблон для настройки параметров сетевого взаимодействия. Значения остальным полям группы присваиваются автоматически (описание параметров приведено на стр. 25). При необходимости значения можно отредактировать вручную.<br>Эти параметры используются при установке сетевого соединения данного СБ с его родительским сервером. Если параметры не заданы (имеют нулевые значения), связь с родительским сервером не будет устанавливаться. Для корневого СБ настройка параметров сетевого взаимодействия не требуется.<br>Программа позволяет управлять шаблонами настройки параметров (см. ниже) |
| **Периодический опрос Active Directory** |
| Установите отметку, чтобы включить на сервере режим периодического запроса сведений об изменениях в AD. Это позволит поддерживать настройки сервера в актуальном состоянии. Периодичность выполнения запросов указывается в поле справа.<br>Следует помнить, что не все данные повторно запрашиваются из AD. Информация о лицензиях и привилегиях считывается только при запуске сервера |

| Наличие сертификата |
| --- |
| Обратите внимание на значение этого поля — перед установкой отношений подчиненности с агентами необходимо установить сертификат. Если срок действия установленного сертификата подходит к концу или истек, в данном поле выводится предупреждение о необходимости установки нового сертификата.<br>Для получения сведений о сертификате сервера безопасности, хранящемся в Active Directory, активируйте ссылку "Просмотреть сертификат" |

### Управление шаблонами настройки параметров

По умолчанию список поля "Шаблоны сетевых настроек" содержит встроенные шаблоны. В этих шаблонах хранятся оптимальные значения параметров сетевого взаимодействия для соответствующих условий передачи данных. Если значения параметров заданы вручную и не совпадают ни с одним из шаблонов, в поле "Шаблоны сетевых настроек" отображается значение "<Нет>".

Программа позволяет расширить список используемых шаблонов. Управление списком шаблонов осуществляется с помощью ссылок, расположенных в нижней части группы полей "Параметры работы с сетью".

| Ссылка | Описание |
| --- | --- |
| **Добавить** | Добавить новый шаблон в список. Перед добавлением необходимо настроить параметры сетевого взаимодействия. При добавлении указывается уникальное имя шаблона, которое не должно совпадать с именами имеющихся шаблонов.<br>В новом шаблоне будут сохранены текущие значения параметров. В дальнейшем значения параметров шаблона изменению не подлежат |
| **Удалить** | Удалить выбранный шаблон из списка (невозможно удаление встроенных шаблонов) |
| **Импорт** | Загрузить конфигурацию шаблонов из xml-файла |
| **Экспорт** | Сохранить текущую конфигурацию шаблонов в xml-файле |

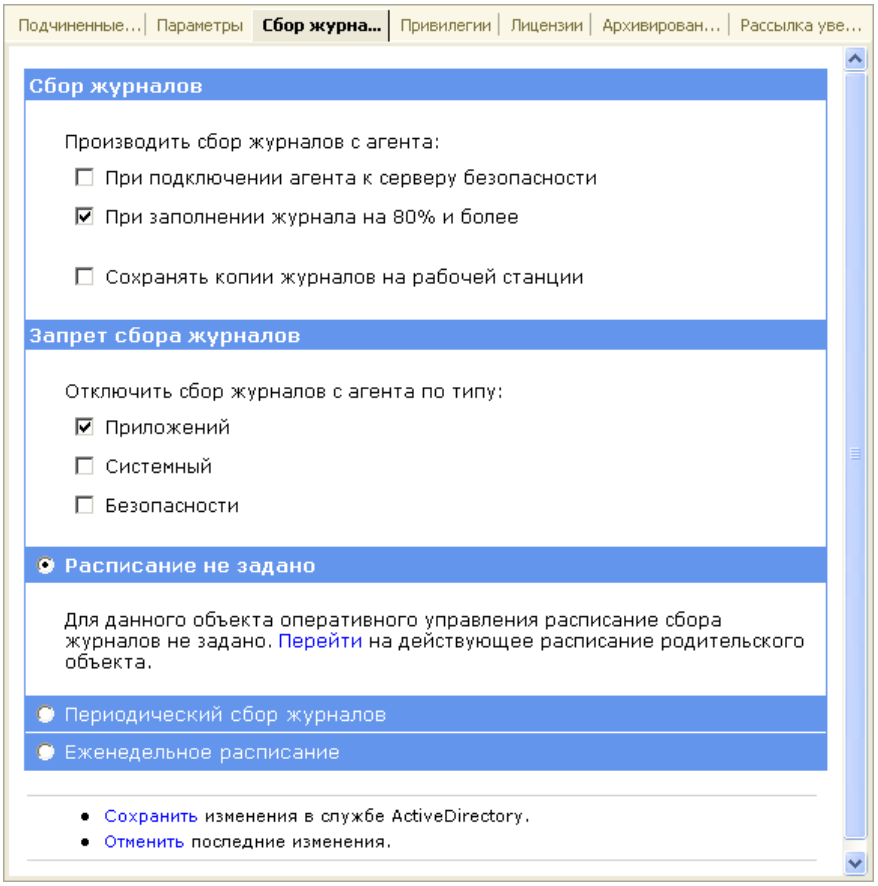
Текущая конфигурация шаблонов загружается в следующих сеансах работы пользователя с программой автоматически.

## Параметры передачи журналов агентами

Параметры, заданные для сервера безопасности, определяют работу механизма передачи журналов всех защищаемых компьютеров, подчиненных данному серверу. Предоставляется возможность индивидуальной настройки параметров для агентов (см. стр. 21). При этом если на агенте задано расписание передачи журналов, то параметры расписания, заданные для сервера, не действуют на данном агенте.

**Для настройки параметров передачи журналов:**

1. Выберите в структуре ОУ сервер безопасности и в окне свойств выберите диалог "Сбор журналов".




