КОД БЕЗОПАСНОСТИ

Средство защиты информации

Secret Net Studio

Руководство администратора

Централизованное управление, мониторинг и аудит

RU.88338853.501400.001 91 4

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

Оглавление

Список сокращений

AD	Active Directory
DNS	Domain Name System
IP	Internet Protocol
RFC	Request for Comments
БД	База данных
ОС	Операционная система
ОУ	Оперативное управление
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СБ	Сервер безопасности

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio" RU.88338853.501400.001 (далее — Secret Net Studio, система защиты, изделие). В нем содержатся сведения о работе с компонентом "Secret Net Studio — Центр управления". Перед изучением данного руководства необходимо ознакомиться с документами [**1**], [**2**].

Условные обозначения

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

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

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

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

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

- Эта пиктограмма сопровождает информацию предостерегающего характера.

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

Другие источники информации

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

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

Глава 1
Общие сведения о программе управления

Для централизованного управления защищаемыми компьютерами используется отдельно устанавливаемый компонент "Secret Net Studio — Центр управления" (далее — программа управления). Данный компонент предоставляет следующие основные возможности:

- настройка параметров защиты и управление компьютерами;
- мониторинг состояния системы;
- конфигурирование сетевой структуры системы Secret Net Studio;
- работа с централизованными журналами.

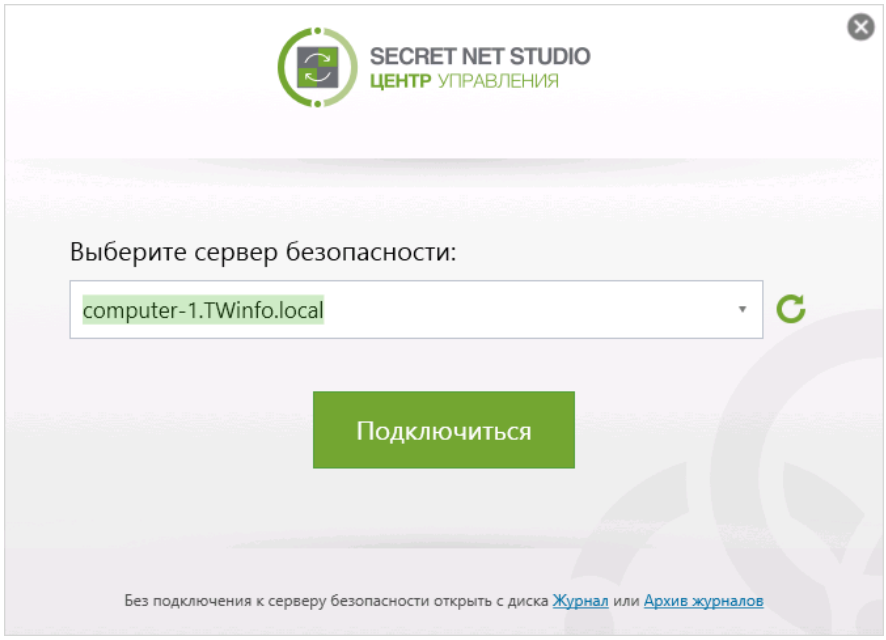
Примечание.
В составе клиентского ПО системы Secret Net Studio устанавливается вариант программы управления для работы в локальном режиме. Режим предназначен для локальной настройки параметров защиты, управления механизмами и загрузки локальных журналов данного компьютера. Возможности централизованного управления в этом режиме недоступны.
В данном документе приведены сведения об использовании программы для централизованного управления. Соответствующие функции для локального управления реализованы аналогично.

Запуск программы

Для запуска программы:

1. Выполните соответствующее действие в зависимости от версии установленной операционной системы:
   - на компьютере под управлением ОС Windows 8 или Windows Server 2012 загрузите начальный экран "Пуск" и выберите элемент "Центр управления" (относится к группе "Код Безопасности");
   - на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код Безопасности | Secret Net Studio | Центр управления".

   На экране появится стартовый диалог программы.



2. В поле "Сервер безопасности" введите или выберите имя сервера безопасности, с которым будет установлено соединение. Для получения списка

всех зарегистрированных серверов безопасности нажмите кнопку справа от поля (выполнение операции может занять длительное время).

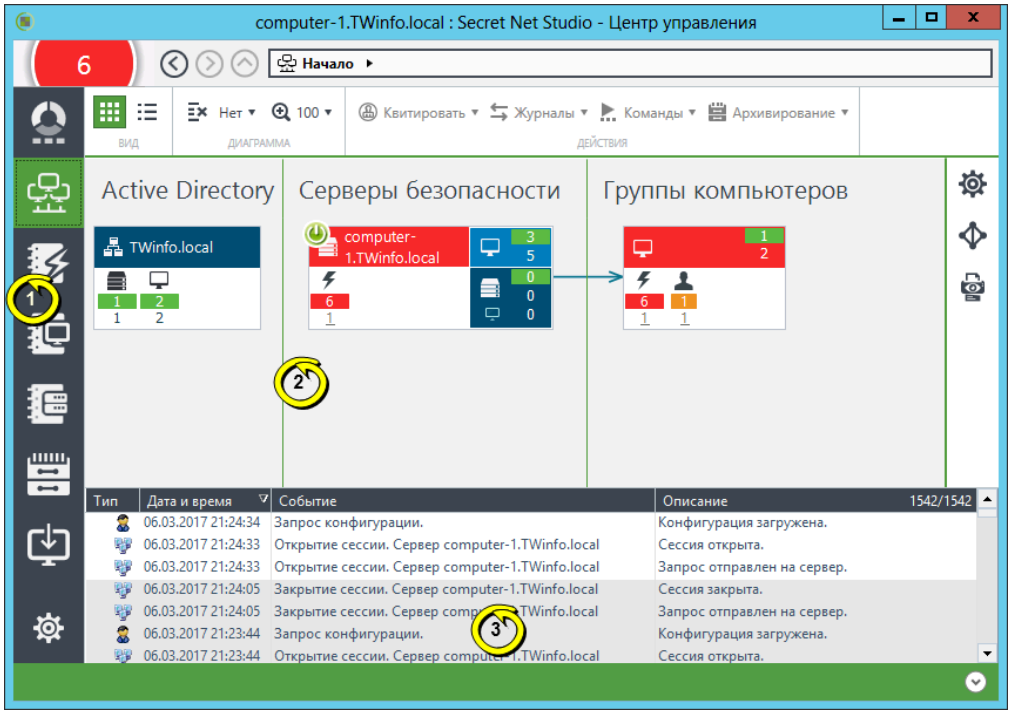
3. Нажмите кнопку "Подключиться".

Примечание.
Программа предусматривает возможность запуска без подключения к серверу безопасности — для просмотра содержимого журналов, сохраненных в файлах. Для открытия файлов используйте следующие команды в нижней части стартового диалога:

- "Журнал" — для загрузки журнала из файла;
- "Архив журналов" — для загрузки архива журналов из файла.

Интерфейс программы

Пример внешнего вида основного окна программы представлен на следующем рисунке.



Пояснение.
На рисунке обозначены: 1 — панель навигации по функциям программы; 2 — панель "Компьютеры" в режиме "Диаграмма"; 3 — панель "События системы".

Элементы интерфейса

Основное окно программы состоит из следующих частей:

- панель навигации по функциям приложения (панель навигации) — отображается в левой части основного окна и содержит ярлыки вызова панелей управления, а также средств настройки программы;
- панели управления — предназначены для отображения сведений и выполнения действий с объектами.

В программе предусмотрены следующие панели управления:

Начало
Содержит сведения о соотношении системных событий тревоги и о состоянии групп объектов управления
Компьютеры
Содержит средства администрирования и управления компьютерами

Журналы тревог
Содержит средства загрузки записей журнала событий тревоги
Журналы станций
Содержит средства загрузки записей журнала станций
Журналы сервера
Содержит средства загрузки записей журнала сервера безопасности
Архивы
Содержит средства загрузки архивов журналов
Развертывание
Содержит средства настройки автоматической установки и обновления ПО на компьютерах
События системы
Выводит сведения о событиях изменения состояния объектов

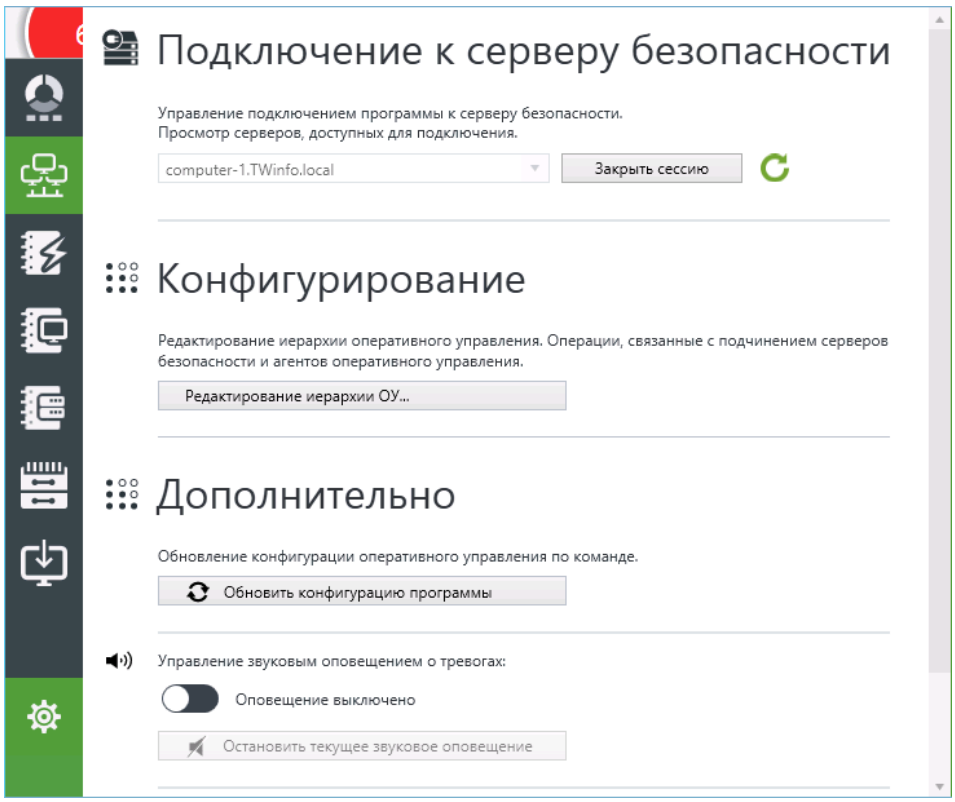
Подключение к серверу безопасности

Сеанс подключения к серверу безопасности начинается при открытии сессии. Если сессия с нужным сервером безопасности не была открыта при запуске программы или потеряно соединение с сервером, подключиться к этому серверу можно без перезапуска. При необходимости подключения к другому серверу безопасности сначала выполняется команда закрытия сессии, после чего можно открыть новую сессию с нужным сервером.

Для открытия сессии:

1. В нижней части панели навигации (слева в основном окне) нажмите кнопку "Настройки".

   На экране появится панель средств настройки и конфигурирования.



2. В разделе "Подключение к серверу безопасности" введите или выберите имя сервера безопасности, с которым будет установлено соединение. Для

получения списка всех зарегистрированных серверов безопасности нажмите кнопку "Поиск серверов безопасности", которая расположена справа.

3. Нажмите кнопку "Открыть сессию".

   После установления соединения в программу будет загружена конфигурация с выбранного сервера.

Процедура закрытия сессии выполняется аналогично. Текущая открытая сессия автоматически закрывается при завершении работы программы.

Настройка параметров работы программы

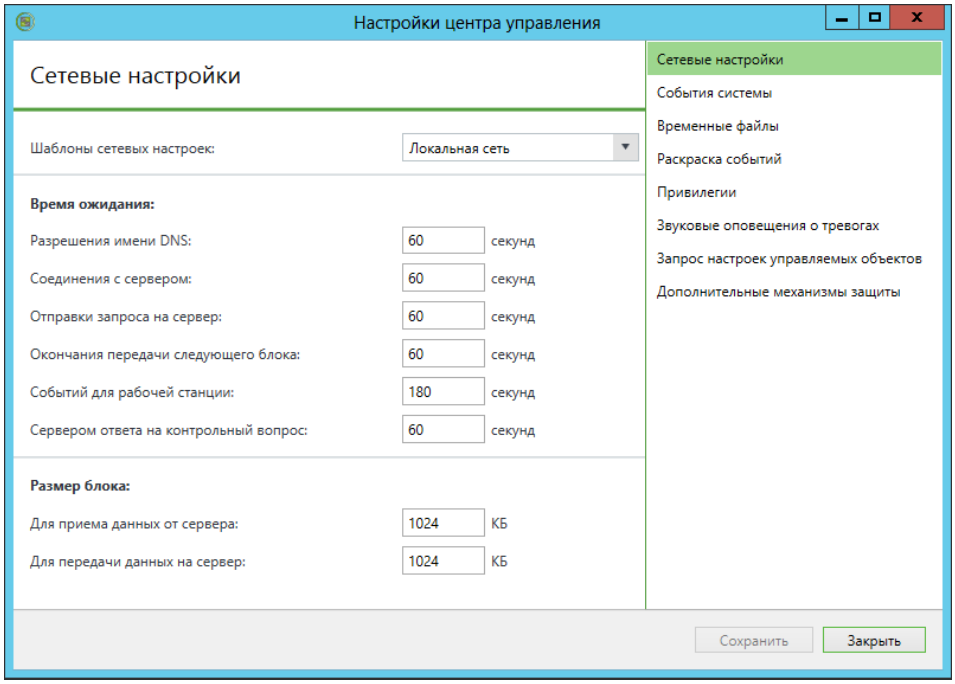
Для настройки параметров:

1. В нижней части панели навигации (слева в основном окне) нажмите кнопку "Настройки".

   На экране появится панель средств настройки и конфигурирования.

2. Выберите ссылку "Настройки центра управления".

   На экране появится одноименный диалог.



3. Укажите нужные значения для параметров. Параметры распределены по группам, которые перечислены в правой части диалога. Чтобы отобразить параметры нужной группы, выберите ее название. Описание параметров по группам см. ниже.

4. После настройки параметров нажмите кнопку "Сохранить".

Примечание.
Некоторые параметры вступают в силу со следующего запуска программы управления.

Группа параметров "Сетевые настройки"

Содержит параметры сетевого взаимодействия программы с сервером безопасности.

Поле "Шаблоны сетевых настроек"
Определяет шаблон настроек сетевого взаимодействия. Выберите нужный шаблон или настройте параметры вручную в остальных полях группы. Описание параметров см. на стр.**75**

Группа параметров "События системы"

Содержит параметры отображения данных в панели событий системы.

Поле "Количество событий в окне "События системы"
Определяет максимальное количество уведомлений, отображаемых в панели событий системы. При достижении заданного ограничения удаляется 80% старых уведомлений и в панели остается 20% последних поступивших уведомлений
Раздел "Раскраска событий"
Поля раздела определяют цвет фона строк таблицы в окне событий системы. В окне событий могут отображаться уведомления следующих типов: • "Сетевые события" — уведомления об изменении состояния объектов и наличии связи с сервером безопасности; • "Действия пользователя" — уведомления, информирующие о действиях пользователя программы управления; • "События тревог" — уведомления о регистрации событий тревоги при работе с программой в централизованном режиме. Для каждого типа уведомлений можно задать особый цвет в соответствующей ячейке. Чтобы изменить текущий цвет, нажмите кнопку в правой части ячейки и выберите нужный цвет в появившемся диалоге

Группа параметров "Временные файлы"

Содержит параметры размещения и хранения временных файлов, создаваемых программой.

Поле "Каталог для временных файлов"
Определяет путь к каталогу, в который помещаются временные файлы программы управления. Чтобы указать другой каталог, введите полный путь к нему или нажмите кнопку справа и выберите нужный каталог в диалоге выбора объектов. Путь может быть задан в явном виде или с использованием переменных окружения
Поле "Время, по истечении которого удаляются временные файлы"
Определяет период хранения временных файлов в минутах с момента последнего обращения. Временные файлы загруженных журналов позволяют ускорить повторное обращение к этим журналам без необходимости новой загрузки данных с сервера. Параметр действует в течение сеанса работы пользователя с программой. При завершении работы с программой временные файлы последнего сеанса удаляются независимо от заданного времени хранения

Группа параметров "Раскраска событий"

Содержит параметры цветового оформления записей журналов в зависимости от источников регистрации, категорий или кодов событий. Оформление осуществляется в соответствии с заданными правилами, которые определяют условия для содержимого полей в записях журналов. Описание настройки параметров см. на стр.**76**.

Группа параметров "Привилегии"

Содержит список привилегий для работы с программой управления, которые предоставлены текущему пользователю (в том числе те привилегии, которые пользователь имеет от групп).

Группа параметров "Звуковые оповещения о тревогах"

Содержит параметры звукового оповещения пользователя программы о возникновении событий тревоги. Управление режимом звукового оповещения осуществляется с помощью выключателя в соответствующем разделе панели средств настройки и конфигурирования (см. действие **1** вышеописанной процедуры).

Поле "Звуковой сигнал"
Определяет тип звукового сигнала, оповещающего о событиях тревоги. Для воспроизведения сигнала на компьютере должен быть установлен звуковой адаптер. Параметр может принимать значения: • "Тревога", "Сирена" — воспроизводится выбранный штатный звуковой сигнал программы; • *<имя_wav-файла>* — воспроизводится звуковой поток из заданного файла. Выбор файла для воспроизведения осуществляется в стандартном диалоге открытия файла. Для вызова диалога укажите значение "Выбрать..."
Поле "Количество повторов сигнала"
Определяет количество повторов звучания сигнала. Для ограничения количества повторов выберите нужное числовое значение. Если задано значение "бесконечно", сигнал будет повторяться до принудительного отключения
Поле "Интервал повторений"
Определяет паузу между повторами звукового сигнала

Группа параметров "Запрос настроек управляемых объектов"

Содержит поле, определяющее количество объектов, параметры которых после загрузки хранятся в оперативной памяти.

Группа параметров "Дополнительные механизмы защиты"

Содержит выключатели для включения/отключения средств управления дополнительными механизмами защиты, не входящими в основной состав комплекта поставки СЗИ.

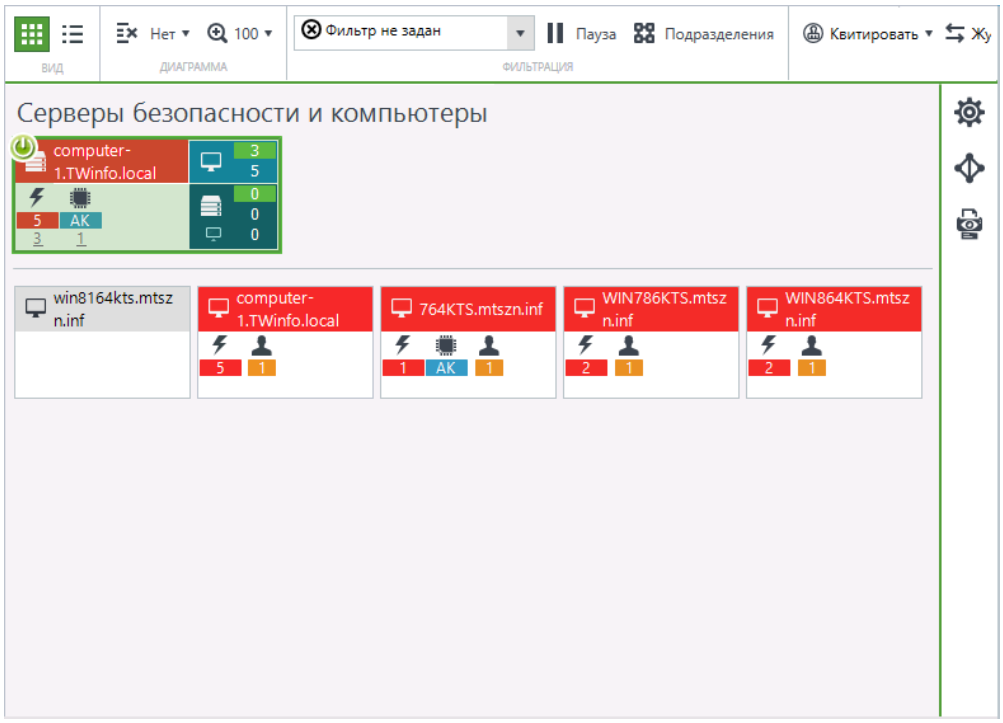
Глава 2
Структура управления

Диаграмма и список объектов управления

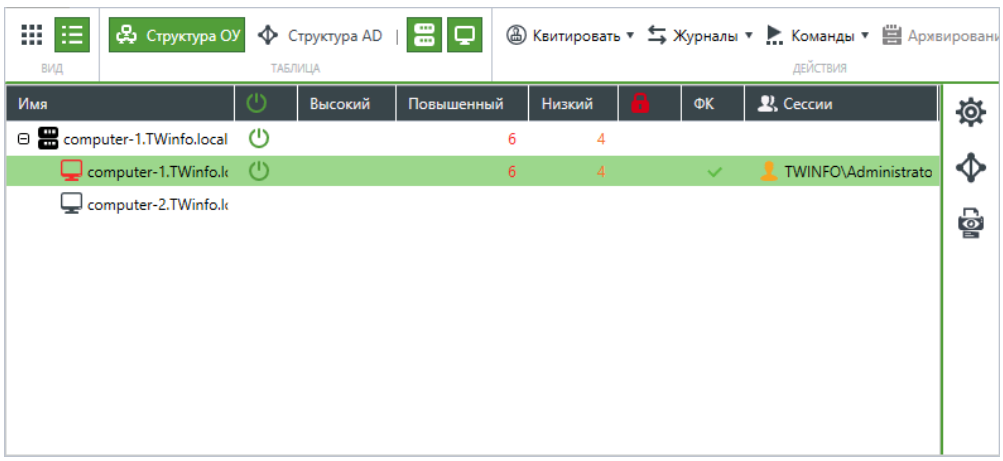
Для панели "Компьютеры" предусмотрены следующие режимы отображения объектов управления:

- "Диаграмма" — режим предназначен для отображения в графическом виде сведений о структуре объектов управления;
- "Таблица" — режим предназначен для вывода иерархического списка объектов управления в табличном виде.

Пример режима диаграммы управления представлен на следующем рисунке.



Пример табличного режима отображения представлен на следующем рисунке.



Переключение режимов отображения осуществляется с помощью кнопок "Диаграмма" и "Таблица", расположенных в верхней части панели "Компьютеры" в разделе "Вид".

Объекты структуры

Структура на диаграмме управления выводится в виде схемы элементов, соответствующих доменам, организационным подразделениям, серверам безопасности и защищаемым компьютерам. Схема базируется на структуре доменов и организационных подразделений в Active Directory.

Для отображения схемы предусмотрены следующие основные режимы:

- режим общей начальной структуры — отображаются домены, организационные подразделения, серверы безопасности и группы компьютеров, подчиненных серверам безопасности в соответствующих подразделениях;
- режим отображения списков компьютеров — отображаются выбранный сервер безопасности и списки компьютеров непосредственного подчинения.

В режиме общей начальной структуры диаграмма разделена на две части: слева отображается структура доменов и организационных подразделений Active Directory, а справа — серверы безопасности и группы компьютеров, расположенные на уровне объектов AD, к которым они относятся. В каждой из частей между элементами схемы проведены связи от родительских элементов к дочерним с указанием направления в виде стрелки. Пример диаграммы управления в режиме общей начальной структуры см. на рисунке на стр.**8**.

Для перехода в режим отображения списков компьютеров наведите указатель на нужный сервер безопасности или группу компьютеров и дважды нажмите левую кнопку мыши. Будет включен режим отображения, при котором верхняя часть диаграммы содержит выбранный сервер безопасности с его подчиненными серверами (если они есть), а ниже представлены компьютеры, непосредственно подчиненные выбранному серверу. Пример диаграммы управления в этом режиме см. на рисунке на стр.**13**. Возврат в режим общей начальной структуры осуществляется с помощью средств навигации в верхней части основного окна.

Пиктограммы объектов на диаграмме управления перечислены в следующей таблице:

Пиктограммы	Описание
	Домен или организационное подразделение
	Сервер безопасности
	Компьютер или группа компьютеров

Фильтрация объектов

Для ограничения количества отображаемых объектов можно использовать следующие возможности фильтрации:

- фильтрация объектов по принадлежности доменам и организационным подразделениям;
- фильтрация компьютеров по их состоянию;
- фильтрация по типам объектов.

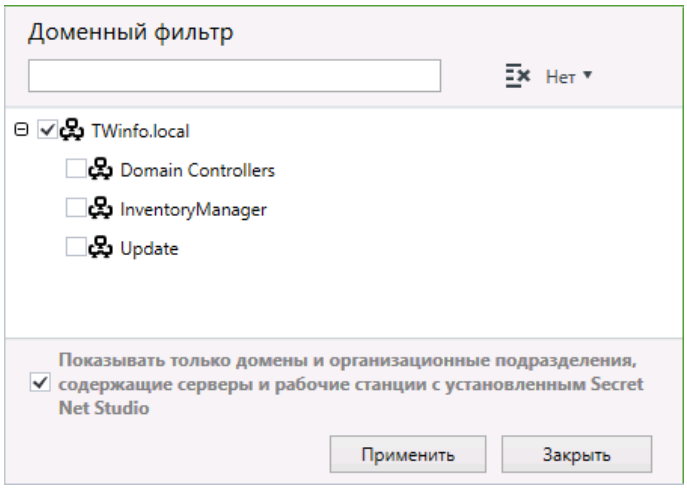
Фильтрация объектов по принадлежности доменам и организационным подразделениям

В структуре Active Directory могут присутствовать организационные подразделения или домены, объекты которых не требуется отображать в панели "Компьютеры". Например, такие организационные подразделения, в которых отсутствуют защищаемые компьютеры. При необходимости можно отключить отображение ненужных объектов с помощью фильтрации доменов и организационных подразделений. Фильтрация действует как для диаграммы управления, так и для табличного списка объектов.

Для включения отображения объектов определенных доменов и организационных подразделений:

1. В правой части панели "Компьютеры" нажмите кнопку "Фильтр AD".

   На экране появится панель "Доменный фильтр" для выбора доменов и организационных подразделений, объекты которых должны присутствовать на диаграмме.



