Код безопасности
ГК «Информзащита»

Средство защиты информации

SECRET NET 6

Руководство администратора

Мониторинг и оперативное управление

RU.88338853.501410.007 91 6

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

Версия: 6.5 Последнее обновление: 14-09-10

Оглавление

Список сокращений **4**

Введение **5**
Основные задачи мониторинга и оперативного управления 5

Глава 1. Начало работы с программой мониторинга **6**
Предоставление прав для работы с программой 6
Запуск программы 6
Интерфейс программы 7
Элементы интерфейса 7
Настройка параметров работы программы 8
Использование срезов 9
Управление файлами срезов 9
Формирование содержимого среза 9
Управление срезами в окне списка срезов 10

Глава 2. Мониторинг системы **11**
Просмотр сведений 11
Сведения в области списка объектов 11
Сведения в окне событий 15
Сведения в окне свойств объектов 17
Сортировка объектов 19
Поиск объектов 20
Отслеживание событий НСД 20
Оповещение о событиях НСД 20
Настройка фильтра событий НСД 21
Настройка счетчика количества событий НСД 22
Сброс признаков НСД 22

Глава 3. Оперативное управление **23**

Глава 4. Дополнительные средства программы **24**
Управление загрузкой данных 24
Формирование отчетов 24
Отчет "Паспорт ПО" 25
Отчет "Ресурсы рабочей станции" 25
Экспорт сведений об устройствах 27
Вызов программы просмотра журналов 27
Вызов программы конфигурирования 27
Вызов программы "Контроль программ и данных" 27
Вызов оснастки для управления групповой политикой домена 27
Вызов оснастки "Active Directory — пользователи и компьютеры" 28

Приложение **29**
Настройка элементов интерфейса 29
Параметры работы программы 29
Средства для работы со списками объектов 32
Навигация при работе со структурами объектов 32
Настройка отображения колонок в таблицах 32
Пиктограммы компьютеров в программе мониторинга 33
Пиктограммы защитных механизмов 33
Параметры сетевого взаимодействия 34

Терминологический справочник **35**

Документация **36**

Предметный указатель **37**

Список сокращений

AD	Active Directory
DNS	Domain Name System
RTF	Reach Text Format
БД	База данных
НСД	Несанкционированный доступ
ОС	Операционная система
ОУ	Оперативное управление
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
РС	Рабочая станция
СБ	Сервер безопасности

Введение

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

Перед изучением данного руководства необходимо предварительно ознакомиться с документом [1].

Условные обозначения

В руководстве для выделения некоторых элементов текста (примечаний и ссылок) используется ряд условных обозначений.

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

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

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.
- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.
- Эта пиктограмма сопровождает информацию предостерегающего характера.

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

Другие источники информации

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru и hotline@infosec.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно на курсах Учебного центра "Информзащита". Перечень курсов и условия обучения представлены на сайте http://www.itsecurity.ru/. Связаться с представителем учебного центра можно по электронной почте (edu@infosec.ru).

Основные задачи мониторинга и оперативного управления

В сетевом режиме функционирования системы Secret Net 6 реализована возможность централизованного мониторинга и оперативного управления системой защиты. Под мониторингом системы защиты подразумевается контролирование состояния компьютеров, на которых установлено клиентское ПО системы Secret Net 6 в сетевом режиме функционирования (далее — защищаемые компьютеры или агенты). Контроль осуществляется в режиме реального времени. Оперативное управление заключается в незамедлительном воздействии на защищаемые компьютеры.

Основными задачами мониторинга и оперативного управления являются:

- контролирование и оповещение о произошедших событиях несанкционированного доступа (НСД);
- контролирование текущего состояния защищаемых компьютеров (какие компьютеры являются активными, какие пользователи работают на компьютерах и пр.);
- выполнение действий с защищаемыми компьютерами при возникновении угроз для безопасности системы.

Мониторинг и оперативное управление системой защиты осуществляет администратор оперативного управления. При необходимости обязанности могут быть возложены и на главного администратора безопасности или его помощников.

Глава 1
Начало работы с программой мониторинга

Предоставление прав для работы с программой

Возможность работы с программой мониторинга предоставляется сотрудникам, ответственным за управление системой защиты. Права на управление защищаемыми компьютерами определяются наличием следующих привилегий:

- "Просмотр информации ОУ" — пользователь может подключиться к определенному серверу безопасности и контролировать состояние компьютеров;
- "Выполнение оперативных команд" — пользователь может использовать команды оперативного управления компьютерами.

Привилегии предоставляются пользователям в программе конфигурирования системы защиты. Сведения о работе с этой программой см. в документе [7].

Запуск программы

Для запуска программы мониторинга:

1. Активируйте команду "Пуск | Все программы | Код безопасности | Secret Net | Монитор".

   На экране появится основное окно программы мониторинга.

2. Если в данной локальной сети имеется несколько серверов безопасности, на экране появится диалог выбора сервера, с которым будет установлено соединение. Выберите в списке нужный сервер безопасности.

   Выбранный сервер безопасности будет корневым элементом иерархии в программе мониторинга (см. стр. 8). Вследствие этого в программу будут загружены сведения только о тех компьютерах, которые относятся к данному серверу и к его подчиненным серверам. Сведения о других компьютерах, которые относятся к вышестоящим серверам безопасности или к серверам других ветвей подчинения, не будут загружены в программу.

   При подключении к серверу безопасности проверяется наличие установленного сертификата сервера, после чего имеющийся сертификат сравнивается с сертификатом, установленным в AD. Если сертификат сервера отсутствует или срок его действия истек, соединение с сервером не устанавливается. Генерацию и установку нового сертификата сервера можно выполнить на компьютере с установленным сервером безопасности в программе генерации сертификатов.

Интерфейс программы

По умолчанию основное окно программы мониторинга имеет вид:

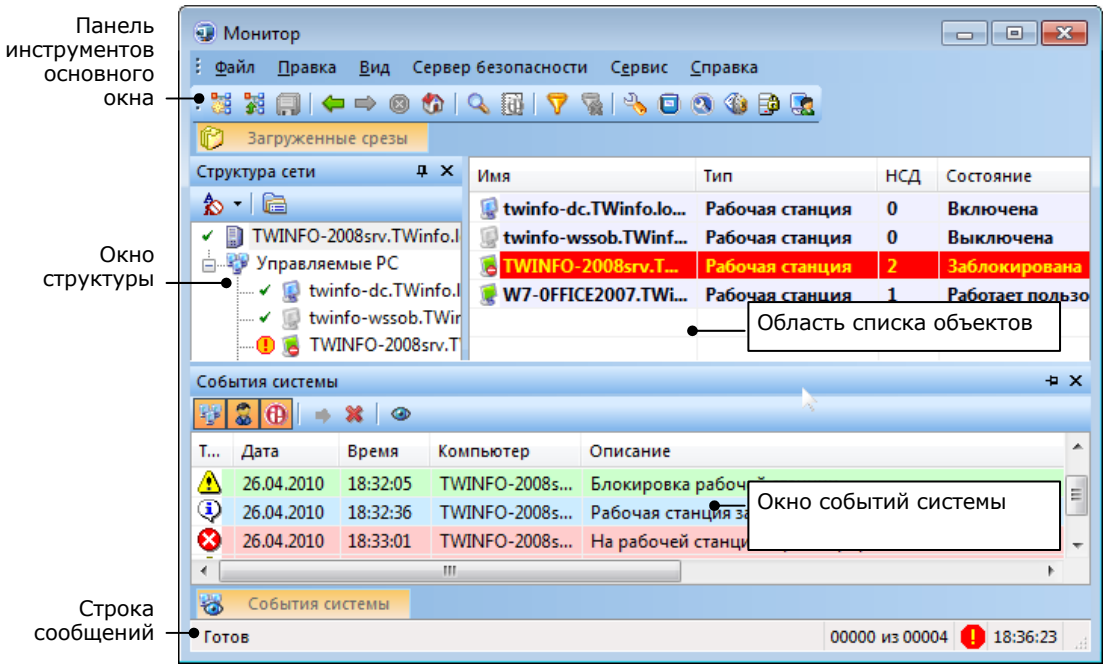


Рис. 1. Основное окно программы мониторинга

Пользователь может изменять состав отображаемых элементов и их расположение на экране (см. стр. 29). Параметры внешнего вида основного окна сохраняются в системном реестре компьютера и используются в следующих сеансах работы пользователя с программой.

При работе с большими объемами данных можно использовать средства навигации по структурам и средства настройки отображения таблиц (см. стр. 32).

Элементы интерфейса

Основное окно программы может содержать следующие элементы интерфейса:

Меню
Содержит команды управления программой
Панель инструментов основного окна
Содержит кнопки быстрого вызова команд управления и программных средств
Строка сообщений
Выводит служебные сообщения программы, а также краткие подсказки к командам и кнопкам панели инструментов. В правой части строки выделены зоны, в которых помещается следующая информация (в порядке следования слева направо): • порядковый номер выбранного элемента и общее количество отображаемых элементов в области списка объектов или в окне событий; • один из индикаторов оповещения. Индикатор НСД ( ) отображается, если в программе включен режим оповещения о событиях НСД (см. стр. 20). Индикатор соединения ( ) оповещает о том, что выполняется запрос к серверу безопасности; • текущее время.
Информационный заголовок
Название программы и имя выбранного элемента структуры (сервера безопасности, компьютера или папки структуры). В правой части заголовка могут отображаться вращающиеся пиктограммы, соответствующие индикаторам оповещения

