



Код безопасности

Средство защиты информации

SECRET NET 7



Руководство администратора

Работа с программой оперативного управления



Код безопасности

© Компания "Код Безопасности", 2014. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

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

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

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

Оглавление

Список сокращений	5
Введение	6
Общие сведения о работе с программой оперативного управления	7
Основные цели и задачи использования программы	7
Конфигурирование	7
Мониторинг и оперативное управление	8
Централизованный аудит	9
Запуск программы	9
Интерфейс программы	11
Элементы интерфейса	11
Настройка интерфейса	12
Настройка параметров работы программы	12
Подключение к серверу безопасности	15
Структура оперативного управления	16
Панель диаграммы управления	16
Объекты структуры	16
Фильтрация объектов	17
Управление отображением объектов	19
Структура ОУ после установки компонентов Secret Net	21
Сохранение изменений	22
Изменение состава структуры ОУ	22
Добавление агентов и серверов в структуру ОУ	22
Удаление агентов и серверов из структуры ОУ	25
Управление отношениями подчиненности в структуре ОУ	25
Вывод агентов и серверов из подчинения	25
Подчинение агентов и серверов	26
Просмотр и изменение параметров объектов	28
Панель свойств объектов	28
Настройка отображения иерархии управления	29
Настройка отображения параметров объектов	30
Настройка параметров объектов	30
Общие параметры объекта	31
Параметры сетевых соединений	33
Параметры передачи локальных журналов	34
Параметры архивирования централизованных журналов	36
Параметры рассылки уведомлений о событиях НСД	38
Параметры Secret Net для групповых политик	41
Привилегии для работы с программой оперативного управления	46
Параметры лицензий на использование компонентов	48
Учетная информация компьютера	49
Параметры функционирования механизмов защиты	50
Параметры трассировки ПО системы Secret Net	52
Параметры фильтра уведомлений о НСД для сервера безопасности	52
Возможности работы с параметрами нескольких объектов	53
Сравнение параметров	54
Настройка параметров нескольких объектов	54
Копирование значений параметров	54
Мониторинг и оперативное управление	56
Просмотр сведений	56
Обозначения объектов на диаграмме управления	56
Сведения в панели свойств объектов	57
Сведения в панели событий системы	59
Отслеживание событий НСД	61
Оповещение о событиях НСД	61
Квитирование событий НСД	62

Сброс счетчиков событий НСД	62
Создание правил фильтрации на основе уведомлений о НСД	63
Оперативное управление	64
Блокировка и разблокирование компьютеров	64
Перезагрузка и выключение компьютеров	65
Обновление групповых политик на компьютерах	65
Команды управления механизмами защиты	65
Утверждение изменений аппаратной конфигурации	66
Сбор локальных журналов по команде администратора	66
Формирование отчетов	66
Отчет "Паспорт ПО"	67
Отчет "Ресурсы АРМ"	69
Отчет "Допуск пользователей к ПАК "Соболь""	70
Отчет "Электронные идентификаторы"	71
Работа с централизованными журналами	73
Централизованные журналы	73
Журнал НСД	73
Объединенный журнал агентов	74
Журнал сервера безопасности	74
Хранение журналов в сетевом режиме функционирования	75
Локальные хранилища журналов	75
Централизованное хранилище	75
Архивы журналов, созданные сервером безопасности	76
Панели для работы с записями журналов	76
Загрузка записей журналов	79
Запросы для журнала НСД	79
Запросы для журнала станций	81
Запросы для журнала сервера безопасности	83
Запросы для архивов журналов	84
Настройка параметров запроса	86
Управление запросами	87
Возможности при просмотре записей	88
Режимы отображения сведений о событиях	88
Квитирование событий НСД в журнале НСД	94
Создание правил фильтрации на основе записей о НСД	94
Сортировка записей	95
Поиск записей	95
Цветовое оформление записей	96
Использование закладок	97
Получение сведений о событиях из внешних баз знаний	98
Печать записей	98
Экспорт записей	99
Архивирование централизованных журналов по команде администратора ...	100
Приложение	101
Пиктограммы защитных механизмов	101
Параметры сетевого взаимодействия	102
Редактирование списков устройств и принтеров в групповых политиках	103
Управление списком устройств	103
Управление списком принтеров	104
Восстановление журналов из архивов	105
Генерация и установка сертификата сервера безопасности	106
Документация	108

Список сокращений

AD	Active Directory
DNS	Domain Name System
IP	Internet Protocol
RFC	Request for Comments
БД	База данных
НСД	Несанкционированный доступ
ОС	Операционная система
ОУ	Оперативное управление
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СБ	Сервер безопасности
СНД	Серийный номер подсистемы защиты дисков
СНК	Серийный номер клиента
СНСБ	Серийный номер сервера безопасности
СНТ	Серийный номер разрешения терминальных подключений
СНУ	Серийный номер средств управления

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net 7" RU.88338853.501410.015 (далее — система Secret Net, система защиты). В руководстве содержатся сведения о работе с компонентом "Secret Net 7 — Программа управления". Компонент используется в сетевом режиме функционирования системы Secret Net.

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

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

Глава 1

Общие сведения о работе с программой оперативного управления

В сетевом режиме функционирования системы Secret Net для централизованного управления защищаемыми компьютерами может использоваться компонент "Secret Net 7 — Программа управления". Данный компонент (далее — программа оперативного управления) предоставляет следующие основные возможности:

- конфигурирование сетевой структуры системы Secret Net;
- мониторинг и оперативное управление защищаемыми компьютерами;
- работа с централизованными журналами.

С целью разделения функций конфигурирования, управления и просмотра сведений в программе оперативного управления предусмотрены следующие режимы работы:

- режим конфигурирования;
- режим мониторинга и централизованного аудита;
- автономный режим без подключения к серверу безопасности.

Выбор нужного режима работы программы осуществляется при ее запуске.

Основные цели и задачи использования программы

Конфигурирование

При установке компонентов системы Secret Net формируется начальная конфигурация структуры оперативного управления (ОУ). Как правило, начальная конфигурация достаточна для функционирования компонентов и выполнения администратором безопасности своих функций. Однако в процессе эксплуатации может возникнуть необходимость в изменении конфигурации с целью создания более удобных условий управления или для актуализации сетевой структуры.

При конфигурировании осуществляется:

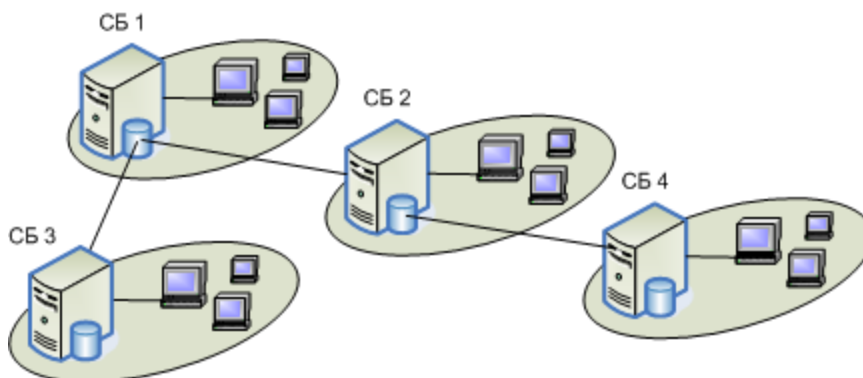
- редактирование структуры оперативного управления;
- настройка конфигурационных параметров серверов безопасности (компьютеры с установленным ПО "Secret Net 7 — Сервер безопасности") и агентов (компьютеры с установленным ПО "Secret Net 7" в сетевом режиме функционирования).

Права для конфигурирования объектов предоставлены пользователям, входящим в группу администраторов домена безопасности. В части конфигурирования агентов (добавление в структуру ОУ, удаление, подчинение и настройка конфигурационных параметров) права также могут быть предоставлены пользователям группы администраторов Secret Net (SecretNetAdmins), если сервер безопасности установлен в варианте размещения хранилища объектов централизованного управления в Active Directory. При этом пользователям группы SecretNetAdmins также должны быть делегированы административные полномочия для управления соответствующими компьютерами (предоставлен доступ к объектам и их параметрам на чтение и запись стандартными средствами Windows).

Серверы безопасности (СБ) и агенты составляют структуру оперативного управления. Между объектами должны быть установлены зависимости, определяющие подчиненность агентов серверам безопасности, а также подчиненность серверов безопасности между собой. Чтобы использовать воз-

возможности оперативного управления агентом, необходимо подчинить его серверу безопасности.

Серверу безопасности можно подчинить только тех агентов, которые включены в состав того же домена безопасности, где находится СБ. Подчинение серверов безопасности другим серверам возможно и в разных доменах безопасности в пределах леса.



Формирование структуры подчиненности объектов осуществляется по следующим правилам:

- в одном домене безопасности обязательно должен быть хотя бы один СБ;
- серверы одних доменов безопасности могут быть подчинены СБ из других доменов в рамках леса доменов безопасности;
- запрещается циклически подчинять серверы безопасности;
- СБ может управлять агентами только того домена безопасности, в котором он установлен.

Корректное и бесперебойное функционирование структуры оперативного управления обеспечивается при правильной настройке параметров объектов. Необходимость изменения заданных параметров может возникнуть в разных случаях. Например, при низкой пропускной способности каналов связи или из-за больших объемов накапливаемых данных.



Внимание!

При работе с программой оперативного управления могут быть ограничены возможности конфигурирования объектов, находящихся в различных доменах безопасности. Если сервер безопасности, к которому подключена программа, установлен в варианте размещения хранилища объектов централизованного управления в Active Directory, не поддерживаются некоторые функции конфигурирования объектов других доменов (удаление, изменение отношений подчинения агентов, настройка параметров). Для конфигурирования таких объектов необходимо выполнить подключение к серверу безопасности соответствующего домена.

Если подключение выполнено к серверу безопасности, который использует базу данных альтернативной службы каталогов (не Active Directory), конфигурирование объектов других доменов безопасности осуществляется без ограничений при наличии соответствующих прав.

Мониторинг и оперативное управление

Под мониторингом системы защиты подразумевается контролирование состояния компьютеров, на которых установлено клиентское ПО системы Secret Net в сетевом режиме функционирования. 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;
- 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.

В дополнение к перечисленным задачам в программе реализована возможность управления параметрами групповых политик. Параметры могут быть настроены как для агентов (в локальных политиках безопасности), так и для других объектов: серверов безопасности, доменов и организационных подразделений.

Централизованный аудит

Под аудитом системы защиты понимается анализ информации о событиях, происходивших в системе в течение некоторого промежутка времени. Информация о событиях накапливается в журналах регистрации событий.

Сведения о возможностях просмотра и управления локальными журналами на защищаемых компьютерах см. в документе [5]. Для работы с централизованными журналами используется программа оперативного управления.

Основными задачами централизованного аудита являются:

- контролирование состояния защищенности системы;
- выявление причин произошедших изменений;
- определение обстоятельств, которые привели к изменению состояния защищенности системы или к НСД;
- установление времени изменений.

Для выполнения перечисленных и сопутствующих задач в программе реализованы различные возможности поиска, фильтрации и представления информации.

Запуск программы

При запуске программы оперативного управления выполняется подключение к серверу безопасности. Если в системе присутствуют несколько серверов, пользователь может выбрать нужный сервер, с которым будет установлено соединение. Для подключения к серверу безопасности в режиме конфигурирования пользователь должен входить в группу администраторов домена безопасности, в котором находится сервер.

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 "Программа 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 | Программа управления".

На экране появится стартовый диалог программы для выбора режима работы.