2. При необходимости в списке можно оставить только те домены и организационные подразделения, имена которых содержат определенную строку символов. Для этого введите искомую строку в верхнем поле.
3. Для управления списком отображаемых объектов используйте кнопку сортировки в верхней части панели.
4. Отметьте нужные элементы списка. Чтобы автоматически отметить только те домены и организационные подразделения, которые содержат компьютеры с установленным ПО Secret Net Studio, установите отметку в нижней части панели.
5. Нажмите кнопку "Применить" и затем кнопку "Закрыть", чтобы свернуть панель фильтра.

   На диаграмме управления будут отображены только те объекты, которые относятся к выбранным доменам и организационным подразделениям.

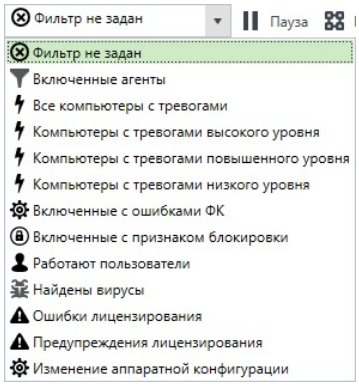
Фильтрация защищаемых компьютеров по их состоянию

В режиме отображения списков компьютеров (см. стр. 14) можно включить отображение только тех объектов, которые имеют определенный признак состояния. Например, компьютеры с обнаруженными ошибками при проверке лицензий или компьютеры с признаком тревоги. Фильтрация действует для диаграммы управления.

Для включения отображения компьютеров с определенным признаком состояния:

1. Включите режим отображения списков компьютеров. Для этого, например, подведите указатель к серверу/группе компьютеров и дважды нажмите левую кнопку мыши.
2. В верхней части панели "Компьютеры" выберите из раскрывающегося списка в разделе "Фильтрация" признак, по которому необходимо выполнить фильтрацию.

   Фрагмент панели со средствами фильтрации компьютеров представлен на следующем рисунке.



После включения фильтрации сервер безопасности в диаграмме управления обозначается специальной пиктограммой включенного фильтра. Данную пиктограмму можно использовать в качестве кнопки отключения фильтрации.

По умолчанию осуществляется динамическая фильтрация. То есть список автоматически обновляется при изменении состояния компьютеров. При необходимости можно отключить динамическую фильтрацию, чтобы зафиксировать текущий список компьютеров.

Для отключения динамической фильтрации:

- В разделе "Фильтрация" нажмите кнопку "Пауза" рядом с выбранным признаком, по которому выполнена фильтрация.

  Динамическая фильтрация будет отключена и кнопка изменит свой вид. Чтобы снова включить фильтрацию, повторно нажмите кнопку.

Фильтрация по типам объектов

При отображении списка объектов в табличном виде можно фильтровать объекты с помощью следующих кнопок, расположенных над списком в разделе "Таблица":

- "Структура ОУ" — включает представление иерархии объектов в виде дерева подчинения серверов безопасности и компьютеров (сервер подключения является корневым элементом иерархии);
- "Структура AD" — включает представление структуры домена Active Directory из компьютеров и организационных подразделений;
- "Отображение серверов" — включает и отключает отображение серверов безопасности;
- "Отображение компьютеров" — включает и отключает отображение защищаемых компьютеров.

Управление отображением объектов

Для управления отображением объектов на диаграмме управления предусмотрены следующие общие возможности:

- переходы по структуре ОУ с помощью средств навигации;
- сортировка объектов;
- масштабирование структуры.

Дополнительно в режиме отображения списков компьютеров (см. стр.**14**) можно группировать объекты в соответствии с их принадлежностью организационным подразделениям.

Переходы по структуре ОУ с помощью средств навигации

Средства навигации, расположенные в верхней части основного окна программы, могут использоваться для переходов по структуре ОУ, а также для поиска нужных объектов. Переходы по структуре осуществляются посредством выбора элементов из числа представленных на диаграмме или из списка ранее выбранных элементов (в истории переходов). Поиск объектов осуществляется по

именам при вводе искомой строки символов.

Методы работы со средствами навигации аналогичны используемым методам в стандартных приложениях ОС Windows Internet Explorer и Проводник.

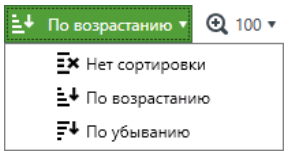
Сортировка объектов

Объекты на диаграмме можно сортировать в алфавитном порядке имен. Сортировка выполняется в прямом или обратном направлении.

Для сортировки объектов:

1. В верхней части панели "Компьютеры" в разделе "Диаграмма" раскройте меню сортировки.

   На экране появится меню выбора направления сортировки. Фрагмент панели после раскрытия меню представлен на следующем рисунке.



2. Выберите нужное направление сортировки.

   Объекты будут упорядочены в выбранном направлении.

Использование средств масштабирования диаграммы

Средства масштабирования предоставляют возможности отображения на диаграмме элементов в выбранном масштабе. За счет этого можно разместить на экране все необходимые элементы.

Для изменения масштаба отображения:

- В верхней части основного окна программы в разделе "Диаграмма" укажите нужный масштаб.

Группировка компьютеров по принадлежности организационным подразделениям

В режиме отображения списков компьютеров по умолчанию выводится общий список подчиненных компьютеров выбранного сервера безопасности. Если серверу безопасности подчинены компьютеры, входящие в различные организационные подразделения, можно включить группировку компьютеров. При включенной группировке список компьютеров разделяется на блоки, соответствующие различным подразделениям. Блоки отделяются горизонтальными линиями с указанием основных сведений о каждом блоке.

Примечание.
В режиме отображения общей начальной структуры в диаграмме всегда действует группировка компьютеров в элементы, называемые группами компьютеров. Каждый такой элемент объединяет компьютеры, подчиненные одному серверу безопасности и входящие в одно организационное подразделение. Чтобы определить, какому серверу подчинены компьютеры из группы, найдите на диаграмме родительский элемент (от которого проведена связь к этой группе) или подведите указатель к элементу группы и дважды нажмите левую кнопку мыши, чтобы перейти в режим отображения списков компьютеров.

Для включения группировки списка компьютеров:

1. Включите режим отображения списков компьютеров. Для этого используйте средства навигации для перехода к нужным объектам (см. выше) или подведите указатель к серверу/группе компьютеров и дважды нажмите левую кнопку мыши.
2. В панели управления отображением объектов нажмите кнопку "Подразделения" ("Группировка по подразделениям").

Список компьютеров будет разделен на блоки, соответствующие организационным подразделениям. Чтобы снова отключить группировку, повторно нажмите кнопку.

Структура ОУ после установки компонентов Secret Net Studio

Установку компонентов системы Secret Net Studio следует выполнять в порядке, описанном в документе [**2**]. Если при установке серверов безопасности и клиентов выполнялось их подчинение соответствующим серверам безопасности, компьютеры с этими компонентами будут включены в структуру оперативного управления. Структура ОУ считается сформированной на достаточном уровне, если все защищаемые компьютеры присутствуют в ней и подчинены серверам безопасности.

Редактирование структуры ОУ

Для реализации функций централизованного управления в составе структуры ОУ должны присутствовать все имеющиеся серверы безопасности и защищаемые компьютеры. Операции добавления объектов в структуру ОУ и исключения из нее могут выполняться автоматически при установке или удалении ПО системы Secret Net Studio на компьютерах. При необходимости в программе управления можно вручную добавить или удалить объекты в структуре. Например, для реализации автоматической установки клиентского ПО Secret Net Studio.

Процедуры редактирования структуры ОУ выполняются в специальном диалоге.

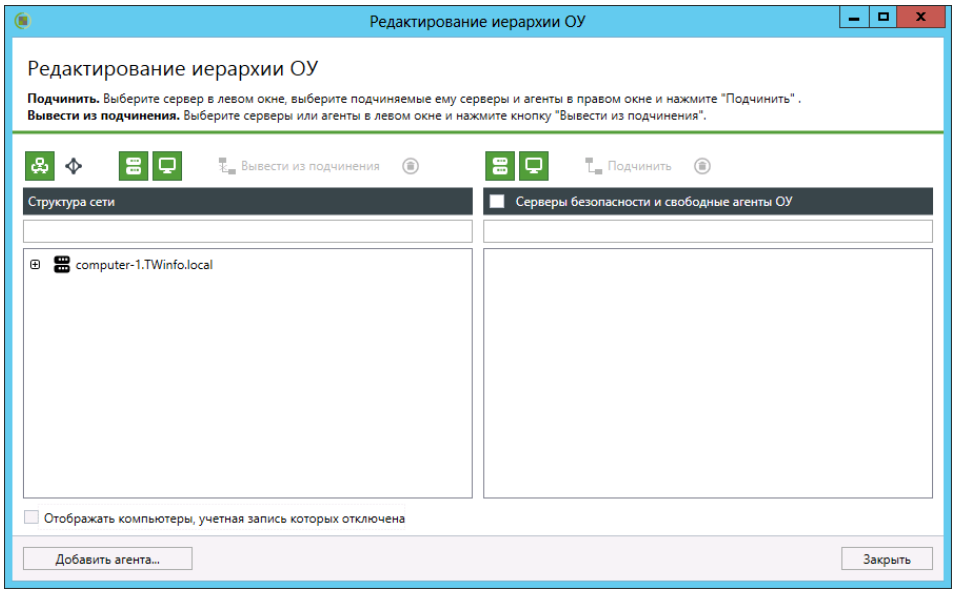
Для вызова диалога редактирования структуры ОУ:

1. В нижней части панели навигации (слева в основном окне) нажмите кнопку "Настройки".

   На экране появится панель средств настройки и конфигурирования.

2. Нажмите кнопку "Редактирование иерархии ОУ".

   На экране появится одноименный диалог.



Текущая структура объектов управления представлена в левой части диалога. В правой части — список защищаемых компьютеров и серверов безопасности, доступных для подчинения выбранному серверу.

Примечание.
При необходимости можно фильтровать списки объектов, исключая из отображения объекты определенных типов, отключенные учетные записи или не имеющие в названии заданную строку символов. Фильтрация выполняется с помощью соответствующих элементов над списками объектов (кнопки и поле ввода строки символов для поиска) и путем установки или удаления отметки в поле "Отображать компьютеры, учетная запись которых отключена".

3. Сформируйте структуру объектов (описания процедур см. ниже) и нажмите кнопку "Закрыть".

Добавление объектов в структуру ОУ

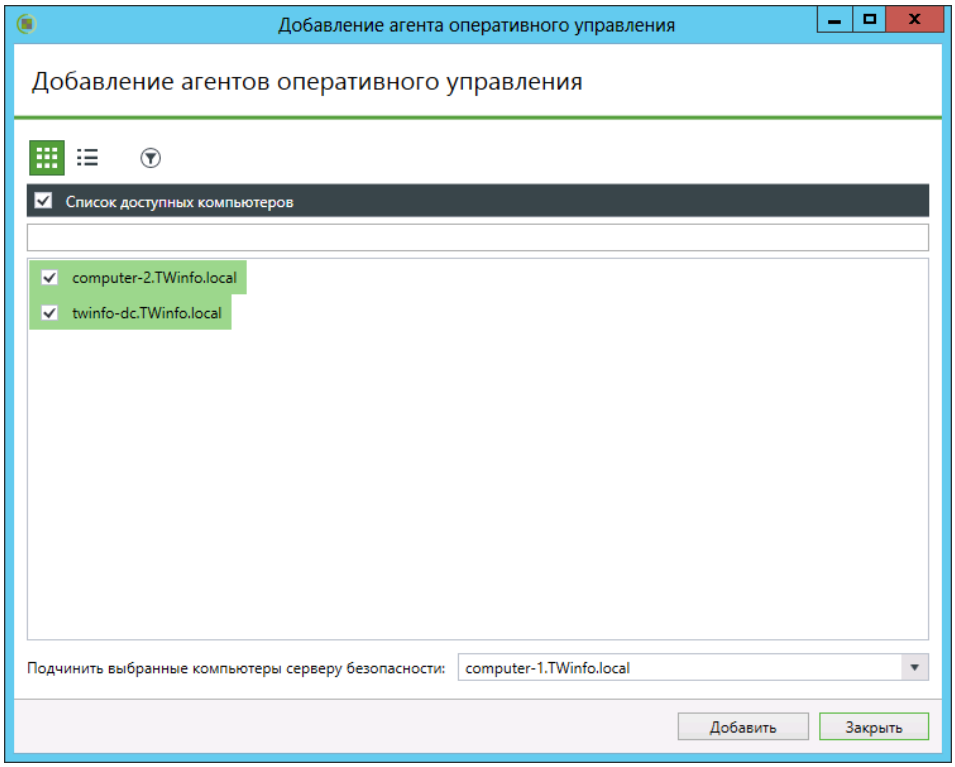
В программе управления можно добавить в качестве объекта структуры ОУ любой компьютер, зарегистрированный в Active Directory.

Если домен безопасности сформирован на базе вложенного контейнера Active Directory (в организационном подразделении), перед добавлением в структуру ОУ компьютеры следует переместить в этот контейнер, используя штатные средства администрирования AD.

Для добавления компьютеров:

1. Вызовите диалог редактирования структуры ОУ (см. стр.**18**).
2. Если добавление объектов будет выполняться с одновременным подчинением серверу безопасности — в списке "Структура сети" (слева) выберите сервер, которому они будут подчинены. Необходимо выбрать сервер в том домене безопасности, которому соответствует контейнер AD с компьютерами для добавления в структуру.
3. Нажмите кнопку "Добавить агента".

   На экране появится диалог со списком свободных компьютеров и корневых серверов, имеющихся в структуре ОУ.



Диалог содержит список компьютеров в контейнере AD, не входящих в структуру ОУ (рассматривается контейнер, на базе которого сформирован домен безопасности выбранного сервера).

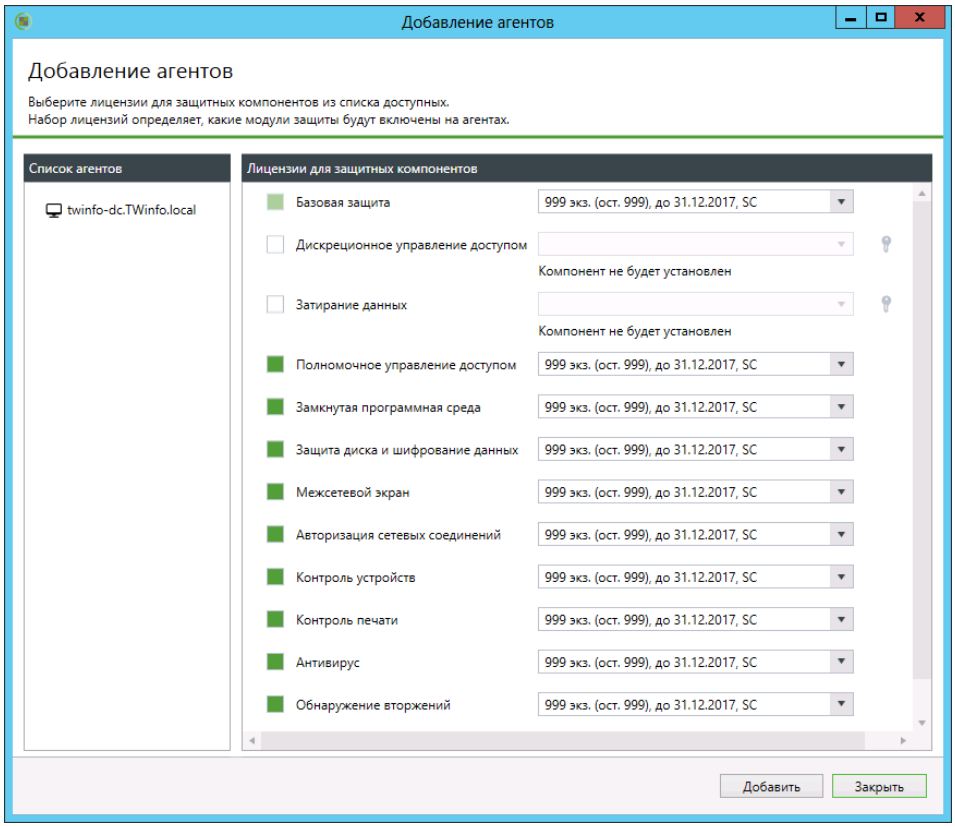
Примечание.
Список компьютеров может быть представлен в простой или табличной форме. При необходимости можно фильтровать список, исключая из отображения отключенные учетные записи и/или не имеющие в названии заданную строку символов. Средства управления списком расположены в верхней части диалога.

4. Отметьте в списке компьютеры, которые нужно добавить в структуру.
5. Чтобы подчинить серверу безопасности, выберите компьютер нужного сервера в поле "Подчинить выбранные компьютеры серверу безопасности".

Примечание.
Подчинение компьютеров можно выполнить позже (см. стр.21).

6. Нажмите кнопку "Добавить".

   На экране появится диалог для выбора лицензий на использование компонентов (подсистем) Secret Net Studio на компьютерах.



7. Отметьте подсистемы, которые будут функционировать. Для управления активацией подсистем (включение и отключение действия лицензий) используйте элементы управления, расположенные слева от названий подсистем. Если на сервере безопасности зарегистрированы различные лицензии для подсистемы, выберите нужную лицензию в раскрывающемся списке.
8. Нажмите кнопку "Добавить".

Управление отношениями подчиненности в структуре ОУ

В структуре ОУ можно изменять отношения подчинения между серверами безопасности или подчинять защищаемые компьютеры другим серверам. Переподчинение объектов (например, при пересмотре сетевой структуры) требует предварительного выполнения процедуры вывода из подчинения этих объектов текущим серверам безопасности.

Вывод объектов из подчинения

При выводе объекта из подчинения текущему серверу безопасности этот объект становится свободным. Свободный компьютер в дальнейшем необходимо

подчинить соответствующему серверу безопасности. Если из подчинения выведен сервер безопасности, этот компонент может продолжать функционировать в качестве независимого объекта управления.

Для вывода объектов из подчинения:

1. Вызовите диалог редактирования структуры ОУ (см. стр.**18**).
2. В списке "Структура сети" (слева) выберите объекты, которые необходимо вывести из подчинения.
3. Нажмите кнопку "Вывести из подчинения". В появившемся диалоге запроса подтвердите выполнение операции.

   Выбранные объекты перестанут отображаться в списке "Структура сети" и будут представлены в списке свободных объектов при выборе сервера безопасности.

Подчинение объектов серверу безопасности

Подчинение новых объектов серверу безопасности выполняется из числа свободных серверов безопасности и защищаемых компьютеров. Если нужный сервер безопасности или защищаемый компьютер отсутствует в списке свободных объектов, перед подчинением необходимо добавить объект в структуру (см. стр.**19**) или вывести его из подчинения другому серверу безопасности (см. выше).

Для подчинения объектов:

1. Вызовите диалог редактирования структуры ОУ (см. стр.**18**).
2. В списке "Структура сети" (слева) выберите сервер безопасности, в подчинение которому необходимо добавить новые объекты.

   В правой части диалога будет выведен список свободных защищаемых компьютеров и корневых серверов, имеющихся в структуре ОУ.
3. В списке объектов правой части диалога отметьте компьютеры, которые нужно подчинить выбранному серверу безопасности. Чтобы установить отметки для всех элементов списка, отметьте поле "Серверы безопасности и свободные агенты ОУ", расположенное над списком.
4. Нажмите кнопку "Подчинить".

Удаление объектов из структуры ОУ

Процедуру удаления защищаемых компьютеров и серверов безопасности из структуры ОУ в программе управления следует выполнять только в случае неработоспособности компонентов на этих компьютерах. Например, из-за некорректного завершения процедуры удаления ПО Secret Net Studio или при необходимости переноса компьютера из одного домена безопасности в другой. Если требуется временно исключить объект, следует вывести этот объект из подчинения серверу безопасности (см. стр.**20**), чтобы впоследствии заново установить отношения подчинения.

Для удаления объектов:

1. Вызовите диалог редактирования структуры ОУ (см. стр.**18**).
2. Выберите объекты для удаления.
3. Нажмите кнопку "Удаление объекта оперативного управления" над списком, в котором выбраны объекты. В появившемся диалоге запроса подтвердите выполнение операции.

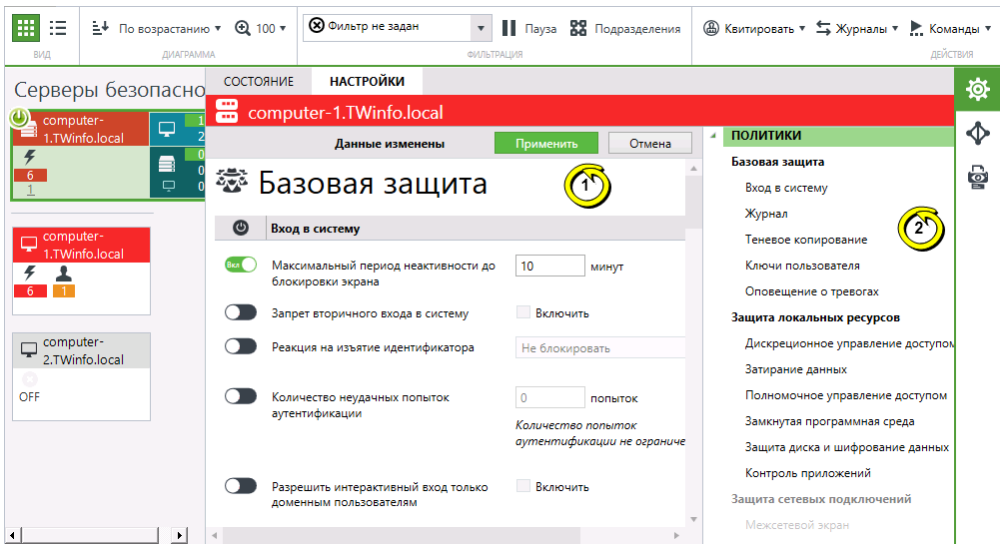
Глава 3
Настройка параметров безопасности

Списки параметров безопасности

Управление параметрами безопасности осуществляется в панели "Компьютеры" на вкладке "Настройки". Вкладка представлена в панели свойств объектов. Чтобы включить или отключить отображение панели свойств, вызовите контекстное меню объекта (например, сервера безопасности) и выберите команду "Свойства".

Для управления параметрами безопасности выбранного объекта необходимо загрузить параметры с сервера безопасности. Для этого перейдите на вкладку "Настройки" и нажмите кнопку "Загрузить настройки". Набор доступных параметров зависит от типа выбранного объекта. После загрузки параметров для их обновления используйте кнопку "Обновить" в верхней части вкладки.

Пример содержимого вкладки "Настройки" представлен на следующем рисунке.



Пояснение.
На рисунке обозначены: 1 — область отображения параметров; 2 — область оглавления.

Назначение элементов:

Область отображения параметров
Предназначена для просмотра и настройки параметров объектов. Параметры распределены по группам. Выбор группы с нужными параметрами осуществляется в области оглавления
Область оглавления
Предназначена для выбора разделов и групп для области отображения параметров. Оглавление содержит следующие разделы верхнего уровня: • "Политики" — объединяет группы параметров для настройки функционирования механизмов защиты на компьютерах; • "Регистрация событий" — объединяет группы параметров для настройки регистрации событий в локальных журналах; • "Параметры" — объединяет группы параметров для настройки и обслуживания серверов безопасности и защищаемых компьютеров

Области отображения разделены между собой передвигаемыми границами. При необходимости можно скрыть какую-либо область, передвинув ее границу. Для

просмотра данных в каждой области используются отдельные средства прокрутки.

Сохранение изменений

Сделанные изменения в программе управления вступают в силу после сохранения. Сохранение изменений возможно при активном сеансе связи с сервером безопасности. В процессе работы с программой рекомендуется регулярно сохранять сделанные изменения, чтобы избежать их потери в случае разрыва соединения с сервером.

Для сохранения изменений используйте кнопку "Применить" в верхней части вкладки. Кнопка появляется при наличии несохраненных изменений.

Уведомление о результатах выполнения действия выводится в панели событий системы.

Настройка параметров в разделах "Политики" и "Регистрация событий"

В разделах "Политики" и "Регистрация событий" представлены параметры, которые применяются на компьютерах посредством групповых политик. Параметры предназначены для настройки функционирования механизмов защиты и регистрации событий в локальных журналах.

Параметры раздела "Политики"

В состав раздела "Политики" входят следующие группы параметров:

- группы базовой защиты ("Вход в систему", "Журнал", "Теневое копирование", "Ключи пользователя", "Оповещение о тревогах") — объединяют параметры функционирования механизмов базовой защиты клиента;
- группы защиты локальных ресурсов ("Дискреционное управление доступом", "Затирание данных", "Полномочное управление доступом", "Замкнутая программная среда", "Защита диска и шифрование данных", "Контроль приложений") — объединяют параметры функционирования механизмов локальной защиты клиента;
- группы защиты сетевых подключений ("Межсетевой экран", "Авторизация сетевых соединений") — объединяют параметры функционирования механизмов сетевой защиты клиента;
- группа "Контроль устройств" — содержит параметры функционирования механизмов контроля подключения и изменения устройств и разграничения доступа к устройствам;
- группа "Контроль печати" — содержит параметры функционирования механизма контроля печати;
- группа "Антивирус" — содержит параметры функционирования антивируса;
- группа "Обнаружение вторжений" — содержит параметры функционирования механизма обнаружения и предотвращения вторжений;
- группа "Шифрование трафика" — содержит параметры функционирования механизма шифрования трафика с использованием VPN клиента;
- группа "Обновление" — содержит параметры автоматической проверки обновлений антивирусных баз.

Сведения о настройке механизмов приведены в соответствующих документах.

Если для механизма предусмотрена возможность управления регистрацией событий, можно выполнить переход к параметрам, относящимся к этому механизму, в разделе "Регистрация событий". Для перехода к соответствующей группе параметров регистрации используйте ссылку "Аудит" в правой части заголовка группы.

Параметры раздела "Регистрация событий"

Параметры раздела "Регистрация событий" предназначены для включения и отключения регистрации определенных событий в журнале Secret Net Studio. Параметры распределены по группам, которые соответствуют категориям событий.

Порядок применения параметров на компьютерах

Применение параметров, заданных в разделах "Политики" и "Регистрация событий", осуществляется на компьютерах в следующей последовательности:

1. Параметры, заданные непосредственно для компьютера (параметры локальной политики).
2. Параметры, заданные для доменов и организационных подразделений, — аналогично механизму групповых политик Windows сначала применяются параметры доменных политик и затем параметры политик для организационных подразделений.
3. Параметры, заданные для серверов безопасности, — сначала применяются параметры сервера, которому компьютеры подчинены непосредственно, а затем вышестоящих серверов по иерархии.

Таким образом, параметры политик, заданные для корневого сервера безопасности, имеют наивысший приоритет и применяются на всех компьютерах, которые находятся в непосредственном или транзитивном подчинении.