Окно структуры
Содержит иерархический список структуры сети. Корневым элементом иерархии является сервер безопасности, с которым установлено соединение программы. Папка "Управляемые РС" содержит защищаемые компьютеры, относящиеся к данному серверу безопасности (включая компьютер самого сервера). Папка "Подчиненные СБ" содержит структуру объектов, относящихся к подчиненному серверу (серверам) безопасности. Для отображения состояния компьютеров используются пиктограммы (см. стр. 33). Дополнительно объекты структуры могут быть отмечены одним из следующих знаков: • — оповещает о зарегистрированных событиях НСД; • — оповещает об изменении аппаратной конфигурации компьютера (отображается, если отсутствует знак). При любых других условиях пиктограмма компьютера отмечена знаком ✔. Панель инструментов, расположенная в верхней части окна, содержит кнопки для сортировки объектов и вызова окна свойств для выбранного объекта
Область списка объектов
Содержит в табличной форме сведения о выбранном объекте. Перемещение колонок и изменение их ширины осуществляется способами, принятыми в среде Windows. В зависимости от выбранного объекта содержит: • для сервера безопасности — список защищаемых компьютеров и серверов всех уровней подчинения относительно данного сервера; • для папки "Управляемые РС" — список защищаемых компьютеров; • для папки "Подчиненные СБ" — список подчиненных серверов безопасности; • для компьютера — список открытых пользовательских сессий (закладка "Сессии"), список зарегистрированных событий НСД (закладка "НСД на станции"), список устройств компьютера (закладка "Конфигурация") или сведения о функционировании механизмов защиты (закладка "Защитные подсистемы"). Порядок следования закладок можно изменить путем их перемещения с помощью мыши. Состояние компьютеров также обозначается пиктограммами. Строки, содержащие сведения о компьютерах с признаком НСД, выделяются цветом (по умолчанию красный). Выбор цвета осуществляется при настройке параметров программы
Окно свойств объектов
Содержит подробную информацию об объекте, выбранном в окне структуры или в окне среза. Сведения представлены в виде списка параметров, который может быть структурирован по разделам или упорядочен по алфавиту. Переключение режима упорядочения осуществляется с помощью панели инструментов этого окна. При выборе параметра в нижней части окна отображается краткое пояснение
Окно среза
По своему назначению аналогично окну структуры объектов. В окне среза представлена структура защищаемых компьютеров, сформированная пользователем. Панель инструментов этого окна содержит кнопки, с помощью которых осуществляется сортировка объектов, вызов окна свойств выбранного объекта и формирование иерархического списка. Окно появляется при открытии среза
Окно списка загруженных срезов
Предназначено для управления срезами. Содержит пиктограммы срезов, загруженных в программу. Если срез содержит компьютеры с признаком НСД, пиктограмма среза выделена красным цветом. Порядок работы со списком срезов см. на стр. 10
Окно событий системы
Предназначено для отображения уведомлений мониторинга, а также записей о событиях НСД, произошедших на защищаемых компьютерах во время текущего сеанса работы программы. Сведения выводятся в виде таблицы в формате записей журналов. Перемещение колонок таблицы и изменение их ширины осуществляется стандартными способами, принятыми в среде Windows. Уведомления и записи о событиях сортируются в порядке времени возникновения. Панель инструментов этого окна содержит кнопки, с помощью которых осуществляется управление списком уведомлений

Настройка параметров работы программы

Для настройки параметров:

1. Активируйте команду "Сервис | Настройки...".

   На экране появится диалог "Настройки приложения".

2. Последовательно выбирая названия групп в левой части диалога, задайте в правой части нужные значения параметров. В большинстве случаев изменение значения осуществляется выбором нужного значения в ячейке с текущим значением параметра. Описание параметров содержится на стр. 29.

Использование срезов

Срез представляет собой совокупность защищаемых компьютеров, выбранных и сгруппированных по некоторым произвольным признакам. Назначение срезов состоит в том, чтобы предоставить пользователю возможность самостоятельно создавать списки компьютеров для более удобной работы с программой. Этим обеспечивается фильтрация общего списка защищаемых компьютеров.

Например, в срезе можно создать структуру помещений с находящимися в них компьютерами. Или, создав нужную структуру папок среза, отсортировать компьютеры в нужном порядке.

Количество одновременно загруженных срезов не ограничивается. Используя несколько загруженных в программу срезов, пользователь может работать с различными списками компьютеров, оперативно переключаясь между ними.

В отличие от общей структуры компьютеров, которая представлена в окне структуры, использование срезов предоставляет пользователю возможность осуществлять фильтрацию компьютеров. В срезе отображаются только те объекты, которые были выбраны при формировании среза. При этом один и тот же компьютер может присутствовать в различных папках среза. Кроме того, при создании списков в срезе не учитывается иерархия подчинения компьютеров серверам безопасности.

Содержимое срезов хранится в файлах специального формата *.slc. Эти файлы могут использоваться как в программе мониторинга, так и в программе просмотра журналов.

Управление файлами срезов

Операции выполняются с помощью команд меню и кнопок панели инструментов.

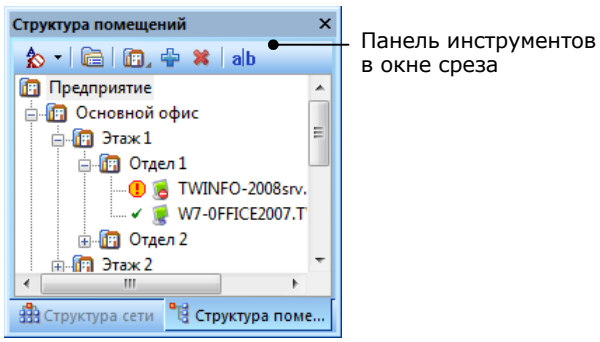
Табл. 1. Команды меню и кнопки для управления файлами срезов

Команда	Кнопка	Описание
Файл | Добавить срез | Новый		Создает новый файл среза. Имя файла и его местоположение указываются в стандартном диалоге сохранения файла ОС Windows
Файл | Сохранить все		Сохраняет изменения во всех загруженных срезах
Файл | Добавить срез | Существующий		Выполняет загрузку среза из файла. Имя файла и его местоположение указываются в стандартном диалоге открытия файла ОС Windows
Файл | Выгрузить срез		Выгружает срез из программы без сохранения изменений. Невыгруженные срезы при следующем запуске программы снова будут загружены (при условии, что файл среза не был удален)

Формирование содержимого среза

В срезе необходимо создать структуру защищаемых компьютеров. В первую очередь создается папка, которая будет являться корневым элементом иерархического списка. Затем в эту папку поочередно добавляются другие элементы (папки и компьютеры).

В приведенном на рисунке примере содержимое среза отражает структуру помещений предприятия с находящимися в них компьютерами:



Операции выполняются с помощью команд меню и кнопок специальной панели инструментов, расположенной в верхней части окна среза (см. рисунок).

Табл. 2. Команды меню и кнопки для формирования содержимого среза

Команда	Кнопка	Описание
Правка | Создать папку		Создает новую дочернюю папку. Если список пуст, будет создана корневая папка. Для пиктограмм папок предусмотрены различные варианты изображений. Выбор варианта пиктограммы осуществляется только при создании папки. Для выбора пиктограммы удерживайте кнопку нажатой до появления меню со списком предусмотренных вариантов. Установите указатель на нужную пиктограмму, после чего отпустите левую кнопку мыши
Правка | Добавить PC		Добавляет компьютеры в выбранную папку. Выбор компьютеров осуществляется в специальном диалоге из списка доступных для добавления объектов
Правка | Удалить узел		Удаляет из среза выбранный элемент структуры (папку или компьютер)
***<имя_папки>* | Удалить выбранные**		Удаляет группу компьютеров, выбранных в области списка объектов
Правка | Переименовать папку		Включает режим редактирования для переименования выбранной папки

Местоположение элементов структуры можно изменять. Перемещение элементов осуществляется стандартным способом с помощью мыши. Кроме того, предусмотрена возможность сортировки объектов в окне среза (см. стр. 19).

Управление срезами в окне списка срезов

Окно списка загруженных срезов предназначено для работы со срезами, загруженными в программу. Управление срезами осуществляется с помощью команд контекстного меню.

Табл. 3. Команды контекстного меню для управления срезами

Команда	Описание
Переименовать	Включает режим редактирования для переименования выбранного среза
Открыть	Открывает окно среза. Окно выбранного среза добавится к отображаемым дополнительным окнам программы. Если окно уже открыто, оно будет активировано (станет текущим окном)
Свойства	Вызывает диалог "Свойства среза"
Добавить | Новый	Создает новый файл среза (см. одноименную команду в Табл. 1 на стр. 9)
Добавить | Существующий	Выполняет загрузку среза из файла (см. одноименную команду в Табл. 1 на стр. 9)
Выгрузить	Выгружает срез из программы без сохранения сделанных изменений (см. одноименную команду в Табл. 1 на стр. 9)

Глава 2
Мониторинг системы

Информация о состоянии защищаемых компьютеров отображается программой мониторинга в режиме реального времени. При работе с программой могут использоваться различные возможности для оповещения о произошедших событиях и получения необходимых сведений.

Просмотр сведений

Сведения в области списка объектов

Область списка объектов предназначена для вывода различных сведений, относящихся к текущему выбранному элементу иерархической структуры (см. Рис. 1 на стр. 7). Сведения могут быть представлены в виде следующих списков:

- список защищаемых компьютеров и серверов безопасности;
- список пользовательских сессий, открытых на защищаемом компьютере;
- список записей о событиях НСД, зарегистрированных на защищаемом компьютере;
- иерархический список устройств аппаратной конфигурации компьютера;
- список механизмов защиты системы Secret Net 6.

Список защищаемых компьютеров и серверов безопасности

При выборе сервера безопасности или папки структуры в области списка объектов отображается список защищаемых компьютеров и серверов безопасности. Используется различное оформление элементов списка:

- полужирный шрифт и затемненный фон строки — объект "прямого" подчинения, т. е. непосредственно подчиненный серверу безопасности, с которым установлено соединение программы. К такому объекту можно применять команды оперативного управления (см. стр. 23);
- обычный шрифт и белый фон строки — объект "транзитивного" подчинения, т. е. относящийся к любому другому серверу. Чтобы применить к такому объекту команды оперативного управления, необходимо открыть другой сеанс работы с программой и установить соединение с соответствующим сервером безопасности (см. стр. 6).

Сведения о компьютерах и серверах безопасности отображаются в колонках:

Имя
Содержит пиктограмму и имя объекта (сервера безопасности или защищаемого компьютера)
Тип
Содержит наименование типа объекта
НСД
Содержит количество событий НСД, произошедших на защищаемом компьютере. При подключении компьютера к серверу безопасности отсчет событий НСД начинается с нуля. Обнуление счетчика происходит после отключения защищаемого компьютера от сервера (при потере соединения на длительное время, перезагрузке или выключении компьютера)
Состояние
Содержит краткое описание текущего состояния компьютера: • "Выключен" — сервер безопасности недоступен в данный момент; • "Выключена" — защищаемый компьютер недоступен в данный момент; • "Включен" — сервер безопасности функционирует нормально; • "Работает пользователь" — на защищаемом компьютере открыта сессия пользователя; • "Работают пользователи" — на защищаемом компьютере открыты несколько сессий; • "Заблокирована" — защищаемый компьютер заблокирован.