2. Настройте базовые параметры сбора журналов:
   - если запуск процесса должен выполняться при каждом подключении агентов к СБ, установите отметку в поле "При подключении агента к серверу безопасности";
   - если на сервер безопасности необходимо передавать журналы, близкие к переполнению, установите отметку в поле "При заполнении журнала на 80% и более";

     **Пояснение**. Система защиты контролирует заполнение локального журнала, если значение максимально допустимого размера этого журнала превышает 256 Кбайт. Передача осуществляется после получения подтверждения о готовности сервера. Во время пиковой загруженности сервера прием переполненного журнала откладывается.

   - если требуется оставлять на компьютерах копии содержимого локальных журналов после передачи на сервер безопасности, установите отметку в поле "Сохранять копии журналов на рабочей станции".

     **Пояснение**. Копии содержимого локальных журналов сохраняются на компьютере в виде evt-файлов в подкаталоге \LogsBackup, расположенном в каталоге установки клиента. Обработка и удаление этих файлов выполняется администратором.

     Функция создания копий журналов предусмотрена для упрощения диагностики возникающих проблем. В нормальном режиме работы данная функция должна быть отключена.

3. При необходимости отключите централизованный сбор журналов определенных типов. Для этого отметьте нужные типы журналов в группе полей "Запрет сбора журналов". Централизованный сбор можно отключить только для штатных журналов ОС Windows.

4. Если запуск процесса передачи локальных журналов должен выполняться по расписанию после подключения агентов к серверу, установите отметку в одном из следующих полей:

| **Периодический сбор журналов** |
| --- |
| Запуск процесса передачи журналов осуществляется через равные промежутки времени. Продолжительность промежутка задается в минутах, часах или днях. Режим начинает действовать с момента наступления определенной даты и времени. Чтобы указать другой момент начала действия режима, активируйте ссылку с текущим значением даты и времени и в появившемся на экране диалоге введите нужные значения. Редактирование значений в этом диалоге выполняется способом, принятым в ОС Windows |
| **Еженедельное расписание** |
| Запуск процесса передачи журналов осуществляется в моменты времени, заданные расписанием. Расписание представлено в виде таблицы, разделенной на две части. В строках таблицы перечислены дни недели, а в столбцах — часы и минуты с шагом в 30 минут. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы.<br>Действие расписания повторяется еженедельно |

Чтобы отключить режим передачи журналов по расписанию, установите отметку в поле "Расписание не задано".

**Примечание**. Параметры расписания, заданные для сервера безопасности, не применяются на агентах с индивидуально настроенными расписаниями передачи журналов (см. стр. 21).

## Привилегии для работы с программами оперативного управления

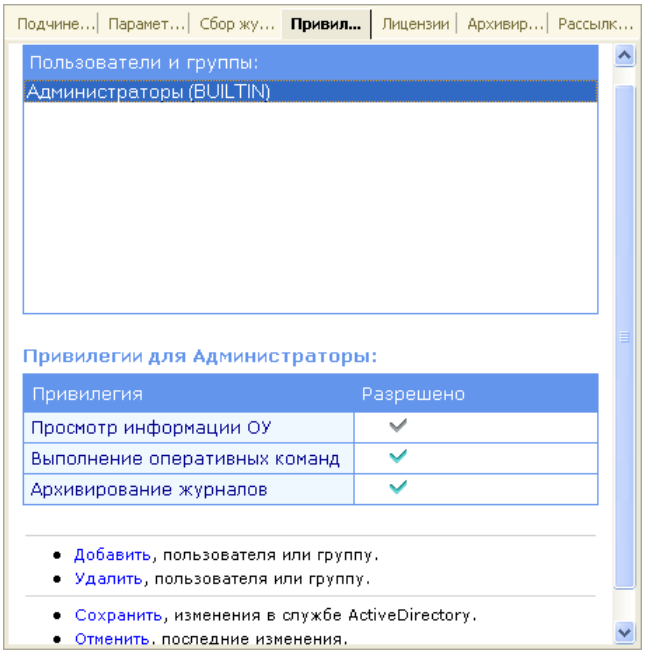
Подключение к серверу безопасности программы мониторинга и программы просмотра журналов разрешается только при наличии у пользователей привилегий:

- "Просмотр информации ОУ" — дает возможность выполнять подключение к серверу безопасности, осуществлять контроль состояния компьютеров и загружать записи журналов для просмотра;
- "Выполнение оперативных команд" — дает возможность использовать команды оперативного управления компьютерами;
- "Архивирование журналов" — дает возможность выполнять архивирование журналов и восстановление архивов.

По умолчанию все перечисленные привилегии предоставлены пользователям, входящим в группу администраторов домена.

**Для предоставления привилегий:**

1. Выберите в структуре ОУ сервер безопасности и в окне свойств выберите диалог "Привилегии".



Список "Пользователи и группы" содержит имена пользователей и групп пользователей, которым предоставлена одна или несколько из перечисленных ниже привилегий.

2. С помощью ссылок в нижней части диалога отредактируйте список пользователей и групп пользователей, которым предоставлены привилегии:
   - Чтобы добавить новый элемент в список, активируйте ссылку "Добавить". На экране появится стандартный диалог выбора объектов ОС Windows.
   - Чтобы удалить элемент из списка, выберите его в списке и активируйте ссылку "Удалить".
3. Предоставьте необходимые привилегии учетным записям. Для предоставления привилегии выберите пользователя или группу пользователей и установите отметку слева от названия привилегии в колонке "Разрешено". Удаление отметки отменяет предоставление привилегии.