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. Выберите одну из следующих команд:
 - для запуска в режиме конфигурирования:
 - "Конфигурирование" — запускает программу с последующим переходом к средствам редактирования структуры оперативного управления (панель "Диаграмма");
 - "Настройки" — запускает программу с последующим переходом к средствам настройки параметров объектов оперативного управления (панель "Свойства");
 - "Лицензирование" — запускает программу с последующим переходом к средствам редактирования списка лицензий на использование компонентов Secret Net (панель "Свойства");
 - для запуска в режиме мониторинга и централизованного аудита:
 - "Мониторинг и управление" — запускает программу с последующим переходом к средствам просмотра структуры оперативного управления (панель "Диаграмма");
 - "Журналы НСД" — запускает программу с последующим переходом к средствам загрузки централизованного журнала НСД (панель "НСД"). Для формирования нового запроса на загрузку записей выберите команду "Новый запрос" (справа от команды "Журналы НСД");
 - "Журналы" — запускает программу с последующим переходом к средствам загрузки журналов, поступивших с защищаемых компьютеров в базу данных сервера безопасности (панель "Журналы"). Для формирования нового запроса на загрузку записей выберите команду "Новый запрос" (справа от команды "Журналы");
 - "Состояние" — запускает программу с последующим переходом к средствам просмотра текущего состояния защищаемых компьютеров (панель "Свойства");
 - для запуска программы в автономном режиме:
 - "Журнал" (в нижней части стартового диалога) — запускает программу с предварительной загрузкой сохраненной копии журнала из файла;

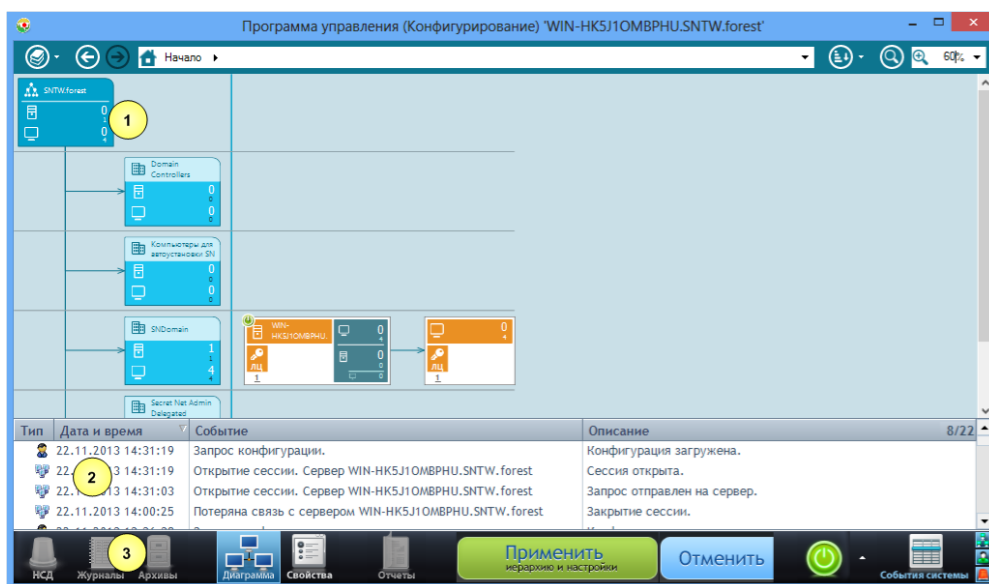
- "Архив журналов" (в нижней части стартового диалога) — запускает программу с предварительной загрузкой архива журналов из файла.

Примечание.

При запуске программы в режиме конфигурирования (а также при обновлении конфигурации ОУ в этом режиме) осуществляется проверка соответствия сохраненной структуры ОУ с объектами "компьютер" в службе каталогов. Если в структуре ОУ обнаружены объекты, для которых отсутствуют соответствующие компьютеры в службе каталогов (например, после некорректного удаления этих компьютеров), программа предлагает удалить эти объекты из структуры ОУ. Перед удалением таких объектов рекомендуется выяснить причины сложившейся ситуации и возможности восстановления удаленных компьютеров в службе каталогов.

Интерфейс программы

Пример внешнего вида основного окна программы в режиме конфигурирования представлен на следующем рисунке.



Пояснение.

На рисунке выносками обозначены элементы: 1 — панель диаграммы управления; 2 — панель событий системы; 3 — панель навигации по функциям программы.

Элементы интерфейса

Основное окно программы может содержать следующие элементы интерфейса:

Панели вывода сведений

Предназначены для отображения информации и выполнения действий с объектами. Предусмотрено несколько панелей, каждая из которых имеет определенное назначение. При работе с программой управления в режиме конфигурирования доступны следующие панели:

- панель диаграммы управления ("Диаграмма");
- панель свойств объектов ("Свойства");
- панель событий системы ("События системы")

Панель навигации по функциям приложения (панель навигации)

Содержит средства управления программой: ярлыки переключения панелей вывода сведений, кнопку сохранения конфигурационных изменений (в режиме конфигурирования), средства вызова диалогов подключения к серверу безопасности и настройки параметров программы

Настройка интерфейса

Основное окно программы управления можно настраивать для оптимизации отображения элементов интерфейса. В данном разделе рассматриваются возможности размещения на экране элементов интерфейса основного окна программы. Настройка представления информации внутри панелей вывода сведений рассматривается ниже в соответствующих разделах.

Панель навигации всегда отображается в нижней части окна программы управления.

Для панелей вывода сведений предусмотрены режимы отображения внутри основного окна программы управления или в виде отдельных окон.

Панель вывода сведений в режиме отображения внутри основного окна представляет собой область в основном окне программы. В основном окне может отображаться содержимое только одной панели вывода сведений (совместно с панелью событий системы или без нее).

Панели вывода сведений можно переключать в режим отображения в виде отдельных окон. В этом режиме панель трансформируется в отдельное окно на рабочем столе Windows. При использовании данного режима можно разместить на экране несколько внутренних окон программы, в том числе и на дополнительных мониторах, подключенных к компьютеру. Для включения режима вызовите контекстное меню ярлыка внутреннего окна в панели навигации и выберите команду "Открыть в отдельном окне".



Примечание.

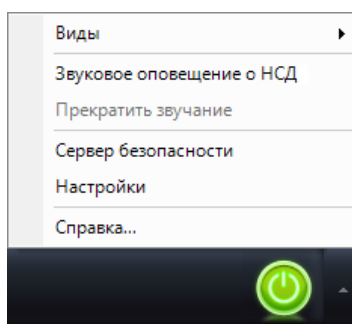
Последнюю панель вывода сведений нельзя переключить в режим отображения в виде отдельного окна, если все остальные панели уже переключены в этот режим (при этом текущий режим отображения панели событий системы не учитывается).

Чтобы вернуть панель в режим отображения внутри основного окна, закройте ее (например, с помощью команды "Закрыть" в контекстном меню ярлыка в панели навигации).

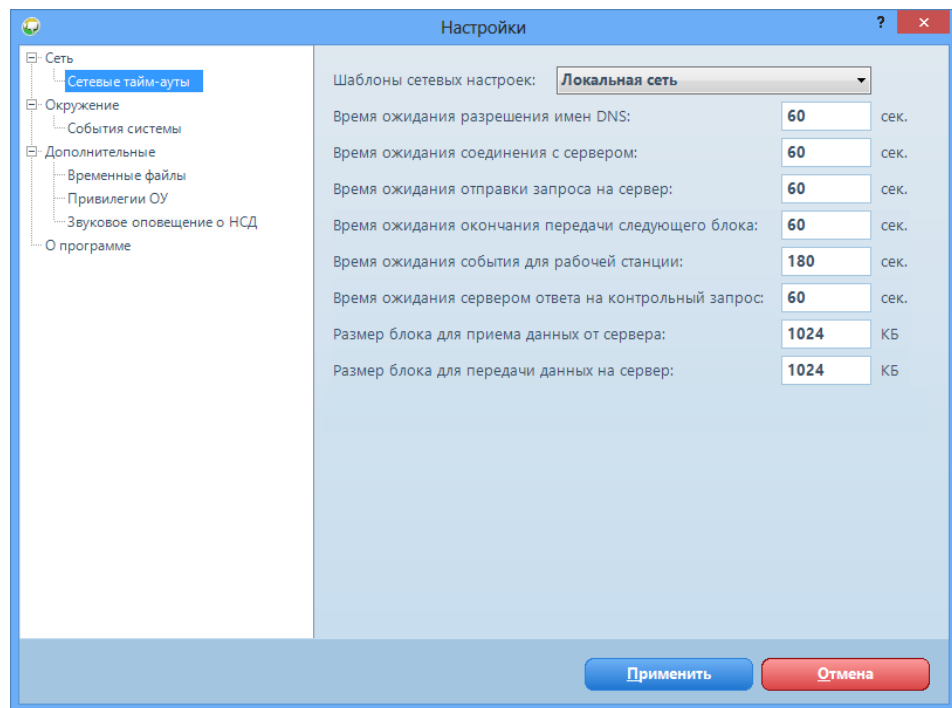
Настройка параметров работы программы

Для настройки параметров:

1. В правой части панели навигации (внизу основного окна программы) нажмите кнопку вызова меню.



2. Выберите команду "Настройки".
На экране появится одноименный диалог.



3. Последовательно выбирая названия групп в левой части диалога, укажите необходимые значения параметров.
4. После настройки параметров нажмите кнопку "Применить".

Примечание.

Некоторые параметры вступают в силу со следующего запуска программы управления.

Ниже приводится описание параметров по группам.

Группа параметров "Сеть | Сетевые тайм-ауты"

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. **102**

Группа параметров "Окружение | 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 оперативного управления;
- "События НСД" — уведомления о регистрации событий НСД.

Для каждого типа уведомлений можно задать особый цвет в соответствующей ячейке. Чтобы выбрать нужный цвет, нажмите кнопку в правой части ячейки

Группа параметров "Дополнительные | Временные файлы"

Содержит параметры размещения и хранения временных файлов, создаваемых программой.

Поле "Каталог для временных файлов"

Определяет путь к каталогу, в который будут помещаться 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

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 "Дополнительные | Привилегии ОУ"

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

Группа параметров "Дополнительные | Звуковое оповещение о НСД"

Содержит параметры звукового оповещения пользователя программы о возникновении событий НСД. Для включения режима звукового оповещения установите отметку в поле "Звуковое оповещение о событиях НСД" и настройте параметры ниже (также для оперативного включения и отключения режима можно использовать соответствующие команды "Звуковое оповещение о НСД" и "Прекратить звучание" в меню — см. действие **1** вышеописанной процедуры).

Поле "Звуковой сигнал"

Определяет тип звукового сигнала, оповещающего о событиях НСД. 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 "Временной интервал"

Определяет паузу в миллисекундах между повторами звукового сигнала

Поле "Количество повторов сигнала"

Определяет количество повторов звучания сигнала. Чтобы указать числовое значение, установите отметку в поле слева. При отсутствии отметки сигнал будет повторяться до принудительного отключения

Группа параметров "О программе"

Содержит сведения о версии и используемой лицензии (лицензия используется, если в это же время программа управления функционирует на другом компьютере), а также поле для включения/отключения информационной заставки при запуске программы.

Подключение к серверу безопасности

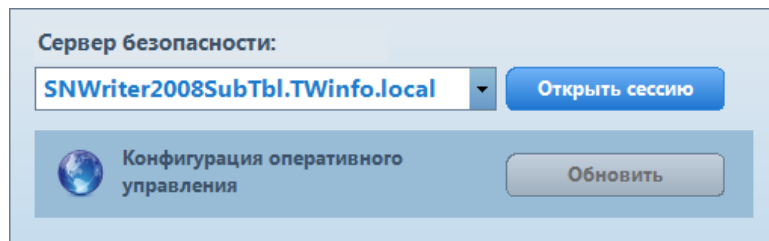
Сеанс подключения к серверу безопасности начинается при открытии сессии. Если сессия с нужным сервером безопасности не была открыта при запуске программы или потеряно соединение с сервером, подключиться к этому серверу можно без перезапуска. При необходимости подключения к другому серверу безопасности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

Для открытия сессии:



1. В правой части панели навигации (внизу основного окна) нажмите кнопку вызова диалога для выбора сервера безопасности.