Неактивность
Содержит время последнего отключения подчиненного сервера безопасности или защищаемого компьютера. Сведения отображаются, если компьютер недоступен в данный момент
Сессии
Содержит количество открытых на защищаемом компьютере сессий пользователей
Версия
Содержит номер версии установленного программного обеспечения (ПО сервера безопасности или клиента)
Вариант
Содержит название текущего варианта применения клиентского ПО на защищаемом компьютере. Вариант применения "Full" предусматривает доступность всех защитных функций клиента
Статус ФК
Содержит результат проведения функционального контроля при запуске компьютера
Лицензирование
Содержит результат проверки лицензий на использование компонентов системы Secret Net (проверяются лицензии, зарегистрированные на данном СБ)
Затирание
Содержит сведения о текущем состоянии механизма затирания удаляемой информации. Если драйвер механизма отключен, отображается признак "выключено" (включение драйвера осуществляется только локально, описание процедуры отключения и включения защитных механизмов см. в документе [3]). Для компьютеров с включенным механизмом указывается заданное количество циклов затирания на локальных дисках, сменных дисках и конфиденциальных файлов
Полном. УД
Содержит сведения о текущем состоянии механизма полномочного разграничения доступа. Если драйвер механизма отключен, отображается признак "выключено" (включение драйвера осуществляется только локально, описание процедуры отключения и включения защитных механизмов см. в документе [3]). Для компьютеров с включенным механизмом указывается текущий режим работы: "контроль потоков", если включен режим контроля потоков конфиденциальной информации, или "контроль доступа", если режим контроля потоков отключен
Печать
Содержит сведения о текущем состоянии механизма контроля печати. Если драйвер механизма отключен, отображается признак "выключено" (драйвер отключается и включается одновременно с механизмом полномочного разграничения доступа — см. выше). Для компьютеров с включенным механизмом указывается текущий режим работы: "контроль конф. док.", если включен режим контроля печати конфиденциальных документов, или "регистрация", если указанный режим отключен
ЗПС
Содержит сведения о текущем состоянии механизма замкнутой программной среды. Если драйвер механизма отключен, отображается признак "выключено" (включение драйвера осуществляется только локально, описание процедуры отключения и включения защитных механизмов см. в документе [3]). Для компьютеров с включенным драйвером указывается текущий режим работы механизма: "жесткий" или "мягкий". Если механизм ЗПС не включен, отображается признак "отключено" (включение механизма можно осуществлять централизованно или локально, описание процедур включения см. в документе [3])
Конфигурация
Содержит сведения о текущем состоянии механизма контроля аппаратной конфигурации. Если драйвер механизма отключен, отображается признак "выключено" (включение драйвера осуществляется только локально, описание процедуры отключения и включения защитных механизмов см. в документе [3]). Для компьютеров с включенным механизмом указывается текущий режим работы: "жесткий", "мягкий" или "прозрачный"
Доступ к устр.
Содержит сведения о текущем состоянии механизма разграничения доступа к устройствам. Если драйвер механизма отключен, отображается признак "выключено" (драйвер отключается и включается одновременно с механизмом контроля аппаратной конфигурации — см. выше). Для компьютеров с включенным драйвером указывается текущий режим работы механизма: "жесткий" или "мягкий". Если механизм не включен, отображается признак "отключено" (включение механизма можно осуществлять централизованно или локально, описание процедур включения см. в документе [3])

Сбор журналов
Содержит признаки выполнения централизованного сбора локальных журналов: журнала приложений (Application Log), системного журнала (System Log) и журнала безопасности (Security Log)

Список пользовательских сессий

Если на защищаемом компьютере открыты сессии пользователей, сведения о них можно вывести в специальном диалоге "Сессии" области списка объектов.

Количество открытых сессий на защищаемых компьютерах выводится, например, при отображении общего списка компьютеров и серверов безопасности — см. выше.

Сведения о сессиях отображаются в колонках:

Пользователь
Имя пользователя, открывшего сессию
Тип
Тип доступа пользователя к компьютеру (локальный или терминальный вход)

Список записей о событиях НСД

Программа мониторинга позволяет оперативно выполнить загрузку записей о событиях НСД, произошедших на защищаемом компьютере. Событиями НСД считаются события, которые имеют тип "Аудит отказов" и регистрируются в журнале Secret Net или штатном журнале безопасности ОС Windows. Вывод списка записей осуществляется в специальном диалоге "НСД на станции".

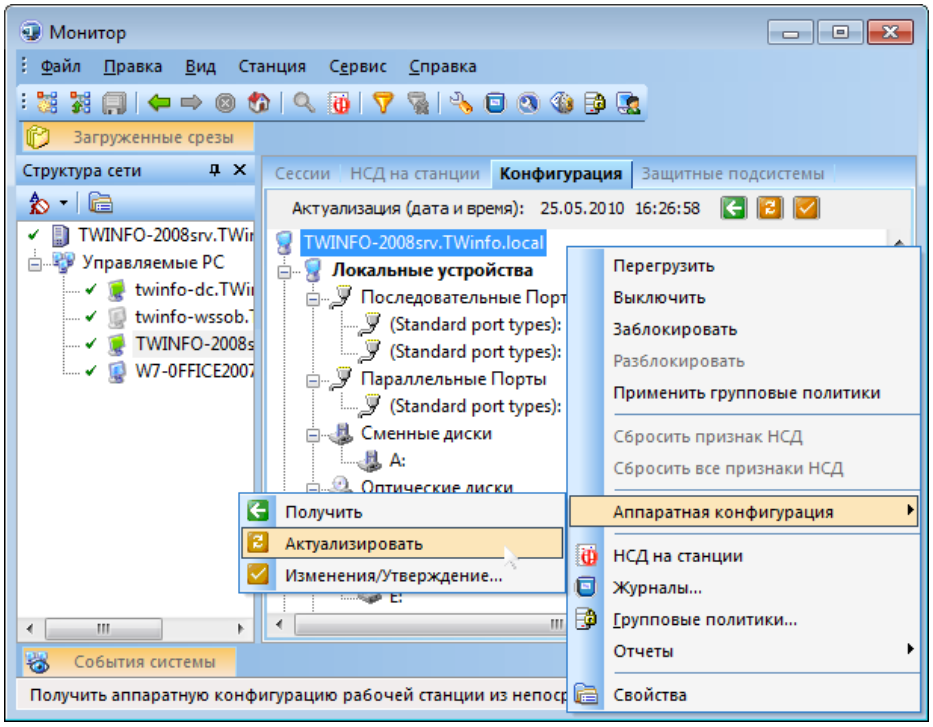
Загрузка записей осуществляется из специального журнала НСД, который ведется на сервере безопасности. В это хранилище оперативно поступают сведения о событиях НСД, зарегистрированных на защищаемых компьютерах. Для каждого компьютера, подчиненного серверу безопасности, в журнале НСД максимально может храниться не более 2000 записей. При достижении максимального количества записей наиболее старые записи замещаются новыми. Очистка содержимого журнала НСД выполняется автоматически при архивировании базы данных сервера безопасности. После очистки в журнале остаются записи, зарегистрированные за 30 и менее дней до момента архивирования.

Чтобы загрузить записи о событиях НСД, произошедших на компьютере, выберите этот компьютер и активируйте команду "Станция | НСД на станции".

Список устройств аппаратной конфигурации

Программа мониторинга позволяет загрузить для просмотра список устройств компьютера, находящегося в непосредственном подчинении корневому серверу безопасности (корневым является сервер, с которым установлено соединение программы). Для получения таких сведений на защищаемом компьютере должно быть установлено клиентское ПО системы Secret Net 6 версии 6.1 и выше.

Вывод списка устройств в программе мониторинга осуществляется в специальном диалоге "Конфигурация". Диалог предназначен для отображения эталонной аппаратной конфигурации защищаемого компьютера.



Описание механизма контроля аппаратной конфигурации см. в документе [1].

Список устройств можно загрузить из базы данных сервера безопасности или непосредственно с защищаемого компьютера, если он включен.

В базе данных сервера безопасности хранится копия списка устройств эталонной аппаратной конфигурации защищаемого компьютера. Эти сведения периодически обновляются, однако они могут не соответствовать текущей эталонной аппаратной конфигурации компьютера. Загрузку списка устройств из БД СБ рекомендуется выполнять только в тех случаях, когда защищаемый компьютер отключен или недоступен в данный момент. Загрузка списка устройств непосредственно с защищаемого компьютера происходит дольше, чем загрузка из БД, однако это позволяет вывести актуальный список устройств текущей эталонной аппаратной конфигурации компьютера и одновременно обновить сведения в БД сервера.

Чтобы загрузить список устройств из БД сервера безопасности, выберите компьютер и активируйте команду "Станция | Аппаратная конфигурация | Получить".

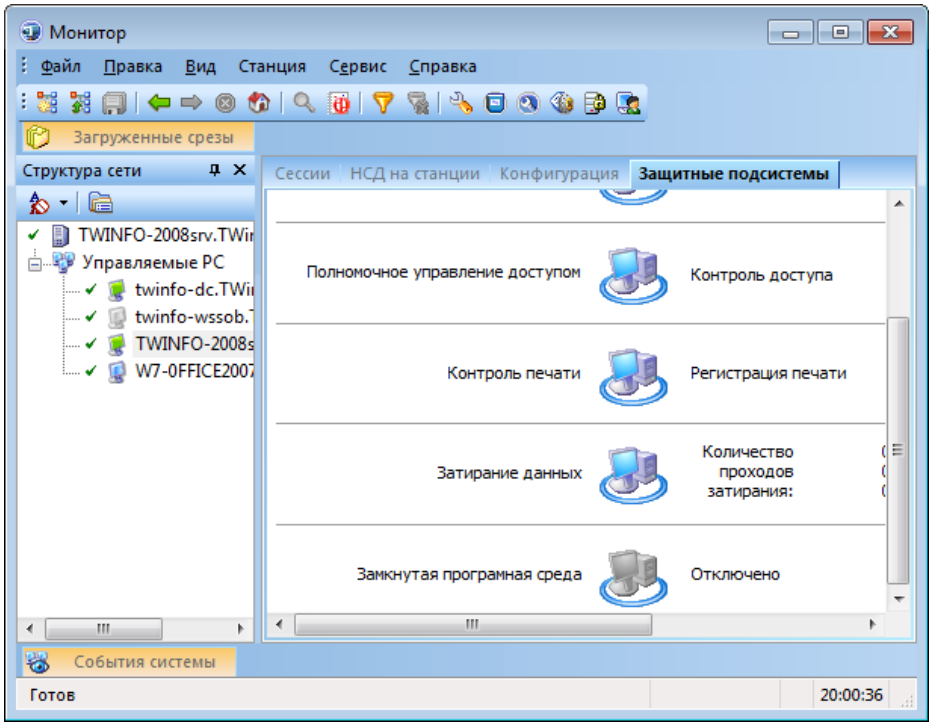
Чтобы загрузить список устройств непосредственно с защищаемого компьютера, выберите компьютер и активируйте команду "Станция | Аппаратная конфигурация | Актуализировать".