**Примечание**. Привилегия "Просмотр информации ОУ" автоматически предоставляется всем пользователям и группам пользователей, добавленным в список "Пользователи и группы". Отменить действие данной привилегии нельзя — привилегия перестает действовать только после удаления учетной записи из списка "Пользователи и группы".

## Параметры лицензий на использование компонентов

В системе Secret Net 6 действуют лицензионные ограничения на использование ряда компонентов программного обеспечения. Регистрация лицензий на использование компонентов осуществляется посредством ввода серийных номеров соответствующих типов. Зарегистрированные лицензии хранятся в AD и контролируются сервером безопасности.

Для лицензирования компонентов применяются следующие типы серийных номеров:

- **Серийный номер сервера безопасности (СНС)** — содержит лицензию на использование компонента "Secret Net 6 — Сервер безопасности" определенной версии (версий). В СНС задано ограничение на максимальное количество клиентов, разрешенных для подчинения серверу безопасности;
- **Серийный номер клиента (СНК)** — содержит лицензию на использование одного или нескольких компонентов "Secret Net 6" определенной версии (версий). СНК определяет разрешенный режим функционирования компонента — сетевой или автономный. Возможности централизованной настройки и оперативного управления доступны на тех компьютерах, на которых зарегистрированы СНК с лицензиями для сетевого режима функционирования. Такие СНК дополнительно задают ограничения на количество клиентов, для которых можно использовать данный серийный номер. Ограничение действует в рамках глобального каталога, где зарегистрирован СНК. В программе конфигурирования выполняются действия только с СНК с лицензиями для сетевого режима функционирования.

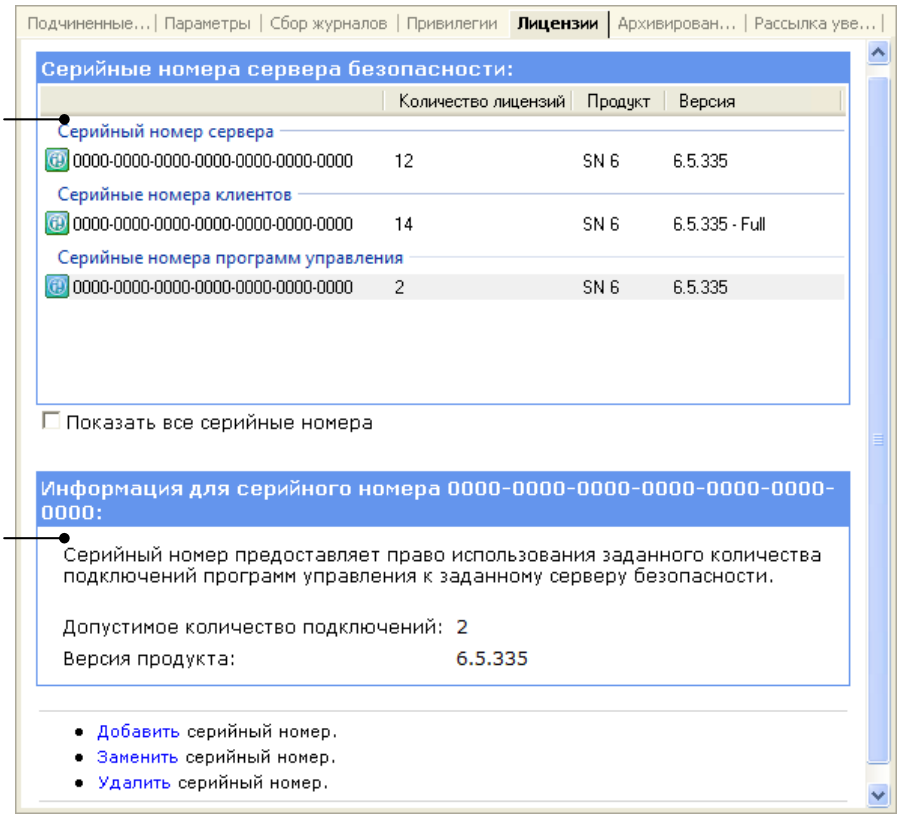
**Примечание**. Сервер безопасности текущей версии может иметь в подчинении компьютеры с установленным клиентским ПО системы защиты версий 5.0.180.4 и выше. Для этого на СБ необходимо зарегистрировать СНК, удовлетворяющий схеме лицензирования соответствующей версии СЗИ Secret Net.

- **Серийный номер средств управления (СНУ)** — содержит лицензию на использование одновременно двух или более компонентов "Secret Net 6 — Средства управления" определенной версии (версий). В лицензии заданы ограничения на количество дополнительных компьютеров, с которых возможно одновременное подключение программ "Монитор" и/или "Журналы" к СБ. Версия ПО средств оперативного управления, заданная в СНУ, должна совпадать с версией ПО СБ в СНС, в противном случае СНУ считается недействительным.

Ввод необходимых серийных номеров выполняется при установке компонентов (см. документ [ 2 ]). В процессе эксплуатации системы при необходимости можно зарегистрировать новые лицензии, а также заменить или удалить серийные номера лицензий. Операции со списком серийных номеров выполняются при настройке параметров сервера безопасности в программе конфигурирования.

**Для редактирования списка серийных номеров лицензий:**

1. Выберите в структуре ОУ сервер безопасности и в окне свойств выберите диалог "Лицензии".




Диалог содержит сведения о серийных номерах, зарегистрированных на сервере безопасности. Если обнаружено нарушение в схеме лицензирования компонентов, в диалоге отображается предупреждение об этом. Текст предупреждения выделяется красным цветом.

2. Выполните необходимые действия со списком серийных номеров. Управление списком осуществляется с помощью ссылок, расположенных в нижней части диалога.