По умолчанию параметры заданы только в локальной политике. Для большинства параметров локальной политики изменение значений возможно как централизованно в программе управления, так и локально на защищаемом компьютере. При этом изменить в локальной политике значение, заданное политикой другого уровня, невозможно. Сведения о политике, определяющей значение параметра, представлены в локальной политике в колонке "Источник".

При использовании нескольких серверов безопасности, если развернута структура доменов безопасности на базе родительских и вложенных контейнеров AD (например, один домен безопасности представляет весь домен AD, а другой — вложенное организационное подразделение в этом домене AD), действуют следующие особенности применения параметров политик:

- параметры политик доменов и организационных подразделений, заданные при подключении программы к серверу в родительском домене безопасности, не применяются на защищаемых компьютерах, которые подчинены серверу другого домена безопасности во вложенном контейнере Active Directory. Для этих компьютеров параметры политик доменов/организационных подразделений необходимо задать при подключении программы к серверу безопасности во вложенном контейнере AD. То есть в каждом домене безопасности используются отдельные наборы параметров для доменов/организационных подразделений;
- параметры политик для сервера безопасности являются уникальными в пределах леса доменов безопасности и могут быть заданы при подключении программы как непосредственно к этому серверу, так и к любым серверам в других доменах безопасности (при наличии соответствующих прав). То есть параметры политик для сервера безопасности будут представлены одним набором независимо от того, как они были заданы — при подключении к этому серверу или к серверам других доменов безопасности.

Настройка параметров в разделе "Параметры"

В разделе "Параметры" представлены группы параметров, применяемых на выбранном сервере безопасности или защищаемом компьютере.

Параметры объектов могут быть представлены в следующих группах:

- "Учетная информация" — содержит сведения о компьютере, используемые для учета;
- "Сетевые настройки" — содержит параметры сетевых соединений при взаимодействии объекта с родительским сервером безопасности;
- "Сбор журналов" — содержит параметры передачи локальных журналов на сервер безопасности;
- "Архивирование журналов" — содержит параметры автоматического архивирования журналов, хранящихся в базе данных сервера безопасности;
- "Почтовая рассылка о тревогах" — содержит параметры рассылки почтовых уведомлений при регистрации событий тревоги на подчиненных компьютерах;
- "Привилегии пользователей" — содержит список учетных записей с привилегиями для работы с программой управления;
- "Фильтр тревог от подчиненных серверов" — содержит параметры фильтрации уведомлений о событиях тревоги, поступающих от серверов безопасности, которые подчинены выбранному серверу безопасности;
- "Управление трассировкой" — содержит параметры трассировки работы ПО системы Secret Net Studio (сервисная функция).

Учетная информация компьютера

Просмотр и редактирование учетной информации компьютеров осуществляются в группе "Учетная информация". Группа присутствует при выборе защищаемого компьютера.

При редактировании учетной информации можно указать уровень важности объекта и ввести данные о компьютере.

Уровень важности объекта определяет присваиваемый уровень для событий тревоги, зарегистрированных на данном компьютере. Если для объекта указан высокий уровень важности, поступающие уведомления о событиях тревоги на этом объекте будут учитываться в системе с более высоким уровнем. То есть события с уровнями тревоги "повышенный" и "низкий" будут интерпретированы системой с уровнями "высокий" и "повышенный" соответственно.

Данные о компьютере в составе учетной информации можно редактировать как в программе управления, так и локально на защищаемом компьютере. Описание процедуры локального редактирования см. в документе [**3**].

После изменения учетной информации нажмите кнопку "Применить" в верхней части вкладки "Настройки".

Параметры сетевых соединений

Управление параметрами сетевых соединений осуществляется в группе "Сетевые настройки". Группа присутствует при выборе сервера безопасности или защищаемого компьютера.

Параметры используются при установлении сетевого соединения объекта с сервером безопасности, которому подчинен данный объект. Для корневого СБ настройка данных параметров не требуется.

Сетевое взаимодействие компонентов системы Secret Net Studio дает определенную нагрузку на каналы связи. Устойчивость сетевых соединений и затрачиваемое время на передачу данных зависят от пропускной способности сети. Если пропускная способность низкая (например, при использовании

модемного соединения), возможны длительные задержки при установлении соединений и даже сбои при передаче данных.

Чтобы обеспечить нормальное функционирование системы на медленных каналах связи, администратору безопасности следует проверить и при необходимости откорректировать параметры сетевого взаимодействия объектов. Данные параметры определяют интервалы времени ожидания при выполнении сетевых запросов.

Примечание.
Снизить нагрузку на каналы связи можно и другими способами. Например, посредством изменения параметров синхронизации заданий контроля целостности, по умолчанию применяемых на компьютерах (см. документ [3]).

Для настройки параметров сетевых соединений:

1. В поле "Шаблоны сетевых настроек" выберите нужный шаблон для настройки параметров сетевого взаимодействия. Значения остальных полей изменяются автоматически в соответствии с выбранным шаблоном. При необходимости значения можно отредактировать вручную (описание параметров см. на стр.**75**).
2. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

Параметры передачи локальных журналов

Управление параметрами передачи локальных журналов осуществляется в группе "Сбор журналов". Группа присутствует при выборе сервера безопасности или защищаемого компьютера.

Параметры сбора локальных журналов, заданные для сервера безопасности, относятся ко всем компьютерам, которые подчинены данному серверу. При этом на отдельных компьютерах можно настроить индивидуальные параметры, которые будут иметь более высокий приоритет по сравнению с заданными параметрами на сервере безопасности.

Содержимое локальных журналов защищаемых компьютеров должно своевременно поступать в централизованные журналы в базе данных сервера безопасности. Длительные перерывы в отправке могут привести к переполнению локальных журналов или к чрезмерной нагрузке на сервер безопасности и каналы связи при получении больших объемов данных.

Чтобы избежать проблем, связанных с несвоевременной передачей данных, администратору безопасности следует проверить и при необходимости откорректировать параметры сбора журналов. Эти параметры задают условия для передачи локальных журналов на сервер безопасности и расписание запуска процесса передачи. Параметры следует настроить таким образом, чтобы, с одной стороны, минимизировать загруженность сетевых каналов в пиковые моменты времени (например, в начале рабочего дня или в запланированное время загрузки обновлений ПО на компьютерах) и, с другой стороны, не допустить переполнение журналов на защищаемых компьютерах (так как при переполнении локального журнала доступ пользователя к компьютеру может быть ограничен).

Для настройки параметров передачи журналов:

1. Настройте базовые параметры в группе полей "Производить сбор журналов":
   - если запуск процесса сбора журналов должен выполняться при каждом подключении компьютеров к серверу безопасности, 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 на компьютере, если заданное значение максимально допустимого размера этого журнала превышает 256 КБ. Передача осуществляется после получения подтверждения о готовности сервера безопасности. Во время пиковой загруженности сервера прием переполненного журнала откладывается.

2. При необходимости отключите централизованный сбор журналов определенных типов. Для этого удалите отметки в соответствующих полях группы "Включить в сбор следующие журналы". Централизованный сбор можно отключить только для штатных журналов ОС Windows.
3. Если требуется оставлять на компьютерах копии содержимого локальных журналов после передачи на сервер безопасности, установите отметку в поле "Сохранять копии журналов на защищаемом компьютере".

Пояснение.
Копии содержимого локальных журналов сохраняются на компьютере в виде evt-файлов в подкаталоге \OmsAgentEvtCopy, 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.

4. Если запуск процесса передачи локальных журналов подключенных компьютеров должен выполняться в определенные моменты времени, настройте расписание сбора журналов. Для этого выберите нужный режим в раскрывающемся списке поля "Расписание сбора журналов":

Периодическое
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, выберите ссылку с текущим значением даты и времени и в появившемся на экране диалоге укажите нужные значения
Еженедельное
Запуск процесса передачи журналов осуществляется в моменты времени, заданные расписанием. Расписание представлено в виде таблицы. В столбцах таблицы перечислены дни недели, а в строках — часы. Выбор времени запуска процесса осуществляется посредством выделения соответствующей ячейки таблицы. Действие расписания повторяется еженедельно

Чтобы отключить режим передачи журналов по расписанию, выберите в раскрывающемся списке значение "Не задано". Если режим отключен для защищаемого компьютера, будут применяться параметры расписания, заданные для родительского объекта. Чтобы перейти к этим параметрам, выберите ссылку "Перейти на действующее расписание родительского объекта".

Примечание.
Параметры расписания, заданные для сервера безопасности, не применяются на компьютерах с индивидуально настроенными расписаниями передачи журналов.

5. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

Параметры архивирования централизованных журналов

Управление параметрами архивирования централизованных журналов осуществляется в группе "Архивирование журналов". Группа присутствует при выборе сервера безопасности.

Параметры задают расписание автоматического архивирования централизованных журналов. Архивирование применяется к записям журналов, которые поступили от подчиненных защищаемых компьютеров и хранятся в базе данных сервера безопасности.

С целью обеспечения сохранности информации следует проводить регулярное архивирование базы данных. В некоторых версиях СУБД действуют ограничения на объем баз данных. Если размер базы превысит ограничение, поступление новой информации будет невозможно до очистки БД.

Наряду с обеспечением сохранности информации архивирование дает возможность вывести из базы данных неактуальные сведения, чтобы сократить время выполнения запросов к БД. При необходимости просмотра старых записей о событиях в программу управления можно загрузить файлы архивных копий.

Архивирование может выполняться по заданному расписанию для сервера безопасности или по специальной команде, доступной в программе управления.

Для настройки параметров архивирования:

1. Выберите в раскрывающемся списке нужный режим:

Периодическое
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, выберите ссылку с текущим значением даты и времени и в появившемся на экране диалоге укажите нужные значения
Еженедельное
Запуск процесса архивирования осуществляется в моменты времени, заданные расписанием. Расписание представлено в виде таблицы. В столбцах таблицы перечислены дни недели, а в строках — часы. Выбор времени запуска процесса осуществляется посредством выделения соответствующей ячейки таблицы. Действие расписания повторяется еженедельно

   Чтобы отключить режим автоматического запуска процесса архивирования, выберите в раскрывающемся списке значение "Не задано".
2. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

Параметры рассылки уведомлений о событиях тревоги

Управление параметрами рассылки уведомлений о событиях тревоги осуществляется в группе "Почтовая рассылка о тревогах". Группа присутствует при выборе сервера безопасности.

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

Рассылка выполняется по специальным правилам, распределяющим уведомления в зависимости от источников регистрации, категорий или кодов событий. В соответствии с заданными правилами на сервере безопасности будет выполняться обработка всех зарегистрированных событий тревоги, сведения о которых были получены сервером.

Например, можно настроить рассылку уведомлений следующим образом:

- при возникновении событий тревоги категории "Вход/выход" уведомления направляются системному администратору;
- при возникновении любого события тревоги уведомления направляются администратору безопасности и аудитору.

Для настройки параметров почтовой рассылки:

1. Сформируйте список правил рассылки уведомлений. Управление списком правил осуществляется с помощью кнопок, расположенных под списком.

Кнопка	Описание
Редактировать	Вызывает диалоговое окно для настройки параметров выбранного правила (см. ниже)
Добавить	Добавляет новое правило в список. Для нового правила выполняется настройка параметров в диалоговом окне (см. ниже)
Удалить	Удаляет выбранный элемент из списка

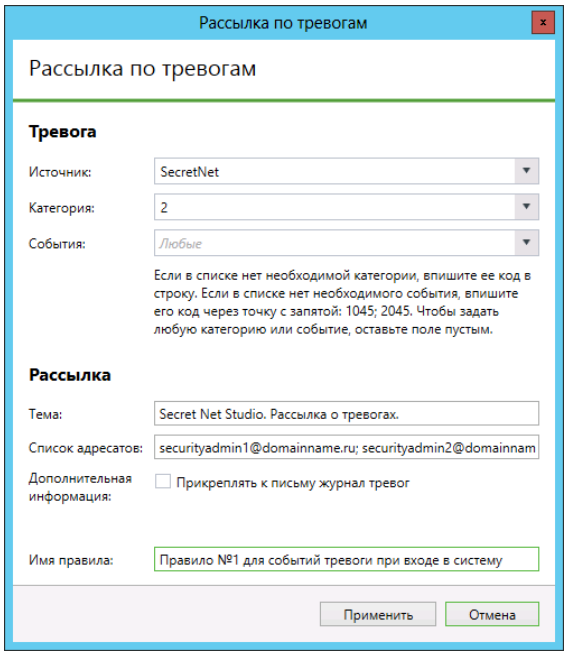
2. В поле "Почтовый сервер" введите имя или IP-адрес почтового сервера, через который будет выполняться рассылка уведомлений. В поле "Порт" укажите номер порта для доступа к серверу.
3. В поле "От кого" введите, если требуется, адрес электронной почты, на который получатели уведомлений смогут направлять 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.

4. При необходимости укажите учетные данные для доступа к почтовому серверу. Для этого установите отметку в поле "Аутентификация" и введите имя и пароль пользователя.
5. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

Настройка параметров правила рассылки

Пример диалогового окна настройки параметров правила рассылки представлен на следующем рисунке.



Для настройки параметров правила рассылки:

1. В поле "Имя правила" отредактируйте имя для элемента в списке правил.
2. В группе полей "Тревога" настройте параметры анализа событий:

Источник
Содержит имя компонента или подсистемы, которое указывается при регистрации событий в качестве источника. Выберите нужный источник
Категория

Содержит числовой код категории событий. Выберите код нужной категории из раскрывающегося списка или введите значение вручную. Список категорий, доступных для выбора, формируется в зависимости от указанного источника
События
Содержит числовые идентификаторы событий. Выберите идентификаторы нужных событий из раскрывающегося списка или введите значение вручную. Список событий, доступных для выбора, формируется в зависимости от указанной категории. Несколько идентификаторов разделяются символом ";"

Примечание.
Сведения о событиях можно получить при просмотре записей журнала событий тревоги на вкладке "Общее" (см. стр.48). Источники, коды категорий и идентификаторы событий представлены, соответственно, в следующих полях вкладки: "Источник", "Код категории" и "Событие".

3. В группе полей "Рассылка" настройте параметры рассылки уведомлений:

Тема
Содержит строку, которая будет указываться в уведомлениях в качестве темы электронного сообщения
Список адресатов
Содержит список электронных адресов получателей уведомлений. Несколько адресов разделяются символом ";"
Дополнительная информация
Если поле содержит отметку, уведомления будут содержать дополнительные сведения о событиях тревоги (в виде прикрепленных к письмам текстовых файлов). Действие параметра распространяется только на компьютеры, подчиненные данному серверу безопасности. Сведения не добавляются в уведомления о событиях тревоги, произошедших на защищаемых компьютерах транзитивного подчинения (относящихся к подчиненным серверам)

4. Нажмите кнопку "Применить".

Привилегии для работы с программой управления

Управление привилегиями пользователей для работы с программой управления осуществляется в группе "Привилегии пользователей". Группа присутствует при выборе сервера безопасности.

Пользователям и группам пользователей могут быть назначены следующие привилегии:

- "Просмотр информации" — привилегия для подключения к серверу безопасности и просмотра информации;
- "Редактирование иерархии и параметров объектов" — привилегия для редактирования конфигурации объектов и управления параметрами в разделе "Параметры";
- "Выполнение оперативных команд" — привилегия на выполнение команд оперативного управления;
- "Редактирование политик" — привилегия для управления параметрами в разделах "Политики" и "Регистрация событий";
- "Квитирование сообщений о тревогах" — привилегия на выполнение команд квитирования событий тревоги;
- "Сбор журналов по команде" — привилегия на выполнение внеочередной передачи локальных журналов компьютеров;
- "Архивирование/восстановление журналов" — привилегия на выполнение процедур архивирования или восстановления централизованных журналов.

По умолчанию все перечисленные привилегии предоставлены пользователям, входящим в группу администраторов домена безопасности. При необходимости привилегии можно назначить и другим учетным записям, исключая привилегию

"Редактирование иерархии и параметров объектов" — данная привилегия в обязательном порядке предоставляется только для группы администраторов домена безопасности.

Для предоставления привилегий:

1. Сформируйте список пользователей и групп, которым необходимо предоставить привилегии. Для добавления и удаления учетных записей используйте кнопки под списком.
2. Предоставьте необходимые привилегии учетным записям. Для предоставления привилегии выберите учетную запись и установите отметку рядом с названием привилегии. Удаление отметки отменяет предоставление привилегии.

Особенности предоставления привилегий:

- Привилегия "Просмотр информации" назначается автоматически для всех учетных записей, представленных в списке "Пользователи и группы".
- Привилегия "Редактирование иерархии и параметров объектов" не может быть предоставлена добавленным учетным записям.
- Чтобы редактировать параметры группы защиты сетевых подключений в разделе "Политики", пользователю должны быть предоставлены привилегии "Редактирование политик" и "Редактирование иерархии и параметров объектов". В связи с этим редактирование указанных параметров доступно только для пользователей группы администраторов домена безопасности.

3. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

Параметры фильтра уведомлений о событиях тревоги на подчиненных СБ

В группе "Фильтр тревог от подчиненных серверов" осуществляется управление фильтрацией событий тревоги для ограничения поступающих уведомлений от защищаемых компьютеров следующих уровней подчинения (подчиненных серверов безопасности). Группа присутствует при выборе сервера безопасности.

За счет использования фильтра можно сократить сетевой трафик и обеспечить поступление уведомлений только о важных для администратора событиях.

Примечание.

При настройке параметров политик (см. стр. 23) можно задать параметр "Фильтр тревог" в группе "Оповещение о тревогах". Этот параметр ограничивает передачу уведомлений непосредственно на защищаемых компьютерах. Таким образом, средства управления фильтрацией событий тревоги можно использовать отдельно для защищаемых компьютеров и серверов. Это позволяет, например, задать разные параметры фильтрации для компьютеров, подчиненных серверу безопасности нижнего уровня (в разделе "Политики"), и для сервера верхнего уровня (в разделе "Параметры"). В этих условиях на сервере нижнего уровня уведомления о событиях тревоги на компьютерах будут отфильтрованы по одним критериям, а на сервере верхнего уровня события от тех же компьютеров — по другим критериям. В программе управления количество поступающих уведомлений будет зависеть от того, к какому серверу выполнено подключение.

Ниже рассматривается процедура настройки фильтрации уведомлений в группе "Фильтр тревог от подчиненных серверов" раздела "Параметры". Настройка фильтрации в разделе "Политики" (группа "Оповещение о тревогах") осуществляется аналогично.

Фильтрация выполняется по списку правил. В правилах указываются условия для содержимого полей в записях журналов.

Список правил можно формировать при работе в группе "Фильтр тревог от подчиненных серверов" или с помощью средств панели событий системы (см. стр. 42).

Для настройки фильтрации событий тревоги:

1. Выберите режим функционирования фильтра. Для этого установите отметку в нужном поле:

- "Не пропускать на сервер события из правил" — фильтр не пропускает уведомления о событиях тревоги, которые удовлетворяют условиям в правилах фильтрации;
- "Пропускать на сервер только события из правил" — инверсный режим, при котором фильтр пропускает уведомления только о событиях тревоги, соответствующих правилам из списка.

Внимание!
Не включайте инверсный режим при пустом списке правил. Иначе фильтр не будет пропускать все события тревоги. Режим "Пропускать на сервер только события из правил" целесообразно использовать, если требуется пропускать поступающие уведомления об определенных событиях, а остальные — блокировать. Для этого необходимо создать правила, описывающие такие события.

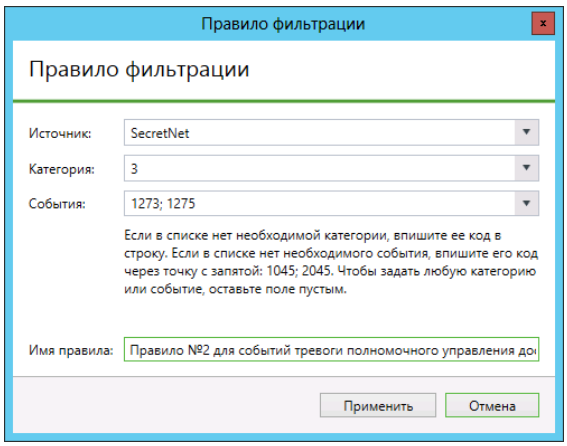
2. Сформируйте список правил фильтрации. Управление списком правил осуществляется с помощью кнопок, расположенных под списком.

Кнопка	Описание
Редактировать	Вызывает диалоговое окно для настройки параметров выбранного правила (см. ниже)
Добавить	Добавляет новое правило в список. Для нового правила выполняется настройка параметров в диалоговом окне (см. ниже)
Удалить	Удаляет выбранный элемент из списка

3. После настройки правил включите действие фильтра. Для этого удалите отметку из поля "Отключить фильтр".
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

Настройка параметров правила фильтрации

Пример диалогового окна настройки параметров правила фильтрации представлен на следующем рисунке.



Для настройки параметров правила фильтрации:

1. В поле "Имя правила" отредактируйте имя для элемента в списке правил.
2. Настройте параметры анализа событий:

Источник
Содержит имя компонента или подсистемы, которое указывается при регистрации событий в качестве источника. Выберите нужный источник
Категория
Содержит числовой код категории событий. Выберите код нужной категории из раскрывающегося списка или введите значение вручную. Список категорий, доступных для выбора, формируется в зависимости от указанного источника
События

Содержит числовые идентификаторы событий. Выберите идентификаторы нужных событий из раскрывающегося списка или введите значение вручную. Список событий, доступных для выбора, формируется в зависимости от указанной категории. Несколько идентификаторов разделяются символом ";"

Примечание.
Сведения о событиях можно получить при просмотре записей журнала событий тревоги на вкладке "Общее" (см. стр.48). Источники, коды категорий и идентификаторы событий представлены, соответственно, в следующих полях вкладки: "Источник", "Код категории" и "Событие".

3. Нажмите кнопку "Применить".

Параметры трассировки ПО системы Secret Net Studio

Программа управления предоставляет возможность централизованного включения и настройки параметров трассировки — сервисной функции для сбора информации о работе системы Secret Net Studio. При трассировке осуществляется запись в специальные файлы служебных данных о функционировании программных модулей. Эти данные необходимы для диагностики возникновения сбойных или ошибочных ситуаций.

Параметры трассировки представлены в группе "Управление трассировкой". Группа присутствует при выборе сервера безопасности или компьютера. Сведения о необходимых действиях для настройки предоставляются при обращении в отдел технической поддержки компании "Код Безопасности".

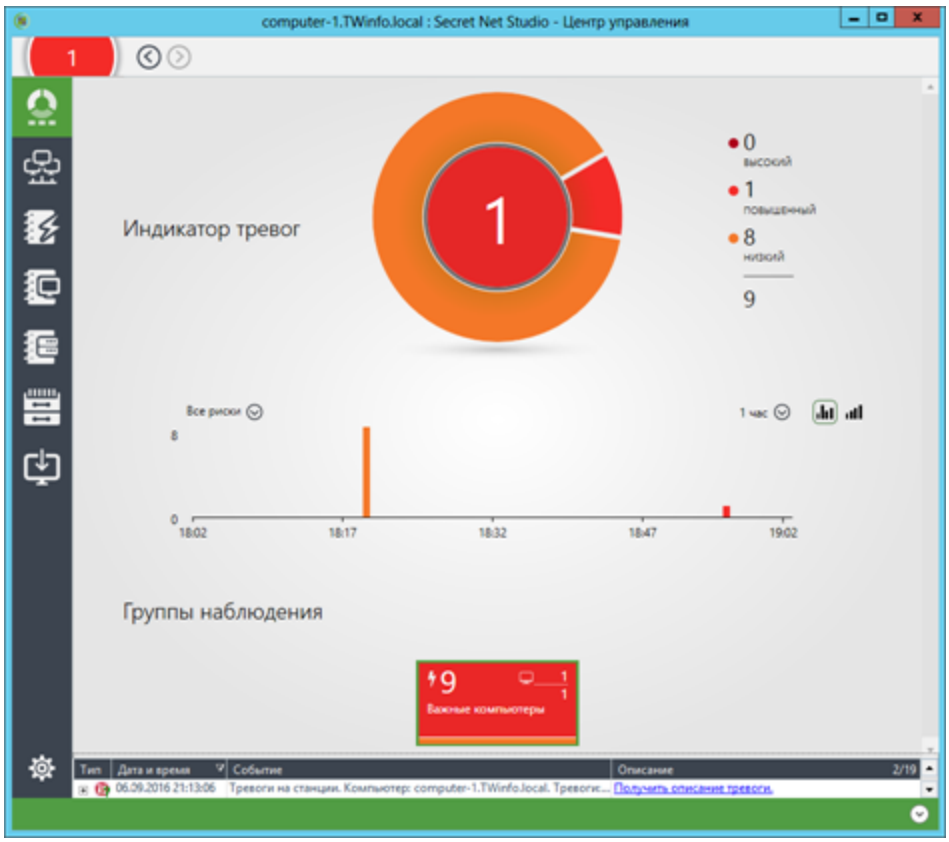
Внимание!
Не рекомендуется без необходимости включать функцию трассировки. В штатном режиме эксплуатации системы Secret Net Studio данная функция должна быть отключена, чтобы не создавать лишнюю нагрузку для компьютера.

Глава 4
Мониторинг и оперативное управление

Просмотр сведений

Общее состояние системы

Сведения об общем состоянии защищенности системы содержатся в панели "Начало", пример которой показан на следующем рисунке. Для просмотра этих сведений нажмите кнопку "Начало" вверху панели навигации (слева в основном окне).



В центре панели находится круговой индикатор тревог, который показывает состояние системы в целом. Внутренняя часть круга содержит число актуальных событий тревоги, уровень которых наивысший на данный момент в системе, и окрашена в соответствующий цвет. Внешняя часть круга является диаграммой, отражающей соотношение имеющихся событий тревоги разного уровня.

Пример.
В ситуации, показанной на рисунке, в системе имеется одно событие тревоги повышенного уровня, которое показано во внутренней части индикатора тревоги, и 8 событий тревоги низкого уровня.

Справа от индикатора перечислены все актуальные события тревоги в системе в зависимости от их уровня.

Пояснение.
- Числа на индикаторе и в перечне справа от него являются гиперссылками, нажатие на которые позволяет посмотреть информацию о данных событиях в журнале тревог.
- После квитирования такие события тревоги больше не будут показаны на этой панели.
- Подробнее об уровнях тревоги читайте на стр.40.