В программе мониторинга предусмотрена возможность удаленного утверждения изменений аппаратной конфигурации компьютера. Утверждение конфигурации выполняется с помощью команды оперативного управления — см. стр. 23. (описание процедуры локального утверждения аппаратной конфигурации см. в документе [3]).

Список механизмов защиты системы Secret Net 6

Программа мониторинга позволяет загрузить для просмотра основные сведения о функционировании механизмов защиты на компьютере (механизмы замкнутой программной среды, затирания данных и др.). Для получения таких сведений на защищаемом компьютере должно быть установлено клиентское ПО системы Secret Net 6 текущей версии.

Вывод списка механизмов осуществляется в специальном диалоге "Защитные подсистемы". В диалоге отображаются сведения о том, какие режимы работы установлены для механизмов.



Описание механизмов защиты и предусмотренные для них режимы работы см. в документе [1].

Для отображения состояния защитных механизмов используются пиктограммы (см. стр. 33).

Краткие сведения о работе механизмов защиты на компьютерах выводятся, например, при отображении общего списка компьютеров и серверов безопасности — см. стр. 11.

Сведения в окне событий

По умолчанию в окне событий (см. Рис. 1 на стр. 7) отображаются уведомления мониторинга, а также записи журналов, описывающие события НСД. Уведомления мониторинга разделяются на следующие группы:

- "События управляемой сети" — уведомления, предупреждающие об изменении состояния контролируемых объектов или о наличии связи с сервером безопасности (например, "Рабочая станция включена", "Потеря соединения с сервером безопасности" и др.);
- "Действия пользователя" — уведомления, информирующие о действиях пользователя программы мониторинга (например, "Блокировка рабочей станции", "Сброшены признаки НСД" и др.);
- "Сообщения о НСД" — уведомления о фактах регистрации событий НСД на защищаемых компьютерах (например, "На рабочей станции зарегистрировано одно или несколько НСД").

Для просмотра подробных сведений о зарегистрированных на компьютере событиях НСД можно использовать диалог "НСД на станции" в области списка объектов (см. стр. 13).

Записи о зарегистрированных событиях НСД отображаются, если включен режим загрузки этих сведений. Включение и отключение режима можно выполнить при настройке параметров программы (см. стр. 31) или оперативно.

Управление отображением уведомлений мониторинга

Окно событий можно настроить на отображение уведомлений мониторинга, принадлежащих определенным группам. Выбор отображаемых групп уведомлений осуществляется с помощью команд меню и кнопок панели инструментов, расположенной в верхней части окна событий.

Табл. 4. Команды меню и кнопки для выбора групп уведомлений

Команда	Кнопка	Описание
Вид | События системы | Управляемая сеть		Включает или отключает отображение уведомлений, относящихся к группе "События управляемой сети"
Вид | События системы | Действия пользователя		Включает или отключает отображение уведомлений, относящихся к группе "Действия пользователя"
Вид | События системы | Сообщения о НСД		Включает или отключает отображение уведомлений, относящихся к группе "Сообщения о НСД"

Переход к защищаемому компьютеру

Каждое уведомление или запись о событии относится к определенному защищаемому компьютеру, имя которого указано в колонке "Компьютер".

Для перехода к этому компьютеру в контекстном меню записи активируйте команду "Перейти к объекту". В окне структуры или в окне среза (в зависимости от того, какое из этих окон является активным в данный момент) будет раскрыта соответствующая ветвь и выделен искомый компьютер.

Автоматическое отображение последних сведений

Новые зарегистрированные уведомления и записи 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 окна событий и активируйте команду "Видеть последний".

Очистка содержимого окна

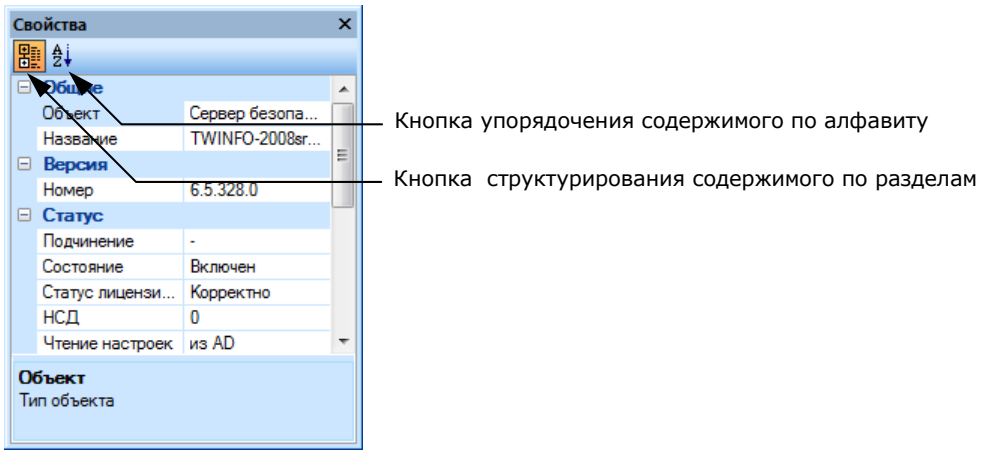
Автоматическая очистка содержимого окна событий осуществляется:

- при выходе из программы мониторинга;
- если количество элементов списка превысило 50000. После очистки в списке остаются последние 1000 уведомлений и записей о событиях.

В процессе работы с программой можно принудительно очистить содержимое окна событий. Для этого вызовите контекстное меню в любом месте окна событий и активируйте команду "Очистить".

Сведения в окне свойств объектов

Окно свойств объектов по умолчанию не отображается. Для вывода сведений об объекте вызовите его контекстное меню и активируйте команду "Свойства".



Сведения в окне свойств объектов зависят от того, какой элемент иерархической структуры выбран в данный момент. Сведения о компьютерах и серверах безопасности отображаются в следующих строках:

Вариант (группа "Версия")
Содержит название текущего варианта применения клиентского ПО на защищаемом компьютере. Вариант применения "Full" предусматривает доступность всех защитных функций клиента
Безопасности (группа "Сбор журналов")
Содержит признак выполнения централизованного сбора локального журнала безопасности
Выключенных РС (группа "Статистика")
Содержит количество недоступных в данный момент защищаемых компьютеров, относящихся к выбранному серверу безопасности и ко всем подчиненным серверам
Выключенных СБ (группа "Статистика")
Содержит количество серверов безопасности, входящих в цепочку серверов, подчиненных выбранному серверу и недоступных в данный момент
Доступ к устр. (группа "Защитные подсистемы")
Содержит сведения о текущем состоянии механизма разграничения доступа к устройствам. Аналогичные сведения приводятся в одноименной колонке области списка объектов (см. стр. 12)
ЗПС (группа "Защитные подсистемы")
Содержит сведения о текущем состоянии механизма замкнутой программной среды. Аналогичные сведения приводятся в одноименной колонке области списка объектов (см. стр. 12)
Затирание (группа "Защитные подсистемы")
Содержит сведения о текущем состоянии механизма затирания удаляемой информации. Аналогичные сведения приводятся в одноименной колонке области списка объектов (см. стр. 12)
Кол-во СБ (группа "Статистика")
Содержит количество серверов безопасности, входящих в цепочку серверов, подчиненных выбранному серверу
Кол-во станций (группа "Статистика")
Содержит количество защищаемых компьютеров, относящихся к выбранному серверу безопасности и ко всем подчиненным серверам
Конфигурация (группа "Защитные подсистемы")
Содержит сведения о текущем состоянии механизма контроля аппаратной конфигурации. Аналогичные сведения приводятся в одноименной колонке области списка объектов (см. стр. 12)
Название (группа "Общие")
Содержит имя сервера безопасности или защищаемого компьютера

Неактивна с (группа "Статус")
Содержит время последнего отключения защищаемого компьютера. Сведения отображаются, если компьютер недоступен в данный момент
Номер (группа "Версия")
Содержит номер версии установленного программного обеспечения (ПО сервера безопасности или клиента). Если с момента предыдущего подключения версия ПО клиента была изменена, отображается статус обновления версии
НСД (группа "Статус")
Содержит количество событий НСД, произошедших на защищаемом компьютере. При подключении компьютера к серверу безопасности отсчет событий НСД начинается с нуля. Обнуление счетчика происходит после отключения защищаемого компьютера от сервера (при потере соединения на длительное время, перезагрузке или выключении компьютера)
НСД на СБ (группа "Статистика")
Содержит количество событий НСД, которые произошли на серверах безопасности, подчиненных выбранному серверу. *Регистрация событий НСД, произошедших на серверах безопасности, в текущей версии не реализована*
НСД на станциях (группа "Статистика")
Содержит общее количество событий НСД, которые произошли на защищаемых компьютерах, относящихся к выбранному серверу безопасности и ко всем подчиненным ему серверам
Объект (группа "Общие")
Содержит наименование типа объекта
Печать (группа "Защитные подсистемы")
Содержит сведения о текущем состоянии механизма контроля печати. Аналогичные сведения приводятся в одноименной колонке области списка объектов (см. стр. 12)
Платформа (группа "Версия")
Содержит наименование типа операционной системы, под управлением которой работает компьютер
Подчинение (группа "Статус")
Содержит признак подчиненности компьютера серверу безопасности, с которым установлено соединение программы мониторинга: • "Прямое" — компьютер подчинен данному серверу безопасности непосредственно; • "Транзитивное" — компьютер подчинен любому другому серверу безопасности.
Полном. УД (группа "Защитные подсистемы")
Содержит сведения о текущем состоянии механизма полномочного разграничения доступа. Аналогичные сведения приводятся в одноименной колонке области списка объектов (см. стр. 12)
Приложений (группа "Сбор журналов")
Содержит признак выполнения централизованного сбора локального журнала приложений
Сессии (группа "Статус")
Содержит количество открытых на защищаемом компьютере сессий пользователей. Строка отображается, если выбран защищаемый компьютер
Системный (группа "Сбор журналов")
Содержит признак выполнения централизованного сбора локального системного журнала
Службы (группа "Версия")
Содержит признак наличия дополнительно установленного ПО, взаимодействующего с системой Secret Net 6 на защищаемом компьютере. Названия ПО указываются в нижней части окна свойств
Состояние (группа "Статус")
Содержит краткое описание текущего состояния компьютера: • "Выключен" — сервер безопасности недоступен в данный момент; • "Выключена" — защищаемый компьютер недоступен в данный момент; • "Включен" — сервер безопасности функционирует нормально; • "Включена" — защищаемый компьютер функционирует без открытых сессий пользователей; • "Работает пользователь" — на защищаемом компьютере открыта сессия пользователя; • "Работают пользователи" — на защищаемом компьютере открыты несколько сессий работы пользователей; • "Заблокирована" — защищаемый компьютер заблокирован.