По умолчанию в списке представлены только серийные номера, относящиеся к текущей версии системы Secret Net 6. Если на сервере безопасности зарегистрированы серийные номера предыдущих версий, для просмотра сведений об этих номерах установите отметку в поле "Показать все серийные номера".

| Ссылка | Описание |
|---|---|
| **Добавить** | Добавить в список новый серийный номер |
| **Заменить** | Заменить выбранный серийный номер новым серийным номером. При смене СНК новый серийный номер автоматически регистрируется на агентах, которые использовали предыдущий серийный номер |
| **Удалить** | Удалить выбранный серийный номер из списка |

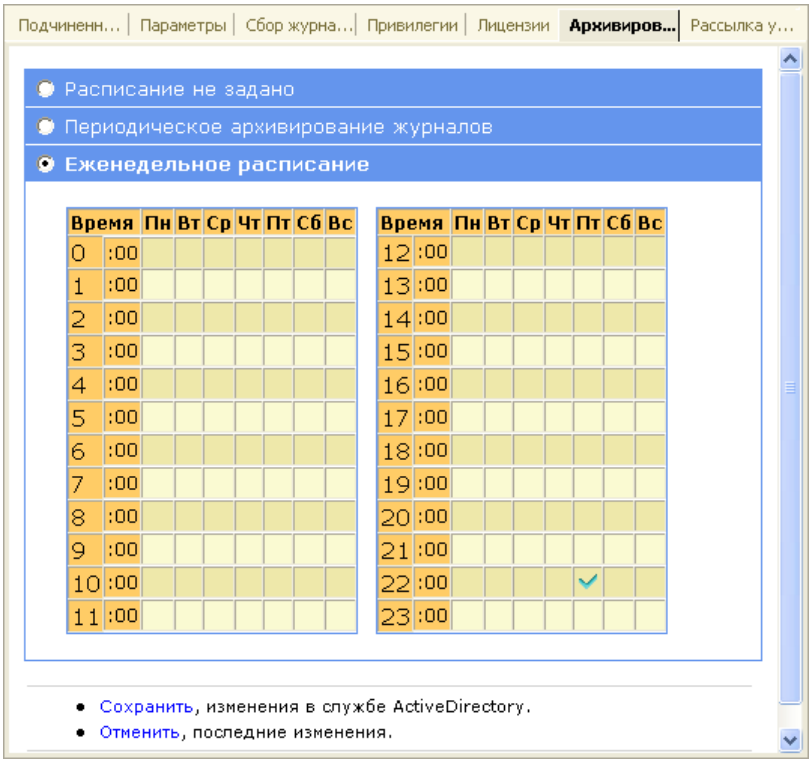
Изменения вступят в силу после перезагрузки сервера безопасности.

## Параметры архивирования журналов

Автоматическое архивирование применяется к записям журналов, которые поступили от подчиненных защищаемых компьютеров и хранятся в базе данных сервера безопасности.

**Для настройки параметров архивирования:**

1. Выберите в структуре ОУ сервер безопасности и в окне свойств выберите диалог "Архивирование журналов".




2. Настройте параметры запуска процесса архивирования. Для этого установите отметку в одном из следующих полей:

| **Периодическое архивирование журналов** |
|---|
| Запуск процесса архивирования осуществляется через равные промежутки времени. Продолжительность промежутка задается в минутах, часах или днях. Режим начинает действовать с момента наступления заданной даты и времени. Чтобы указать другой момент начала действия режима, активируйте ссылку с текущим значением даты и времени и в появившемся на экране диалоге введите нужные значения. Редактирование значений в этом диалоге выполняется способом, принятым в ОС Windows |
| **Еженедельное расписание** |
| Запуск процесса архивирования осуществляется в моменты времени, заданные расписанием. Расписание представлено в виде таблицы, разделенной на две части. В строках таблицы перечислены дни недели, а в столбцах — часы. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы.<br>Действие расписания повторяется еженедельно |

Чтобы отключить режим автоматического запуска, установите отметку в поле "Расписание не задано".

## Параметры рассылки почтовых уведомлений

При регистрации событий НСД на защищаемых компьютерах, подчиненных серверу безопасности или его подчиненным серверам, система Secret Net 6 может автоматически оповещать об этом ответственных сотрудников. Оповещение осуществляется в виде рассылаемых уведомлений по электронной почте.

Рассылка выполняется по специальным правилам, распределяющим уведомления в зависимости от источников регистрации событий. При этом система защиты мо-

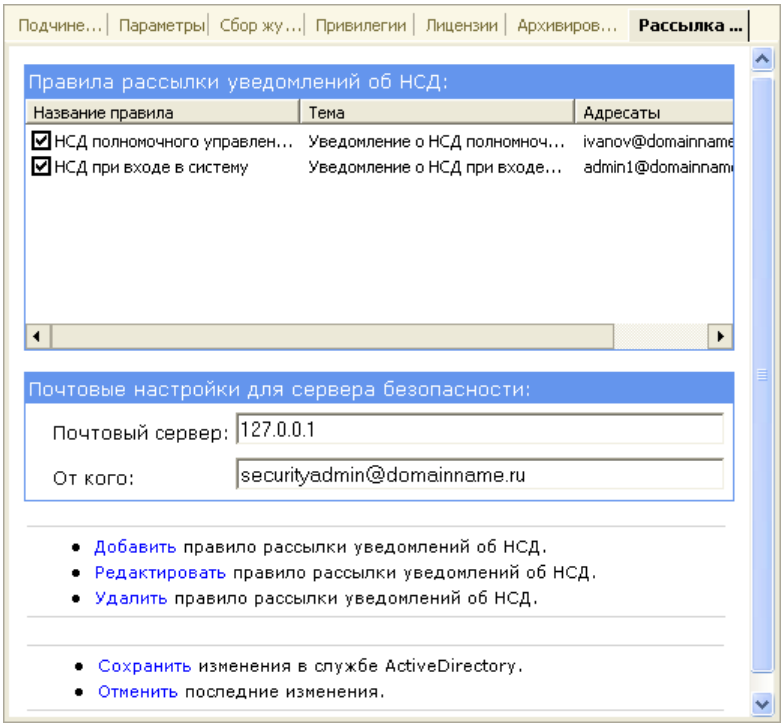
жет отслеживать события определенных категорий (только при регистрации событий на защищаемых компьютерах, подчиненных данному серверу безопасности).