На экране появится диалог.



2. Если для открытия сессии доступно несколько серверов безопасности, выберите нужный сервер в поле "Сервер безопасности".
3. Нажмите кнопку "Открыть сессию".

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

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

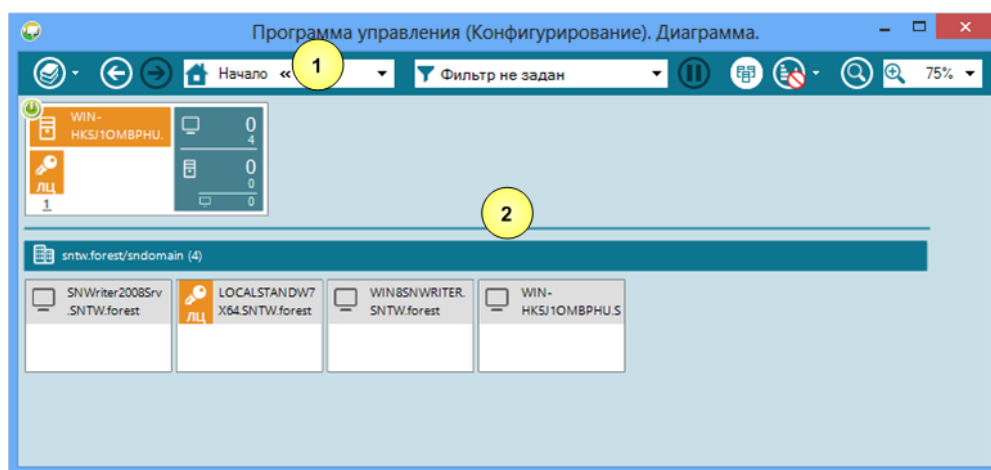
Глава 2

Структура оперативного управления

Панель диаграммы управления

Просмотр и редактирование структуры ОУ осуществляется в панели диаграммы управления. Панель открывается по умолчанию, если при запуске программы оперативного управления в диалоге выбора режима работы выбрана команда "Конфигурирование" или "Мониторинг и управление" (см. стр.9). Во время работы с программой переход к панели диаграммы управления можно выполнить с помощью ярлыка "Диаграмма" в панели навигации.

Панель диаграммы управления имеет вид, подобный представленному на рисунке.



Пояснение.

На рисунке обозначены элементы: 1 — панель управления отображением объектов; 2 — область отображения диаграммы.

Элементы интерфейса панели диаграммы управления:

Панель управления отображением объектов

Содержит средства для управления отображением объектов на диаграмме. С помощью средств панели осуществляются фильтрация отображаемых объектов, переходы к элементам структуры, управление режимами группировки, сортировки элементов и масштабирование структуры

Область отображения диаграммы

Предназначена для графического представления сведений о структуре объектов оперативного управления

Объекты структуры

Структура ОУ на диаграмме управления выводится в виде схемы элементов, соответствующих доменам, организационным подразделениям, серверам безопасности и агентам. 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 агентов, подчиненных серверам безопасности в соответствующих подразделениях;

- режим отображения списков агентов — отображаются выбранный сервер безопасности и списки агентов непосредственного подчинения.

В режиме общей начальной структуры диаграмма разделена на две части: слева отображается структура доменов и организационных подразделений, а справа — серверы безопасности и группы агентов, 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. **11**.

Для перехода в режим отображения списков агентов наведите указатель на нужный сервер безопасности или группу агентов 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 агенты, непосредственно подчиненные выбранному серверу. Пример диаграммы управления в этом режиме см. на рисунке на стр. **16**. Возврат в режим общей начальной структуры осуществляется с помощью средств навигации на панели управления отображением объектов.

Пиктограммы объектов на диаграмме управления перечислены в следующей таблице:

Пиктограмма	Описание
	Домен
	Организационное подразделение
	Сервер безопасности
	Агент или группа агентов

Фильтрация объектов

Для ограничения количества отображаемых объектов на диаграмме управления можно использовать следующие возможности:

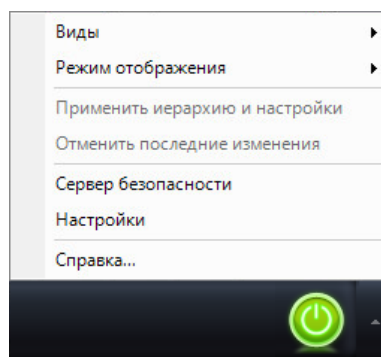
- фильтрация объектов по отношению к серверу подключения;
- фильтрация объектов по принадлежности доменам и организационным подразделениям;
- фильтрация агентов по их состоянию.

Фильтрация объектов по отношению к серверу подключения

При работе с программой управления в режиме конфигурирования по умолчанию отображается вся структура оперативного управления — все серверы безопасности и агенты, имеющиеся в структуре. Некоторые из этих объектов могут не иметь отношения к серверу подключения (сервер безопасности, с которым установлено соединение программы). Например, агенты, подчиненные серверам других доменов безопасности. При необходимости можно отключить отображение на диаграмме таких объектов с помощью фильтрации по отношению к серверу подключения. Фильтрация действует как для диаграммы управления, так и для списка иерархии управления в панели свойств объектов.

Для отключения отображения объектов, не относящихся к серверу подключения:

1. В правой части панели навигации (внизу основного окна программы) нажмите кнопку вызова меню.



2. В подменю "Режим отображения" выберите соответствующую команду:

- "Объекты домена безопасности сервера подключения" — чтобы отобразить на диаграмме все объекты домена безопасности, в который входит сервер подключения;
- "Сервер подключения и его дочерние объекты" — чтобы отобразить на диаграмме только подчиненные объекты сервера подключения (включая и сам сервер безопасности).

На диаграмме управления будут отображены объекты в соответствии с выбранным вариантом. Если требуется отключить данный тип фильтрации, в подменю "Режим отображения" выберите команду "Все объекты оперативного управления" (текущий вариант фильтрации обозначается отметкой напротив соответствующей команды).

Фильтрация объектов по принадлежности доменам и организационным подразделениям

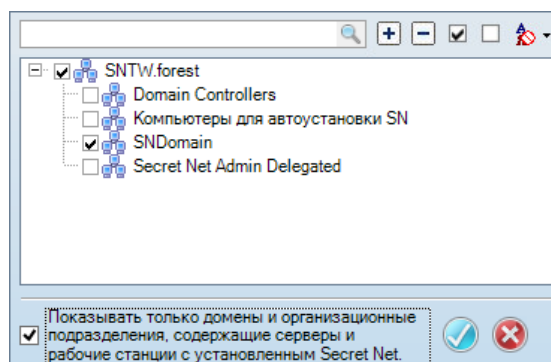
В структуре Active Directory могут присутствовать организационные подразделения или домены, объекты которых не требуется отображать на диаграмме управления. Например, такие организационные подразделения, в которых отсутствуют защищаемые компьютеры. При необходимости можно отключить отображение на диаграмме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

Для включения отображения объектов определенных доменов и организационных подразделений:



1. В панели управления отображением объектов (см. стр. 16) нажмите кнопку "Фильтр AD".

На экране появится диалог 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 кнопки раскрытия и сворачивания иерархии, а также кнопку сортировки. Соответствующие средства расположены в верхней части окна.
4. Отметьте нужные элементы списка. Для установки или удаления отметок во всех полях используйте соответствующие кнопки в верхней части окна. Чтобы автоматически отметить только те домены и организационные подразделения, которые содержат компьютеры с установленным ПО Secret Net, установите отметку в нижней части диалога. После выбора элементов нажмите кнопку принятия изменений.

На диаграмме управления будут отображены только те объекты, которые относятся к выбранным доменам и организационным подразделениям. Если отображаются не все объекты структуры ОУ, на фоне кнопки "Фильтр AD" выводится специальная пиктограмма включенного фильтра.

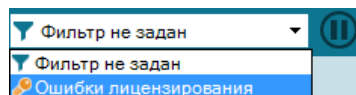
Фильтрация агентов по их состоянию

В режиме отображения списков агентов (см. стр. 16) на диаграмме можно отобразить только те объекты, которые имеют определенный признак состояния. Например, агенты с обнаруженными ошибками при проверке серийных номеров или агенты с признаком НСД. Список доступных для выбора признаков состояния зависит от режима работы программы — большинство из них могут отслеживаться только при работе в режиме мониторинга и централизованного аудита.

Для включения отображения агентов с определенным признаком состояния:

1. Включите режим отображения списков агентов. Для этого, например, подведите указатель к серверу/группе агентов и дважды нажмите левую кнопку мыши.
2. В панели управления отображением объектов (см. стр. 16) выберите из раскрывающегося списка признак, по которому необходимо выполнить фильтрацию агентов.

Фрагмент панели со средствами фильтрации агентов 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 агентов. При необходимости можно отключить динамическую фильтрацию, чтобы зафиксировать текущий список агентов.

Для отключения динамической фильтрации:



- В панели управления отображением объектов нажмите кнопку рядом с выбранным признаком, по которому выполнена фильтрация агентов.

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

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.

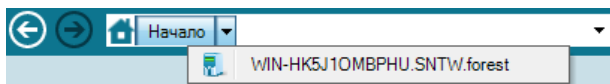
Дополнительно в режиме отображения списков агентов (см. стр. 16) можно группировать объекты в соответствии с их принадлежностью организационным подразделениям.

Перечисленные действия выполняются с использованием средств панели управления отображением объектов (см. стр. 16).

Переходы по структуре ОУ с помощью средств навигации

Средства навигации могут использоваться для переходов по структуре ОУ, а также для поиска серверов безопасности и агентов. Переходы по структуре осуществляются посредством выбора нужных элементов из числа представленных на диаграмме или из списка ранее выбранных элементов (в истории переходов). Поиск объектов осуществляется по введенной строке символов, которая должна присутствовать в имени компьютера.

Фрагмент панели управления отображением объектов со средствами навигации представлен на следующем рисунке.



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

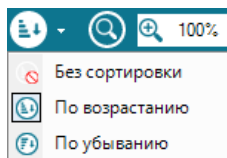
Сортировка объектов

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

Для сортировки объектов:

1. В панели управления отображением объектов нажмите кнопку "Режимы сортировки". Кнопка расположена рядом со средствами масштабирования.

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



2. Выберите нужное направление сортировки.

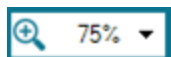
Объекты будут упорядочены в выбранном направлении, и кнопка "Режимы сортировки" примет соответствующий вид.

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 или вывести увеличенное изображение нужного фрагмента.

Для изменения масштаба отображения:

- В панели управления отображением объектов введите или выберите нужный масштаб. Элемент панели для настройки масштаба представлен на следующем рисунке.



При просмотре диаграммы в масштабе, отличном от 100%, можно использовать специальный инструмент "Линза". Данный инструмент действует аналогично стандартному инструменту ОС Windows "Экранная лупа" и позволяет отобразить область на экране рядом с курсором в масштабе 100%.



Для включения и отключения инструмента "Линза":

- В панели управления отображением объектов нажмите кнопку рядом со средством изменения масштаба.

После включения инструмента наведите курсор на нужную область диаграммы — вокруг курсора будет показано изображение в масштабе 100%.

Группировка агентов по принадлежности организационным подразделениям

В режиме отображения списков агентов по умолчанию выводится общий список подчиненных агентов выбранного сервера безопасности. Если серверу безопасности подчинены агенты, входящие в различные организационные подразделения, можно включить группировку агентов. При включенной группировке список агентов 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 агентов в элементы, называемые группами агентов. Каждый такой элемент объединяет агентов, подчиненных одному серверу безопасности и входящих в одно организационное подразделение. Чтобы определить, какому серверу подчинены агенты 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 агентов.