Ниже индикатора тревог расположен график распределения на интервале времени зарегистрированных событий тревоги. Для выбора нужного интервала используйте поле с открывающимся списком в правом верхнем углу графика, а для настройки отображения событий тревоги в зависимости от их уровня — поле с открывающимся списком в левом верхнем углу графика.

Пример.
В ситуации, показанной на рисунке, на графике столбик оранжевого цвета соответствует моменту регистрации 8 событий тревоги низкого уровня, а столбик красного цвета — моменту регистрации одного события тревоги повышенного уровня.

В нижней части панели находятся группы наблюдения, представляющие собой прямоугольные индикаторы с информацией о состоянии компьютеров, входящих в такие группы. Подробные сведения об отображаемой на индикаторах информации содержатся на стр.**35**.

Первоначально список групп наблюдения пуст. Для его формирования перейдите на панель "Компьютеры" и выберите нужный сервер безопасности или группу компьютеров. В списке компьютеров используйте в контекстном меню команды из подменю "Наблюдение" для создания новых групп и управления их составом (команды доступны в режиме "Диаграмма").

Обозначения объектов на диаграмме управления

Элементы диаграммы управления отображают основные сведения о состоянии объектов. Сведения представлены в виде пиктограмм и расположенных рядом числовых данных (например, количество событий тревоги на защищаемом компьютере или количество открытых сессий пользователей).

Пример диаграммы управления с отображаемыми сведениями представлен на рисунке на стр.**13**.

Сервер безопасности, с которым установлено соединение, обозначается специальной пиктограммой.

Для серверов безопасности и групп компьютеров числовые данные приводятся в двух или более строках: верхняя строка содержит общее количество событий/признаков на всех подчиненных компьютерах (например, сводное количество событий тревоги или количество включенных компьютеров), а нижние строки отображают количество компьютеров или подчиненных серверов безопасности с компьютерами. Некоторые числовые данные являются ссылками, которые можно использовать для фильтрации списков компьютеров. Например, чтобы отобразить в диаграмме только компьютеры с признаками тревоги.

Дополнительные сведения об объектах отображаются во всплывающих окнах, которые появляются при наведении указателя мыши на объекты.

Перечень предусмотренных пиктограмм представлен в следующей таблице:

Пиктограмма	Описание
	Включена блокировка компьютера (компьютеров). Число соответствует количеству причин блокировки. В приведенном примере — одна причина
	На компьютере (компьютерах) обнаружен вирус. Число является счетчиком зарегистрированных событий обнаружения вирусов
	На компьютере (компьютерах) зафиксированы события тревоги. Число является счетчиком зарегистрированных событий наивысшего уровня тревоги. Максимальное числовое значение счетчика — 999 событий. В случае превышения ограничения счетчик отображает значение "99+"
	На компьютере (компьютерах) зафиксированы ошибки (красный цвет пиктограммы) или предупреждения (желтый цвет) при проверке лицензий на использование компонентов системы Secret Net Studio. Число является счетчиком событий соответствующего типа

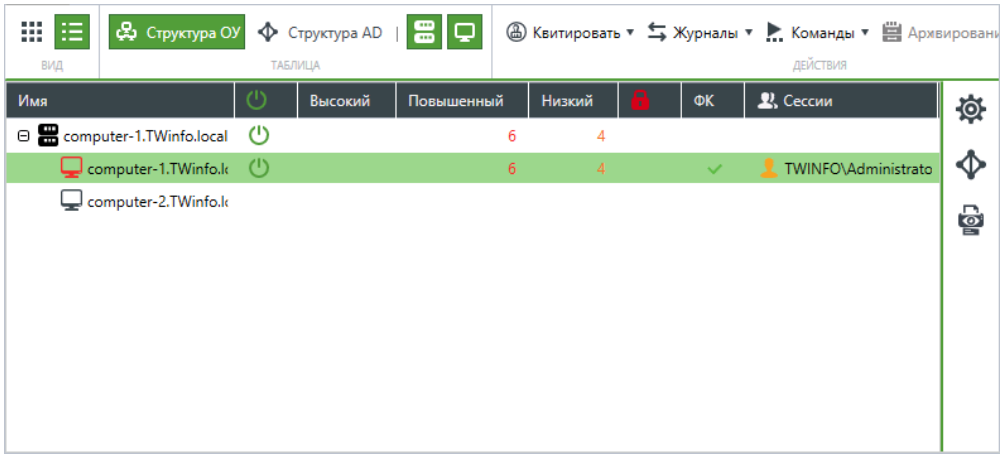
Пиктограмма	Описание
АК	На компьютере (компьютерах) зафиксировано изменение аппаратной конфигурации
1	На компьютере (компьютерах) открыты сессии работы пользователей. Число соответствует количеству открытых сессий. Цветной фон обозначает сессию локального администратора
	На компьютере (компьютерах) действует фильтр событий тревоги
ЛЦ	На компьютерах, подчиненных серверу безопасности, зафиксированы ошибки (красный цвет пиктограммы) или предупреждения (желтый цвет) при проверке лицензий на использование компонентов системы Secret Net Studio
	База данных сервера безопасности переполнена
OFF	Учетная запись компьютера отключена

Пиктограммы приведены в порядке уменьшения приоритета отображения. В элементах диаграммы в первую очередь отображаются пиктограммы с более высоким приоритетом. Если в элементе не хватает отведенной зоны для вывода всех пиктограмм, исключаются наименее значимые.

Сведения в иерархическом списке объектов управления

В панели "Компьютеры" при отображении списка объектов управления сведения о состоянии объектов представлены в табличном виде. Включение табличного режима отображения осуществляется с помощью кнопки "Таблица" в разделе "Вид" верхней части панели "Компьютеры".

Пример списка объектов управления в табличном виде представлен на следующем рисунке.



Сведения о компьютерах и серверах безопасности отображаются в колонках:

Пиктограмма включенного состояния
Содержит пиктограмму, если компьютер или сервер включен
Высокий, Повышенный, Низкий
Содержит количество событий тревоги, произошедших на защищаемом компьютере и ожидающих квитирования (подтверждение приема) администратором безопасности. В колонке "Высокий" указано количество критических событий тревоги (с уровнем тревоги "высокий"). В остальных колонках — количество менее значимых событий тревоги (с уровнями тревоги "повышенный" и "низкий" соответственно)
Пиктограмма блокировки

Содержит пиктограмму включенной блокировки, если компьютер заблокирован. Чтобы получить дополнительные сведения о причине блокировки, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором
ФК
Содержит пиктограмму, соответствующую результату проведения функционального контроля при запуске компьютера. Чтобы получить дополнительные сведения, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором
Сессии
Содержит краткие сведения об активных сессиях или имя пользователя, открывшего сессию. Чтобы получить дополнительные сведения, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором
Последнее подключение
Содержит время последнего подключения к серверу безопасности для выключенного компьютера
Лицензии
Содержит пиктограммы, если зафиксированы ошибки (красный цвет пиктограммы) или предупреждения (желтый цвет) при проверке лицензий на использование компонентов системы Secret Net Studio. Количество ошибок или предупреждений указывается рядом с пиктограммой.
Домен безопасности
Содержит имя домена безопасности, к которому относится объект
Версия
Содержит номер версии установленного программного обеспечения Secret Net Studio (ПО сервера безопасности или клиента)

Управление отображением сведений в списке объектов управления

Сведения о состоянии объектов управления можно сортировать по содержимому колонок таблицы. Сортировка выполняется стандартными методами с помощью заголовков колонок.

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

Печать и экспорт сведений о компьютерах

Программа позволяет отправлять на печать и/или сохранять (экспортировать) сведения о компьютерах, которые отображаются в списке объектов управления.

Экспорт сведений осуществляется в файлы формата RTF. Для загрузки содержимого RTF-файлов необходимо использовать соответствующие приложения, поддерживающие возможность просмотра таких файлов. Например, редактор Microsoft Word.

Внимание!

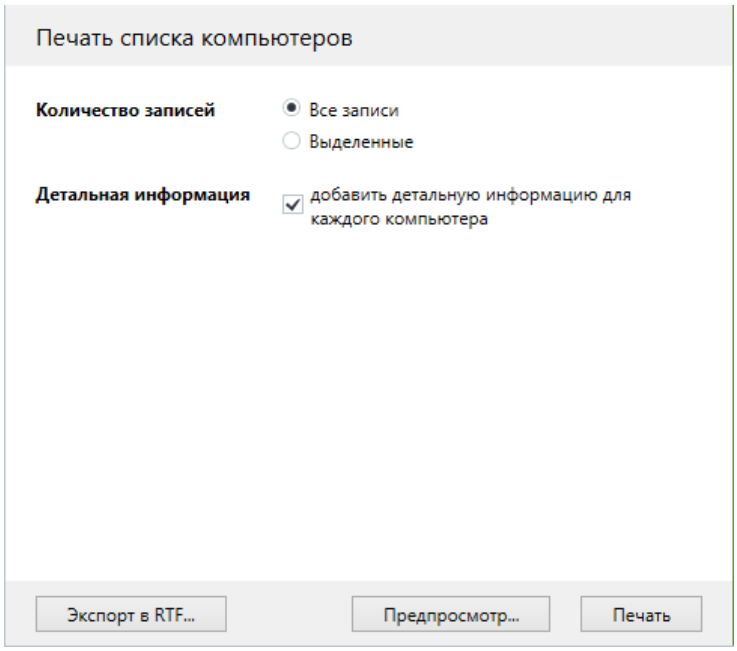
Не рекомендуется загружать полученный файл во встроенный редактор ОС Windows WordPad, так как в этом редакторе возможны искажения оформления. При отсутствии редактора Microsoft Word для просмотра и печати RTF-файлов можно использовать средство просмотра Word Viewer. Данное приложение распространяется бесплатно и доступно для загрузки на веб-узле компании Microsoft: http://www.microsoft.com/downloads/details.aspx?familyid=3657CE88-7CFA-457A-9AEC-F4F827F20CAC&displaylang=ru.

Настройка параметров печати и экспорта осуществляется в специальной панели настройки.

Для печати или экспорта сведений:

1. Подготовьте таблицу со списком объектов управления для вывода данных: настройте отображение сведений (при необходимости) и не отключайте отображение серверов и компьютеров в таблице.
2. Если требуется распечатать или сохранить сведения по отдельным компьютерам из числа отображаемых, выделите нужные компьютеры в таблице.
3. В правой части панели "Компьютеры" нажмите кнопку "Печать".

   На экране появится панель настройки параметров.



4. Настройте параметры вывода сведений.

Группа полей "Количество записей"
Определяет, какие записи о компьютерах будут распечатаны или сохранены: • "Все записи" — операция выполняется для всех компьютеров списка; • "Выделенные" — операция выполняется только для тех компьютеров, которые выделены в таблице
Поле "Детальная информация"
Если установлена отметка, для компьютеров дополнительно будут приведены сведения, не указанные явно в таблице (например, причина блокировки)

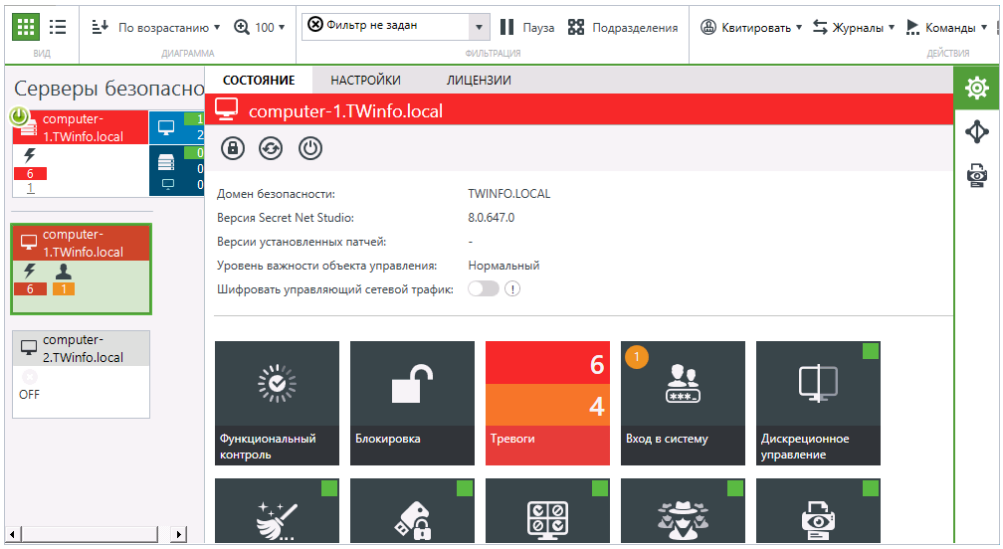
5. Чтобы открыть окно предварительного просмотра страниц, нажмите кнопку "Предпросмотр" в нижней части панели настройки параметров печати. После просмотра подготовленных сведений закройте окно.

   Примечание.
   В окне предварительного просмотра можно отправить документ на печать с помощью стандартной кнопки на панели инструментов.

6. В нижней части панели настройки параметров нажмите нужную кнопку:
   - чтобы запустить процесс печати — нажмите кнопку "Печать" и укажите общие параметры печати (выбранный принтер, число копий и др.) в диалоге настройки ОС Windows;
   - чтобы сохранить сведения в файле — нажмите кнопку "Экспорт в RTF" и укажите файл в диалоге сохранения файла ОС Windows.

Сведения о состоянии объектов

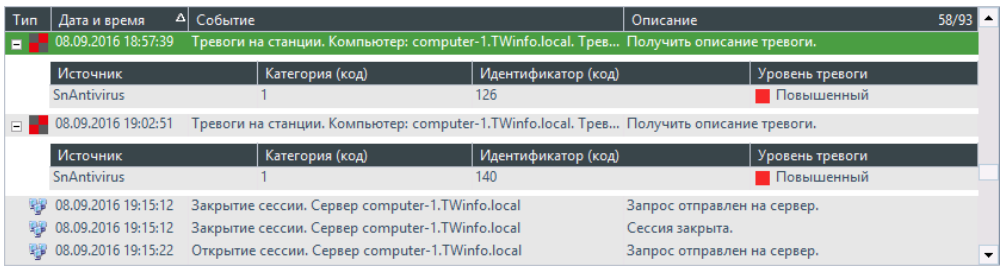
Вывод сведений о состоянии объектов осуществляется в панели "Компьютеры" на вкладке "Состояние". При включении отображения сведений панель "Компьютеры" имеет вид, подобный представленному на рисунке.



На вкладке "Состояние" представлены основные сведения об объекте и домене безопасности, к которому он относится, а также доступные средства для управления объектом.

Сведения в панели событий системы

Панель событий системы может использоваться для получения сведений об изменении состояния защищаемых компьютеров. Пример содержимого панели представлен на следующем рисунке.



В панели событий системы могут выводиться сведения следующих типов:

- "События сети" — уведомления об изменении состояния контролируемых объектов, их конфигурации и о связи с сервером безопасности (например, "*<имя_компьютера>* заблокирован", "Потеряна связь с сервером..." и др.);
- "Действия пользователя" — уведомления, информирующие о действиях пользователей (например, "Команда "заблокировать" отправлена для агента (ов)...", "Квитирование тревог для агентов..." и др.);
- "События тревог" — уведомления о фактах регистрации событий тревоги на защищаемых компьютерах (например, "Тревоги на станции").

Если не заданы особые цвета для уведомлений, сведения, полученные во время текущей сессии работы с программой, отображаются на белом фоне. Сведения других сессий — на сером фоне.

Параметры отображения данных в панели событий системы можно изменять (см. стр.**10**).

Просмотр расширенной информации о событиях

В панели событий системы может выводиться расширенная информация о

событиях. Например, в уведомлениях о событиях изменения политики контроля устройств или о событиях тревоги. Расширенная информация выводится в виде табличного блока, для отображения которого используется кнопка раскрытия иерархии в левой части строки.

Табличный блок уведомления об изменении политики содержит список политик и их измененных значений. Для событий тревоги выводятся основные сведения, полученные в уведомлениях. Чтобы загрузить все сведения о событиях тревоги в блоке, выберите ссылку "Получить описание тревоги" — в блок будут загружены сведения в виде записей журнала с описанием событий. При просмотре записей могут использоваться те же функции настройки отображения, как и в основной таблице с записями журнала (сортировка, группировка, выбор колонок и др.).

Предусмотрена возможность отображения дополнительных данных о событии. Для этого вызовите контекстное меню записи о событии и выберите команду "Детально" — в правой части панели событий системы откроется панель детального описания. Если данные о событии содержат информацию о каком-либо устройстве, можно скопировать эту информацию в буфер обмена, чтобы потом добавить устройство с этими параметрами в групповую политику. Действие выполняется с помощью команды "Копировать устройство" в контекстном меню панели детального описания.

Автоматическое отображение последних сведений

Новые уведомления о событиях помещаются в конец списка. Для удобства просмотра актуальных сведений предусмотрен режим автоматического прокручивания списка к последнему добавленному элементу.

Для включения этого режима вызовите контекстное меню в любом месте панели событий системы и выберите команду "Автоматическая прокрутка".

Экспорт сведений

Программа позволяет сохранять (экспортировать) в файлы сведения, отображаемые в панели событий системы. Экспорт выполняется в файлы формата XML.

Экспорт осуществляется с помощью команд контекстного меню "Экспорт" и "Экспортировать все". Команда "Экспорт" применяется, чтобы экспортировать отдельные выбранные строки таблицы сведений. Если требуется экспортировать всю таблицу, вызовите контекстное меню в любом месте панели событий системы и выберите команду "Экспортировать все".

Отслеживание событий тревоги

Программа управления информирует о событиях, на которые необходимо обратить внимание администратора безопасности (события тревоги). Такие события регистрируются на защищаемых компьютерах в журнале Secret Net Studio или штатном журнале безопасности ОС и имеют тип "Аудит отказов" или "Ошибки".

События тревоги различаются по степени значимости самих событий и уровню важности объекта, на котором они произошли. Критические события могут иметь уровень тревоги "высокий" для объектов с высоким уровнем важности или "повышенный" — для объектов с нормальным уровнем важности. Менее значимые события имеют уровень тревоги "повышенный" или "низкий" соответственно уровню важности объектов.

Сервер безопасности накапливает сведения о событиях тревоги в отдельном журнале. Журнал событий тревоги формируется из уведомлений, направляемых серверу от защищаемых компьютеров.

Оповещение о событиях тревоги

При получении уведомлений о произошедших событиях тревоги программа управления незамедлительно оповещает пользователя об этом. Оповещение

происходит путем подачи различных визуальных сигналов. Например, соответствующие элементы диаграммы управления выделяются красным цветом. Также для оповещения могут использоваться и звуковые сигналы.

Отключение оповещения и возвращение обычного вида объектов происходит после квитирования событий тревоги.

Статистические сведения о неквитированных событиях тревоги выводятся на панели "Начало" в виде индикаторов и графиков распределения событий.

Внимание!
Квитирование событий тревоги необходимо выполнять до архивирования журнала событий тревоги. Если в архив были помещены записи, не прошедшие процедуру квитирования, значение счетчика событий тревоги уменьшается, и администратор безопасности может пропустить информацию о несанкционированном доступе. В этом случае для квитирования событий следует восстановить журнал событий тревоги из архива в базу данных сервера безопасности, после чего появится возможность обработать информацию в обычном порядке.

Квитирование событий тревоги

Под квитированием событий тревоги понимается подтверждение о получении информации администратором безопасности с описанием принятых мер. Как правило, каждое событие тревоги требует выяснения причин его возникновения и выполнения экстренных действий для обеспечения безопасности информационной системы. После того как администратор безопасности принял к сведению и проанализировал обстоятельства возникновения события тревоги, необходимо подтвердить прием информации, выполнив процедуру квитирования.

При квитировании администратор вводит текстовый комментарий с описанием причин и принятых мер, и этот комментарий сохраняется в системе вместе с признаком квитирования события. Информация о самом событии тревоги не удаляется из журнала. В дальнейшем по журналу событий тревоги можно определить, кто, когда и как отреагировал на произошедшие события. После квитирования всех событий, полученных от компьютера, этому объекту возвращается нормальный вид отображения.

Примечание.
Помимо квитирования событий тревоги с обязательным вводом комментария администратором безопасности, в программе предусмотрена возможность сброса счетчиков событий (см. ниже). Процедура сброса счетчиков предназначена только для случаев, связанных с настройкой системы защиты, и не должна применяться в штатном режиме функционирования.

Квитирование событий тревоги выполняется при работе с журналом событий тревоги в панели "Журналы тревог" (см. стр.**63**).

Сброс счетчиков событий тревоги

При получении уведомлений о зарегистрированных событиях тревоги счетчики событий и измененные пиктограммы объектов отображаются до тех пор, пока не будут обнулены значения счетчиков для этих объектов.

Уменьшение значений счетчиков происходит при квитировании событий тревоги (см. выше). В штатном режиме функционирования системы защиты обнуление счетчиков необходимо выполнять только посредством квитирования событий, так как процедура квитирования предусматривает просмотр информации о событиях и добавление уточняющих комментариев администратора безопасности.

Во время настройки параметров системы защиты на этапе пробной эксплуатации допускается сбрасывать значения счетчиков событий тревоги для оперативного возврата к нормальному виду отображения объектов. При сбросе счетчиков система воспринимает в качестве принятых к сведению все события тревоги, произошедшие на защищаемом компьютере (компьютерах) на момент поступления команды. Однако в отличие от процедуры квитирования при сбросе счетчиков не запрашивается уточняющий комментарий администратора

безопасности. При этом в системе сохраняются сведения о том, кто и когда выполнил обнуление значений, вместе с информацией о событиях тревоги.

Для сброса счетчиков событий тревоги:

1. В диаграмме управления или в списке объектов выберите нужные объекты.
2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Квитировать" и выберите нужную команду:
   - "Все тревоги" — для квитирования всех событий независимо от уровней тревоги;
   - "Тревоги высокого уровня" — для квитирования только событий с уровнем тревоги "высокий";
   - "Тревоги повышенного уровня" — для квитирования только событий с уровнем тревоги "повышенный";
   - "Тревоги низкого уровня" — для квитирования только событий с уровнем тревоги "низкий".
3. При появлении диалога запроса на продолжение действия подтвердите выполнение операции.

   Для объектов будет возвращен нормальный вид отображения. О результатах выполнения действия выводится уведомление в панели событий системы.

Создание правил фильтрации на основе уведомлений о событиях тревоги

Для выборочного отслеживания событий можно настроить фильтр, который будет определять, какие уведомления о событиях тревоги должны поступать на сервер безопасности. Фильтр тревог действует независимо от политики регистрации событий в локальных журналах, что дает возможность контроля важных изменений в системе без уменьшения объема сохраняемой информации в локальных журналах. Фильтр может применяться при передаче уведомлений от защищаемых компьютеров на сервер безопасности (настраивается в группе "Оповещения о тревогах" раздела "Политики" панели свойств объектов), а также при передаче уведомлений, полученных подчиненными серверами безопасности (настраивается в разделе "Параметры").

В создаваемых правилах автоматически добавляются условия фильтрации на основе выбранных сведений. Создание правил в панели событий предусмотрено для уведомлений о событиях тревоги, полученных во время текущей сессии работы с программой.

Для добавления правила в панели событий системы:

1. В панели событий системы перейдите к уведомлению о событиях тревоги и раскройте блок с расширенной информацией о событиях. Для этого наведите указатель на строку уведомления и дважды нажмите левую кнопку мыши или нажмите кнопку раскрытия иерархии в левой части строки.

   Примечание.
   Описание панели событий системы и возможностей для управления отображением сведений см. на стр. 39.
2. В блоке с расширенной информацией вызовите контекстное меню события и раскройте подменю "Добавить правило для фильтрации тревоги".
3. Выберите команду добавления правила в нужный фильтр. Фильтр событий тревоги может быть задан в групповых политиках (при наличии возможности изменения политик) или в параметрах сервера безопасности.

   После выбора команды в панели "Компьютеры" будет открыта соответствующая группа параметров, и в списке правил фильтра появится новое правило. Если добавляемое правило может повлиять на применение ранее заданных параметров, перед добавлением на экране появится запрос на выполнение дальнейших действий. В этом случае перед продолжением операции рекомендуется проверить заданные параметры.

Оперативное управление

Оперативное управление защищаемыми компьютерами осуществляется с помощью команд. Команды оперативного управления могут применяться к компьютерам как самого сервера подключения (сервер безопасности, с которым установлено соединение программы), так и подчиненных серверов. При этом выбранный для управления компьютер должен быть включен.

Примечание.
Если в данный момент исполнение какой-либо оперативной команды невозможно, эта команда или отсутствует в меню, или неактивна.

Блокировка и разблокирование компьютеров

Включенные компьютеры можно удаленно заблокировать или снять блокировку (разблокировать). Команды для выполнения действий могут применяться к компьютерам или серверам безопасности. Если команда применяется для сервера безопасности, соответствующее действие будет выполнено для всех компьютеров, подчиненных данному серверу.

При поступлении команды блокировки на экране компьютера появляется сообщение об этом и прерывается сеанс работы текущего пользователя. Одновременно в журнале Secret Net Studio регистрируется событие "Компьютер заблокирован системой защиты", которое является событием тревоги. Локально разблокировать компьютер может только пользователь, входящий в локальную группу администраторов.

Если компьютер заблокирован системой защиты, соответствующие объекты в программе управления отображаются с измененными пиктограммами (см. стр.**35**). Для такого компьютера может применяться команда разблокирования. После получения команды на разблокирование на экране компьютера появляется сообщение об этом и пользователь может продолжить работу.

Для блокировки компьютеров:

1. В диаграмме управления или в списке объектов выберите нужный объект (компьютер, группа, сервер безопасности) или выделите несколько нужных объектов.
2. Вызовите контекстное меню выбранного объекта (одного из выделенных объектов), раскройте подменю "Команды" и выберите команду "Заблокировать". При появлении диалога запроса на продолжение действия подтвердите выполнение операции.

Для разблокирования компьютеров:

1. В диаграмме управления или в списке объектов выберите нужный объект (компьютер, группа, сервер безопасности) или выделите несколько нужных объектов.
2. Вызовите контекстное меню выбранного объекта (одного из выделенных объектов), раскройте подменю "Команды" и выберите команду "Разблокировать". При появлении диалога запроса на продолжение действия подтвердите выполнение операции.

Перезагрузка и выключение компьютеров

Для включенных компьютеров можно удаленно инициировать перезагрузку или выключение. Команды для выполнения действий могут применяться к компьютерам или серверам безопасности. Если команда применяется для сервера безопасности, соответствующее действие (перезагрузка или выключение) будет выполнено для всех компьютеров, подчиненных данному серверу.