Например, можно настроить рассылку уведомлений следующим образом:

- при возникновении событий НСД категории "Вход/выход" на защищаемых компьютерах, подчиненных данному серверу безопасности, уведомления направляются системному администратору;
- при возникновении событий НСД категории "Полномочное управление доступом" на компьютерах, подчиненных данному серверу безопасности и входящих в отдельное подразделение, уведомления направляются начальнику этого подразделения;
- при возникновении любого события НСД на любом защищаемом компьютере (из числа компьютеров, подчиненных данному серверу безопасности или его подчиненным серверам) уведомления направляются администратору безопасности и аудитору.

**Для настройки параметров почтовой рассылки:**

1. Выберите в структуре ОУ сервер безопасности и в окне свойств выберите диалог "Рассылка уведомлений".




2. Настройте нужным образом список правил рассылки уведомлений. Управление списком осуществляется с помощью ссылок, расположенных в нижней части диалога.

| Ссылка | Описание |
|---|---|
| **Добавить** | Добавить новое правило в список. При добавлении правила на экране появляется диалоговое окно для настройки параметров. Процедура настройки описана ниже |
| **Редактировать** | Вызвать диалоговое окно для настройки параметров выбранного правила. Процедура настройки описана ниже |
| **Удалить** | Удалить выбранный элемент из списка |

3. Укажите действующие правила (т. е. правила, по которым будет выполняться рассылка уведомлений), установив отметки слева от их названий. Для отключения действия удалите отметку.
4. В поле "Почтовый сервер" введите имя или IP-адрес почтового сервера, через который будет выполняться рассылка уведомлений.
5. В поле "От кого" введите, если требуется, адрес электронной почты, на который получатели уведомлений смогут направлять ответные сообщения.

Например, для этих целей может быть указан адрес электронной почты администратора безопасности.

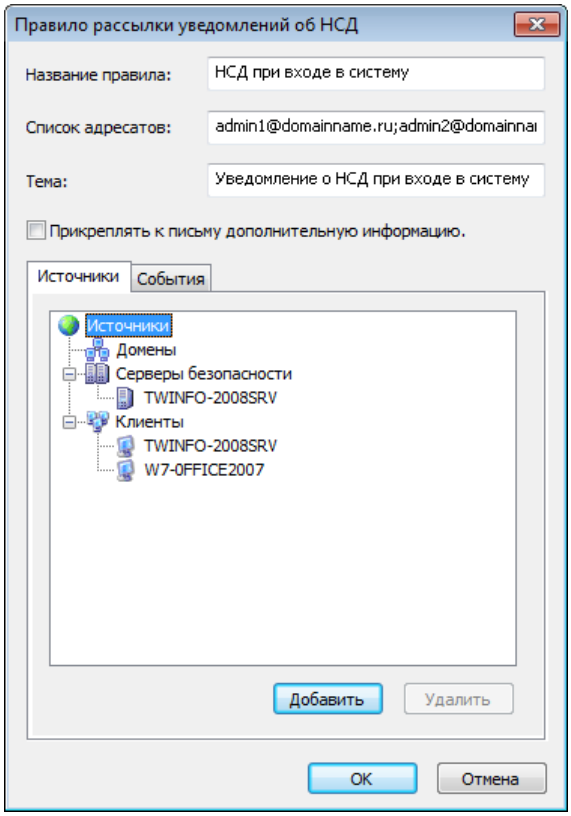
**Примечание**. Введенная строка символов должна удовлетворять требованиям, изложенным в RFC 821. В частности, запрещается использовать символы кириллицы или пробелы.

### Настройка параметров правила рассылки

При создании нового правила или при изменении существующего правила осуществляется настройка его параметров.

**Для настройки параметров правила рассылки:**

1. Вызовите диалоговое окно настройки параметров правила (см. действие **2** вышеописанной процедуры).




2. В верхней части диалогового окна укажите необходимые значения параметров:

| |
|---|
| **Название правила** |
| Содержит имя правила, отображаемое в списке правил |
| **Список адресатов** |
| Содержит список электронных адресов получателей уведомлений. Несколько адресов разделяются символом ";" |
| **Тема** |
| Содержит строку, которая будет указываться в уведомлениях в качестве темы электронного сообщения |
| **Прикреплять к письму дополнительную информацию** |
| Если поле содержит отметку, уведомления будут содержать описания событий НСД (в виде прикрепленных к письмам текстовых файлов).<br>Действие параметра распространяется только на компьютеры, подчиненные данному серверу безопасности. Описания не добавляются в уведомления о событиях НСД, произошедших на других защищаемых компьютерах |

3. В диалоге "Источники" сформируйте список объектов для контроля событий НСД. В соответствующих разделах списка могут быть указаны домены, серверы безопасности или агенты. Наличие в списке домена или сервера безопасности означает, что контроль событий НСД должен осуществляться для всех защищаемых компьютеров, относящихся, соответственно, к указанно-

му домену или серверу безопасности. Если в списке не указан ни один объект, это равносильно наличию в списке всех объектов структуры сети.