Для включения группировки списка агентов:



- Включите режим отображения списков агентов. Для этого используйте средства навигации для перехода к нужным объектам (см. выше) или подведите указатель к серверу/группе агентов и дважды нажмите левую кнопку мыши.
- В панели управления отображением объектов нажмите кнопку "Включить группировку".

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

Структура ОУ после установки компонентов Secret Net

Установку компонентов системы Secret Net 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 подчинены серверам безопасности.

Программа оперативного управления в режиме конфигурирования предоставляет следующие возможности для редактирования структуры ОУ:

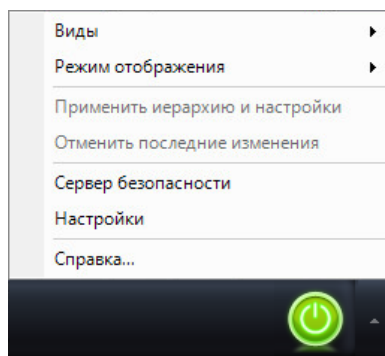
- изменение состава объектов управления (серверов безопасности и агентов), включенных в структуру ОУ;
- управление отношениями подчинения между серверами безопасности и агентами.

Формирование структуры ОУ в программе оперативного управления можно выполнить до установки клиентского ПО на компьютерах. В частности, при подготовке системы к автоматической установке клиентского ПО Secret Net на компьютерах (так как при автоматической установке клиента не выполняется подчинение компьютера серверу безопасности). В этом случае необходимо установить ПО сервера безопасности на всех компьютерах, которые будут функционировать в качестве серверов безопасности. После этого станут доступны возможности для формирования структуры ОУ в программе оперативного

управления. В структуру можно добавить компьютеры, на которых будет установлено клиентское ПО, и подчинить эти компьютеры соответствующим серверам безопасности.

Сохранение изменений

При работе с программой в режиме конфигурирования для сохранения изменений используйте кнопку "Применить иерархию и настройки" в панели навигации. Также с этой целью можно использовать одноименную команду меню, которое вызывается из панели навигации (например, если кнопка "Применить иерархию и настройки" закрыта другими элементами панели):



Перед сохранением необходимо убедиться в корректности структуры. Чтобы вернуться к последнему сохраненному варианту диаграммы управления, нажмите кнопку "Отменить" или используйте команду "Отменить последние изменения" в меню.

Указанные кнопки и команды меню присутствуют только в режиме конфигурирования и активны при наличии изменений, требующих сохранения.

О результатах выполнения действия выводится уведомление в панели событий системы.

Изменение состава структуры ОУ

Для реализации функций централизованного управления в состав структуры ОУ должны быть включены все серверы безопасности и агенты, имеющиеся в домене. Объекты добавляются в структуру ОУ при установке на компьютерах ПО системы Secret Net с подчинением серверам безопасности (при установке сервера безопасности подчинение другому серверу не обязательно). Исключение объектов из структуры происходит при удалении ПО.

Программа оперативного управления в режиме конфигурирования предоставляет возможности для включения в состав структуры ОУ указанных объектов и их исключения из структуры без выполнения установки или удаления ПО. Данные возможности следует использовать в особых случаях. В штатном режиме работы системы Secret Net состав объектов структуры ОУ должен в точности соответствовать количеству защищаемых компьютеров.

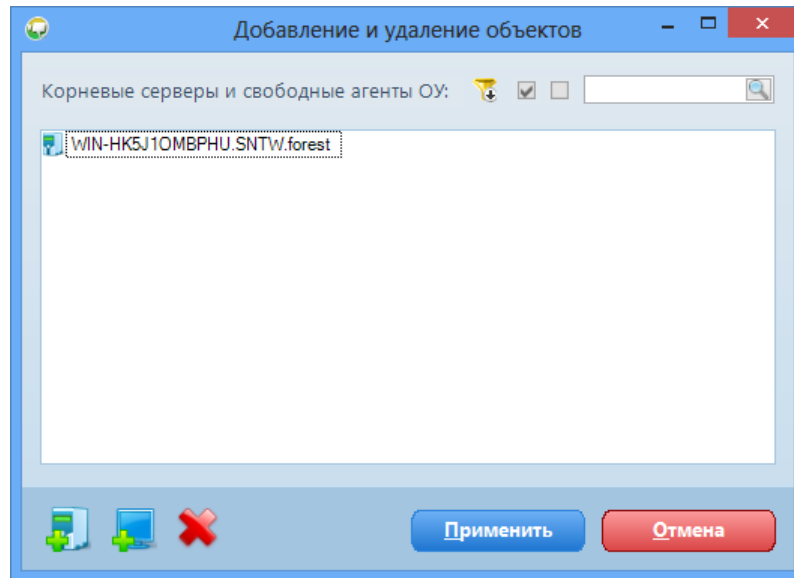
Добавление агентов и серверов в структуру ОУ

Добавляемый объект (агент или сервер безопасности) может включаться в структуру ОУ в качестве "свободного" объекта или подчиненного выбранному серверу безопасности. Свободных агентов в дальнейшем необходимо подчинить какому-либо серверу. Серверы безопасности могут быть добавлены в структуру как отдельные объекты без подчинения другим серверам.

Для добавления агентов:

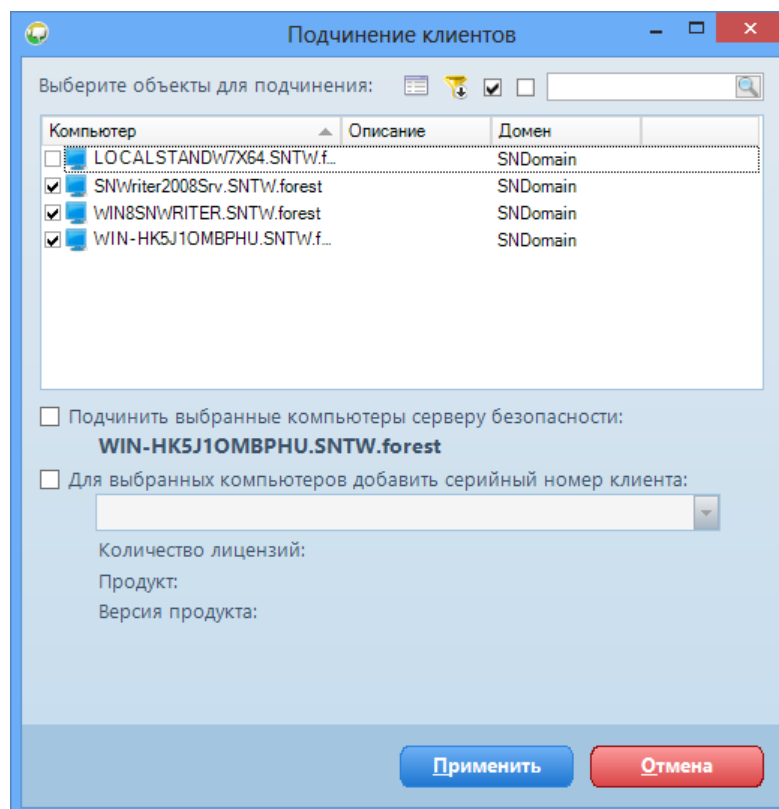
1. В диаграмме управления выберите сервер безопасности.
2. Вызовите контекстное меню сервера и выберите команду "Добавить/Удалить".

На экране появится диалог со списком свободных агентов и корневых серверов, имеющих в структуре ОУ.



3. В нижней части диалога нажмите кнопку "Выбор агентов".

После получения данных от сервера безопасности на экране появится диалог для выбора компьютеров, добавляемых в структуру ОУ. Диалог содержит список компьютеров, не входящих в структуру и относящихся к домену, в состав которого входит выбранный сервер.



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 в качестве агентов.
5. Чтобы подчинить новых агентов выбранному серверу безопасности, установите отметку в поле "Подчинить выбранные компьютеры серверу безопасности". При этом можно сразу указать серийный номер клиента (СНК) для этих агентов — для этого установите отметку в поле "Для выбранных компьютеров добавить серийный номер клиента" и введите или выберите нужный СНК.

Примечание.

Подчинение агентов можно выполнить позже (см. стр. 26).

6. Нажмите кнопку "Применить".
7. Если при выполнении действия 5 не был указан СНК, на экране появится диалог для выбора версии установленного на компьютерах клиентского ПО системы Secret Net. В диалоге отметьте поле, в котором указана версия установленного ПО, и нажмите кнопку "ОК".

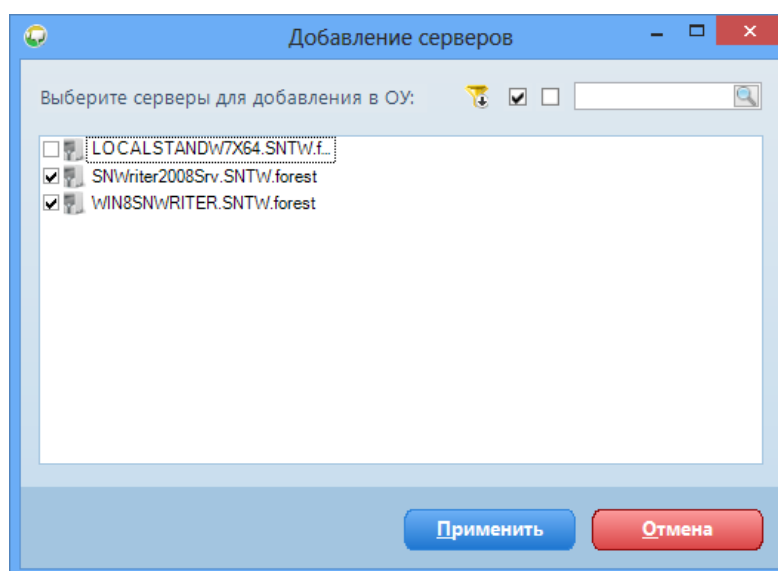
Для добавления серверов безопасности:

1. В диаграмме управления выберите сервер безопасности.
2. Вызовите контекстное меню сервера и выберите команду "Добавить/Удалить".

На экране появится диалог со списком свободных агентов и корневых серверов, имеющих в структуре ОУ (см. выше).



3. В нижней части диалога нажмите кнопку "Выбор серверов безопасности". После получения данных от сервера безопасности на экране появится диалог для выбора компьютеров, добавляемых в структуру ОУ. Диалог содержит список компьютеров, не входящих в структуру и относящихся к домену, в состав которого входит выбранный сервер.

**Примечание.**

При необходимости можно фильтровать список компьютеров, 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 в качестве серверов безопасности.
5. Нажмите кнопку "Применить".
Диалог со списком добавляемых компьютеров закроется, и выбранный компьютер появится в списке диалога со списком свободных агентов и корневых серверов.
6. Нажмите кнопку "Применить".

7. Сохраните изменения (см. стр.22).**Примечание.**

Дальнейшие действия с добавленными серверами безопасности (например, подчинение агентов) можно выполнять после обновления конфигурации оперативного управления.

Удаление агентов и серверов из структуры ОУ

Процедуры удаления агентов и серверов безопасности из структуры ОУ в программе оперативного управления следует выполнять только в случае неработоспособности компонентов Secret Net на этих компьютерах. Например, из-за некорректного завершения процедуры удаления ПО Secret Net или при необходимости переноса агента из одного домена безопасности в другой. Если требуется временно исключить объект, следует вывести этот объект из подчинения серверу безопасности (см. стр.25), чтобы впоследствии заново установить отношения подчинения.

Для удаления объектов в диаграмме управления:

1. В диаграмме управления выберите объекты для удаления.
2. Вызовите контекстное меню одного из выбранных объектов и выберите команду "Удалить". В появившемся диалоге запроса подтвердите выполнение операции.

Для удаления объектов в списке неподчиненных объектов:

1. В диаграмме управления выберите сервер безопасности.
2. Вызовите контекстное меню сервера и выберите команду "Добавить/Удалить".

На экране появится диалог со списком свободных агентов и корневых серверов, имеющих в структуре ОУ (см. стр.22).