Перезагрузка или выключение компьютера выполняется независимо от количества открытых приложений и наличия несохраненных документов. При поступлении команды на экране компьютера появляется сообщение об этом, и в

течение 15 секунд с момента появления сообщения пользователь компьютера может сохранить открытые документы.

Для перезагрузки или выключения компьютеров:

1. В диаграмме управления или в списке объектов выберите нужный объект (компьютер, группа, сервер безопасности) или выделите несколько нужных объектов.
2. Вызовите контекстное меню выбранного объекта (одного из выделенных объектов), раскройте подменю "Команды" и выберите команду "Перезагрузить" или "Выключить" для перезагрузки или выключения компьютера соответственно. При появлении диалога запроса на продолжение действия подтвердите выполнение операции.

Обновление групповых политик на компьютерах

Для включенных компьютеров можно удаленно инициировать запуск обновления групповых политик. Команда применяется к отдельным компьютерам, серверам безопасности и группам компьютеров. Если выбран сервер безопасности или группа, обновление групповых политик выполняется на всех компьютерах под управлением ОС Windows, подчиненных серверу безопасности или включенных в группу.

Принудительное обновление ускоряет процесс применения централизованно заданных групповых политик на компьютерах.

Для обновления групповых политик на компьютерах:

1. В диаграмме управления или в списке объектов выберите нужный объект (компьютер, группа, сервер безопасности) или выделите несколько нужных объектов.
2. Вызовите контекстное меню выбранного объекта (одного из выделенных объектов), раскройте подменю "Команды" и выберите команду "Применить групповые политики".

Утверждение изменений аппаратной конфигурации

Для включенных компьютеров можно удаленно утвердить изменения аппаратной конфигурации.

Компьютер, на котором зафиксировано изменение аппаратной конфигурации, обозначается в диаграмме управления специальной пиктограммой (см. стр.**35**).

Для утверждения аппаратной конфигурации на компьютере:

1. Вызовите контекстное меню компьютера с измененной аппаратной конфигурацией и выберите команду "Утвердить аппаратную конфигурацию".

   На экране появится диалог со списком устройств, не совпадающих с эталонной аппаратной конфигурацией компьютера.
2. Для учета изменений в составе эталонной аппаратной конфигурации компьютера нажмите кнопку "Утвердить".

Примечание.
Утвердить аппаратную конфигурацию можно также при просмотре сведений в панели событий системы. Для утверждения конфигурации вызовите контекстное меню уведомления "На агенте <*имя_компьютера*> изменилась аппаратная конфигурация" и выберите команду "Утвердить аппаратную конфигурацию".

Сбор локальных журналов по команде администратора

Передача локальных журналов защищаемых компьютеров в БД сервера безопасности выполняется регулярно в соответствии с заданными параметрами (см. стр.**26**).

Для включенных компьютеров можно выполнить запуск процесса внеочередной передачи локальных журналов. Команды применяются к отдельным компьютерам, серверам безопасности и группам компьютеров. Если выбран сервер безопасности или группа, сбор локальных журналов выполняется со всех компьютеров, подчиненных серверу безопасности или включенных в группу.

Для запуска процесса передачи локальных журналов:

1. В диаграмме управления или в списке объектов выберите нужные объекты.
2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Журналы / Собрать журналы с компьютера".
3. Выберите команду с названием нужного журнала или команду "Все", если требуется передать в БД сервера безопасности все локальные журналы.

   В панели событий системы появится уведомление о запуске процесса сбора локальных журналов. Статус выполнения процесса отображается в колонке "Описание".

Управление функционированием механизмов защиты на компьютерах

Для включенных компьютеров можно использовать средства оперативной настройки функционирования механизмов защиты.

Для настройки функционирования механизмов защиты на компьютерах:

1. В диаграмме управления или в списке объектов выберите нужные объекты.
2. Включите отображение параметров объектов (с помощью команды "Свойства" в контекстном меню) и перейдите на вкладку "Состояние" (см. стр.**39**).
3. Нажмите кнопку нужного механизма (например, "Затирание данных").

   Под кнопкой появится блок, содержащий сведения о механизме.
4. Чтобы включить или отключить механизм защиты, переведите в нужное положение выключатель, расположенный справа от заголовка блока. При появлении диалога запроса на продолжение действия подтвердите выполнение операции.

   Примечание.
   Включение механизма защиты возможно при наличии действующей лицензии для данного механизма. Выключатель присутствует в заголовке блока, если лицензия на данный механизм включена. Управление списком лицензий осуществляется на вкладке "Лицензии".
5. Если для механизма предусмотрены дополнительные возможности настройки, выполните нужные действия с помощью средств управления, представленных в блоке.

Глава 5
Работа с централизованными журналами

Возможность загрузки централизованных журналов из базы данных сервера безопасности доступна при подключении программы к серверу. Загрузку записей из файлов можно выполнять при работе программы как с подключением к серверу безопасности, так и в автономном режиме.

Централизованные журналы

В базе данных сервера безопасности накапливаются следующие журналы:

- журнал событий тревоги, объединяющий все записи о событиях тревоги со всех управляемых компьютеров;
- журнал событий, объединяющий журнал Secret Net Studio и штатные журналы ОС Windows со всех управляемых компьютеров;
- журнал сервера безопасности.

Информацию из этих журналов можно загружать частично или полностью в программу управления.

Журнал событий тревоги

Журнал событий тревоги предназначен для централизованного хранения информации о событиях тревоги, произошедших на защищаемых компьютерах. Событиями тревоги считаются события, которые регистрируются локально в журнале Secret Net Studio или штатном журнале безопасности ОС и имеют тип "Аудит отказов" или "Ошибки". Журнал событий тревоги формируется из уведомлений о событиях тревоги, направляемых серверу безопасности.

Сведения, содержащиеся в журнале событий тревоги, позволяют администратору безопасности оперативно получать наиболее важную информацию о попытках несанкционированного доступа в системе. При возникновении события тревоги сведения о нем регистрируются в соответствующем локальном журнале и одновременно отправляются серверу безопасности, который сохраняет их в журнале событий тревоги. Таким образом, в системе дублируются сведения о таком событии, что уменьшает риск потери информации.

Для компьютеров может действовать фильтр событий тревоги, который определяет критерии выборочного отслеживания событий. Если правила фильтрации не заданы, в журнал событий тревоги поступает информация о каждом событии тревоги на компьютере.

Сведения о событиях сохраняются в журнале в виде записей. Каждая запись включает в себя набор полей с данными из локального журнала, а также поля с дополнительными данными (тип локального журнала, сведения об агенте, уровень угрозы, квитирование и другие параметры).

Объединенный журнал компьютеров

Объединенный журнал компьютеров (называемый также журнал станций) предназначен для централизованного хранения содержимого локальных журналов, поступивших с защищаемых компьютеров. К локальным журналам относятся журнал Secret Net Studio и штатные журналы ОС Windows (журнал приложений, системный журнал и журнал безопасности). Описание назначения локальных журналов см. в документе [**3**].

Передача локальных журналов для централизованного хранения в базу данных сервера безопасности осуществляется в соответствии с заданными параметрами (см. стр.**26**).

Сведения, полученные из локальных журналов, сохраняются в полном объеме в объединенном журнале. Вместе с этими сведениями в каждой записи о событии

фиксируются дополнительные данные (тип локального журнала, сведения об агенте, уровень угрозы и другие параметры).

Журнал сервера безопасности

В журнале сервера безопасности протоколируются сессии доступа к серверу, открываемые компонентами и программами Secret Net Studio, включая внутренние сессии самого сервера безопасности.

Сведения о сессиях сохраняются в журнале в виде записей. Каждая запись включает в себя набор полей, в которых представлены следующие данные:

- общие данные о сессии: имя компьютера, инициаторы открытия (компонент и пользователь), время открытия и закрытия сессии;
- основные данные о выполнявшихся действиях в сессии: время выполнения каждого действия, результат, описание самого действия;
- дополнительные данные с детальными описаниями событий (системные идентификаторы объектов, кодовые обозначения результатов и другие параметры).

Хранение журналов

Журналы с записями о событиях могут храниться в следующих хранилищах:

- локальные хранилища на компьютерах, где были зарегистрированы события (локальные журналы);
- централизованное хранилище в БД сервера безопасности;
- файлы архивов, созданных сервером безопасности.

В программе управления осуществляется просмотр журналов, хранящихся в централизованном хранилище или в файлах архивов. Для просмотра в программе текущего содержимого локальных журналов требуется предварительная передача журналов на хранение в БД сервера безопасности.

Локальные хранилища журналов

При регистрации событий записи о них помещаются в соответствующие локальные журналы и хранятся на защищаемом компьютере. Пока записи хранятся в локальном хранилище, их можно загрузить локально на компьютере.

Локальные журналы хранятся до тех пор, пока они не будут переданы в централизованное хранилище на сервере безопасности. После передачи записей происходит очистка содержимого локальных журналов.

Внимание!
При работе с локальными журналами пользователь, наделенный соответствующими полномочиями, может выполнять очистку журналов до их передачи на сервер безопасности. Чтобы исключить возможность несанкционированного удаления информации, необходимо предоставлять полномочия управления локальными журналами только доверенным пользователям.

Централизованное хранилище

Централизованное хранилище журналов размещается в БД сервера безопасности. Сведения о событиях, регистрируемых в журнале событий тревоги или в журнале сервера безопасности, поступают непосредственно в централизованное хранилище без промежуточного размещения в других хранилищах. В объединенном журнале компьютеров размещается содержимое локальных журналов при их передаче из локальных хранилищ в БД сервера безопасности. Запуск процесса передачи локальных журналов с защищаемых компьютеров осуществляется в следующих случаях:

- в моменты времени, заданные параметрами автоматической передачи журналов (см. стр.**26**);
- по команде пользователя программы управления (см. стр.**44**).

Примечание.
Для штатных журналов ОС Windows можно отключить передачу записей в централизованное хранилище. Если для журнала отключена функция централизованного сбора, этот журнал игнорируется при запросе локальных журналов и содержимое этого журнала остается в локальном хранилище.

Удаление записей журналов из централизованного хранилища происходит при архивировании журналов.

Просмотр и управление записями журналов, хранящихся в БД сервера безопасности, осуществляется только в программе управления.

Архивы журналов, созданные сервером безопасности

Для уменьшения объема базы данных сервера безопасности предусмотрена возможность архивирования содержимого централизованных журналов. Архивируются все записи журналов, имеющиеся в БД сервера безопасности на момент начала процесса архивирования (для журнала сервера безопасности — архивируются сведения о завершенных сессиях). Записи, помещенные в архив, удаляются из централизованного хранилища.

Запуск процесса архивирования осуществляется в следующих случаях:

- в моменты времени, заданные параметрами автоматического архивирования журналов (см. стр.**27**);
- по команде пользователя программы управления (см. стр.**66**).

Архивированные записи журналов хранятся в файлах. Для каждого архива создается отдельный файл. По умолчанию для размещения архивов используется подкаталог \Archive, расположенный в каталоге установки сервера безопасности.

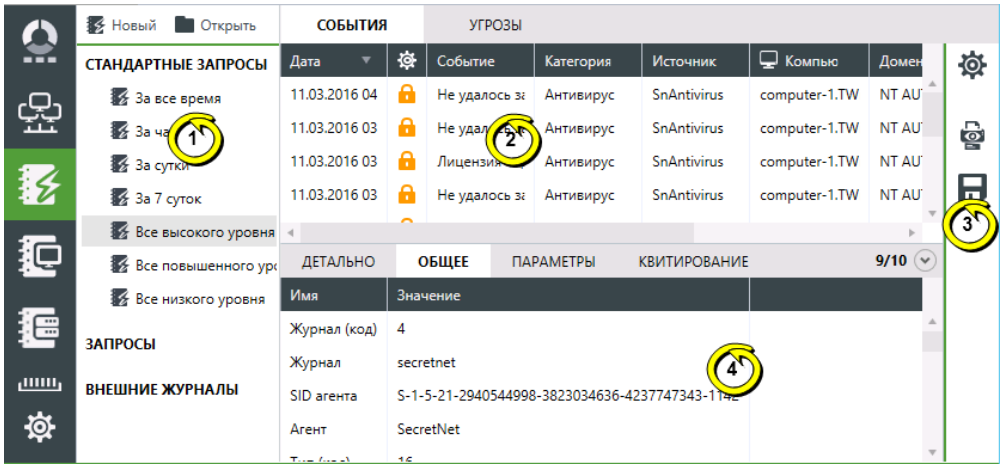
Панели для работы с записями журналов

Вывод записей централизованных журналов осуществляется в следующих панелях:

- панель журнала событий тревоги. Во время работы с программой переход к панели журнала осуществляется с помощью ярлыка "Журналы тревог" в панели навигации или по ссылке "Журнал получен" в уведомлении о запросе журнала в панели событий системы;
- панель журнала станций. Во время работы с программой переход к панели журналов осуществляется с помощью ярлыка "Журналы станций" в панели навигации или по ссылке "Журнал получен" в уведомлении о запросе журнала событий в панели событий системы;
- панель журнала сервера безопасности. Во время работы с программой переход к панели журналов осуществляется с помощью ярлыка "Журнал сервера" в панели навигации или по ссылке "Журнал получен" в уведомлении о запросе журнала сервера в панели событий системы;
- панель архивов журналов — открывается по умолчанию, если при запуске программы управления в диалоге выбора режима работы выбрана команда запуска в автономном режиме "Архив журналов" и указан файл архива для загрузки. Во время работы с программой переход к панели архивов осуществляется с помощью ярлыка "Архивы" в панели навигации.

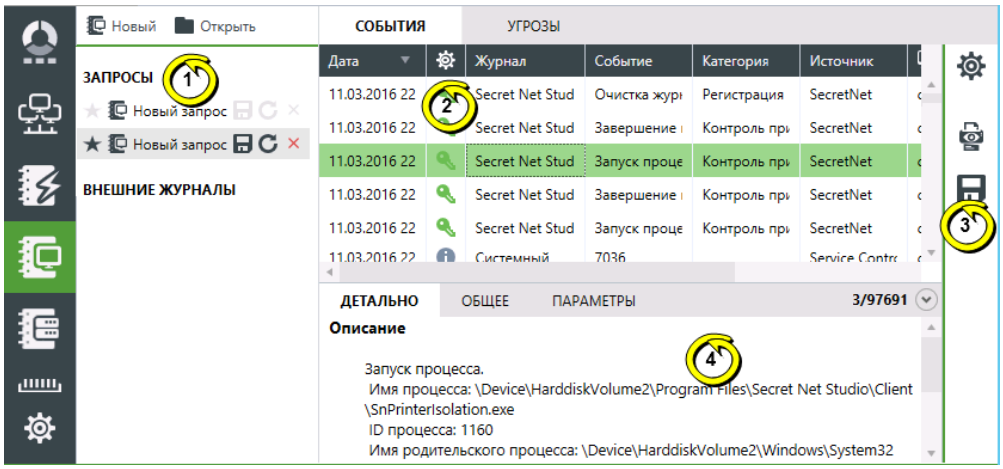
Для загрузки записей в панели создается вкладка, называемая запросом. В панели можно работать с несколькими запросами. Переходы между ними осуществляются посредством выбора нужного запроса в панели управления запросами.

Панель журнала событий тревоги имеет вид, подобный представленному на следующем рисунке.



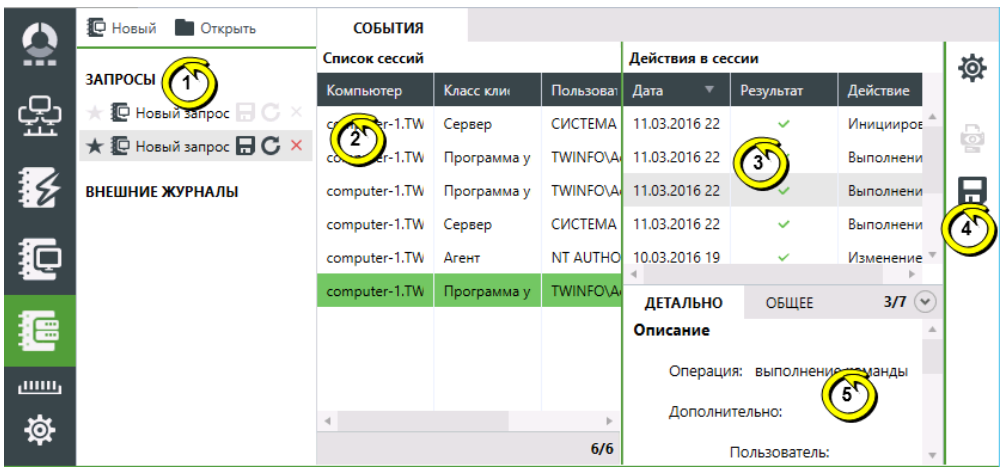
Пояснение.
На рисунке обозначены: 1 — панель управления запросами; 2 — область отображения сведений; 3 — панель настройки вывода сведений; 4 — область описания событий.

Панель журнала станций имеет вид, подобный представленному на следующем рисунке.



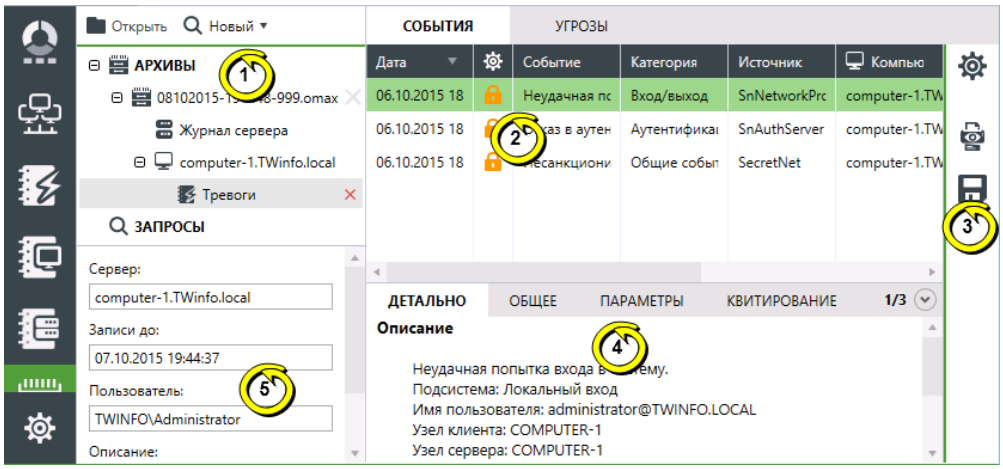
Пояснение.
На рисунке обозначены: 1 — панель управления запросами; 2 — область отображения сведений; 3 — панель управления записями; 4 — область описания событий.

Панель журнала сервера безопасности имеет вид, подобный представленному на следующем рисунке.



Пояснение.
На рисунке обозначены: 1 — панель управления запросами; 2 — область отображения списка сессий; 3 — область отображения сведений о выбранной сессии; 4 — панель настройки вывода сведений; 5 — область описания событий.

Панель архивов журналов имеет вид, подобный представленному на следующем рисунке.



Пояснение.
На рисунке обозначены: 1 — панель управления запросами; 2 — область отображения сведений; 3 — панель настройки вывода сведений; 4 — область описания событий; 5 — область основных сведений об архиве.

Основные элементы интерфейса:

Панель управления запросами
Содержит списки запросов для загрузки записей. Запросы группируются в следующих разделах: • "Стандартные запросы" — запросы с предопределенными критериями отбора записей, загружаемых из журнала (только для журнала событий тревоги); • "Запросы" — запросы, созданные пользователем для загрузки записей из журнала; • "Внешние журналы" — запросы, созданные при загрузке записей из файлов; • "Архивы" — запросы, полученные по результатам анализа содержимого загруженных архивов.
Область отображения сведений
Содержит сведения о событиях в журнале в виде таблицы со списком записей.
Панель настройки вывода сведений
Содержит кнопки вызова средств конфигурирования запроса, печати и экспорта записей
Область описания событий

Содержит подробную информацию о выбранном событии. Информация о событиях группируется в следующих вкладках:

- "Детально" — содержит детальное описание и полученные данные. Если данные о событии содержат информацию о каком-либо устройстве, можно скопировать эту информацию в буфер обмена, чтобы потом добавить устройство с этими параметрами в групповую политику;
- "Общее" — содержит полный список полей и их значений в записи о зарегистрированном событии. Список представлен в табличной форме;
- "Параметры" — содержит список параметров системы Secret Net Studio, полученных из детального описания события. Список представлен в табличной форме;
- "Квитирование" — содержит сведения о том, кто и когда выполнил процедуру квитирования (подтверждение приема) для выбранной записи, и текстовый комментарий с описанием действий. Вкладка отображается только для журнала событий тревоги при выборе записи с признаком квитирования.

Включение и отключение области описания событий осуществляется при выборе команды "Детально" в контекстном меню записи о событии или с помощью кнопки, расположенной справа в нижней строке области отображения сведений

Загрузка записей журналов

Запросы для журнала событий тревоги

В программе предусмотрены следующие способы создания запросов на загрузку записей журнала событий тревоги:

- создание запросов по статистическим данным;
- контекстное создание запросов для объектов;
- создание запросов с предопределенными критериями отбора;
- создание запросов с произвольными критериями отбора;
- создание запросов на загрузку записей журнала из файлов.

Создание запросов по статистическим данным

Статистические данные о событиях тревоги представлены в панели "Начало". Также в левом верхнем углу основного окна программы управления отображается индикатор состояния системы, который содержит общее количество событий тревоги (при наличии неквитированных событий).

Счетчики количества событий тревоги в панели "Начало" и в индикаторе состояния системы могут использоваться для создания запросов на загрузку записей журнала событий тревоги. Чтобы создать новый запрос, выберите значение нужного счетчика. В панели журнала событий тревоги появится новый запрос, в котором автоматически будет выполнена загрузка записей.

Контекстное создание запросов для объектов

Запросы на загрузку записей журнала событий тревоги можно создавать применительно к объектам, выбранным в панели диаграммы управления или в списке объектов. Для таких запросов автоматически создаются правила отбора и фильтрации по контексту выбранных объектов и команд.

Для контекстного создания запроса:

1. В диаграмме управления или в списке объектов выберите нужные объекты.

   Примечание.
   О наличии зарегистрированных событий тревоги, ожидающих квитирования (подтверждения приема) администратором безопасности, оповещают счетчики событий, которые отображаются рядом с объектами (см. стр.35 и стр.36).

2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Журналы / Журнал тревог" и выберите нужную команду:
   - "Все тревоги" — для получения сведений о событиях всех уровней тревоги;

- "Тревоги высокого уровня", "Тревоги повышенного уровня", "Тревоги низкого уровня" — для получения сведений только о событиях с соответствующим уровнем тревоги.

По окончании загрузки записей в панели событий системы появится уведомление о получении журнала. Для перехода к записям журнала выберите в уведомлении ссылку "Журнал получен".

Создание запросов с предопределенными критериями отбора

Запросы с предопределенными критериями отбора позволяют оперативно загрузить в программу неквитированные записи о событиях тревоги, которые были зарегистрированы в течение заданного периода времени или имеют определенный уровень тревоги.

Создание запросов с предопределенными критериями отбора выполняется в панели журнала. Такие запросы целесообразно создавать при наличии в системе неквитированных записей о событиях тревоги.

Для создания запроса с предопределенными критериями отбора:

- В разделе "Стандартные запросы" панели управления запросами наведите указатель на элемент списка, соответствующий нужному периоду времени или уровню важности событий, и дважды нажмите левую кнопку мыши.

  В панели журнала будет создан новый запрос с соответствующими параметрами, после чего автоматически инициируется процесс получения записей из журнала. По окончании загрузки записей в панели событий системы появится уведомление о получении журнала со ссылкой для перехода к новому запросу.

Создание запросов с произвольными критериями отбора

Запросы с произвольными критериями отбора записей создаются для последующей настройки параметров и запуска процесса получения записей вручную.

Создание запросов выполняется в панели журнала событий тревоги.

Для создания запроса:

1. В панели управления запросами нажмите кнопку "Новый".

   В панели журнала будет создан новый запрос, и справа появится панель для настройки его параметров.

2. Настройте параметры нового запроса (см. стр.**56**) и нажмите кнопку "Выполнить запрос к БД" в нижней части панели настройки параметров.

   Будет инициирован процесс получения записей из журнала. По окончании загрузки записей в панели событий системы появится уведомление о получении журнала со ссылкой для перехода к новому запросу.

Создание запросов на загрузку записей журнала событий тревоги из файлов

Записи журнала событий тревоги могут храниться в файлах специального формата *.snua. Загрузка записей из таких файлов в панель журнала событий тревоги осуществляется путем создания отдельных запросов для каждого файла.

Файл для загрузки можно указать при запуске программы в автономном режиме (см. стр.**7**) или во время работы с программой в панели журнала событий тревоги.

Для создания запроса на загрузку записей из файла в панели журнала событий тревоги:

1. В панели управления запросами нажмите кнопку "Открыть".

   На экране появится диалог открытия файла ОС Windows.

2. Выберите нужный файл.

В панели журнала будет создан новый запрос, в который будут загружены записи из файла.

Запросы для журнала станций

В программе предусмотрены следующие способы создания запросов на загрузку записей журнала станций:

- контекстное создание запросов для объектов;
- создание запросов с произвольными критериями отбора;
- создание запросов на загрузку записей журнала станций или локальных журналов из файлов.

Контекстное создание запросов для объектов

Запросы на загрузку записей журнала станций можно создавать применительно к объектам, выбранным в панели диаграммы управления или в списке объектов. Для таких запросов автоматически создаются правила отбора и фильтрации по контексту выбранных объектов и команд.

Для контекстного создания запроса:

1. В диаграмме управления или в списке объектов выберите нужные объекты.
2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Журналы / Журналы компьютеров из БД" и выберите команду, соответствующую нужным критериям отбора записей. Можно загрузить записи о событиях, поступившие из определенных локальных журналов по отдельности или журнала Secret Net Studio совместно с журналом безопасности. По команде "Создать запрос" выполняется создание запроса с переходом в панель "Журналы станций" для настройки параметров запроса (см. стр.56).

   После выбора команды на загрузку записей о событиях, поступивших из определенных локальных журналов, автоматически инициируется процесс получения записей из журнала станций. По окончании загрузки записей в панели событий системы появится уведомление о получении журнала. Для перехода к записям журнала выберите в уведомлении ссылку "Журнал получен".

Создание запросов с произвольными критериями отбора

Запросы с произвольными критериями отбора записей создаются для последующей настройки параметров и запуска процесса получения записей вручную.

Создание запросов для загрузки записей журнала станций выполняется в панели "Журналы станций".

Для создания запроса:

1. В панели управления запросами нажмите кнопку "Новый".