Правило рассылки действует в полном объеме только для компьютеров, непосредственно подчиненных данному серверу безопасности. События НСД на компьютерах, относящихся к подчиненным СБ, будут контролироваться, но без возможности отслеживания категорий и получения описаний событий. Адресатам будут приходить уведомления о любых событиях НСД, независимо от выбранных категорий. Все остальные защищаемые компьютеры, входящие в другие ветви подчинения серверов безопасности или свободные, не учитываются правилом рассылки, даже если эти компьютеры указаны в качестве источников.

Список объектов формируется с помощью команд на добавление или удаление элементов.

4. Перейдите к диалогу "События".

   Диалог содержит список категорий для событий НСД. Категории разделены на следующие группы:

   - "ОС Windows" — в группу входят категории событий, регистрируемых в штатном журнале безопасности ОС Windows;
   - "Secret Net" — в группу входят категории событий, регистрируемых в журнале Secret Net.

5. Отметьте нужные категории событий НСД. При регистрации таких событий на защищаемых компьютерах, подчиненных серверу безопасности, система защиты будет направлять уведомления указанным адресатам.

   Если в иерархическом списке не отмечен ни один элемент, это равносильно установке отметок для всех элементов.

6. Нажмите кнопку "ОК".

# Настройка параметров агента ОУ

Настройка параметров осуществляется в соответствующих диалогах области свойств объектов.

## Общие параметры

**Для настройки общих параметров:**

1. Выберите агента в структуре ОУ и в окне свойств выберите диалог "Параметры".

   Диалог содержит общие сведения о защищаемом компьютере (имя, IP-адрес компьютера и версия клиентского ПО) и настраиваемые параметры агента.

**Примечание**. Версия клиентского ПО определяется по СНК, который хранится в Active Directory и закреплен за данным агентом. Если в параметрах агента отображается неправильная версия (например, в случае повреждения или удаления СНК в AD или после некорректного завершения процедуры обновления версии ПО), для данного агента можно зарегистрировать СНК нужной версии. Для ввода СНК активируйте ссылку "Сменить версию".

2. Укажите необходимые значения параметров:

**Шаблоны сетевых настроек**

Выберите нужный шаблон для настройки параметров сетевого взаимодействия. Значения остальным полям группы присваиваются автоматически (описание параметров приведено на стр. 25). При необходимости значения можно отредактировать вручную.

Эти параметры используются при установке сетевого соединения данного агента с сервером безопасности, которому подчинен агент. Если параметры не заданы (имеют нулевые значения), связь с сервером не будет устанавливаться.

Программа позволяет управлять шаблонами настройки параметров (см. стр. 13)

## Параметры передачи локальных журналов

Передача локальных журналов в БД сервера безопасности может осуществляться в соответствии с параметрами, заданными для СБ, которому подчинен агент. При необходимости параметры можно настроить индивидуально для агента.

Чтобы настроить параметры, выберите агента в структуре ОУ и в окне свойств выберите диалог "Сбор журналов" (диалог присутствует только для агентов,

подчиненных серверу безопасности). Процедура выполняется так же, как при настройке параметров передачи журналов для сервера безопасности (см. стр. 13).

### Параметры лицензии на использование агента

Чтобы отобразить сведения о СНК, который присвоен агенту, выберите агента в структуре ОУ и в окне свойств выберите диалог "Лицензии" (диалог присутствует только для агентов версии 6.1 и выше). При необходимости для данного агента можно выполнить смену СНК на другой серийный номер — для этого активируйте ссылку "Заменить". Изменения вступят в силу после перезагрузки компьютера, на котором установлен агент.

## Сохранение изменений

Завершающим действием в большинстве процедур настройки параметров является сохранение или отмена изменений. Объект, параметры которого были изменены, но не сохранены в текущем сеансе работы с программой, помечается в дереве объектов "звездочкой".

Чтобы сохранить или отменить изменения, сделанные в текущем диалоге, активируйте ссылку "Сохранить" или "Отменить". Кроме того, сохранение или отмену изменений параметров можно выполнять с помощью кнопок панели инструментов в основном окне.

Параметры объектов сохраняются в Active Directory. Сохранение изменений осуществляется от имени пользователя, открывшего сеанс работы с программой. Если пользователю не предоставлены права на изменение AD, для сохранения изменений программа предложит ввести учетные данные пользователя, имеющего необходимые права.

# Глава 3
# Дополнительные средства программы

## Обновление данных

При обновлении данных программа заново выполняет загрузку сведений об объектах.

**Для обновления данных:**

1. Активируйте команду "Вид | Обновить".

   Если пользователь не имеет прав на изменение AD, на экране появится диалог запроса имени и пароля пользователя, обладающего такими правами.
2. Введите имя и пароль пользователя и нажмите кнопку "ОК".

## Сортировка компьютеров в окне структуры

Программа позволяет сортировать списки компьютеров, отображаемые в окне структуры ОУ. Сортировка осуществляется в алфавитном порядке имен компьютеров внутри соответствующих уровней иерархии. Можно применить прямой или обратный порядок сортировки. Если сортировка отключена, компьютеры располагаются в том порядке, в каком они были загружены в структуру.

**Для сортировки компьютеров:**

- Нажмите кнопку с изображением текущего режима сортировки на панели инструментов в верхней части окна структуры ОУ. В появившемся меню выберите нужный режим сортировки.

# Приложение

## Настройка элементов интерфейса

Меню и панель инструментов перемещаются в основном окне программы стандартными способами, принятыми в большинстве приложений Windows.

Для дополнительных окон предусмотрены режимы отображения в виде отдельного окна, внутри основного окна или внутри другого дополнительного окна. Режимы отображения автоматически изменяются при перемещении дополнительных окон. Для перемещения используются стандартные способы управления внутренними окнами и панелями. После перемещения окно будет зафиксировано в том режиме отображения, который соответствует положению контура окна. Если требуется зафиксировать окно в режиме отдельного окна, во время перемещения нажмите и удерживайте клавишу <Ctrl>.