Статус лицензирования (группа "Статус")
Содержит результат проверки лицензий на использование компонентов системы Secret Net (проверяются лицензии, зарегистрированные на данном СБ)
Статус ФК (группа "Статус")
Содержит результат проведения функционального контроля при запуске компьютера
Чтение настроек (группа "Статус")
Содержит пояснение, из какого источника были загружены конфигурационные параметры сервера безопасности: • из Active Directory — основной метод загрузки параметров; • из файла кэша — резервный метод загрузки. Если на момент запроса параметров схема AD недоступна, осуществляется загрузка параметров, которые были получены и сохранены в файле при последнем обращении к AD.

Если в иерархической структуре выбрана папка "Управляемые РС" или "Подчиненные СБ", информация отображается в следующих строках:

Выключенных (группа "Статистика")
В зависимости от выбранной папки содержит количество недоступных в данный момент защищаемых компьютеров или серверов безопасности (из числа включенных в папку)
Кол-во СБ (группа "Статистика")
Содержит количество серверов безопасности, включенных в папку. Строка отображается, если выбрана папка "Подчиненные СБ"
Кол-во НСД (группа "Статистика")
В зависимости от выбранной папки содержит общее количество произошедших событий НСД на защищаемых компьютерах или серверах безопасности, включенных в папку. *Регистрация событий НСД, произошедших на серверах безопасности, в текущей версии не реализована*
Кол-во станций (группа "Статистика")
Содержит количество защищаемых компьютеров, включенных в папку. Строка отображается, если выбрана папка "Управляемые РС"
Название (группа "Общие")
Содержит имя папки
Объект (группа "Общие")
Содержит описание назначения папки
Прямого подчин. (группа "Статистика")
В зависимости от выбранной папки содержит количество включенных в папку защищаемых компьютеров или серверов безопасности

Сортировка объектов

Сортировка иерархических списков

Программа позволяет сортировать иерархические списки в окне структуры объектов и в окнах срезов. Сортировка осуществляется в алфавитном порядке имен компьютеров (и папок среза) на каждом уровне иерархии. Можно применить прямой или обратный порядок сортировки. Если сортировка отключена, объекты располагаются в том порядке, в каком они были добавлены в структуру.

Для сортировки иерархических списков:

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

  Выбранный режим будет установлен для отображения объектов в окне структуры и во всех окнах срезов.

Сортировка таблиц в области списка объектов

Таблица в области списка объектов сортируется по значениям, содержащимся в колонках. Методы сортировки аналогичны стандартным методам управления таблицами, принятым в большинстве приложений Windows. В заголовке колонки, по которой отсортирована таблица, указывается соответствующее направление сортировки.

Поиск объектов

Поиск осуществляется по значениям, содержащимся в отображаемых колонках таблицы в области списка объектов или окна событий системы.

Для поиска объекта:

1. Выберите в таблице объект, с которого начнется поиск.
2. Активируйте команду "Правка | Найти...".

   На экране появится диалог настройки параметров поиска.
3. В поле "Что" введите строку поиска, настройте параметры поиска и нажмите кнопку "ОК".

Учитывать регистр
Если поле содержит отметку, будут найдены только те объекты, в сведениях о которых содержится заданная строка символов в том же регистре. При отсутствии отметки регистр символов введенной строки не учитывается
Целиком значение
Если поле содержит отметку, будут найдены только те объекты, в сведениях о которых заданная строка символов содержится в виде отдельного слова (слов). При отсутствии отметки строка символов может являться частью других строк
Искать в поле
Если поле содержит отметку, поиск в таблице осуществляется только по значениям выбранной колонки. После установки отметки выберите имя колонки в поле справа. При отсутствии отметки искомая строка символов может находиться в любой из отображаемых в таблице колонок

Отслеживание событий НСД

Программа мониторинга информирует о событиях НСД, произошедших на защищаемых компьютерах в текущем сеансе работы программы. Событиями НСД считаются события, которые имеют тип "Аудит отказов" и регистрируются в журнале Secret Net или штатном журнале безопасности ОС Windows.

Оповещение о событиях НСД

При регистрации событий НСД в программе мониторинга включается режим оповещения. В этом режиме программой выполняются следующие действия:

- в строке сообщений мерцает индикатор НСД. При этом в информационном заголовке отображается вращающаяся пиктограмма предупреждения;
- в окне структуры пиктограмма компьютера отмечена специальным знаком, а в области списка объектов строка со сведениями об этом компьютере отображается в таблице на красном фоне;
- пиктограммы срезов, содержащих компьютер, выделяются красным цветом в окне списка срезов;
- в окне событий выводятся сведения о произошедших событиях НСД (если включен режим загрузки этих сведений — см. стр. 31);
- значок (пиктограмма) программы мониторинга в области уведомлений Панели задач Windows выделяется красным цветом (если окно программы минимизировано и включен режим сворачивания окна в область уведомлений — см. стр. 30);
- воспроизводится звуковой сигнал, заданный при настройке параметров работы программы (см. стр. 30);
- выполняется запуск указанной внешней программы (см. стр. 30).

Включение режима оповещения происходит при следующих условиях:

- если зарегистрировано событие, удовлетворяющее фильтру событий НСД;
- если на одном из защищаемых компьютеров зарегистрировано пороговое количество событий НСД.

Режим оповещения о событиях НСД отключается после сброса признаков НСД для всех компьютеров, на которых произошли события.

Настройка фильтра событий НСД

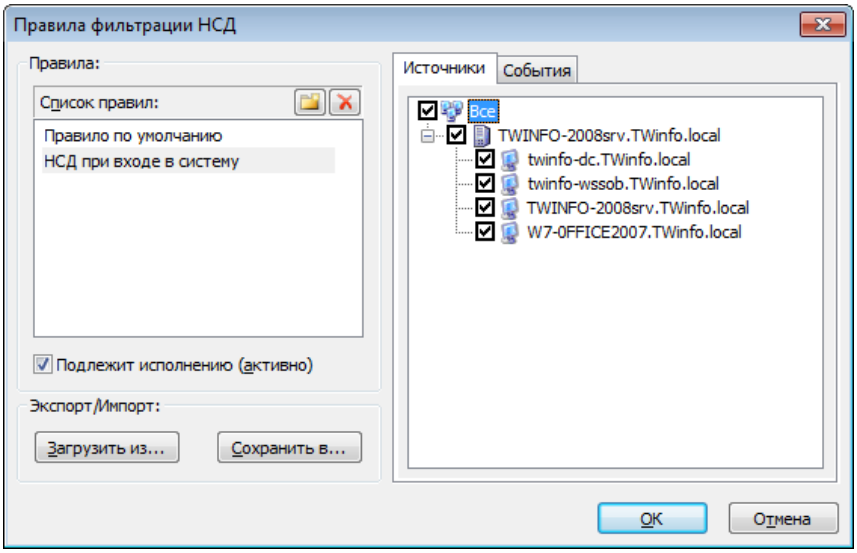
Фильтр событий НСД позволяет отслеживать события НСД выборочно. При регистрации события, удовлетворяющего фильтру, программа мониторинга сигнализирует об этом путем включения режима оповещения (см. выше).

Фильтрация выполняется по специальным "правилам отслеживания НСД". С помощью правил контролируются события в зависимости от источников их регистрации. При этом программа может отслеживать события определенных категорий (только при регистрации на защищаемых компьютерах, подчиненных серверу безопасности, с которым установлено соединение программы).

Для активации и настройки параметров фильтра:

1. Если в программе отключена загрузка сведений о событиях НСД, включите режим загрузки этих сведений (см. стр. 31).
2. Активируйте команду "Сервис | Фильтр тревоги НСД".

   На экране появится диалоговое окно для настройки параметров фильтра.



3. Используя стандартные процедуры редактирования списка элементов, сформируйте список правил отслеживания событий. Для добавления и удаления элементов используйте соответствующие кнопки или клавиши <Insert> и <Delete>. Чтобы ввести другое имя правила, выберите нужный элемент в списке и нажмите клавишу <F2>.
4. Определите действующие правила (т. е. правила, по которым будет выполняться отслеживание событий). Чтобы включить действие правила, выберите его в списке и установите отметку в поле "Подлежит исполнению (активно)". Для отключения действия удалите отметку из поля.
5. Выберите правило для указания источников регистрации и категорий событий.
6. В диалоге "Источники" отметьте компьютеры, на которых будут отслеживаться события НСД. Компьютеры сгруппированы по подчинению серверам безопасности. Если в иерархическом списке не отмечен ни один элемент, это равносильно установке отметок для всех элементов.
7. Перейдите к диалогу "События". Диалог содержит список категорий для событий НСД. Категории разделены на следующие группы:
   - "ОС Windows" — в группу входят категории событий, регистрируемых в штатном журнале безопасности ОС Windows;
   - "Дополнительно" — в группу входят категории событий, регистрируемых в журнале Secret Net.
8. Отметьте категории событий НСД, которые будут отслеживаться программой. Если в иерархическом списке не отмечен ни один элемент, это равносильно установке отметок для всех элементов.

Категории учитываются только при регистрации событий на компьютерах, непосредственно подчиненных серверу безопасности, с которым установлено соединение программы. Для компьютеров, относящихся к подчиненным серверам безопасности, режим оповещения будет включаться при регистрации любого события НСД.

9. Повторите действия **5**–**8** для других правил, представленных в списке.