   В панели "Журналы станций" будет создан новый запрос, и справа появится панель для настройки его параметров.
2. Настройте параметры нового запроса (см. стр.56) и нажмите кнопку "Выполнить запрос к БД" в нижней части панели настройки параметров запроса.

   Будет инициирован процесс получения записей из журнала. По окончании загрузки записей в панели событий системы появится уведомление о получении журнала со ссылкой для перехода к новому запросу.

Создание запросов на загрузку записей журнала станций или локальных журналов из файлов

Записи журнала станций могут храниться в файлах специального формата *.snlog. Загрузка записей из таких файлов в панель "Журналы станций" осуществляется путем создания отдельных запросов для каждого файла.

Кроме того, отдельные запросы, аналогичные запросам на загрузку журнала станций, можно создавать для файлов стандартного формата журнала событий ОС Windows *.evt*.

Файл для загрузки можно указать при запуске программы в автономном режиме (см. стр.**7**) или во время работы с программой в панели "Журналы станций".

Для создания запроса на загрузку записей из файла в панели "Журналы станций":

1. В панели управления запросами нажмите кнопку "Открыть".

   На экране появится диалог открытия файла ОС Windows.

2. Выберите нужный файл.

   В панели "Журналы станций" будет создан новый запрос, в который будут загружены записи из файла.

Запросы для журнала сервера безопасности

В программе предусмотрены следующие способы создания запросов на загрузку записей журнала сервера безопасности:

- контекстное создание запросов;
- создание запросов с произвольными критериями отбора;
- создание запросов на загрузку записей журнала сервера безопасности из файлов.

Контекстное создание запросов

Запросы на загрузку записей журнала сервера безопасности можно создавать при работе в панели диаграммы управления или в списке объектов. Для таких запросов автоматически могут создаваться правила отбора и фильтрации по контексту выбранных команд.

Для контекстного создания запроса:

1. В диаграмме управления или в списке объектов вызовите контекстное меню сервера безопасности, журнал которого требуется загрузить. В контекстном меню раскройте подменю "Журналы / Журналы сервера".
2. Выберите команду, соответствующую нужным критериям отбора записей. Можно загрузить записи о событиях, зарегистрированных в течение последнего часа, последних суток, или все записи. По команде "Создать запрос" выполняется создание запроса с переходом в панель "Журнал сервера" для настройки параметров запроса (см. стр.**56**).

   После выбора команды на загрузку записей о событиях, зарегистрированных в течение последнего часа, последних суток, или всех записей автоматически инициируется процесс получения записей из журнала сервера безопасности. По окончании загрузки записей в панели событий системы появится уведомление о получении журнала. Для перехода к записям журнала выберите в уведомлении ссылку "Журнал получен".

Создание запросов с произвольными критериями отбора

Запросы с произвольными критериями отбора записей создаются для последующей настройки параметров и запуска процесса получения записей вручную.

Создание запросов для загрузки записей журнала сервера безопасности выполняется в панели "Журнал сервера".

Для создания общего запроса:

1. В панели управления запросами нажмите кнопку "Новый".

   В панели "Журнал сервера" будет создан новый запрос, и справа появится панель для настройки его параметров.

2. Настройте параметры нового запроса (см. стр.**56**) и нажмите кнопку "Выполнить запрос к БД" в нижней части панели настройки параметров запроса.

Будет инициирован процесс получения записей из журнала. По окончании загрузки записей в панели событий системы появится уведомление о получении журнала со ссылкой для перехода к новому запросу.

Создание запросов на загрузку записей журнала сервера безопасности из файлов

Записи журнала сервера безопасности могут храниться в файлах специального формата *.snsrv. Загрузка записей из таких файлов в панель "Журнал сервера" осуществляется путем создания отдельных запросов для каждого файла.

Файл для загрузки можно указать при запуске программы в автономном режиме (см. стр.7) или во время работы с программой в панели "Журнал сервера".

Для создания запроса на загрузку записей из файла в панели "Журнал сервера":

1. В панели управления запросами нажмите кнопку "Открыть".

   На экране появится диалог открытия файла ОС Windows.
2. Выберите нужный файл.

   В панели "Журнал сервера" будет создан новый запрос, в который будут загружены записи из файла.

Запросы для архивов журналов

Для просмотра записей журналов, помещенных в архивы, необходимо загрузить файлы нужных архивов в программу.

Внимание!

Для загрузки архивов требуется достаточное свободное пространство на диске, который используется для временных файлов (разархивирование осуществляется в папке временных файлов пользователя). Чтобы загружать архивы размером до 80—100 МБ, необходимо около 4 ГБ свободного пространства. Для работы с архивами размером 200-300 МБ требуется не менее 10 ГБ.

После загрузки архивов создаются запросы для отбора нужных записей. Создание запросов выполняется в панели "Архивы". В программе предусмотрены следующие способы создания запросов:

- создание запроса для отбора записей отдельного журнала в загруженном архиве;
- создание запросов для отбора записей журнала событий тревоги или журнала станций в загруженных архивах.

Загрузка файлов архивов

Сервер безопасности создает архивы журналов в файлах специального формата *.omax.

Файлы архивов для загрузки можно указать при запуске программы в автономном режиме (см. стр.7) или во время работы с программой в панели "Архивы".

Примечание.

В программе управления поддерживается загрузка файлов архивов, созданных сервером безопасности СЗИ Secret Net версии 7.0 и выше.

Для загрузки файлов архивов в панели "Архивы":

1. В панели управления запросами нажмите кнопку "Открыть".

   На экране появится диалог открытия файла ОС Windows.
2. Выберите нужные файлы.

   В панели "Архивы" будут созданы новые подразделы, количество и названия которых соответствуют выбранным файлам архивов. Подразделы содержат иерархические списки компьютеров и журналов, записи которых получены из архивов. Основные сведения о загруженных архивах отображаются в области сведений, которая расположена под панелью управления запросами.

Создание запроса для отбора записей отдельного журнала в загруженном архиве

В загруженном архиве можно создавать запросы для отбора записей отдельных журналов, представленных в иерархическом списке архива. Такие запросы относятся только к выбранному журналу соответствующего компьютера и не допускают загрузку других записей, хранящихся в архиве.

Для создания запроса для отбора записей отдельного журнала:

1. В разделе "Архивы" панели управления запросами раскройте список подраздела с названием нужного архива.
2. Наведите указатель на строку журнала и дважды нажмите левую кнопку мыши.

   В панели "Архивы" будет создан новый запрос, в котором отобразятся сведения из выбранного журнала.

Создание запроса для отбора записей журнала событий тревоги или журнала станций в загруженных архивах

Среди загруженных архивов можно сделать выборку из всех записей журналов событий тревоги или журналов станций, хранящихся в архивах. Запрос для отбора записей этих журналов позволяет получить записи, поступившие с различных компьютеров, и может применяться к нескольким выбранным архивам.

Для создания запроса для отбора записей журнала событий тревоги или журнала станций:

1. В панели управления запросами нажмите кнопку "Новый" и в появившемся меню выберите нужный тип запроса:
   - "Найти в журналах тревог" — создает запрос для выборки записей из журналов событий тревоги;
   - "Найти в журналах станций" — создает запрос для выборки записей из журналов станций.

   В панели "Архивы" будет создан новый запрос, и справа появится панель для настройки его параметров.
2. Настройте параметры нового запроса (см. стр.**56**) и нажмите кнопку "Найти в архивах" в нижней части панели настройки параметров запроса.

   Будет инициирован процесс получения записей из выбранных архивов.

Настройка параметров запроса

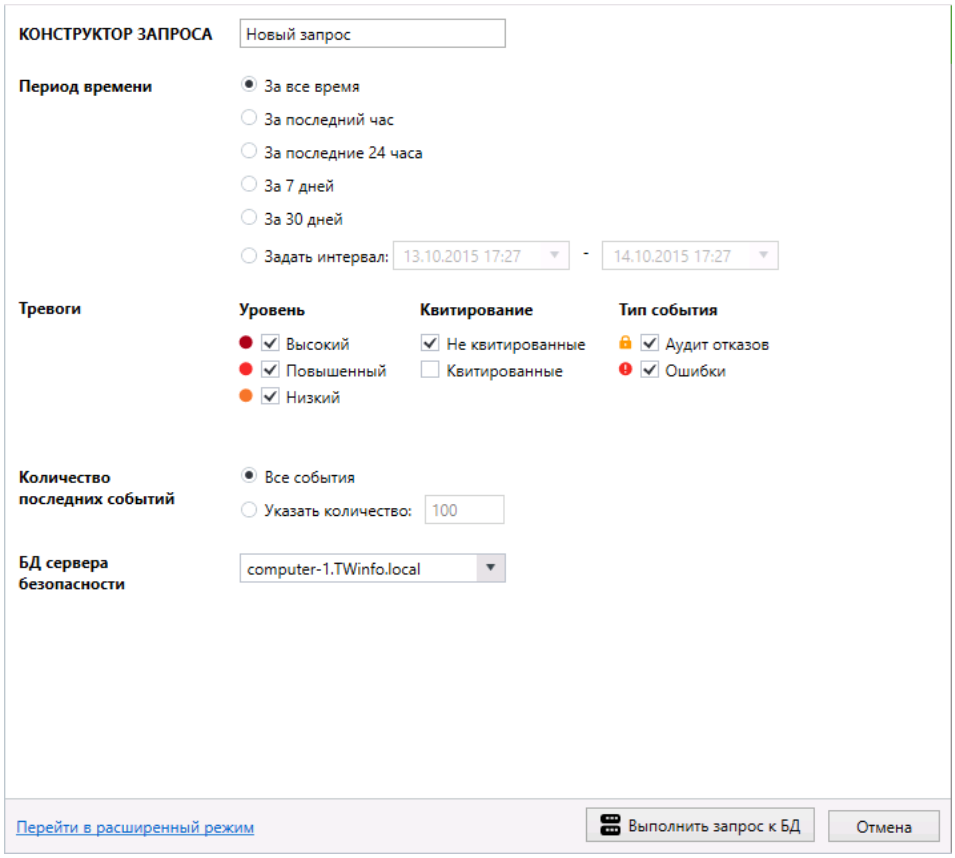
Для получения нужных сведений в запросе записей журнала можно изменять параметры загрузки и фильтрации записей. Настройка параметров осуществляется в специальной панели настройки.

Для настройки параметров запроса записей:

1. Включите отображение панели настройки параметров запроса. Чтобы включить или отключить отображение панели, используйте кнопку "Запрос" в панели настройки вывода сведений (справа от области отображения сведений).

   Примечание.
   Панель настройки параметров запроса отображается по умолчанию для созданного запроса с произвольными критериями отбора.

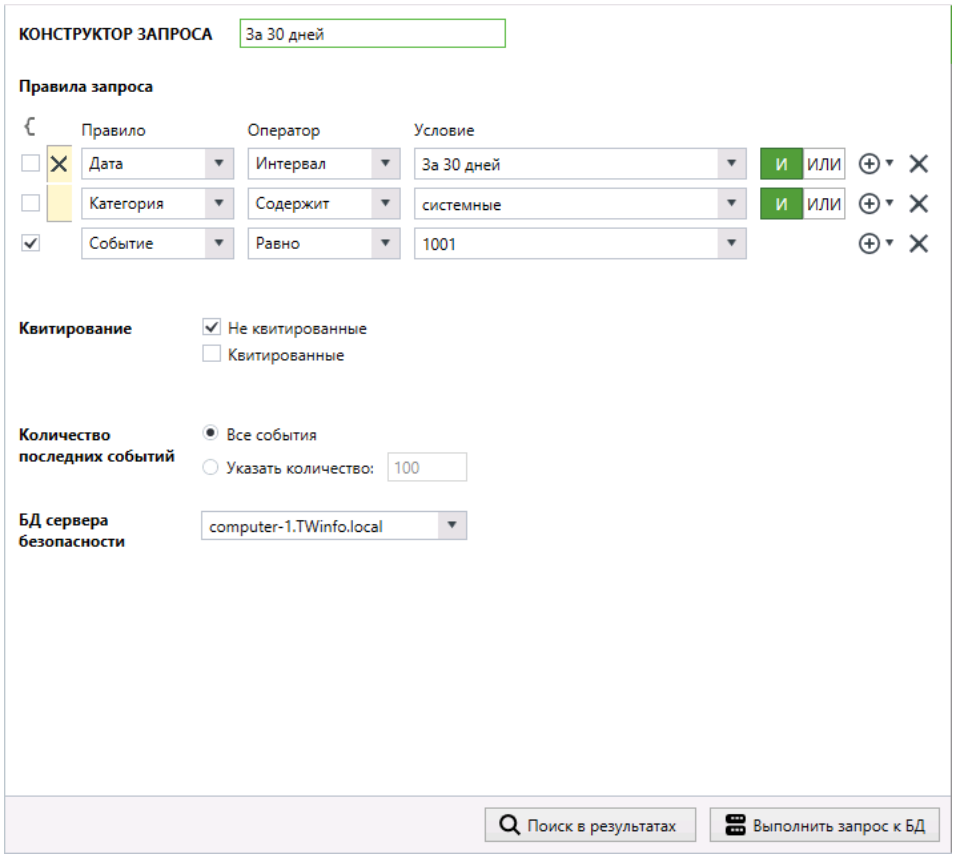
   Пример содержимого панели для журнала событий тревоги представлен на следующем рисунке.



2. Введите имя запроса и настройте параметры отбора записей в соответствующих полях. Состав настраиваемых параметров зависит от источника сведений, типов журналов и текущего режима панели настройки.

Для созданного запроса с произвольными критериями отбора по умолчанию панель представлена в упрощенном режиме, который позволяет указать основные параметры отбора записей (см. рисунок выше). При необходимости детализировать параметры включите расширенный режим настройки с помощью ссылки "Перейти в расширенный режим" в нижней части панели.

Пример содержимого панели в расширенном режиме настройки представлен на следующем рисунке.



3. Для применения заданных параметров используйте соответствующую кнопку в нижней части панели настройки:
   - Чтобы сделать новую выборку записей журнала из базы данных сервера безопасности, нажмите кнопку "Выполнить запрос к БД".
   - Чтобы сделать выборку записей из числа загруженных, нажмите кнопку "Поиск в результатах".

   Совет.
   В этом случае изменение параметров "Количество последних событий" и "БД сервера безопасности" не будет учтено при повторной выборке записей. Для применения этих параметров нажмите кнопку "Выполнить запрос к БД".

Управление запросами

В панелях "Журналы тревог", "Журналы станций" и "Журналы сервера" предусмотрены следующие возможности управления запросами (кроме запросов с предопределенными критериями отбора и запросов на загрузку из файлов):

- включение и отключение режима автоматической загрузки запроса;
- сохранение параметров запроса в файле;
- загрузка параметров запроса из файла;
- повторная загрузка записей из БД сервера безопасности.

Операции по управлению запросами выполняются с помощью кнопок в панели управления запросами. Средства управления перечислены в следующей таблице:

Кнопка	Описание
★	Включает и отключает режим автоматической загрузки запроса в следующих сеансах работы с программой. При включенном режиме кнопка выделена цветом

Кнопка	Описание
	Сохраняет выбранный запрос в файле. Сохранение осуществляется в файл формата *.snreq
	Запускает процесс новой загрузки записей в соответствии с текущими параметрами запроса
Открыть	Вызывает диалог открытия файла для загрузки запроса. Чтобы загрузить ранее сохраненный запрос, укажите тип файла "Запрос (*.snreq)". После загрузки запрос добавляется в раздел "Запросы" соответствующей панели журналов (в панель того журнала, для которого был создан запрос)

Для закрытия запроса используйте кнопку "Закрыть" справа от его названия.

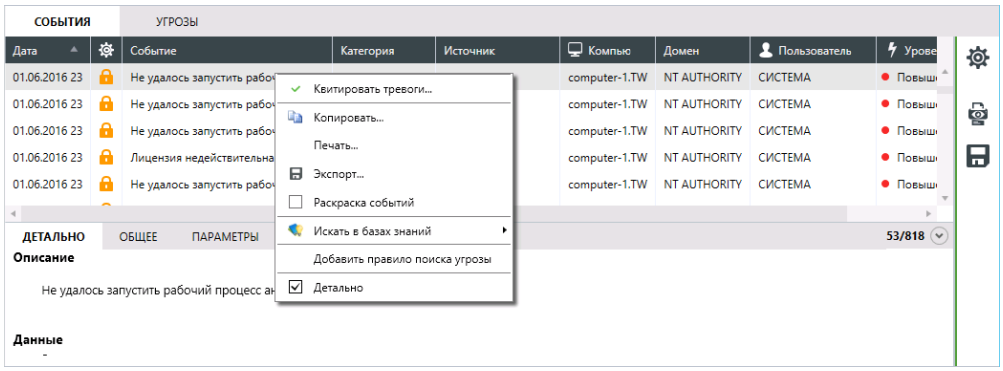
Возможности при просмотре записей

Режимы отображения сведений о событиях

Загруженная информация о событиях выводится в области отображения сведений соответствующей панели (см. стр. **48**). Для анализа содержимого журналов предусмотрены различные режимы отображения сведений (кроме журнала сервера безопасности). Помимо вывода информации в виде обычного списка записей программа предоставляет возможность просмотра сведений в виде списков событий угроз.

Режим "События"

В режиме "События" выводится список загруженных записей журналов в табличной форме. Это основной и наиболее функциональный режим для просмотра и управления записями. Пример содержимого окна с таблицей записей представлен на следующем рисунке.

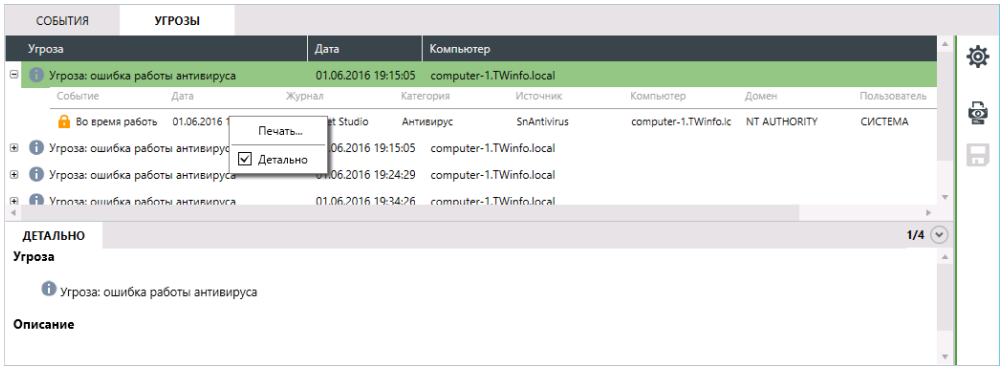


С помощью контекстного меню записей выполняются необходимые действия: копирование, печать, сохранение и др.

В правой части строки под таблицей содержится счетчик записей: <номер выбранной записи>/<количество выбранных записей>/<общее количество загруженных записей>.

Режим "Угрозы"

В режиме "Угрозы" выводится список событий угроз, полученных в результате анализа загруженных записей. События угроз представляют собой сжатые или разъясняющие сведения о зарегистрированных событиях (например, событие угрозы с признаками подбора пароля). Режим предназначен для представления администратору или аудитору наиболее важной для них информации из журналов. Пример содержимого окна с полученным списком представлен на следующем рисунке.



Информация выводится в табличной форме с возможностью раскрытия списков зарегистрированных событий, относящихся к событиям угроз. При просмотре табличных блоков с записями журналов могут использоваться те же функции настройки отображения, как и в основной таблице с записями журнала.

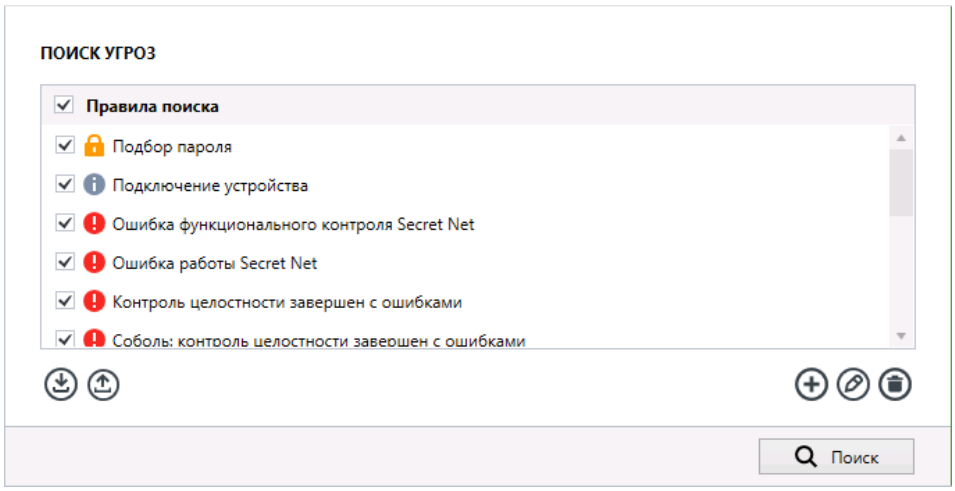
С помощью команд контекстного меню событий угроз (такое меню показано на рисунке) можно отправить список на печать или включить/отключить отображение области описания событий.

В правой части строки под таблицей содержится счетчик событий угроз: <номер выбранного события>/<общее количество событий>.

Для настройки анализа записей и поиска событий угроз:

1. Загрузите записи журнала.
2. Переключите область отображения сведений в режим "угрозы" с помощью кнопки в верхней части области.
3. Нажмите кнопку "Запрос" в панели настройки вывода сведений (справа от области отображения сведений).

   На экране появится панель настройки параметров поиска угроз.



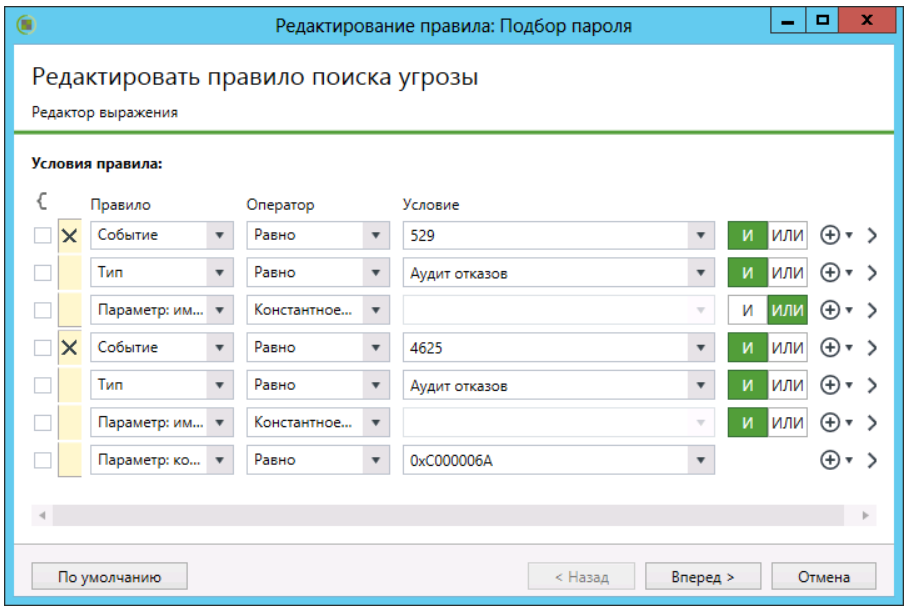
   В списке представлены правила поиска событий угроз в загруженных записях журнала. По умолчанию список содержит предустановленные правила поиска общего характера. Эти правила поиска нельзя удалить из списка.

4. Сформируйте список правил поиска событий угроз. Управление правилами осуществляется с помощью кнопок под списком. Для формирования списка предусмотрены следующие возможности:
   - добавление и удаление правил поиска угроз (с помощью кнопок "Добавить правило поиска угрозы" и "Удалить правило угрозы" справа под списком правил);
   - загрузка списка правил, сохраненного в файле (с помощью кнопки "Импорт правил угроз" слева под списком правил).

5. Настройте параметры поиска событий угроз. Настройка осуществляется отдельно для каждого правила с помощью мастера. При создании нового правила запуск мастера происходит автоматически. Чтобы настроить параметры имеющегося правила, выберите его в списке и нажмите кнопку "Редактировать правило угрозы" справа под списком правил.

   Диалоги мастера настройки параметров правила:

   - Диалог "Редактор выражения". Пример диалога представлен на следующем рисунке.



   Составьте список условий, которым должны удовлетворять записи для соответствия данному событию угрозы. Условия определяют содержимое полей в записях о событиях или параметров в описаниях событий. Для контроля содержимого поля или параметра в списке должно присутствовать выражение, задающее допустимые значения. Например, для поля "Тип" можно задать значение "Аудит отказов", чтобы при анализе рассматривались записи о событиях только этого типа.

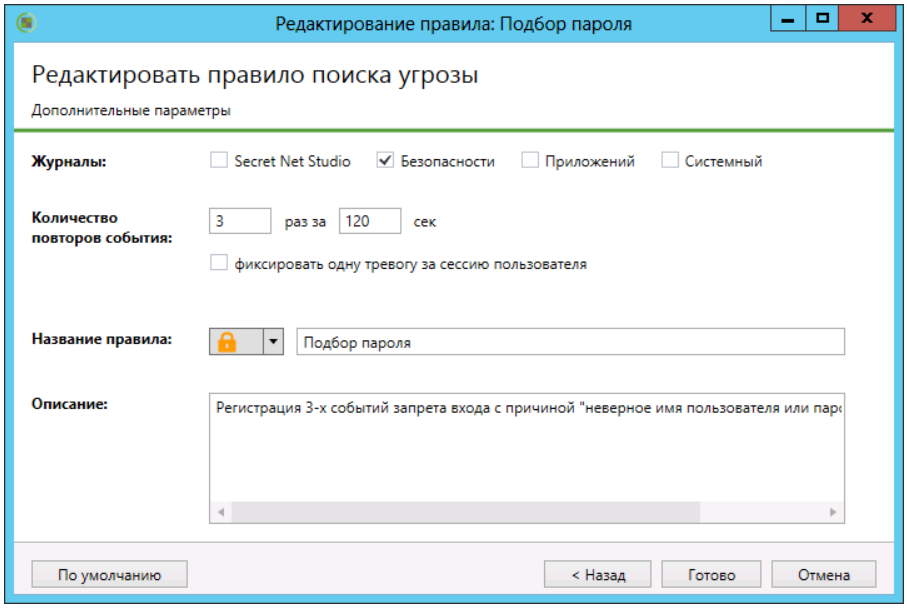
   Несколько выражений логически связываются между собой. Предусмотрены возможности использования логических операторов И, ИЛИ, а также группирования выражений. Например, можно задать обязательное совпадение заданных значений для полей "Тип", "Источник" и "Компьютер", чтобы при анализе не рассматривались записи, у которых хотя бы одно из значений в указанных полях не совпадает с заданным.