Дополнительное окно можно перевести в режим автоматического сворачивания. В этом режиме окно отображается на экране, пока указатель находится в пределах окна или если оно активировано. Во всех остальных случаях происходит автоматическое сворачивание окна в кнопку, которая размещается на соответствующей границе основного окна. Чтобы развернуть свернутое окно, достаточно навести указатель мыши на кнопку этого окна. Перевод окна в режим автоматического сворачивания и возвращение исходного вида выполняются с помощью кнопки  в заголовке окна.

Состав отображаемых элементов интерфейса настраивается командами меню "Вид".

**Табл. 1. Команды меню для управления элементами интерфейса**

| Команда | Описание |
|---|---|
| **Вид \| Строка состояния** | Включает или отключает отображение строки сообщений |
| **Вид \| Панели \| Команды** | Включает или отключает отображение панели инструментов |
| **Вид \| Панели \| Заголовок** | Включает или отключает отображение информационного заголовка |
| **Вид \| Панели \| Структура сети** | Включает или отключает отображение окна структуры |
| **Вид \| Панели \| Палитра** | Включает или отключает отображение окна "Палитра объектов" |

## Навигация при работе со структурами объектов

Переходы между элементами структуры в некоторых случаях удобно выполнять с помощью стандартных команд навигации и кнопок панели инструментов.

| Команда | Кнопка | Описание |
|---|---|---|
| **Вид \| Назад** |  | Выполняет переход к предыдущему выбранному элементу структуры |
| **Вид \| Вперед** |  | Выполняет переход к следующему выбранному элементу структуры |
| **Вид \| Домой** |  | Выполняет переход к корневому элементу структуры |
| |  | Выполняет переход на один уровень вверх |

# Параметры сетевого взаимодействия

**Табл. 2. Перечень параметров сетевого взаимодействия компонентов**

| Наименование параметра, пояснение | Диапазон |
|---|---|
| **Время ожидания разрешения имен DNS**<br>Значение "0" соответствует бесконечному времени ожидания | 0–360 с |
| **Время ожидания соединения с сервером** | 1–540 с |
| **Время ожидания отправки запроса на сервер** | 1–540 с |
| **Время ожидания ответа на запрос** | 1–540 с |
| **Размер буфера транспортной подсистемы**<br>Определяет размер буфера транспортной подсистемы для приема потоковых данных. Параметр предназначен для оптимизации процесса передачи по сети потоковой информации. Его значение определяется пропускной способностью сети — чем она выше, тем больше может быть размер буфера | 8–256 Кб |
| **Размер блока передачи данных**<br>Параметр предназначен для оптимизации процесса передачи по сети потоковой информации. Его значение определяется пропускной способностью сети — чем она выше, тем больше может быть размер блока | 1–2000 Кб |
| **Время ожидания окончания передачи блока**<br>Определяет временной интервал, в течение которого ожидается подтверждение о доставке или сообщение об ошибке доставки блока. Параметр предназначен для корректного отслеживания времени жизни операций, связанных с передачей потоковых данных по сети. Определяется пропускной способностью сети — чем она выше, тем меньше может быть временной интервал. В случае уменьшения значения параметра до недопустимого уровня корректная работа транспортной подсистемы может быть нарушена. Ускорить работу транспортной подсистемы параметр не может | 1–540 с |
| **Период контрольного опроса клиента сервером**<br>Определяет промежуток времени, через который отправляется контрольный запрос. Параметр предназначен для контроля соединения. Принцип контроля основан на периодической отправке служебного запроса и получении ответа на него. В случае получения корректного ответа соединение считается работающим. При получении некорректного ответа или по истечении времени ожидания ответа (см. следующий параметр) соединение считается отключенным. При увеличении значения параметра теряется оперативность получения достоверной информации о состоянии соединения | 1–540 с |
| **Время ожидания сервером ответа на контрольный запрос**<br>Определяет максимальное время ожидания ответа на отправленный контрольный запрос. Параметр предназначен для контроля установленного соединения | 1–1080 с |

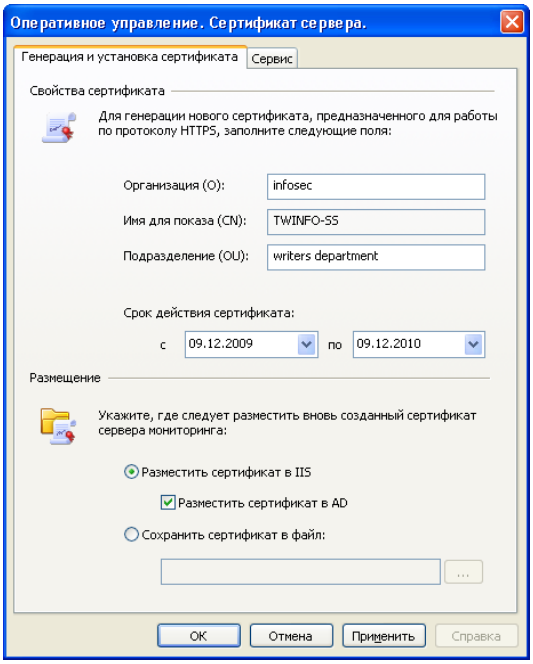
# Генерация и установка сертификата сервера безопасности

Процедура выполняется на компьютере сервера безопасности.

**Для генерации и установки нового сертификата СБ:**

1. Активируйте в главном меню Windows команду "Пуск | Все программы | Код безопасности | Secret Net | Сертификаты".

   На экране появится диалоговое окно настройки:




2. В группе полей "Свойства сертификата" укажите нужные значения.