Отключение фильтра событий НСД

При отключении фильтра событий НСД автоматически активируется счетчик порогового количества событий НСД (см. ниже).

Чтобы отключить фильтр, активируйте команду "Сервис | Отключить фильтр НСД".

Фильтр событий НСД отключается автоматически при отключении режима загрузки сведений о событиях НСД (см. стр. 31).

Сохранение и загрузка параметров фильтра

Программа мониторинга автоматически сохраняет параметры фильтра событий НСД в файле UAFilter.xml в личной папке текущего пользователя. Этот файл используется по умолчанию для чтения и загрузки параметров фильтра в следующих сеансах работы пользователя с программой.

Для сохранения параметров фильтра в другом xml-файле нажмите в окне настройки параметров фильтра кнопку "Сохранить в…". Для загрузки параметров в программу используйте кнопку "Загрузить из…".

Настройка счетчика количества событий НСД

Режим оповещения может включаться по счетчику событий НСД. Если во время сеанса работы программы на одном из компьютеров было зарегистрировано некоторое пороговое количество любых событий НСД, программа мониторинга сигнализирует об этом путем включения режима оповещения (см. стр. 20).

Для активации и настройки параметров счетчика событий:

1. Отключите фильтр НСД (см. выше).
2. В параметрах работы программы укажите пороговое количество событий НСД, после которого будет включаться режим оповещения (см. стр. 30).

Сброс признаков НСД

После выяснения причин возникновения событий НСД и принятия соответствующих мер следует вернуть нормальное состояние отображаемых объектов в программе мониторинга. Сброс признаков НСД осуществляется при обновлении структуры объектов, при выходе из программы или с помощью команд.

Чтобы сбросить признак НСД на отдельном компьютере, выберите компьютер и активируйте команду "Станция | Сбросить признак НСД".

Чтобы сбросить признаки НСД на всех компьютерах, выберите в окне структуры или окне среза любой объект и в меню с названием выбранного объекта (например, "Сервер безопасности") активируйте команду "Сбросить все признаки НСД".

После исполнения команды программа переводит отображение компьютера (компьютеров) в нормальное состояние. Если компьютеров с признаками НСД больше нет, режим оповещения о событиях НСД отключается.

Сброс признаков НСД не приводит к удалению записей в окне событий. Содержимое журналов, в которых хранятся записи о событиях НСД, также остается без изменений.

Глава 3
Оперативное управление

Команды оперативного управления могут применяться только к защищаемым компьютерам, которые находятся в непосредственном подчинении корневому серверу безопасности (корневым является сервер, с которым установлено соединение программы). При этом выбранный для управления компьютер должен быть включен.

Если в данный момент исполнение какой-либо оперативной команды невозможно, эта команда либо отсутствует в меню, либо отображается в "затененном" виде.

Для выполнения команды оперативного управления выберите в программе мониторинга защищаемый компьютер и активируйте в меню "Станция" нужную команду.

Табл. 5. Команды оперативного управления

Команда	Описание
Заблокировать	Под блокировкой компьютера понимается запрет доступа пользователей (исключая локального администратора) к работе на данном компьютере. Сеанс работы пользователя на защищаемом компьютере будет незамедлительно прерван, и на экране компьютера появится сообщение об этом. Одновременно в журнале Secret Net регистрируется событие "Компьютер заблокирован системой защиты", которое является событием НСД. Сведения о блокировке компьютера отражаются в программе мониторинга после автоматического обновления данных о состоянии системы
Разблокировать	Заблокированный компьютер отображается в программе мониторинга с измененной пиктограммой (см. стр. 33). На экране разблокированного компьютера появится соответствующее сообщение. После этого пользователь, сеанс которого был прерван при блокировании компьютера, может продолжить работу
Перегрузить	Перезагрузка осуществляется независимо от количества открытых приложений и наличия несохраненных документов на компьютере. На экране перезагружаемого компьютера появится соответствующее сообщение. В течение 15 секунд с момента появления сообщения пользователь компьютера может выполнить сохранение открытых документов. Длительность паузы на сохранение документов можно изменить. Для этого предварительно на защищаемом компьютере необходимо создать параметр DWORD ShDownTimeout в ключе системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Infosec\Secret Net 5\SnAgent. Значение, заданное для этого параметра, определяет количество секунд паузы
Выключить	Выключение осуществляется независимо от количества открытых приложений и наличия несохраненных документов на компьютере. На экране выключаемого компьютера появится соответствующее сообщение. В течение 15 секунд с момента появления сообщения (если не установлена другая длительность паузы — см. описание команды "Перегрузить") пользователь компьютера может выполнить сохранение открытых документов
Применить групповые политики	Выполняется немедленный запуск обновления групповых политик на защищаемом компьютере. Принудительное обновление ускоряет процесс применения групповых политик, заданных централизованно. Обновление групповых политик по команде из программы мониторинга происходит на компьютере так же, как и при использовании локальной утилиты gpupdate
Аппаратная конфигурация | Изменения / Утверждение...	Компьютер с измененной аппаратной конфигурацией отмечается в структуре знаком ? (знак отображается, если для этого компьютера не включен режим оповещения о событиях НСД). После запуска команды на экране появляется диалог со списком устройств, не совпадающих с эталонной аппаратной конфигурацией компьютера. Чтобы учесть перечисленные устройства в составе эталонной конфигурации, нажмите кнопку "Утвердить"

Глава 4
Дополнительные средства программы

Управление загрузкой данных

Для управления процессом загрузки данных предоставляются следующие возможности:

- принудительное обновление структуры объектов системы;
- принудительная остановка процесса загрузки.

Обновление структуры объектов

Процедура обновления структуры объектов позволяет выполнить новую загрузку иерархического списка защищаемых компьютеров и других данных.

Для обновления структуры объектов:

- Активируйте команду "Вид | Обновить структуру".

Принудительная остановка загрузки данных

Процесс загрузки данных может занять продолжительное время. Длительность процесса зависит от степени загруженности локальной сети и объема данных.

Для остановки процесса загрузки:

- Активируйте команду "Вид | Стоп".

Формирование отчетов

Программа мониторинга предоставляет возможность создавать отчеты, содержащие сведения о защищаемых компьютерах. Для выбранного компьютера можно запросить следующие отчеты:

- отчет "Паспорт ПО" — содержит сведения о программном обеспечении, установленном на компьютере;
- отчет "Ресурсы рабочей станции" — содержит сведения о ресурсах, объектах и параметрах компьютера.

Перечисленные отчеты также можно сформировать локально на защищаемом компьютере. Локальное построение отчетов осуществляется с помощью программы "Контроль программ и данных" (см. документ [3]).

Возможность централизованного создания отчетов поддерживается только для включенных компьютеров.

Отчеты сохраняются в файлы формата rtf. Для загрузки содержимого rtf-файлов необходимо использовать соответствующие приложения, поддерживающие возможность просмотра таких файлов. Например, редактор Microsoft Word.

Не рекомендуется загружать файл отчета 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

Отчет "Паспорт ПО"

В отчете "Паспорт ПО" содержатся следующие сведения:

- учетная информация компьютера (имя компьютера, название подразделения, к которому относится компьютер, номер системного блока и др.). Сведения загружаются из Active Directory;
- перечень установленного программного обеспечения. Для каждого программного пакета указываются компания-производитель, суммарный объем занимаемого пространства и др. Построение перечня осуществляется локально на основе сведений, хранящихся в базе данных сервиса Windows Installer;
- Ф.И.О. сотрудников, ответственных за эксплуатацию компьютера. Имена сотрудников указываются при формировании отчета.

Для формирования отчета "Паспорт ПО":

1. В окне структуры или в окне среза выберите компьютер.
2. Активируйте команду "Станция | Отчеты | Паспорт ПО".

   На экране появится стартовый диалог мастера формирования отчета.
3. В соответствующих полях введите Ф.И.О. сотрудников, ответственных за эксплуатацию данного компьютера. При необходимости настройте параметры нумерации страниц отчета (расположение номеров и отображение общего количества страниц). Для этого нажмите кнопку "Дополнительно...", в появившемся диалоге отметьте нужные параметры и нажмите кнопку "ОК".
4. Нажмите кнопку "Далее >".

   На экране появится следующий диалог мастера.
5. Введите полное имя файла отчета. Для ввода используйте клавиатуру или нажмите кнопку справа от поля, чтобы указать файл в стандартном диалоге сохранения файла ОС Windows.
6. Нажмите кнопку "Построить".

   Программа начнет процесс получения и обработки данных, и на экране появится соответствующее сообщение. По завершении подготовки отчета нажмите кнопку "ОК".

Отчет "Ресурсы рабочей станции"

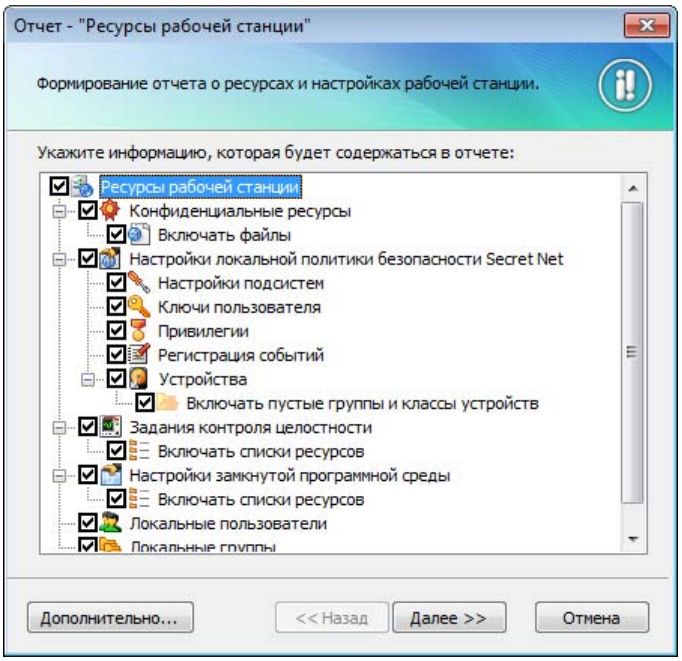
В отчете "Ресурсы рабочей станции" содержатся следующие сведения:

- учетная информация компьютера (имя компьютера, название подразделения, к которому относится компьютер, номер системного блока и др.). Сведения загружаются из Active Directory;
- общие сведения о СЗИ Secret Net 6 – Клиент (номер версии и серийный номер);
- сведения о наличии на компьютере изделия "Программно-аппаратный комплекс "Соболь". Если ПАК "Соболь" установлен, указывается режим работы устройства (при включенном режиме интеграции, кроме того, указывается заводской номер платы этого изделия);
- перечень защитных механизмов с указанием текущего состояния работы каждого механизма (включен или отключен);
- сведения о ресурсах, объектах и параметрах компьютера. Выбор необходимых сведений осуществляется при формировании отчета (см. ниже).