   Для формирования списка условий используйте следующие средства управления:

   - средства группировки выражений (слева) — для объединения в группу отметьте нужные выражения и нажмите кнопку с фигурной скобкой, которая расположена над списком. Чтобы отменить группировку, нажмите кнопку в виде крестика в зоне группирования;
   - средства определения условий для содержимого поля или параметра (в центре) — чтобы задать условие, укажите в раскрывающихся списках название нужного поля или параметра и его значения;
   - средства выбора логической операции со следующим выражением или группой (кнопки "И/ИЛИ") — чтобы включить действие логического оператора, нажмите его кнопку (действующий оператор выделен зеленым цветом);
   - средства добавления и удаления выражений (справа).

   После формирования списка условий нажмите кнопку "Вперед" для перехода к следующему диалогу мастера.

- Диалог "Дополнительные параметры". Пример диалога представлен на следующем рисунке.



Отметьте журналы, записи которых будут рассматриваться при анализе на соответствие данному событию угрозы.

В группе полей "Количество повторов события" укажите параметры отслеживания нескольких записей, удовлетворяющих заданным условиям. Если требуется отследить повторяющиеся события, произошедшие в течение некоторого промежутка времени (например, для контроля попыток подбора пароля), укажите нужное количество повторов и интервал времени в секундах.

При необходимости можно включить режим сжатия в одно событие угрозы для случаев, когда при анализе выявляется несколько таких событий за время одного сеанса работы пользователя (к которому относятся записи). За счет этого сокращается список событий угроз. Данный режим следует использовать, если последовательность событий угроз в пределах одного сеанса работы не важна. Для включения режима сжатия установите отметку в поле "фиксировать одну тревогу за сессию пользователя".

В полях групп "Название правила" и "Описание" укажите пиктограмму для события угрозы, его название и дополнительные сведения.

Примечание.
Если редактируемое правило поиска входит в список предустановленных правил, можно вернуться к конфигурации параметров по умолчанию, которая предусмотрена для данного правила. Для этого нажмите кнопку "По умолчанию" в нижней части диалога и подтвердите выполнение операции в появившемся диалоге запроса.

Чтобы применить заданные параметры, нажмите кнопку "Готово" в диалоге мастера настройки параметров правила.

6. После настройки правил поиска событий угроз при необходимости сохраните список правил в файл для дальнейшего использования. Для этого нажмите кнопку "Экспорт правил угроз" слева под списком правил.
7. Отметьте в списке события угроз, поиск которых нужно выполнить, и нажмите кнопку "Поиск" в нижней части панели настройки параметров поиска угроз.

   После анализа загруженных записей появится список полученных событий угроз.

Примечание.
Правила поиска угроз можно создавать непосредственно при работе с записями журналов. Для этого выделите нужные записи, вызовите контекстное меню и выберите команду "Добавить правило поиска угрозы". Далее настройте параметры правила в диалогах мастера настройки (аналогично вышеописанной процедуре).

Квитирование событий тревоги в журнале

Для квитирования в запросе с записями журнала событий тревоги:

1. Загрузите записи журнала событий тревоги из БД сервера безопасности (см. стр.**51**).
2. В списке записей журнала выделите записи о событиях, которые необходимо квитировать.
3. Вызовите контекстное меню одной из выбранных записей и выберите команду "Квитировать тревоги".

   На экране появится диалог для ввода текстового комментария.
4. Введите текстовый комментарий с описанием причин и принятых мер по факту возникновения событий и нажмите кнопку "Квитировать".

   В панели событий системы появится уведомление о квитировании событий тревоги, и признак квитирования будет присвоен выбранным записям.

Сортировка записей

Отображаемые записи сортируются по значениям, содержащимся в определенных колонках таблицы записей. Сортировка таблицы записей выполняется стандартными способами. Для сортировки по содержимому колонки наведите указатель на ее заголовок и нажмите левую кнопку мыши.

Поиск записей

Программа позволяет выполнить поиск записей, удовлетворяющих заданным параметрам или содержащих текстовую строку. Поиск осуществляется только среди отображаемых записей в текущем запросе.

Для поиска записей по заданным параметрам:

1. Загрузите записи журнала и настройте параметры запроса (см. стр.**51**).
2. Нажмите кнопку "Поиск в результатах".

   В таблице записей будут выделены все записи, удовлетворяющие заданным параметрам в запросе.

Цветовое оформление записей

Для наглядного представления информации предусмотрено цветовое оформление отображаемых записей (кроме журнала сервера безопасности).

При включенном режиме цветового оформления записи выделяются заданными цветами. Описание настройки параметров цветового оформления см. на стр.**76**.

Для включения режима цветового оформления:

1. Загрузите записи журнала (см. стр.**51**).
2. Вызовите контекстное меню любой записи и выберите команду "Раскраска событий".

   Записи будут выделены цветами, соответствующими характеристикам событий.

   Отключение режима цветового оформления выполняется аналогично.

Получение сведений о событиях из внешних баз знаний

При необходимости получения дополнительных сведений о зарегистрированном событии программа позволяет выполнить запрос информации во внешних базах знаний, размещаемых в сети Интернет. Внешние базы знаний могут содержать полезную информацию о причинах возникновения конкретных событий и рекомендации для пользователей. Предоставление информации во внешних базах знаний регулируется владельцами информационных ресурсов.

Получение информации во внешних базах знаний не предусмотрено для записей журнала сервера безопасности.

Для загрузки сведений компьютер должен иметь доступ в сеть Интернет.

Для формирования запроса информации во внешней базе знаний:

1. Загрузите записи журнала (см. стр.**51**).
2. Вызовите контекстное меню записи о событии, по которому требуется получить информацию, раскройте подменю "Искать в базах знаний" и выберите соответствующую команду:
   - Microsoft Knowledge Base — для поиска в базе знаний на сайте http://www.microsoft.com;
   - Event ID Database — для поиска в базе знаний на сайте http://www.eventid.net.

   На экране появится окно веб-обозревателя, в котором будет загружена страница с результатами поиска в базе знаний.

Печать записей

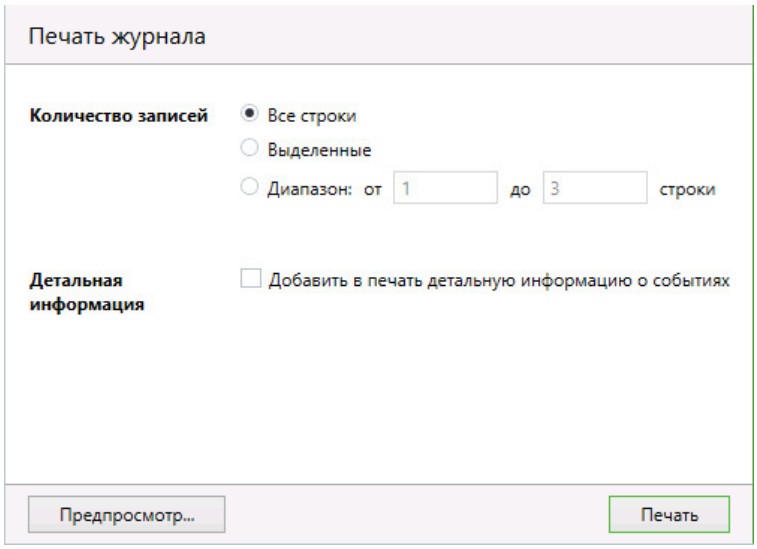
Программа позволяет отправлять на печать записи текущего запроса. Настройка параметров осуществляется в специальной панели настройки.

Возможность печати не предусмотрена для журнала сервера безопасности.

Для печати записей:

1. Загрузите записи журнала (см. стр.**51**).
2. Если требуется распечатать часть загруженных записей, выделите нужные записи в таблице.
3. Нажмите кнопку "Печать журнала" в панели настройки вывода сведений (справа от области отображения сведений).

   На экране появится панель настройки параметров печати.



4. Настройте параметры печати.

Группа полей "Количество записей"
Определяет, какие записи будут распечатаны: • "Все строки" — выполняется печать записей, отображаемых в соответствии с текущими параметрами фильтрации; • "Выделенные" — выполняется печать только тех записей, которые выделены в таблице; • "Диапазон" — позволяет задать диапазон записей для печати по порядку их следования в таблице (в соответствии с текущими параметрами сортировки). Границы диапазона определяются в полях "от" и "до". Первая и последняя записи диапазона также будут распечатаны
Поле "Детальная информация"
Если установлена отметка, будет распечатано содержимое полей с детальным описанием событий

5. Чтобы открыть окно предварительного просмотра страниц, нажмите кнопку "Предпросмотр" в нижней части панели настройки параметров печати. После просмотра запустите процесс с помощью стандартной кнопки отправки на печать на панели инструментов окна предварительного просмотра.

   Примечание.
   Запуск процесса печати можно выполнить без открытия окна предварительного просмотра. Для этого нажмите кнопку "Печать" в нижней части панели настройки параметров печати.

   На экране появится диалог ОС Windows для выбора принтера и настройки общих параметров печати.
6. Выберите принтер и нажмите кнопку "OK".

Экспорт записей

Программа позволяет экспортировать (сохранять) в файлы записи текущего запроса. Настройка параметров осуществляется в специальной панели настройки.

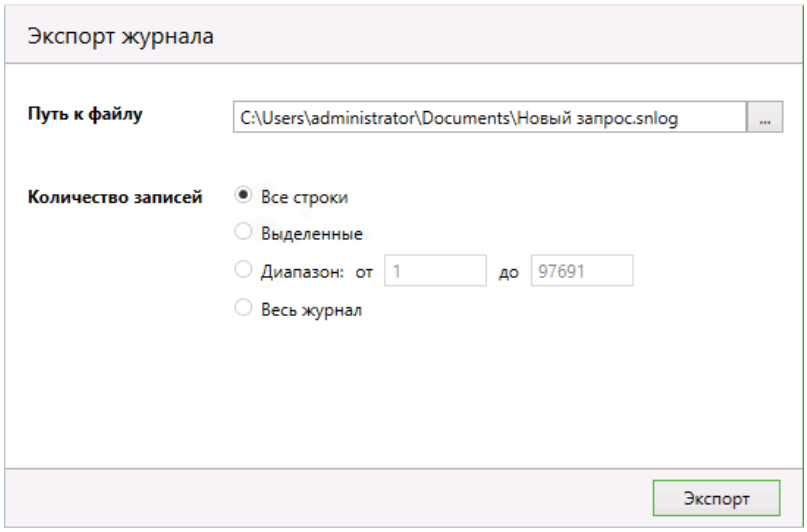
Экспорт осуществляется в файлы специальных форматов:

- записи журнала событий тревоги — экспортируются в файлы формата *.snua;
- записи журнала станций — экспортируются в файлы формата *.snlog;
- записи журнала сервера безопасности — экспортируются в файлы формата *.snsrv.

Для экспорта записей:

1. Загрузите записи журнала (см. стр.51).
2. Если требуется экспортировать часть загруженных записей, выделите нужные записи в таблице.
3. Нажмите кнопку "Экспорт журнала" в панели настройки вывода сведений (справа от области отображения сведений).

   На экране появится панель настройки параметров экспорта.



4. Чтобы указать файл для сохранения, нажмите кнопку в правой части поля "Путь к файлу" и выберите размещение в диалоге сохранения файла ОС Windows.
5. Настройте параметры экспорта.

Группа полей "Количество записей"
Определяет, какие записи будут экспортированы: • "Все строки" — выполняется экспорт записей, отображаемых в соответствии с текущими параметрами фильтрации; • "Выделенные" — выполняется экспорт только тех записей, которые выделены в таблице; • "Диапазон" — позволяет задать диапазон записей для экспорта по порядку их следования в таблице (в соответствии с текущими параметрами сортировки). Границы диапазона определяются в полях "от" и "до". Первая и последняя записи диапазона также будут экспортированы; • "Весь журнал" — выполняется экспорт всех записей, загруженных в запрос (в том числе тех, которые не удовлетворяют текущим параметрам фильтрации)

6. Нажмите кнопку "Экспорт".

Архивирование централизованных журналов по команде администратора

Архивирование централизованных журналов, хранящихся в БД сервера безопасности, выполняется регулярно в соответствии с заданными параметрами для сервера безопасности (см. стр.**27**).

При работе с программой управления можно выполнить запуск процесса внеочередного архивирования централизованных журналов. Команда архивирования применяется к серверу безопасности, с которым установлено соединение программы.

Для запуска процесса архивирования журналов:

1. В диаграмме управления или в списке объектов вызовите контекстное меню сервера безопасности, раскройте подменю "Архивирование" и выберите команду "Создать архив журналов".

   На экране появится диалог для настройки параметров архивирования.
2. Настройте параметры архивирования, представленные ниже. После настройки нажмите кнопку "Архивировать".

Поля "События до"
Поля определяют границу интервала времени. В архив будут помещены записи, которые были зарегистрированы до указанного момента времени

Поле "Журналы"
Поле определяет типы журналов, записи которых должны архивироваться
Поле "Комментарий"
Введите в этом поле краткое описание создаваемого архива

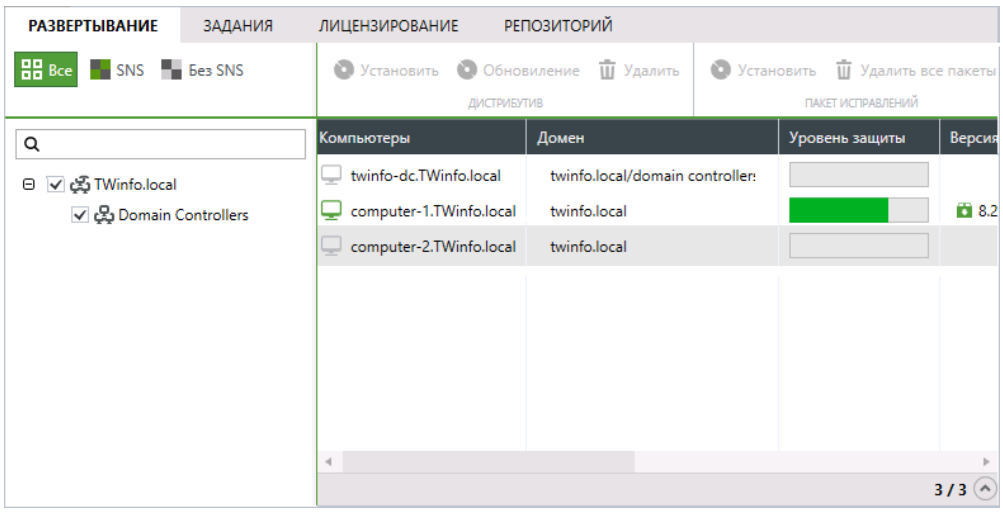
Глава 6
Настройка и контроль централизованного развертывания ПО

Программа управления содержит средства организации централизованного развертывания клиентского ПО системы Secret Net Studio на компьютерах. При развертывании автоматически выполняются заданные действия по установке или удалению на компьютерах клиента Secret Net Studio, его компонентов или обновлений. Запуск установки или удаления ПО на компьютерах осуществляется под управлением сервера безопасности от имени специальной службы.

Внимание!
Для централизованного развертывания ПО компьютеры должны удовлетворять требованиям к аппаратному и программному обеспечению для установки клиента (см. документ [**2**]). В частности, необходимо разрешить использование портов для доступа к общим ресурсам: 137, 138, 139, 445. Данные порты по умолчанию закрыты брандмауэром при отсутствии на компьютере сетевых папок общего доступа.

Панель средств настройки и контроля

Настройка и контроль централизованного развертывания ПО осуществляются в панели "Развертывание". Панель имеет вид, подобный представленному на следующем рисунке.



Для работы со средствами настройки и контроля развертывания ПО в панели предусмотрены следующие вкладки:

- "Развертывание" — предназначена для отображения структуры управления (слева) и вывода списка компьютеров со сведениями о наличии ПО и статусе (справа);
- "Задания" — предназначена для отображения заданий развертывания (слева) и компьютеров, связанных с заданиями (справа);
- "Лицензирование" — предназначена для просмотра сведений о зарегистрированных лицензиях на сервере безопасности и управления лицензиями;
- "Репозиторий" — предназначена для формирования списка централизованно устанавливаемого ПО.

Переключение между вкладками осуществляется с помощью соответствующих кнопок в верхней части панели.

Управление лицензиями на использование механизмов защиты

В системе Secret Net Studio действуют лицензионные ограничения на использование подсистем, реализующих применение механизмов защиты. Лицензии поставляются в виде файлов, содержащих данные для регистрации в системе Secret Net Studio.

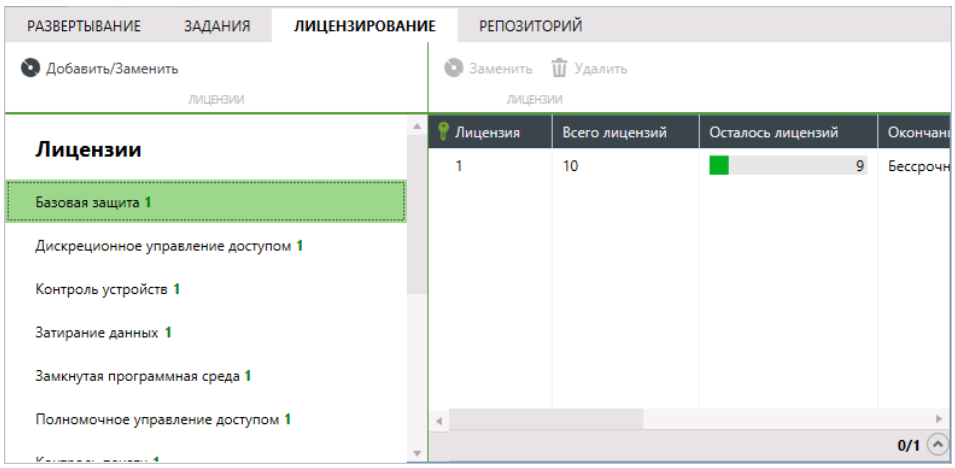
При формировании заданий развертывания ПО (см. стр.71) необходимо указать соответствующие лицензии. Лицензии можно выбрать из списка зарегистрированных на сервере безопасности или добавить отдельно для задания развертывания.

Для управления зарегистрированными лицензиями используется вкладка "Лицензирование" в панели "Развертывание". Вкладка содержит сведения о лицензиях, зарегистрированных в домене безопасности сервера подключения (сервер безопасности, с которым установлено соединение программы):

- назначение лицензий (для каких подсистем применяются);
- общее количество и текущее количество незадействованных (оставшихся) лицензий;
- время окончания действия лицензированных возможностей;
- типы лицензий;
- сведения о компании — получателе лицензии.

Для регистрации лицензий:

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



2. Нажмите кнопку "Добавить/Заменить", которая расположена над списком лицензируемых подсистем в разделе "Лицензии".

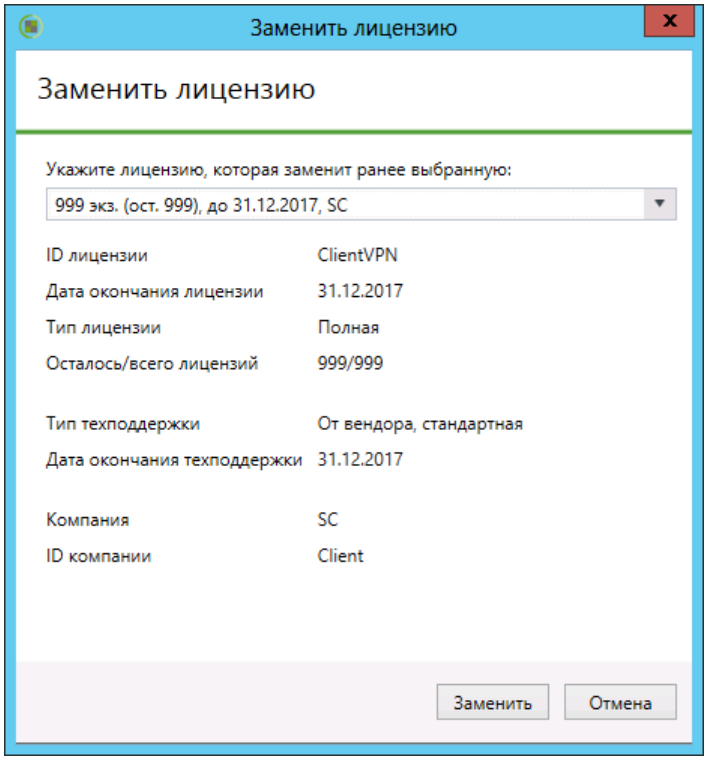
   На экране появится диалог для выбора файла.

3. Выберите нужный файл с лицензиями.

Для замены зарегистрированных лицензий:

1. В панели "Развертывание" перейдите на вкладку "Лицензирование".
2. В списке "Лицензии" (слева) выберите подсистему, для которой нужно заменить используемые лицензии.
3. В списке доступных лицензий на использование подсистемы (справа) выберите лицензии для замены.
4. Нажмите кнопку "Заменить", которая расположена над списком лицензий.

   На экране появится диалог для выбора лицензии.



5. Выберите лицензию в раскрывающемся списке и нажмите кнопку "Заменить".

Для удаления зарегистрированных лицензий:

1. В панели "Развертывание" перейдите на вкладку "Лицензирование".
2. В списке "Лицензии" (слева) выберите подсистему, для которой нужно удалить используемые лицензии.
3. В списке доступных лицензий на использование подсистемы (справа) выберите лицензии для удаления.

> **Примечание.**
> Удаление лицензии невозможно, если она используется хотя бы на одном защищаемом компьютере.

4. Нажмите кнопку "Удалить", которая расположена над списком лицензий.

   На экране появится запрос на продолжение операции.
5. Нажмите кнопку "Да" в диалоге запроса.

Настройка развертывания

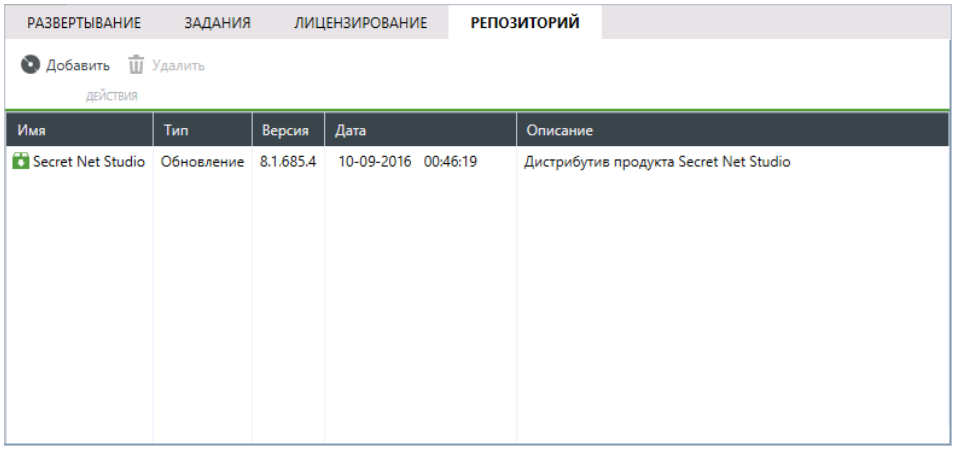
Формирование списка централизованно устанавливаемого ПО

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

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

Для добавления комплекта установочных файлов:

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



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

   На экране появится диалог для добавления.

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

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

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

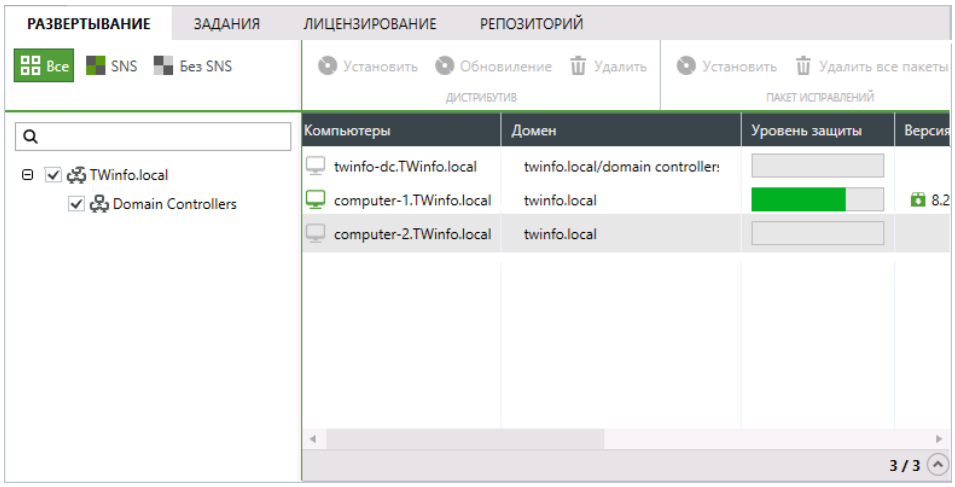
   По окончании процесса в списке появится новый элемент, содержащий сведения о загруженном комплекте.

Формирование заданий развертывания

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

Для добавления задания развертывания:

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



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

   Список компьютеров можно фильтровать по наличию или отсутствию установленного ПО клиента (кнопки "SNS", "Без SNS"), по принадлежности

контейнерам Active Directory (отображаются компьютеры тех контейнеров, которые отмечены в структуре управления слева), а также по наличию в названии заданной строки символов (поля для поиска расположены над списком контейнеров AD и над таблицей со списком компьютеров). Сортировка списка компьютеров выполняется стандартными методами с помощью заголовков колонок.