3. Выберите в списке объекты для удаления.
4. В нижней части диалога нажмите кнопку "Удалить".



Выбранные объекты будут удалены из списка.

5. Нажмите кнопку "Применить".

Управление отношениями подчиненности в структуре ОУ

При работе с программой в режиме конфигурирования в структуре оперативного управления 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 агентов и серверов из подчинения

При выводе объекта из подчинения текущему серверу безопасности этот объект становится "свободным". Свободный агент 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. В диаграмме управления выберите объекты, которые необходимо вывести из подчинения.
2. Вызовите контекстное меню одного из выбранных объектов и выберите команду "Вывести из подчинения".

Выбранные объекты перестанут отображаться в диаграмме управления и будут переведены в список свободных объектов, который выводится в диа-

логе со списком свободных агентов и корневых серверов, имеющих в структуре ОУ (см. стр.22).

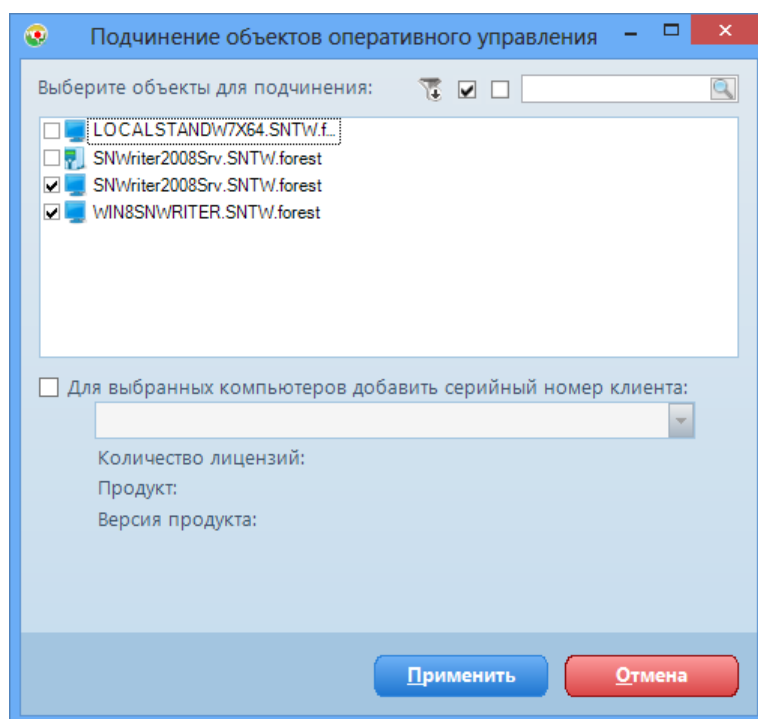
Подчинение агентов и серверов

Подчинение новых объектов серверу безопасности выполняется из числа свободных серверов безопасности и агентов. Если нужный сервер безопасности или агент отсутствует в списке свободных объектов, перед подчинением необходимо добавить объект в структуру (см. стр.22) или вывести его из подчинения другому серверу безопасности (см. выше).

Для подчинения объектов:

1. В диаграмме управления выберите сервер безопасности, в подчинение которому необходимо добавить новые объекты.
2. Вызовите контекстное меню сервера и выберите команду "Подчинить объекты".

На экране появится диалог со списком свободных агентов и корневых серверов, имеющих в структуре ОУ.



Примечание.

При необходимости можно фильтровать список компьютеров, исключая из отображения отключенные учетные записи и/или не имеющие в названии заданную строку символов. Средства управления списком расположены в верхней части диалога.

3. Отметьте в списке компьютеры, которые нужно подчинить выбранному серверу безопасности.
4. Если в списке отмечены только агенты, можно указать серийный номер клиента (СНК) для этих агентов — для этого установите отметку в поле "Для выбранных компьютеров добавить серийный номер клиента" и введите или выберите нужный СНК.

Примечание.

Настройку параметров лицензий для агента можно выполнить позже (см. стр.48).

5. Нажмите кнопку "Применить".

Объекты появятся в диаграмме управления в качестве подчиненных объектов выбранного сервера. Изменения в структуре ОУ будут сохранены после нажатия кнопки "Применить иерархию и настройки".

Подчинение агентов другим серверам безопасности после удаления сервера предыдущего подчинения

В большинстве случаев подчинение агентов другим серверам безопасности выполняется без особенностей. Для этого следует выполнять процедуры, описанные выше.

Однако при удалении сервера безопасности, который был установлен в варианте размещения хранилища объектов централизованного управления в Active Directory, централизованное переподчинение агентов этого сервера будет возможно только для такого же варианта установки нового сервера. Если новый сервер безопасности использует базу данных альтернативной службы каталогов (не Active Directory), подчинение таких агентов следует выполнять локально на компьютерах с помощью программы локального конфигурирования клиента SnLDAPConfig.exe. При этом нужно учитывать структуру доменов безопасности и серверов, если компьютеры входят в различные организационные подразделения. Сведения о работе с программой SnLDAPConfig.exe см. в документе [2]. После локального конфигурирования агентов проверьте полученную конфигурацию в программе оперативного управления.

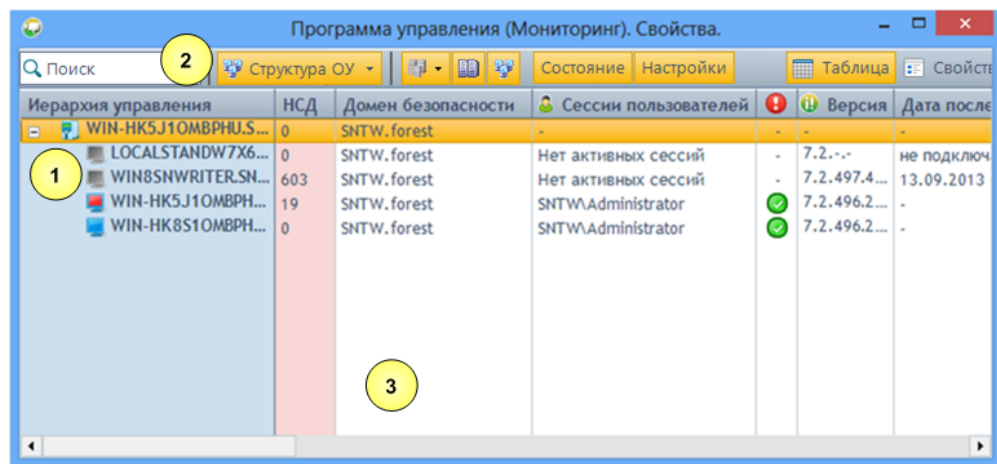
Глава 3

Просмотр и изменение параметров объектов

Панель свойств объектов

Просмотр состояния и управление параметрами объектов осуществляются в панели свойств объектов. Панель открывается по умолчанию, если при запуске программы оперативного управления в диалоге выбора режима работы выбрана команда "Настройки" или "Состояние" (см. стр. 9). Во время работы с программой переход к панели свойств можно выполнить с помощью ярлыка "Свойства" в панели навигации.

Панель свойств объектов при работе программы в режиме мониторинга и централизованного аудита имеет вид, подобный представленному на рисунке.



Пояснение.

На рисунке выносками обозначены элементы: 1 — панель иерархии управления; 2 — панель выбора режимов отображения; 3 — область отображения параметров объектов.

Элементы интерфейса панели настройки свойств:

Панель иерархии управления

Содержит иерархический список объектов управления. Для списка можно включить один из следующих видов отображения (с помощью кнопки на панели выбора режимов):

- отображение структуры ОУ — иерархия объектов представлена в виде дерева подчинения серверов безопасности и агентов. При работе с программой в режиме конфигурирования список по умолчанию содержит все серверы безопасности и агенты, имеющиеся в структуре ОУ. В режиме мониторинга и централизованного аудита — только объекты, относящиеся к серверу безопасности, с которым установлено соединение программы (сервер подключения является корневым элементом иерархии);
- отображение структуры AD — в списке представлена структура домена Active Directory из компьютеров и организационных подразделений.

Аналогично объектам в диаграмме управления в иерархии отображаются состояния объектов: признаки НСД, включен/выключен компьютер и другие оперативные состояния

Панель выбора режимов отображения

Содержит средства для управления отображением данных: поиск и переход к объекту в иерархическом списке, выбор вида отображения для списка, фильтрация содержимого и переключение вида отображаемых свойств (табличное представление или представление в виде вкладок)

Область отображения параметров объектов

Предназначена для просмотра и настройки параметров объектов, представленных в иерархии управления. Может использоваться табличный режим представления или режим группировки параметров по вкладкам.

В табличном режиме представления предусмотрены возможности сортировки и выбора отображаемых колонок. Сортировка объектов осуществляется внутри уровней иерархии

Настройка отображения иерархии управления

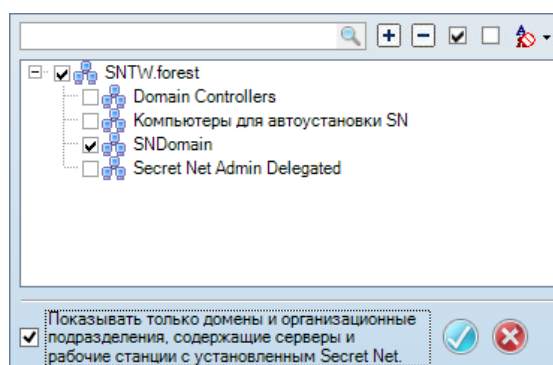
Панель отображения иерархии управления представляет собой колонку таблицы, примыкающую к области отображения параметров объектов. Колонка всегда отображается в левой части панели свойств объектов. Предусмотрены возможности фильтрации содержимого по принадлежности объектов доменам и организационным подразделениям, а также по типам объектов.

Для включения отображения объектов определенных доменов и организационных подразделений:



1. В панели выбора режимов отображения нажмите кнопку настройки фильтрации.

На экране появится диалог для выбора доменов и организационных подразделений, компьютеры которых будут включены в иерархию управления.



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 кнопки раскрытия и сворачивания иерархии, а также кнопку сортировки. Соответствующие средства расположены в верхней части окна.
4. Отметьте нужные элементы списка. Для установки или удаления отметок во всех полях используйте соответствующие кнопки в верхней части окна справа. Чтобы автоматически отметить только те домены и организационные подразделения, которые содержат компьютеры с установленным ПО Secret Net, установите отметку в нижней части диалога. После выбора элементов нажмите кнопку принятия изменений.

В списке панели иерархии управления будут отображены только те серверы и компьютеры, которые относятся к выбранным доменам и организационным подразделениям. Фильтрация действует как для списка иерархии управления в панели свойств объектов, так и для диаграммы управления.

Для включения и отключения отображения серверов безопасности:



- В панели выбора режимов отображения нажмите кнопку "Серверы".



Для включения и отключения отображения агентов:

- В панели выбора режимов отображения нажмите кнопку "Агенты".

Настройка отображения параметров объектов

В области отображения параметров объектов предусмотрены следующие режимы представления параметров:

- табличный режим представления — все параметры выводятся в колонках единой таблицы, строки которой соответствуют списку объектов в иерархии управления. Режим включается с помощью кнопки "Таблица" в панели выбора режимов отображения;
- режим группирования по вкладкам — параметры выбранных объектов сгруппированы в отдельных вкладках, переключение между которыми осуществляется с помощью закладок в верхней части области. Режим включается с помощью кнопки "Свойства" в панели выбора режимов отображения.