Для формирования отчета "Ресурсы рабочей станции":

1. В окне структуры или в окне среза выберите компьютер.
2. Активируйте команду "Станция | Отчеты | Ресурсы рабочей станции".

На экране появится стартовый диалог мастера формирования отчета:



3. Отметьте нужные элементы списка для сохранения соответствующих сведений в отчете. Можно сохранить следующие сведения:
   - **Список конфиденциальных ресурсов.** Если установлена отметка у элемента "Конфиденциальные ресурсы" — в отчете будет сохранен список конфиденциальных каталогов компьютера. Если установлена отметка у подчиненного элемента "Включать файлы" — в отчет будет добавлен список конфиденциальных файлов.
   - **Список результирующих значений параметров политики безопасности Secret Net 6, действующей на компьютере.** Чтобы сохранить список, отметьте элемент "Настройки локальной политики безопасности Secret Net". Для выборочного сохранения сведений отметьте подчиненные элементы с названиями нужных групп параметров. Если установлена отметка у элемента "Включать пустые группы и классы устройств", подчиненного элементу "Устройства", — в отчет будет добавлен список групп и классов, к которым не относится ни одно устройство.
   - **Список заданий контроля целостности.** Чтобы сохранить список, отметьте элемент "Задания контроля целостности". Если установлена отметка у подчиненного элемента "Включать списки ресурсов" — для каждого задания в отчет будет добавлен список контролируемых ресурсов.
   - **Параметры и список заданий замкнутой программной среды.** Чтобы сохранить сведения, отметьте элемент "Настройки замкнутой программной среды". Если установлена отметка у подчиненного элемента "Включать списки ресурсов" — для каждого задания в отчет будет добавлен список контролируемых ресурсов.
   - **Список локальных пользователей.** Чтобы сохранить список, отметьте элемент "Локальные пользователи".
   - **Список локальных групп пользователей.** Чтобы сохранить список, отметьте элемент "Локальные группы".
4. При необходимости настройте параметры нумерации страниц отчета (расположение номеров и отображение общего количества страниц). Для этого нажмите кнопку "Дополнительно...", в появившемся диалоге отметьте нужные параметры и нажмите кнопку "OK".
5. Нажмите кнопку "Далее >".

   На экране появится следующий диалог мастера.
6. Введите полное имя файла отчета. Для ввода используйте клавиатуру или нажмите кнопку справа от поля, чтобы указать файл в стандартном диалоге сохранения файла ОС Windows.

7. Нажмите кнопку "Построить".

   Программа начнет процесс получения и обработки данных, и на экране появится соответствующее сообщение. По завершении подготовки отчета нажмите кнопку "OK".

Экспорт сведений об устройствах

Программа мониторинга позволяет экспортировать в файлы сведения об устройствах аппаратной конфигурации защищаемых компьютеров.

Сведения сохраняются в файлах специального формата (*.sndev). Содержимое файлов в дальнейшем можно импортировать в групповые политики безопасности с помощью процедуры добавления устройств в аппаратную конфигурацию. Описание процедуры добавления устройств см. в документе [3].

Чтобы экспортировать сведения об устройстве, загрузите список устройств компьютера (см. стр. 14), вызовите контекстное меню нужного устройства и активируйте команду "Экспорт". В появившемся стандартном диалоге сохранения файла ОС Windows укажите имя файла и нужный каталог.

Вызов программы просмотра журналов

При вызове из программы мониторинга запуск программы просмотра журналов осуществляется в сетевом режиме работы. Программа просмотра журналов автоматически устанавливает соединение с тем сервером безопасности, с которым установлено текущее соединение программы мониторинга.

Используются следующие способы для вызова программы просмотра журналов:

- общий вызов — обычный запуск программы. Для этого выберите сервер безопасности или любую папку и активируйте команду "Сервис | Журналы…";
- контекстный вызов — после запуска в программе просмотра журналов выполняется переход к заданному компьютеру. Для этого выберите защищаемый компьютер и активируйте команду "Станция | Журналы…".

Сведения о работе с программой просмотра журналов см. в документе [5].

Вызов программы конфигурирования

Чтобы выполнить запуск программы конфигурирования, активируйте команду "Сервис | Программа конфигурирования…".

Сведения о работе с этой программой содержатся в документе [7].

Вызов программы "Контроль программ и данных"

При вызове из программы мониторинга запуск программы "Контроль программ и данных" осуществляется в централизованном режиме работы. Для вызова программы активируйте команду "Сервис | Контроль программ и данных…".

Сведения о работе с этой программой содержатся в документе [3].

Вызов оснастки для управления групповой политикой домена

Из программы мониторинга можно вызвать оснастку для просмотра и изменения параметров групповой политики, применяемой к домену по умолчанию. В оснастку загружаются параметры групповой политики того домена, к которому относится текущий компьютер, выбранный в программе. Если выбрана любая папка структуры (например, "Подчиненные СБ"), в оснастку загружаются параметры групповой политики домена сервера безопасности, с которым установлено соединение программы.

Вызов оснастки осуществляется при наличии на компьютере пакета Administration Tools. Для работы с оснасткой текущий пользователь должен обладать правами администратора домена.

Чтобы вызвать оснастку, выберите компьютер нужного домена или папку структуры и активируйте команду "Сервис | Групповые политики…".

Сведения о настройке параметров содержатся в документе [3].

Вызов оснастки "Active Directory — пользователи и компьютеры"

Вызов оснастки "Active Directory — пользователи и компьютеры" осуществляется при наличии на компьютере пакета Administration Tools. Для работы с оснасткой текущий пользователь должен обладать правами администратора домена.

Чтобы вызвать оснастку, активируйте команду "Сервис | Доменные пользователи и компьютеры...".

Сведения об управлении пользователями содержатся в документе [3].

Приложение

Настройка элементов интерфейса

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

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

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

Состав отображаемых элементов интерфейса настраивается командами меню "Вид".

Табл. 6. Команды меню для управления элементами интерфейса

Команда	Описание
Вид | Строка статуса	Включает или отключает отображение строки сообщений
Вид | Панели | Кнопки	Включает или отключает отображение панели инструментов
Вид | Панели | Заголовок	Включает или отключает отображение информационного заголовка
Вид | Панели | Загруженные срезы	Включает или отключает отображение окна списка загруженных срезов
Вид | Панели | Структура сети	Включает или отключает отображение окна структуры
Вид | Панели | События системы	Включает или отключает отображение окна событий системы
Свойства (контекстное меню)	Включает отображение окна дополнительных сведений

Параметры работы программы

Настройка параметров работы программы мониторинга осуществляется в диалоге "Настройки приложения". Ниже приводится описание параметров по группам.

Группа параметров "Общие | Подтверждения"

Группа содержит параметры вывода диалогов запроса для подтверждения операций. Если установлено значение "Да", при выполнении данной операции будет выводиться диалог запроса для подтверждения операции.

Группа параметров "Общие | Транспорт"

Группа содержит параметры сетевого взаимодействия программы с сервером безопасности.

Тип соединения
Определяет шаблон настроек сетевого взаимодействия. Выберите нужный шаблон или настройте параметры вручную, раскрыв список "Ручные настройки" (описание параметров содержится на стр. 34)

Группа параметров "Общие | Привилегии"

Группа содержит список привилегий для работы с программой мониторинга и программой просмотра журналов. Список предназначен для ознакомления с текущим набором привилегий пользователя программы. Значение "Да" соответствует предоставленной привилегии. Предоставление привилегий пользователям осуществляется в программе конфигурирования. Возможен вызов этой программы из программы мониторинга (см. стр. 27).

Группа параметров "Общие | Внешний вид"

Группа содержит параметры отображения данных в программе. Для параметров цветового оформления таблиц текущий выбранный цвет представлен в ячейке со значением параметра. Изменение цвета осуществляется стандартными средствами, для вызова которых используется кнопка в правой части ячейки.

Признак НСД
Определяет цвет фона строк таблицы в области списка объектов. Этот цвет выделяет строки, содержащие сведения о компьютерах с признаком НСД
Управляемая сеть
Определяет цвет фона строк таблицы в окне событий системы. Этот цвет выделяет уведомления об изменении состояния объектов и наличии связи с сервером безопасности (уведомления группы "События управляемой сети")
Действия пользователя
Определяет цвет фона строк таблицы в окне событий системы. Этот цвет выделяет уведомления, информирующие о действиях пользователя программы мониторинга (уведомления группы "Действия пользователя")
НСД на станциях
Определяет цвет фона строк таблицы в окне событий системы. Этот цвет выделяет уведомления о регистрации событий НСД (уведомления группы "Сообщения об НСД")
Описания НСД
Определяет цвет фона строк таблицы в окне событий системы. Этот цвет выделяет сведения о событиях НСД (записи журналов)
Доменные имена
Если установлено значение "Да", то в окне структуры и в окнах срезов отображаются полные имена компьютеров (в формате <*имя_компьютера*>.<*имя_домена*>). При отключенном режиме имена доменов в иерархических списках не указываются
Имя пользователя
Если установлено значение "Да", то в окне структуры и в окнах срезов отображаются имена пользователей, открывших рабочие сессии. Имена пользователей указываются в скобках после имени компьютера
Сворачивать в панель
Если установлено значение "Да", при выполнении стандартной команды "Свернуть" окно программы минимизируется и отображается в Панели задач Windows не в виде кнопки, а в виде значка (пиктограммы) в области уведомлений

Группа параметров "Оповещение | Общие"

Группа содержит параметры реакции программы на возникновение событий НСД.