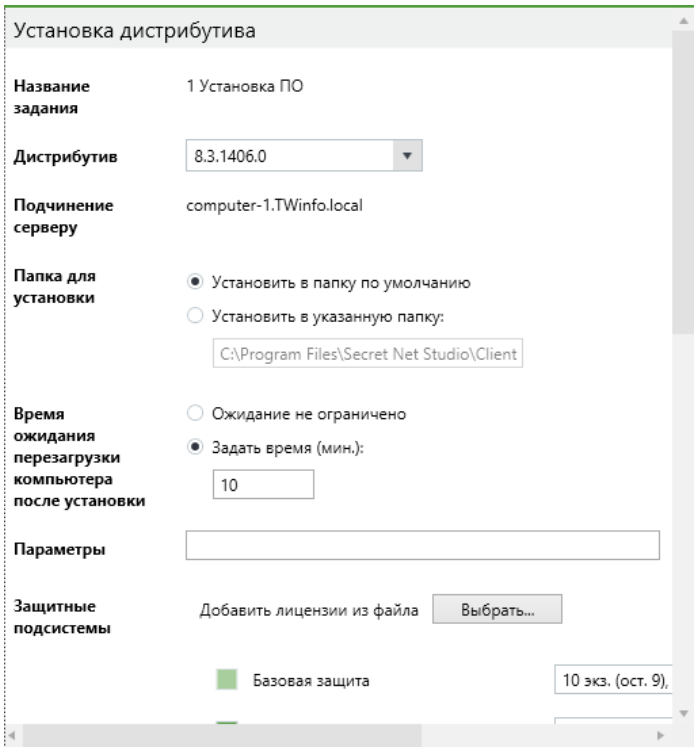
В таблице можно изменять состав отображаемых колонок и порядок их следования. Чтобы настроить колонки, вызовите контекстное меню в строке заголовков, выберите команду "Настройка колонок" и в появившемся диалоге сформируйте список отображаемых колонок.

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

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

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

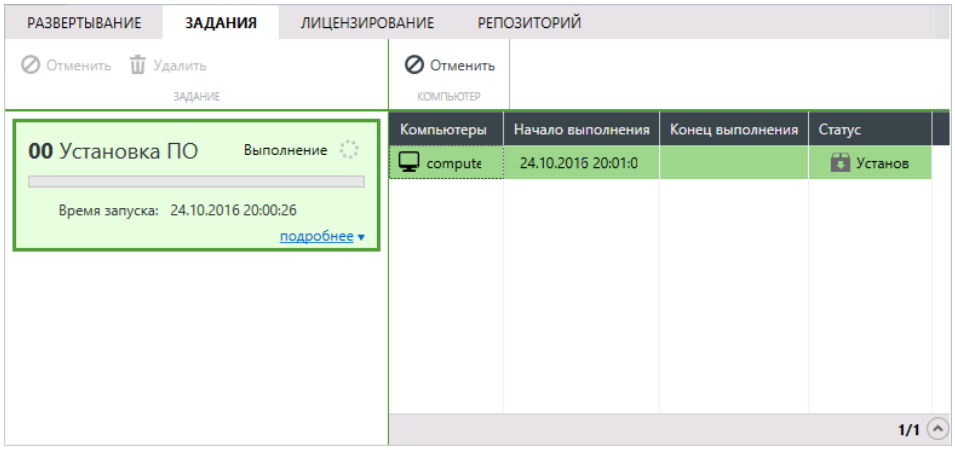
   В правой части окна появится панель настройки параметров задания.



4. Настройте параметры задания и нажмите кнопку "Установить" в нижней части панели. Для задания на установку ПО клиента выполняется настройка следующих параметров:
   - версия устанавливаемого ПО;
   - папка для установки ПО;

- время ожидания перезагрузки компьютера после установки — если выбран вариант "Ожидание не ограничено", автоматическая перезагрузка компьютера после установки ПО не выполняется. Для включения режима автоматической перезагрузки выберите вариант "Задать время" и в поле ввода укажите, через сколько минут после завершения установки следует выполнить автоматическую перезагрузку;
- параметры — определяет параметры командной строки, с которыми будет запущена программа установки;
- лицензии на использование компонентов;
- учетные данные локального администратора (доменного пользователя, входящего в локальные группы администраторов на выбранных компьютерах).

5. После создания задания перейдите к списку заданий на вкладке "Задания" для проверки добавления нового элемента.



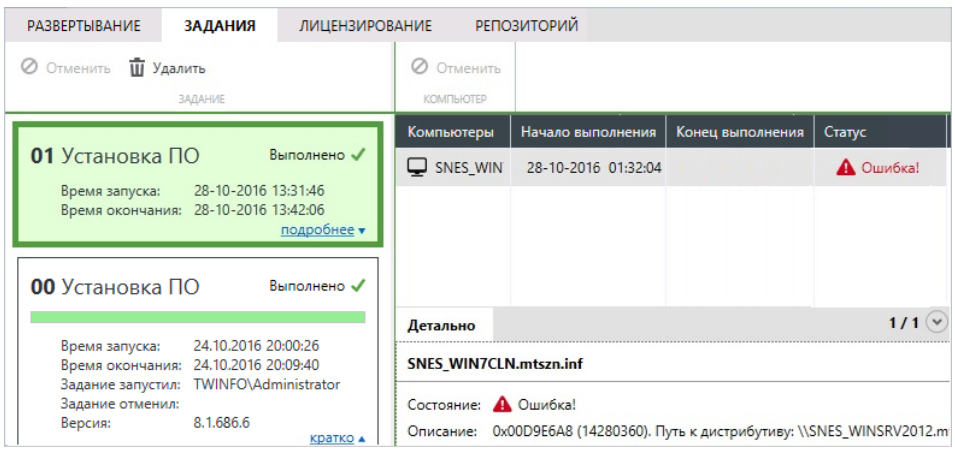
Контроль выполнения заданий

Сформированные задания применяются на компьютерах в соответствии с заданными параметрами. Администратор может контролировать процесс развертывания ПО с помощью списка заданий.

Для контроля выполнения заданий:

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

   Пример содержимого вкладки представлен на следующем рисунке.



   Для заданий и компьютеров выводятся сведения о времени и статусе выполнения процессов.

2. Для вывода дополнительных сведений о задании нажмите кнопку "Подробнее" в нижней части информационного блока. Для просмотра подробных сведений о компьютере можно включить отображение области сведений с

помощью кнопки, которая расположена в правой части строки под списком компьютеров.

Примечание.
Если для нормально функционирующего компьютера статус ожидания запуска процесса сохраняется длительное время, проверьте соответствие компьютера требованиям к аппаратному и программному обеспечению для установки клиента (см. документ [**2**]). Например, выполнение задания возможно при условии, что на компьютере разрешено использование портов для доступа к общим ресурсам: 137, 138, 139, 445. Данные порты по умолчанию закрыты брандмауэром при отсутствии на компьютере сетевых папок общего доступа. Для разрешения использования указанных портов можно изменить параметры брандмауэра или создать произвольную папку и открыть к ней общий доступ.

3. При необходимости прервать выполнение задания:
   - чтобы прервать выполнение на всех компьютерах, к которым относится задание, — выберите его и нажмите кнопку "Отменить", которая расположена над списком заданий в разделе "Задание";
   - чтобы прервать выполнение на отдельных компьютерах — выберите их в списке и нажмите кнопку "Отменить", которая расположена над списком компьютеров в разделе "Компьютер".
4. После завершения выполнения задания его можно удалить из списка. Для этого выберите его и нажмите кнопку "Удалить", которая расположена над списком заданий в разделе "Задание".

Приложение

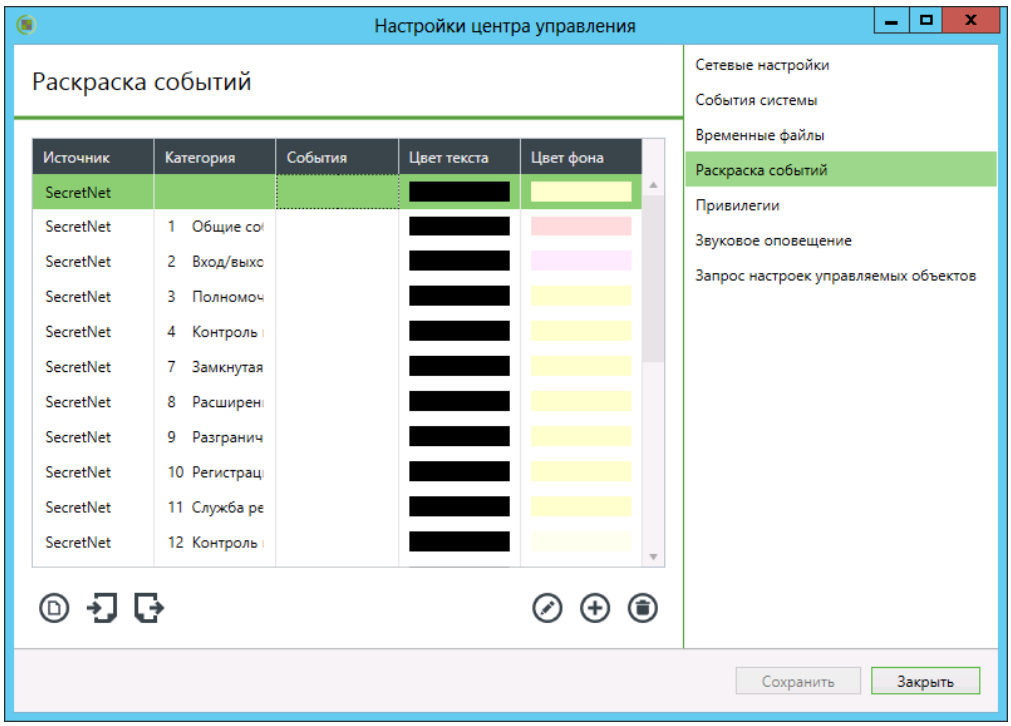
Параметры сетевого взаимодействия

Наименование параметра, пояснение	Диапазон
Группа параметров "Время ожидания"	
Разрешения имени DNS	30–1000 с
Соединения с сервером	30–1000 с
Отправки запроса на сервер	30–1000 с
Окончания передачи следующего блока 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	30–1000 с
Событий для рабочей станции Определяет промежуток времени, через который сервером 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	30–1000 с
Сервером ответа на контрольный запрос Определяет максимальное время ожидания ответа на отправленный контрольный запрос. Параметр предназначен для контроля установленного соединения	30–1000 с
Группа параметров "Размер блока"	
Для приема данных от сервера 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	48–10240 Кб
Для передачи данных на сервер 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	48–10240 Кб

Параметры цветового оформления записей журналов

При настройке параметров работы программы (см. стр. **10**) можно сформировать список правил, определяющих цвет текста и фона отображаемых записей журналов в зависимости от заданных условий. Список правил представлен в группе "Раскраска событий" диалога настройки параметров программы.

Пример списка правил представлен на следующем рисунке.

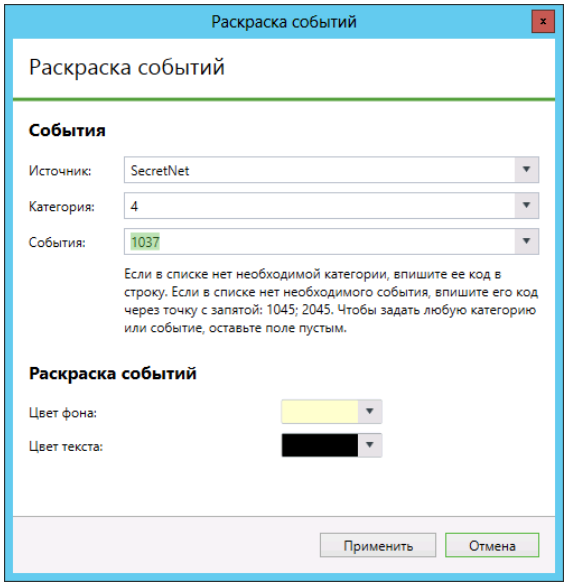


Управление списком правил осуществляется с помощью кнопок, расположенных под списком:

Кнопка	Описание
Взять значения по умолчанию	Возвращает исходный список правил, используемый по умолчанию
Импортировать	Загружает список правил, сохраненный в файле
Экспортировать	Сохраняет текущий список правил в файле
Редактировать	Вызывает диалоговое окно для настройки параметров выбранного правила (см. ниже)
Добавить	Добавляет новое правило в список. Для нового правила выполняется настройка параметров в диалоговом окне (см. ниже)
Удалить	Удаляет выбранный элемент из списка

Настройка параметров правила

Пример диалогового окна настройки параметров правила представлен на следующем рисунке.



Для настройки параметров правила:

1. В группе полей "События" настройте параметры анализа событий:

Источник
Содержит имя компонента или подсистемы, которое указывается при регистрации событий в качестве источника. Выберите нужный источник
Категория
Содержит числовой код категории событий. Выберите код нужной категории из раскрывающегося списка или введите значение вручную. Список категорий, доступных для выбора, формируется в зависимости от указанного источника
События
Содержит числовые идентификаторы событий. Выберите идентификаторы нужных событий из раскрывающегося списка или введите значение вручную. Список событий, доступных для выбора, формируется в зависимости от указанной категории. Несколько идентификаторов разделяются символом ";"

Примечание.
Сведения о событиях можно получить при просмотре записей журнала на вкладке "Общее" (см. стр.48). Источники, коды категорий и идентификаторы событий представлены, соответственно, в следующих полях вкладки: "Источник", "Код категории" и "Событие".

2. В группе полей "Раскраска событий" настройте параметры цветового оформления фона и текста строк в таблице записей. Для вызова средств изменения цвета нажмите кнопку в правой части поля.
3. Нажмите кнопку "Применить".

Восстановление журналов из архивов

Записи централизованных журналов, помещенные в архив из БД сервера безопасности, могут быть снова восстановлены в базе данных сервера с помощью программы управления. Восстановленные записи могут быть загружены для просмотра так же, как и другие записи, хранящиеся в БД.

Внимание!
Выполнять восстановление архивов может только пользователь, которому предоставлена привилегия "Архивирование/восстановление журналов".

Для восстановления записей из архива:

1. В диаграмме управления или в списке объектов вызовите контекстное меню сервера безопасности, раскройте подменю "Архивирование" и выберите команду "Восстановить архив журналов".

   На экране появится диалог, содержащий список доступных для восстановления архивов.

2. Выберите нужный архив, журналы (если архив содержит несколько журналов) и нажмите кнопку "Восстановить".

Рекомендации по обслуживанию СУБД для сервера безопасности

Перестроение индексов

Для ускорения обработки запросов к БД сервера безопасности в СУБД автоматически создаются специальные объекты — индексы. Индексы содержат сведения для поиска по массивам в базе данных.

В процессе эксплуатации сервера безопасности содержимое базы данных меняется. Наиболее объемные изменения в БД связаны, как правило, с обработкой централизованных журналов. В частности, после архивирования журналов высвобождается часть отведенной памяти в базе данных. Эти изменения со временем могут приводить к фрагментации данных, что в свою очередь повлияет на производительность сервера.

Чтобы поддерживать нормальный режим работы базы данных, рекомендуется регулярно запускать процедуру перестроения индексов на сервере СУБД (в среднем, достаточно одного раза в неделю). Процедура перестроения индексов не требует остановки функционирования сервера, однако для оптимального выполнения рекомендуется запускать команду в моменты наименьшей нагрузки.

Для перестроения индексов можно использовать командные файлы, прилагаемые на установочном диске комплекта поставки системы Secret Net Studio. Перед использованием файлов выполните следующие действия:

1. На сервере СУБД создайте каталог на локальном диске и скопируйте в него с установочного диска содержимое каталога \Tools\SecurityCode\ClearMSSQL\.
2. Откройте для редактирования скопированные файлы с расширением *.cmd и укажите в них пароль администратора БД, заданный при установке сервера СУБД. Пароль должен быть указан вместо подстроки manager.

После этого запустите на исполнение файл rebuild.cmd во время наименьшей загруженности сервера СУБД. Для запуска файла в определенный момент можно использовать, например, Планировщик заданий Windows.

Примечание.

Периодическое перестроение индексов также можно настроить с помощью штатных средств управления сервером СУБД. Для этого нужно создать для сервера задание на выполнение процедуры в определенные моменты времени. Пример последовательности команд для такого задания представлен в файле \Tools\SecurityCode\ClearMSSQL\runjob.sql. Сформировать задание на основе последовательности команд в файле runjob.sql можно с помощью файла runjob.cmd.

Контроль заполнения базы данных

Если база данных сервера безопасности размещена в СУБД свободно распространяемого варианта (например, MS SQL Server 2012 Express), размер базы не может превышать внутреннее ограничение СУБД. В зависимости от версии ограничение может быть установлено 4 или 10 Гб.

Сервер безопасности отслеживает заполнение базы данных. При достижении определенного объема БД (по умолчанию от 80%) объект сервера в программе оперативного управления отображается с особой пиктограммой, сигнализирующей о переполнении базы (см. стр.**35**). Кроме того, в общих параметрах сервера выводится соответствующее предупреждение.

При угрозе переполнения базы данных необходимо срочно уменьшить ее размер. Для этого, например, можно выполнить внеочередное архивирование централизованных журналов по команде администратора (см. стр.**66**).

Очистка базы данных в случае переполнения

При переполнении базы данных сервера безопасности работа с базой блокируется, и сервер становится неработоспособен. Чтобы этого не произошло,

необходимо контролировать заполнение базы (см. выше) и регулярно выполнять действия для поддержания приемлемого объема БД. В частности, нужно соответствующим образом настроить параметры автоматического архивирования централизованных журналов (см. стр.**27**).

Если переполнение БД все же произошло, для восстановления работы сервера необходимо очистить базу данных.

Внимание!

Очистка базы данных приведет к потере всей хранящейся в ней информации, включая содержимое журналов, поступивших на централизованное хранение.

Для очистки базы данных:

1. На сервере безопасности остановите работу служб IIS (служба веб-публикации) и Secret Net Studio Security Server (служба сервера).
2. Если на сервере СУБД отсутствует каталог с командными файлами для перестроения индексов, создайте такой каталог на локальном диске и подготовьте файлы (см. действия **1**–**2** в разделе о настройке перестроения индексов).
3. Запустите на исполнение файл clear.cmd. После успешного завершения обработки этого файла запустите процедуру перестроения индексов с помощью файла rebuild.cmd.
4. Перезагрузите сервер безопасности.

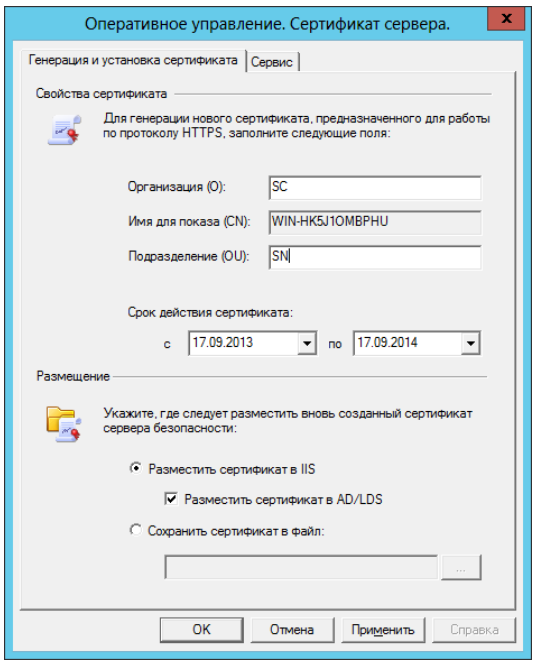
Генерация и установка сертификата сервера безопасности

Процедура выполняется на компьютере сервера безопасности.

Для генерации и установки нового сертификата СБ:

1. Выполните соответствующее действие в зависимости от версии установленной операционной системы:
   - на компьютере под управлением ОС Windows Server 2012 загрузите начальный экран "Пуск" и выберите элемент "Сертификаты" (относится к группе "Код Безопасности");
   - на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код Безопасности | Secret Net Studio | Сертификаты".

   На экране появится диалоговое окно настройки:



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

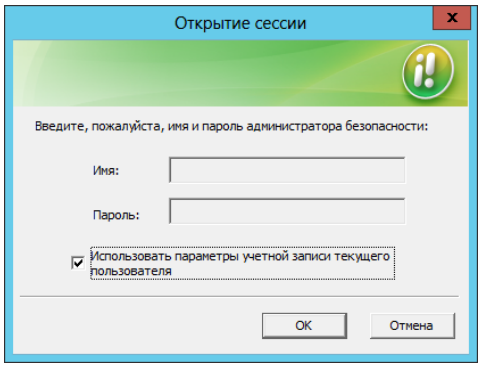
   Примечание.
   Поля "Организация" и "Подразделение" необязательны для заполнения.

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 хранилище объектов централизованного управления, и нажмите кнопку "ОК".

Пояснения.

Если текущий пользователь имеет права на запись — отметьте поле "Использовать параметры учетной записи текущего пользователя". Если права не предоставлены — введите данные соответствующей учетной записи. По умолчанию правами на запись в хранилище обладают пользователи, входящие в группу администраторов домена безопасности.

После установки нового сертификата на экране появится сообщение об этом.

Сведения о настройке защищенного соединения со службами каталогов

В системе Secret Net Studio предусмотрен режим усиленной защиты доступа к хранилищу объектов централизованного управления Secret Net Studio. В этом режиме сетевые обращения к службам AD LDS, выполняемые компонентами системы Secret Net Studio, осуществляются с использованием протоколов Secure Socket Layer/Transport Layer Security (SSL/TLS). Данные протоколы предусматривают проверку подлинности компьютера, на котором развернута служба каталогов (сервер безопасности), и реализуют функции установления безопасного соединения с использованием сертификатов.

Для использования режима усиленной защиты в системе должна быть организована и настроена инфраструктура открытых ключей (PKI). Реализация PKI может обеспечиваться стандартными средствами ОС Windows или ПО сторонних производителей. Ниже в данном разделе приводятся общие сведения о порядке организации и настройки PKI с применением стандартных средств ОС.

Защита взаимодействия с AD LDS

Для защиты взаимодействия со службами AD LDS настройка PKI выполняется в следующем порядке:

1. В доверенном центре сертификации (Certification Authority, ЦС) запросите сертификат для сервера безопасности. Для сертификата необходимо указать полное доменное имя компьютера сервера безопасности и метод использования "Проверка подлинности сервера" (Server Authentication). Полученный сертификат сохраните в хранилище в контексте компьютера, раздел "Личное" (или "Личные").

   Примечание.
   Если в системе отсутствует ЦС, для организации защищенных соединений можно использовать самозаверенный сертификат, созданный на сервере безопасности. Этот сертификат в дальнейшем применяется и как сертификат компьютера, и как сертификат ЦС.

2. Установите полученный сертификат в IIS. Для этого запустите диспетчер служб IIS (IIS Manager) и в зависимости от версии ОС выполните соответствующие действия:
   - В иерархическом списке раскройте раздел сайтов, вызовите контекстное меню элемента "Default Web Site" и выберите команду "Изменить привязки" (Edit Bindings).
   - В появившемся списке привязок сайта вызовите диалог настройки для элемента с типом "https" и выберите полученный сертификат в списке SSL-сертификатов.
   - После установки сертификата выполните перезапуск IIS с помощью соответствующей команды управления в контекстном меню элемента "Default Web Site".

3. Предоставьте необходимые разрешения для доступа к файлу ключа сертификата. Для этого в программе Проводник перейдите к каталогу по умолчанию, в котором хранятся ключи. Местоположение каталога в ОС Windows Server 2012: %ProgramData%\Microsoft\Crypto\RSA\MachineKeys. В других версиях ОС: %ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA\MachineKeys. В каталоге вызовите окно настройки свойств файла ключа сертификата (определить нужный файл в списке можно по дате и времени создания), перейдите на вкладку "Безопасность" и добавьте в список нужную учетную запись с разрешениями по умолчанию. Имя добавляемой учетной записи зависит от того, на каком компьютере установлен сервер безопасности:
   - если СБ установлен на контроллере домена под управлением ОС Windows Server 2012 — учетная запись с именем SecretNetLDS;

- если СБ установлен на контроллере домена под управлением другой ОС — учетная запись с именем SecretNetLDS$;
- если СБ установлен на любом другом компьютере — учетная запись с именем NETWORK SERVICE.

4. На компьютере сервера безопасности поместите сертификат сервера в раздел "Личное" (или "Личные") хранилищ в контексте экземпляров служб SecretNet и SecretNet-GC. Для этого загрузите оснастку "Сертификаты" в режиме управления сертификатами компьютера и в режиме управления сертификатами каждой службы (т. е. загружаются три оснастки). Выполните экспорт сертификата сервера вместе с закрытым ключом из раздела "Личное" (или "Личные") оснастки с сертификатами компьютера и затем импорт в разделы "ADAM_ SecretNet\Личное" и "ADAM_ SecretNet-GC\Личное" (или "ADAM_ SecretNet\Личные" и "ADAM_ SecretNet-GC\Личные") оснасток с сертификатами служб. После этого предоставьте разрешения для доступа к файлам ключей импортированных сертификатов (см. действие **3**).

Примечание.
На компьютере под управлением ОС Windows Server 2008 вместо процедур экспорта и импорта можно выполнить копирование сертификата вместе с закрытым ключом непосредственно в оснастке "Сертификаты". Сертификат копируется из раздела "Личное" (или "Личные") оснастки с сертификатами компьютера в разделы "ADAM_ SecretNet\Личное" и "ADAM_ SecretNet-GC\Личное" (или "ADAM_ SecretNet\Личные" и "ADAM_ SecretNet-GC\Личные") оснасток с сертификатами служб. После этого не требуется выполнять процедуру предоставления разрешений доступа к файлам ключей сертификатов.

5. На компьютерах, подчиненных серверу безопасности, поместите сертификат центра сертификации в раздел "Доверенные корневые центры сертификации" хранилища в контексте компьютера. Распространение сертификата можно выполнить, например, с помощью групповых политик. Для этого используется файл с этим сертификатом (если файл отсутствует, его можно создать путем экспорта сертификата из хранилища). Файл с сертификатом импортируется в оснастке групповой политики в раздел "Параметры безопасности | Политики открытого ключа | Доверенные корневые центры сертификации".

6. Если имеется еще один сервер безопасности, выполните вышеперечисленные действия применительно к этому серверу.

7. На каждом сервере безопасности выполните следующие действия:

- Загрузите программу управления сертификатами сервера безопасности (с помощью элемента "Сертификаты" в разделе основного меню "Код Безопасности") и выполните синхронизацию сертификата, установленного в IIS, с сертификатом сервера безопасности. Для этого в диалоговом окне настройки перейдите на вкладку "Сервис" и нажмите кнопку "Синхронизировать".
- Откройте конфигурационный файл ServerConfig.xml, который размещается в каталоге установки сервера безопасности. Найдите параметр UseSSLConnection и измените значение false на true. В параметре Name (расположен ниже) измените значение на полное доменное имя компьютера сервера безопасности. Сохраните изменения и перезагрузите компьютер.

8. Включите режим усиленной защиты трафика на защищаемых компьютерах. Для этого в программе управления выберите нужные объекты в панели "Компьютеры", перейдите на вкладку "Состояние" и включите параметр "Шифровать управляющий сетевой трафик". Параметр начнет действовать на компьютерах после их перезагрузки.

Документация

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