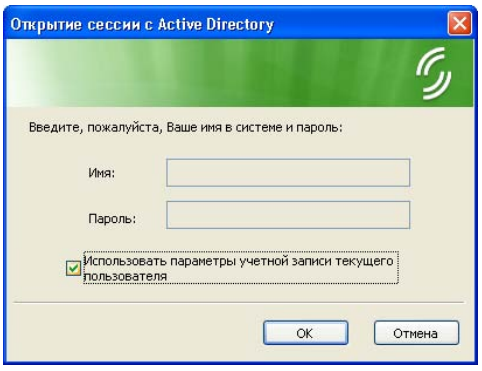
   **Примечание**. Поля "Организация" и "Подразделение" необязательны для заполнения.

3. В группе полей "Размещение" укажите места размещения сертификата и нажмите кнопку "Применить".

   При наличии в IIS установленного ранее сертификата на экране появится запрос на продолжение записи нового сертификата.

4. Нажмите кнопку "Да" в диалоге запроса.

   На экране появится диалог:




5. Укажите учетные данные пользователя, обладающего правами записи в AD, и нажмите кнопку "OK".

   **Пояснения**. Если текущий пользователь имеет права на запись в AD — отметьте поле "Использовать параметры учетной записи текущего пользователя". Если права не предоставлены — введите данные соответствующей учетной записи. По умолчанию правами на запись в AD обладают пользователи, входящие в группу Domain Admins.

   После установки нового сертификата на экране появится сообщение об этом.

# Терминологический справочник

| | |
|---|---|
| **А** | |
| **Администратор безопасности** | Лицо, ответственное за обеспечение безопасности системы, реализацию и соблюдение установленных административных мер защиты и осуществляющее постоянную организационную поддержку функционирования применяемых физических и технических средств защиты |
| **Администратор оперативного управления** | Лицо, ответственное за контроль состояния защищаемых компьютеров системы, за отслеживание в режиме реального времени нарушений, связанных с попытками несанкционированного доступа пользователей |
| **Аудит** | Систематическая, независимая и документированная ревизия, позволяющая получить обзор и провести анализ системных записей и активности системы с целью установления ее текущего состояния безопасности или степени выполнения согласованных критериев аудита |
| **Ж** | |
| **Журнал регистрации событий** | Хранилище с информацией о событиях, зарегистрированных в системе, например, попытках входа в систему |
| **З** | |
| **Защищаемый компьютер** | Компьютер с установленным клиентом системы защиты. Обеспечивает защищенную работу пользователя системы |
| **М** | |
| **Мониторинг** | Контроль работы компьютеров в режиме реального времени |
| **Н** | |
| **НСД** | Несанкционированный доступ, заключающийся в получении нарушителем доступа к ресурсу (объекту) в нарушение установленных правил разграничения доступа |
| **О** | |
| **Оперативное управление** | Незамедлительное воздействие на компьютеры с целью предотвращения попыток несанкционированного доступа |
| **С** | |
| **Сервер безопасности** | Компьютер с установленным серверным программным обеспечением системы защиты. Обеспечивает взаимодействие всех компонентов системы, сбор, обработку и передачу данных, передачу команд оперативного управления |

# Документация

| | | |
|---|---|---|
| **1** | Средство защиты информации Secret Net 6.<br>Принципы построения.<br>Руководство администратора | RU.88338853.501410.<br>007 91 1 |
| **2** | Средство защиты информации Secret Net 6.<br>Установка, обновление и удаление.<br>Руководство администратора | RU.88338853.501410.<br>007 91 2 |
| **3** | Средство защиты информации Secret Net 6. Управление.<br>Основные механизмы защиты.<br>Руководство администратора | RU.88338853.501410.<br>007 91 3 |
| **4** | Средство защиты информации Secret Net 6. Управление.<br>Полномочное управление доступом и контроль печати.<br>Руководство администратора | RU.88338853.501410.<br>007 91 4 |
| **5** | Средство защиты информации Secret Net 6.<br>Аудит.<br>Руководство администратора | RU.88338853.501410.<br>007 91 5 |
| **6** | Средство защиты информации Secret Net 6.<br>Мониторинг и оперативное управление.<br>Руководство администратора | RU.88338853.501410.<br>007 91 6 |
| **7** | Средство защиты информации Secret Net 6.<br>Конфигурирование.<br>Руководство администратора | RU.88338853.501410.<br>007 91 7 |
| **8** | Средство защиты информации Secret Net 6.<br>Аппаратные средства.<br>Руководство администратора | RU.88338853.501410.<br>007 91 8 |
| **9** | Средство защиты информации Secret Net 6.<br>Руководство пользователя | RU.88338853.501410.<br>007 92 |
| **10** | Программно-аппаратный комплекс "Соболь". Версия 2.1.<br>Руководство администратора | УВАЛ. 00300-58-01 91 |
| **11** | Программно-аппаратный комплекс "Соболь". Версия 2.1.<br>Руководство пользователя | УВАЛ. 00300-58-01 92 |
| **12** | Программно-аппаратный комплекс "Соболь". Версия 3.0.<br>Руководство администратора | RU.40308570.501410.<br>001 91 |
| **13** | Программно-аппаратный комплекс "Соболь". Версия 3.0.<br>Руководство пользователя | RU.40308570.501410.<br>001 92 |

# Предметный указатель


**А**

Агент ОУ ..... 6, 10
Архивирование журналов .... 15, 18

**И**

Интерфейс
  настройка ..... 24
  программа конфигурирования ..... 7

**Л**

Лицензии ..... 10

**Н**

НСД ..... 18

**О**

Оперативное управление ..... 15

**П**

Передача журналов ..... 13, 21
Привилегии ..... 15

**Р**

Рассылка уведомлений о НСД ..... 18

**С**

Сервер безопасности ..... 6, 9
Структура оперативного управления ..... 6, 9