Срабатывание тревоги
Определяет вариант отслеживания событий НСД. Параметр может принимать значения: • "по лимиту НСД" — программа отслеживает пороговое количество любых событий НСД, произошедших на каком-либо защищаемом компьютере; • "по фильтру НСД" — программа отслеживает события НСД выборочно, в зависимости от источников и/или категорий событий. В соответствии с выбранным вариантом программа при определенных условиях включает режим оповещения пользователя (см. стр. 20)
Лимит НСД на компьютер
Определяет пороговое количество зарегистрированных событий НСД. Если в текущем сеансе работы с программой на одном из компьютеров зарегистрировано указанное количество любых событий НСД, включается режим оповещения. Отслеживание количества событий НСД осуществляется, если установлено значение "по лимиту НСД" для параметра "Срабатывание тревоги". Параметр может принимать значения от 1 до 65 535

Звуковой сигнал
Определяет тип звукового сигнала, оповещающего о событиях НСД. Для воспроизведения сигнала на компьютере должен быть установлен звуковой адаптер. Параметр может принимать значения: • "Нет" — звуковое оповещение отключено; • "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…".
Временной интервал
Определяет паузу в миллисекундах между повторами звукового сигнала. Параметр может принимать значения от 0 до 65 535
Запускать программу
Определяет автоматически запускаемую программу при включении режима оповещения о событиях НСД. Программа должна быть установлена на компьютере, на котором запущена программа мониторинга. Параметр может принимать значения: • "Нет" — запуск программы не осуществляется; • *<имя_файла>* — имя файла автоматически запускаемой программы. Выбор файла осуществляется в стандартном диалоге открытия файла. Чтобы вызвать диалог, выберите значение "Выбрать…".
Аргументы программы
Определяет аргументы командной строки для запуска программы, заданной параметром "Запускать программу". Значение параметра представлено в виде текстовой строки
НСД в иерархии
Если установлено значение "Да", то все элементы иерархии, к которым относится компьютер с признаком НСД, отмечаются в структуре соответствующей пиктограммой или выделяются красным цветом

Группа параметров "Оповещение | События системы"

Группа содержит параметры загрузки записей о событиях НСД.

Детально о НСД
Если установлено значение "Да", в программу мониторинга загружаются записи журналов, описывающие события НСД. Записи отображаются в окне событий системы. В целях уменьшения объема данных, загружаемых с сервера безопасности, можно отключить загрузку сведений о событиях НСД. Для этого установите значение "Нет" (при этом автоматически отключится фильтр событий НСД, если он был включен). Программа позволяет оперативно переключать режим загрузки записей. Для этого используйте команду "Сервис | Детально о НСД"

Средства для работы со списками объектов

Навигация при работе со структурами объектов

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

Табл. 7. Команды меню и кнопки для навигации в структуре объектов

Команда	Кнопка	Описание
Вид | Назад		Выполняет переход к предыдущему выбранному элементу структуры
Вид | Вперед		Выполняет переход к следующему выбранному элементу структуры
Вид | Домой		Выполняет переход к корневому элементу структуры

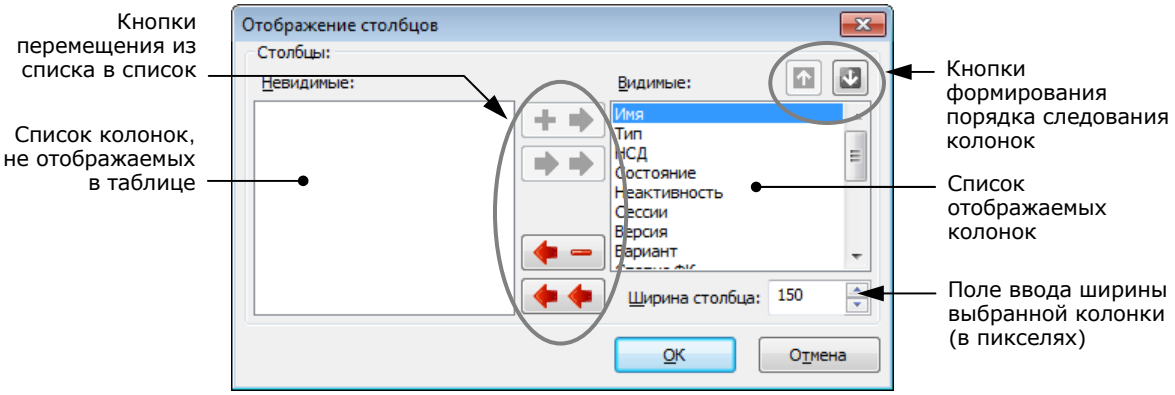
Настройка отображения колонок в таблицах

В программе мониторинга можно настраивать отображение информации в таблицах со списками объектов. Методы настройки аналогичны стандартным методам управления таблицами, принятым в большинстве приложений Windows.

Для управления колонками с помощью диалога настройки:

1. Вызовите контекстное меню в строке заголовков колонок и активируйте команду "Столбцы...".

   На экране появится диалог настройки параметров отображения колонок:



2. Настройте параметры отображения колонок (см. выноски к рисунку).

Для восстановления исходного состояния таблицы:

- Вызовите контекстное меню заголовка колонки и активируйте команду "По умолчанию".

Внешний вид таблицы (ширина и состав колонок) будет восстановлен в соответствии с исходными настройками программы.

Пиктограммы компьютеров в программе мониторинга

Табл. 8. Пиктограммы компьютеров

Пиктограмма	Описание
 (затененное изображение)	Компьютер отключен или недоступен в данный момент
 (синяя подсветка экрана)	Компьютер включен. Сессии пользователей не открыты
 (зеленая подсветка экрана)	Компьютер включен. Открыты сессии пользователей
 (синяя подсветка экрана)	Компьютер включен и заблокирован
 (зеленая подсветка экрана)	Компьютер включен и заблокирован, когда на нем работал пользователь или если не пройден функциональный контроль
	Сервер безопасности включен
 (затененное изображение)	Сервер безопасности отключен или недоступен в данный момент
 (выделено красным цветом)	На сервере безопасности заблокированы функции по управлению подчиненными агентами (доступно только подключение к серверу программ оперативного управления). Причина блокировки — нарушена лицензионная схема оперативного управления
	"Неизвестный объект". Программе не удалось идентифицировать объект

Пиктограммы защитных механизмов

Табл. 9. Пиктограммы защитных механизмов

Пиктограмма	Описание
 (затененное изображение)	Драйвер механизма отключен. Включение драйвера осуществляется только локально, описание процедуры отключения и включения защитных механизмов см. в документе [3]
 (затененное изображение компьютера)	Драйвер механизма включен, но механизм не функционирует — требуется включить механизм и установить "жесткий" или "мягкий" режим работы. Включение механизма можно осуществлять централизованно или локально, описание процедур включения см. в документе [3]
 (синяя подсветка экрана и контура)	Механизм защиты функционирует
	Обнаружен сбой в работе защитного механизма

Параметры сетевого взаимодействия

Табл. 10. Перечень параметров сетевого взаимодействия компонентов

Наименование параметра, пояснение	Диапазон
Имена DNS Определяет время ожидания разрешения имен DNS. Значение "0" соответствует бесконечному времени ожидания	0–120 с
Соединение с СБ Определяет время ожидания установления соединения с сервером безопасности	1–180 с
Отправка запроса Определяет время ожидания отправки запроса	1–180 с
Получение ответа Определяет время ожидания получения ответа на отправленный запрос	1–180 с
Буфер приема Определяет размер буфера транспортной подсистемы для приема потоковых данных. Параметр предназначен для оптимизации процесса передачи по сети потоковой информации. Его значение определяется пропускной способностью сети — чем она выше, тем больше может быть размер буфера	8–128 Кб
Блок передачи Определяет размер блока передачи 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 блока	1–1000 Кб
Окончание 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	1–180 с
Интервал опроса Определяет промежуток времени, через который отправляется контрольный запрос. Параметр предназначен для контроля соединения. Принцип контроля основан на периодической отправке служебного запроса и получении ответа на него. В случае получения корректного ответа соединение считается работающим. При получении некорректного ответа или по истечении времени ожидания ответа (см. следующий параметр) соединение считается отключенным. При увеличении значения параметра теряется оперативность получения достоверной информации о состоянии соединения	1–180 с
Ответ клиента Определяет максимальное время ожидания ответа на отправленный контрольный запрос. Параметр предназначен для контроля установленного соединения	1–360 с

Терминологический справочник

А	
Администратор безопасности	Лицо, ответственное за обеспечение безопасности системы, реализацию и соблюдение установленных административных мер защиты и осуществляющее постоянную организационную поддержку функционирования применяемых физических и технических средств защиты
Администратор оперативного управления	Лицо, ответственное за контроль состояния защищаемых компьютеров системы, за отслеживание в режиме реального времени нарушений, связанных с попытками несанкционированного доступа пользователей
Ж	
Журнал регистрации событий	Хранилище с информацией о событиях, зарегистрированных в системе защиты, например, попытках входа в систему
З	
Защищаемый компьютер	Компьютер с установленным клиентом системы защиты. Обеспечивает защищенную работу пользователя системы
М	
Мониторинг	Контроль работы компьютеров в режиме реального времени
Н	
НСД	Несанкционированный доступ, заключающийся в получении нарушителем доступа к ресурсу (объекту) в нарушение установленных правил разграничения доступа
О	
Оперативное управление	Незамедлительное воздействие на компьютеры с целью предотвращения попыток несанкционированного доступа
С	
Сервер безопасности	Компьютер с установленным серверным программным обеспечением системы защиты. Обеспечивает взаимодействие всех компонентов системы, сбор, обработку и передачу данных, передачу команд оперативного управления
Срез	Совокупность защищаемых компьютеров, выбранных и сгруппированных по некоторым произвольным признакам

Документация

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

Предметный указатель

А

Администратор безопасности 5
Администратор оперативного управления 5
Аппаратная конфигурация
  сведения 14
  экспорт 27

Б

Блокировка компьютера 23

В

Выключение компьютера 23

Ж

Журнал Secret Net 13, 20

З

Задачи мониторинга 5
Запуск программы 6

И

Интерфейс
  настройка 29
  программа мониторинга 7

М

Механизмы защиты 15

Н

НСД 13, 15, 20, 30

О

Обновление групповых политик 23
Объекты
  свойства 17
  список 11
Отчеты 24

П

Параметры программы 29
Перезагрузка компьютера 23
Пиктограммы компьютеров 33
Поиск
  объектов 20
Привилегии 6, 30

Р

Разблокирование компьютера 23

С

Сетевое взаимодействие
  программа мониторинга 29
Сортировка
  объектов 19
Срез 9
Счетчик НСД 22

У

Уведомления мониторинга 15

Ф

Фильтр НСД 21

Ш

Штатные журналы 13, 20