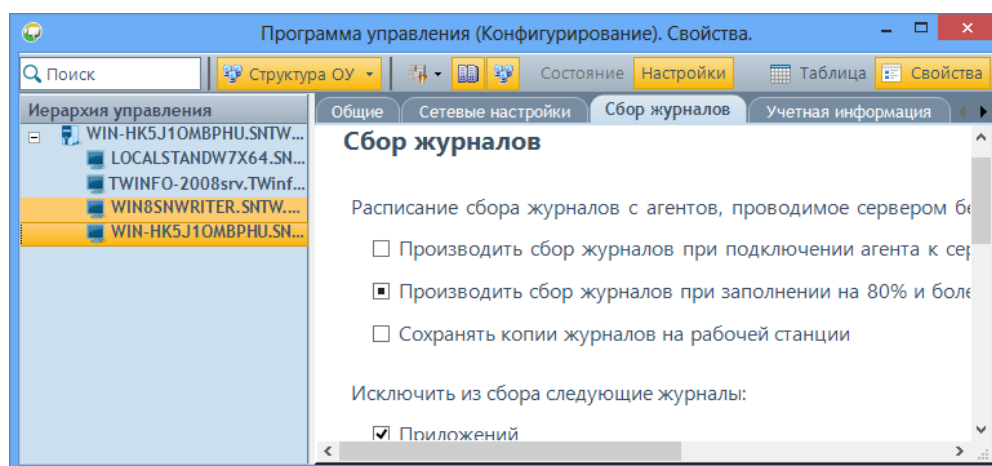
В табличном режиме представления можно изменять порядок и состав отображаемых колонок и сортировать таблицу по их содержимому (с учетом структуры списка объектов в иерархии управления). Для выполнения действий используются заголовки колонок. Кроме того, для оперативного изменения состава отображаемых колонок можно использовать кнопки фильтрации параметров в панели выбора режимов отображения:

- включение и отключение динамически изменяющихся параметров (например, количество событий НСД) осуществляется с помощью кнопки "Состояние". Возможность доступна только в режиме мониторинга и централизованного аудита;
- включение и отключение статически заданных параметров (например, номер системного блока) осуществляется с помощью кнопки "Настройки".

Настройка параметров объектов

Настройка параметров осуществляется в панели свойств объектов. Краткие сведения о состоянии параметров выводятся в табличном режиме представления. Для детального просмотра значений и настройки параметров следует использовать режим группирования по вкладкам.

Пример панели свойств объектов с включенным режимом группирования параметров по вкладкам (при работе программы в режиме конфигурирования) представлен на следующем рисунке.



Набор параметров, доступных для просмотра и изменения, зависит от типа объектов и текущего режима работы программы.

Параметры объектов могут быть представлены в следующих вкладках:

- "Общие" — содержит общие параметры объекта;
- "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 НСД" — содержит параметры рассылки почтовых уведомлений при регистрации событий НСД на подчиненных агентах;
- "Локальные политики", "Политики Secret Net" — содержит параметры Secret Net для групповых политик;
- "Привилегии пользователей" — содержит список учетных записей с привилегиями для работы с программой оперативного управления;
- "Лицензии" — содержит сведения о зарегистрированных лицензиях на использование компонентов системы Secret Net;
- "Учетная информация" — содержит сведения о компьютере, используемые для учета;
- "Защитные подсистемы" — содержит основные параметры функционирования механизмов защиты на компьютере;
- "Управление трассировкой" — содержит параметры трассировки работы ПО системы Secret Net (сервисная функция);
- "Фильтр уведомлений о НСД" — содержит параметры фильтрации уведомлений о событиях НСД, поступающих от серверов безопасности, которые непосредственно подчинены выбранному серверу безопасности.

Выбор объектов осуществляется в панели иерархии управления или в диаграмме управления. Переход в панель свойств объектов из диаграммы управления осуществляется с использованием команды "Свойства" в контекстном меню объектов, с помощью команд "Защитные подсистемы" и "Локальные политики" (только в режиме мониторинга и централизованного аудита), а также при выборе ярлыка или команды "Свойства" в панели навигации (команда представлена в подменю "Виды").

Общие параметры объекта

Для просмотра и изменения общих параметров объектов предназначена вкладка "Общие". Вкладка присутствует при выборе любого объекта. Пример содержимого вкладки, когда выбран сервер безопасности, представлен на следующем рисунке.

Общие

Имя компьютера: WIN-HK5J1OMBPHU.SNTW.forest

Домен безопасности: SNDomain

Версия Secret Net: 7.3.545.1

Администраторы домена безопасности: SNTW\Domain Admins

Администраторы леса доменов безопасности: SNTW\Domain Admins

Сертификат сервера: установлен [Просмотр...](#)

Расположение файлов на сервере

Каталог архивов: C:\Program Files\Secret Net\OM [Применить](#)

Каталог для временных файлов: C:\Program Files\Secret Net\OM [Применить](#)

На вкладке "Общие" отображаются основные сведения об объекте: какому серверу безопасности подчинен, имя объекта, домен безопасности, к которому он относится, а также версия ПО Secret Net. Также в зависимости от типа объекта и режима работы программы могут выводиться следующие сведения:

- для сервера безопасности:
 - сведения о наличии установленного сертификата сервера;
 - сведения о заполнении базы данных (актуально для СУБД с ограничением объема);
 - пути к каталогам размещения файлов, создаваемых сервером безопасности;
- для агента:
 - признак текущего состояния компьютера;
 - количество событий НСД, ожидающих квитирования (подтверждение приема) администратором безопасности;
 - время последнего подключения компьютера к серверу безопасности;
 - результат проведения функционального контроля при запуске компьютера;
 - список текущих пользовательских сессий, содержащий сведения о типах сессий, уровнях конфиденциальности сессий, полномочиях пользователей и др.

Примечание.

Перечисленные сведения для агента выводятся только в режиме мониторинга и централизованного аудита. Часть сведений дублируется в соответствующих колонках таблицы: "НСД", "Дата последнего подключения", "Статус функционального контроля", "Сессии пользователей".

Особенности настройки общих параметров сервера безопасности

На сервере должен быть установлен сертификат для обеспечения возможности подчинения агентов. При наличии корректного сертификата отображается признак "установлен". Если срок действия сертификата подходит к концу или истек, выводится предупреждение о необходимости установки нового

сертификата. С помощью кнопки "Просмотр" можно вызвать стандартное диалоговое окно с подробными сведениями о сертификате сервера безопасности. Генерация и установка нового сертификата осуществляется на компьютере сервера безопасности с использованием специальной утилиты (описание процедуры см. в Приложении на стр. **106**).

По умолчанию для размещения файлов, создаваемых сервером безопасности, используются локальные папки в каталоге установки ПО сервера. При необходимости можно указать другие пути размещения файлов — для этого введите полный путь в соответствующем поле и нажмите кнопку "Применить" рядом с этим полем. Изменения вступают в силу после перезагрузки сервера безопасности.

Примечание.

В случае использования сетевого пути необходимо на компьютере, где находится сетевой ресурс, стандартными средствами предоставить права доступа к папке для учетной записи компьютера сервера безопасности. При этом права доступа других учетных записей следует ограничить. Настройка прав доступа осуществляется в диалоговом окне настройки свойств папки на вкладках "Безопасность" (разрешения на доступ к папке) и "Доступ" (разрешения для общего ресурса). В списках учетных записей нужно добавить учетную запись компьютера сервера безопасности и при настройке разрешений на доступ к папке назначить разрешения "Чтение" и "Запись", а при настройке разрешений для общего ресурса — назначить разрешения "Чтение" и "Изменение".

Параметры сетевых соединений

Для просмотра и изменения параметров сетевых соединений предназначена вкладка "Сетевые настройки". Вкладка присутствует при выборе сервера безопасности или агента. Пример содержимого вкладки представлен на следующем рисунке.

Параметр	Значение	Единица
Шаблоны сетевых настроек:	Локальная сеть	
Время ожидания разрешения имен DNS:	60	сек.
Время ожидания соединения с сервером:	60	сек.
Время ожидания отправки запроса на сервер:	60	сек.
Время ожидания окончания передачи следующего блока:	60	сек.
Время ожидания события для рабочей станции:	180	сек.
Время ожидания сервером ответа на контрольный запрос:	60	сек.
Размер блока для приема данных от сервера:	1024	КБ
Размер блока для передачи данных на сервер:	1024	КБ

Параметры используются при установке сетевого соединения объекта с сервером безопасности, которому подчинен данный объект. Если параметры сетевых соединений не заданы (имеют нулевые значения), связь объекта с родительским сервером не будет устанавливаться. Для корневого СБ настройка данных параметров не требуется.

Сетевое взаимодействие компонентов системы Secret Net 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), могут проявляться длительные задержки при установлении соединений и даже сбой 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.

Первичный выбор шаблонов настройки параметров сетевого взаимодействия осуществляется при установке клиентов Secret Net и серверов безопасности. Список шаблонов содержит специальный встроенный шаблон для медленных каналов связи, на базе которого могут быть созданы дополнительные шаблоны с учетом специфических особенностей сети.



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]).

Настройка параметров осуществляется только при работе программы в режиме конфигурирования.

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. [102](#)).

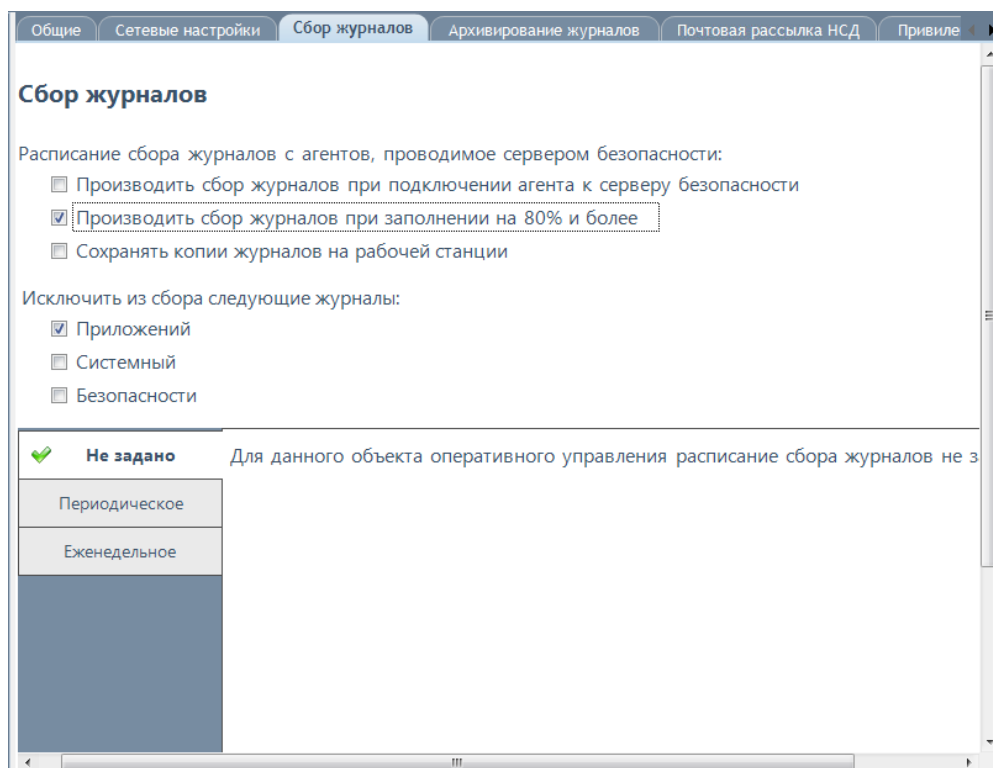
Примечание.

В табличном режиме представления можно указать шаблон в колонке "Сетевые настройки". Однако возможность редактирования параметров сетевого взаимодействия по отдельности предоставляется только при работе во вкладке.

2. Сохраните изменения (см. стр. [22](#)).

Параметры передачи локальных журналов

Для просмотра и изменения параметров передачи локальных журналов предназначена вкладка "Сбор журналов". Вкладка присутствует при выборе сервера безопасности или агента. Пример содержимого вкладки представлен на следующем рисунке.



Параметры сбора локальных журналов, заданные для сервера безопасности, относятся ко всем агентам, которые подчинены данному серверу. При этом на отдельных агентах 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 локальных журналов защищаемых компьютеров. 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 переполнения журналов на защищаемых компьютерах (так как при переполнении локального журнала доступ пользователя к компьютеру может быть ограничен).

Настройка параметров осуществляется только при работе программы в режиме конфигурирования.

Для настройки параметров передачи журналов:

1. Настройте базовые параметры сбора журналов:

- если запуск процесса сбора журналов должен выполняться при каждом подключении агентов к серверу безопасности, установите отметку в поле "Производить сбор журналов при подключении агента к серверу безопасности";
- если на сервер безопасности необходимо передавать журналы, близкие к переполнению, установите отметку в поле "Производить сбор журналов при заполнении 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 агентом подтверждения о готовности сервера безопасности. Во время пиковой загруженности сервера прием переполненного журнала откладывается.

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

Пояснение.

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

2. При необходимости отключите централизованный сбор журналов определенных типов. Для этого отметьте нужные типы журналов в группе полей "Исключить из сбора следующие журналы". Централизованный сбор можно отключить только для штатных журналов ОС Windows.
3. Если запуск процесса передачи локальных журналов подключенных агентов должен выполняться в определенные моменты времени, настройте расписание сбора журналов.

Для выбора типа расписания нажмите одну из следующих кнопок:

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, разделенной на две части. В столбцах таблицы перечислены дни недели, а в строках — часы и минуты с шагом в 30 минут. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы. Действие расписания повторяется еженедельно

Чтобы отключить режим передачи журналов по расписанию, нажмите кнопку "Не задано".

Примечание.

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

4. Сохраните изменения (см. стр. 22).

Примечание.

В табличном режиме представления в колонке "Сбор журналов" отображается только тип заданного расписания. Возможность изменения параметров передачи журналов в ячейке таблицы не предоставляется.

Параметры архивирования централизованных журналов

Для просмотра и изменения параметров архивирования централизованных журналов предназначена вкладка "Архивирование журналов". Вкладка присутствует при выборе сервера безопасности. Пример содержимого вкладки представлен на следующем рисунке.

Общие Сетевые настройки Сбор журналов **Архивирование журналов** Почтовая рассылка НСД Привилегии

Архивирование журналов

Расписание архивирования журналов с агентов, проводимое сервером безопасности:

Не задано	Время	Пн	Вт	Ср	Чт	Пт	Сб	Вс	Время	Пн	Вт	Ср	Чт	Пт	Сб	Вс
Периодическое	12:00								00:00							
	12:30								00:30							
	13:00								01:00							
Еженедельное	13:30								01:30							
	14:00								02:00							
	14:30								02:30							
	15:00								03:00							
	15:30								03:30							
	16:00								04:00							
	16:30								04:30							
	17:00								05:00							
	17:30								05:30							
	18:00								06:00							
	18:30								06:30							
	19:00								07:00							
	19:30								07:30							
	20:00								08:00							
20:30								08:30								
21:00							✓	09:00								
21:30								09:30								

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. Например, в некоторых версиях СУБД Oracle 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 оперативного управления можно загрузить файлы архивных копий.

Архивирование может выполняться по заданному расписанию для сервера безопасности или по специальной команде, доступной в программе оперативного управления в режиме мониторинга и централизованного аудита.

Настройка параметров осуществляется только при работе программы в режиме конфигурирования.

Для настройки параметров архивирования:

1. Нажмите одну из следующих кнопок:

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, разделенной на две части. В столбцах таблицы перечислены дни недели, а в строках — часы и минуты с шагом в 30 минут. Выбор времени запуска процесса осуществляется посредством установки отметки в соответствующей ячейке таблицы. Действие расписания повторяется еженедельно

Чтобы отключить режим автоматического запуска процесса архивирования, нажмите кнопку "Не задано".

2. Сохраните изменения (см. стр.22).

Примечание.

В табличном режиме представления в колонке "Архивирование" отображается только тип заданного расписания. Возможность изменения параметров архивирования в ячейке таблицы не предоставляется.

Параметры рассылки уведомлений о событиях НСД

Для просмотра и изменения параметров рассылки уведомлений о событиях НСД предназначена вкладка "Почтовая рассылка НСД". Вкладка присутствует при выборе сервера безопасности. Пример содержимого вкладки представлен на следующем рисунке.

Почтовая рассылка НСД

Почтовые настройки для сервера безопасности:

Почтовый сервер: Порт:

От кого:

☐ Аутентификация:

Имя пользователя:

Пароль:

Правила рассылки уведомлений об НСД:

Название правила	Адресаты	Тема
<input checked="" type="checkbox"/> НСД полномочного управ...	ivanov@domainname.ru; petrov@domai...	Уведомление о НСД полномочного уп...
<input checked="" type="checkbox"/> НСД при входе в систему	securityadmin1@domainname.ru; securit...	Уведомление о НСД при входе в систе...

Добавить Редактировать Удалить

При регистрации событий НСД на защищаемых компьютерах, подчиненных серверу безопасности или его подчиненным серверам, система Secret Net 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 событий. При этом система защиты может отслеживать события определенных категорий (только при регистрации событий на защищаемых компьютерах, подчиненных данному серверу безопасности).

Например, можно настроить рассылку уведомлений следующим образом:

- при возникновении событий НСД категории "Вход/выход" на защищаемых компьютерах, подчиненных данному серверу безопасности, уведомления направляются системному администратору;

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

Настройка параметров рассылки уведомлений осуществляется только при работе программы в режиме конфигурирования.

Для настройки параметров почтовой рассылки:

1. Сформируйте список правил рассылки уведомлений. Управление списком осуществляется с помощью кнопок, расположенных в нижней части вкладки.

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

2. Укажите действующие правила (т. е. правила, по которым будет выполняться рассылка уведомлений), установив отметки слева от их названий. Для отключения действия удалите отметку.
3. 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.
4. 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.

5. При необходимости укажите учетные данные для доступа к почтовому серверу. Для этого установите отметку в поле "Аутентификация" и введите имя и пароль пользователя.
6. Сохраните изменения (см. стр. [22](#)).

Примечание.

В табличном режиме представления в колонке "Уведомления об НСД" отображается только количество правил рассылки. Возможность изменения параметров в ячейке таблицы не предоставляется.

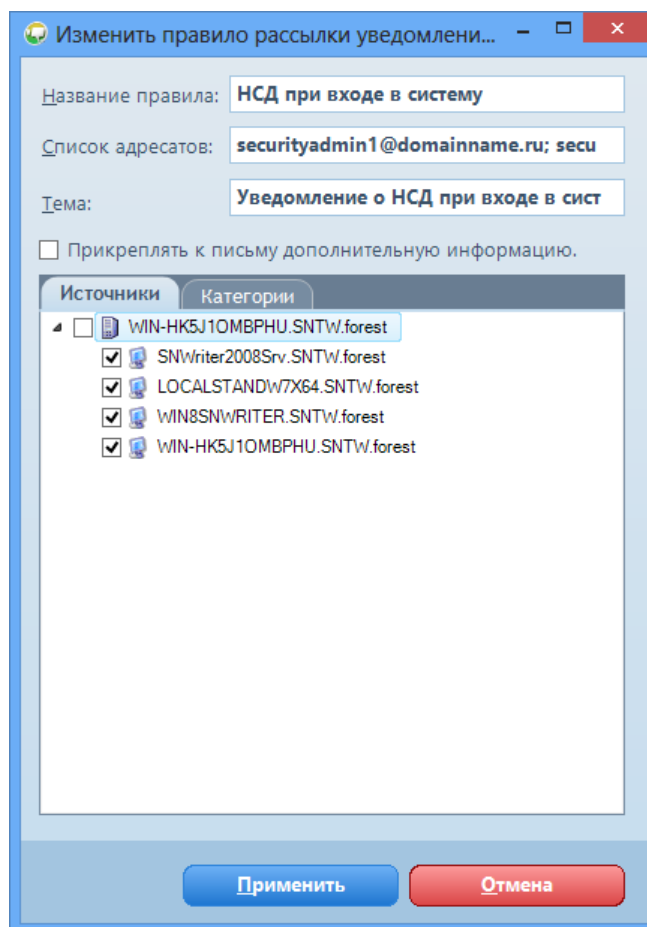
Настройка параметров правила рассылки

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

Для настройки параметров правила рассылки:

1. Вызовите диалоговое окно настройки параметров правила (см. выше).

Пример диалогового окна представлен на следующем рисунке.



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

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

3. На вкладке "Источники" отметьте объекты для контроля событий НСД. Если отмечен сервер безопасности, это означает, что контроль событий НСД должен осуществляться для всех защищаемых компьютеров, относящихся к серверу. Если в списке не отмечен ни один объект, это равносильно установке отметок для всех элементов списка.

Внимание!

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

4. Перейдите на вкладку "Категории".

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

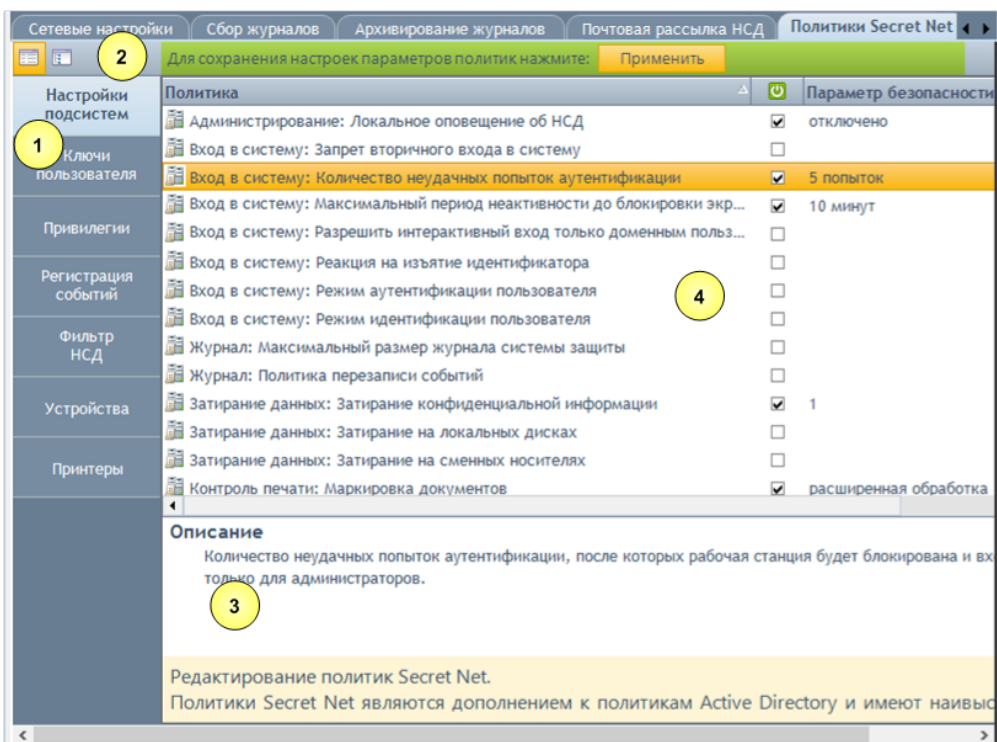
- "События Secret Net" — в группу входят категории событий, регистрируемых в журнале Secret Net;
- "События Windows" — в группу входят категории событий, регистрируемых в штатном журнале безопасности ОС Windows.

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

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

6. Нажмите кнопку "Применить".**Параметры Secret Net для групповых политик**

Для просмотра и изменения параметров Secret Net, применяемых на компьютерах средствами групповых политик, предназначены вкладки "Локальные политики" (если выбран агент) и "Политики Secret Net" (если выбран любой другой объект). Пример содержимого вкладки, когда выбран сервер безопасности, представлен на следующем рисунке.

**Пояснение.**

На рисунке выносками обозначены элементы: 1 — панель выбора групп параметров; 2 — панель управления и выбора режимов; 3 — область описания параметров; 4 — область списка параметров.

Вкладка содержит списки параметров, соответствующих содержимому раздела "Параметры Secret Net" в стандартных оснастках управления групповыми политиками. На вкладке "Локальные политики" представлены параметры локальной политики безопасности выбранного агента. Вкладка "Политики Secret Net" содержит списки параметров, которые могут применяться на компьютерах, относящихся к домену, к организационному подразделению или к серверу безопасности — в зависимости от того, какой объект выбран в иерархии управления.

Аналогично стандартным оснасткам управления групповыми политиками режим группировки параметров может быть установлен по умолчанию или в соответствии с принадлежностью защитным механизмам (подсистемам). Переключение режима группировки выполняется с помощью кнопок, расположенных в левой части панели управления и выбора режимов.



Примечание.

Списки групп параметров формируются так же, как и в стандартных оснастках управления групповыми политиками. Исключение составляет группа "Фильтр НСД", которая в стандартных оснастках отсутствует. Настройка параметров этой группы осуществляется только в программе оперативного управления.

Область описания параметров содержит дополнительные сведения о выбранном параметре. При необходимости можно отключить ее отображение на вкладке. Включение и отключение области описания параметров осуществляется с помощью кнопки "Описание", расположенной в правой части панели управления и выбора режимов.

Управление параметрами Secret Net для групповых политик осуществляется только при работе программы в режиме мониторинга и централизованного аудита. Правами для изменения параметров обладают пользователи, которым предоставлена привилегия "Управлять настройками Secret Net" (см. стр. 46). При этом изменять параметры групповых политик доменов и организационных подразделений разрешено только пользователям, входящим в группу администраторов домена безопасности.

Общие сведения о применении групповых политик

Заданные параметры групповых политик применяются на компьютерах в следующей последовательности:

1. Параметры локальной политики безопасности.
2. Параметры политик, заданные в стандартных оснастках управления — в соответствии с действием механизма групповых политик Windows, сначала применяются параметры доменных политик и затем параметры политик для организационных подразделений.
3. Параметры политик, заданные в программе оперативного управления для доменов и организационных подразделений — аналогично механизму групповых политик Windows сначала применяются параметры доменных политик и затем параметры политик для организационных подразделений.
4. Параметры политик, заданные в программе оперативного управления 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.

Значения параметров локальной политики, измененные в программе оперативного управления, отправляются агенту и сохраняются в локальной политике безопасности. Возможности изменения этих параметров доступны как в программе оперативного управления (только для включенных компьютеров), так и локально на защищаемом компьютере.

Значения параметров политик, заданные в программе оперативного управления для других объектов (доменов, организационных подразделений и серверов безопасности), недоступны в стандартных оснастках управления. Изменение этих параметров осуществляется только в программе оперативного управления.

При использовании нескольких серверов безопасности, установленных с размещением хранилища объектов централизованного управления вне Active Directory, 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 групповых политик, заданных в программе оперативного управления:

- параметры политик доменов и организационных подразделений, заданные при подключении программы к серверу в родительском домене безопасности, не применяются на агентах, которые подчинены серверу другого домена безопасности во вложенном контейнере Active Directory. Для этих агентов 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 групповой политики

Для настройки параметров групповой политики:

1. В панели выбора групп параметров выберите группу, к которой относятся нужные параметры.
2. Задайте значения в области списка параметров. Принципы изменения значений аналогичны методам работы в стандартных оснастках управления групповыми политиками (описания процедур при работе в стандартных оснастках см. в документе [3]). Особенности редактирования параметров различных групп описаны ниже.
3. Для сохранения изменений нажмите кнопку "Применить" в панели управления и выбора режимов (кнопка появляется при наличии изменений, требующих сохранения).

Настройка параметров, входящих в группы "Настройки подсистем", "Ключи пользователя", "Привилегии" и "Регистрация событий"

Значения параметров, входящих в группы "Настройки подсистем", "Ключи пользователя", "Привилегии" и "Регистрация событий", редактируются в колонке "Параметр безопасности". Чтобы указать значение параметра в политиках домена, организационного подразделения или сервера безопасности, этот параметр предварительно необходимо задать. Для этого выберите параметр и установите отметку в колонке включения (по умолчанию справа от названия параметра).

Для изменения значения выберите параметр и нажмите клавишу <Enter> (или установите курсор на ячейку колонки "Параметр безопасности" и нажмите левую кнопку мыши). Ячейка со значением параметра перейдет в состояние редактирования. В зависимости от предусмотренного метода изменения параметра новое значение можно указать путем установки или удаления отметки, вводом или перебором значений из диапазона, а также с использованием

диалоговых панелей, вызываемых с помощью кнопки раскрытия в правой части ячейки.



Примечание.

Параметры представлены в группах "Настройки подсистем", "Ключи пользователя", "Привилегии" и "Регистрация событий", если включена группировка по умолчанию. При включенной группировке по принадлежности защитным механизмам эти параметры распределяются по другим группам, однако методы изменения параметров не изменяются.

Настройка параметров, входящих в группу "Фильтр НСД"

В группе "Фильтр НСД" осуществляется управление фильтрацией событий НСД для ограничения поступающих уведомлений от агентов на сервер безопасности. Параметры данной группы применяются на агентах средствами групповых политик. Для сервера безопасности отдельно можно задать аналогичные параметры фильтрации, ограничивающие поступление уведомлений от агентов тех серверов, которые непосредственно подчинены выбранному серверу безопасности (см. стр. 52).



Внимание!

Функция фильтрации событий НСД не поддерживается на компьютерах с установленным клиентским ПО Secret Net версии 7.0 и ниже.

Чтобы централизованно управлять фильтрацией событий НСД в политиках домена, организационного подразделения или сервера безопасности, необходимо задать политику фильтра. Для этого выберите ссылку "Задать политику фильтр НСД" (если отображается предупреждение о том, что политика не определена).

Фильтрация выполняется по списку правил. В правилах указываются условия для содержимого полей в записях журналов. Фильтр не пропускает уведомления о событиях НСД, которые удовлетворяют условиям в правилах фильтрации. Также предусмотрен режим инверсии правил, при котором фильтр пропускает уведомления только о событиях НСД, соответствующих правилам из списка.

Список правил можно формировать при работе в группе "Фильтр НСД", с помощью средств панели событий системы (см. стр. 63) или при работе с журналом НСД в панели "НСД" (см. стр. 94).

Для формирования списка правил в группе "Фильтр НСД" используйте команды контекстного меню "Добавить правило" и "Удалить". Редактирование правил осуществляется по отдельности в соответствующих колонках таблицы. Для правила можно задать следующие условия, которым должны удовлетворять записи журналов:

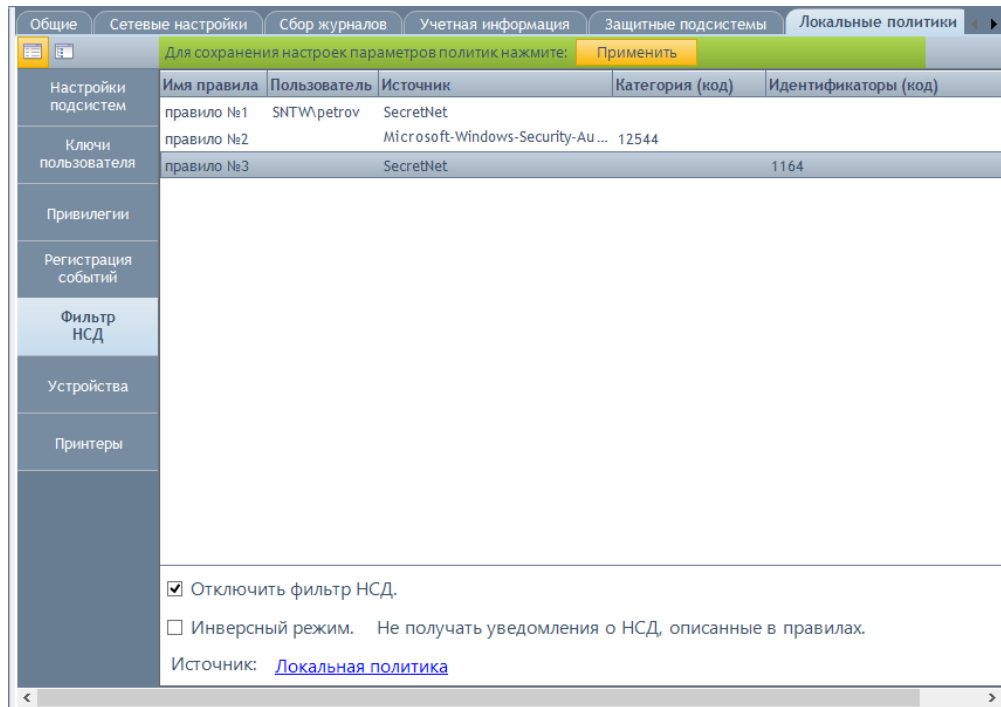
- имя пользователя;
- название источника;
- числовой код категории события;
- числовой идентификатор события.



Примечание.

Данные для формирования условий можно получить в области описания событий при просмотре записей журнала НСД. Необходимые сведения представлены в панели журнала НСД на вкладке "Общее" (см. стр. 76). Колонкам списка правил фильтрации соответствуют следующие поля вкладки: колонке "Пользователь" — поле "Пользователь", колонке "Источник" — поле "Источник", колонке "Категория (код)" — поле "Код категории" и колонке "Идентификаторы (код)" — поле "Событие".

Пример списка правил фильтрации представлен на следующем рисунке.



При необходимости включите режим инверсии правил. Для этого установите отметку в поле "Инверсный режим".



Внимание!

Не включайте режим инверсии при пустом списке правил. Иначе после включения фильтр не будет пропускать все события НСД. Режим целесообразно использовать, если требуется пропускать поступающие уведомления об определенных событиях, а остальные — блокировать. Для этого создайте правила, описывающие такие события, и включите режим инверсии.

После настройки правил включите действие фильтра. Для этого удалите отметку из поля "Отключить фильтр НСД".

Отменить фильтрацию можно следующими способами:

- отключить действие фильтра — для этого установите отметку в поле "Отключить фильтр НСД";
- вернуть политику фильтра в состояние "не задана" — для этого вызовите контекстное меню в любом месте списка правил и выберите команду "Выключить политику фильтр НСД" (не применяется в локальной политике).

Настройка параметров, входящих в группу "Устройства"

В группе "Устройства" осуществляется управление списком устройств и параметрами контроля и доступа к устройствам.

Чтобы централизованно управлять устройствами в политиках домена, организационного подразделения или сервера безопасности, необходимо задать политику контроля устройств. Для этого выберите ссылку "Задать политику устройств" (если отображается предупреждение о том, что политика не определена). Если требуется вернуть политику контроля устройств в состояние "не задана", вызовите контекстное меню в любом месте списка устройств и выберите команду "Выключить политику устройств" (не применяется в локальной политике).

Для удобной работы с параметрами список устройств представлен в табличном виде. Колонка "Устройства" всегда отображается в левой позиции и содержит иерархический список групп, классов, моделей и устройств. Список оформлен так же, как в оснастке управления групповой политикой. Остальные колонки таблицы отображают заданные параметры для элементов списка.

Настройку параметров можно выполнять в диалоговых панелях, вызов которых осуществляется при нажатии кнопки справа от названия элемента списка или по

команде контекстного меню "Свойства". Диалоговые панели представляют собой аналоги диалогов настройки в оснастках управления групповыми политиками, но отличаются тем, что не блокируют возможность выполнения других действий в программе до закрытия панели. Кроме того, изменять значения параметров можно непосредственно в ячейках таблицы. Для этого необходимо установить курсор на нужную ячейку и нажать левую кнопку мыши. Если изменение параметра разрешено, ячейка перейдет в состояние редактирования. В зависимости от предусмотренного метода изменения параметра новое значение можно указать путем установки или удаления отметки, вводом или выбором значения. При выборе ячейки с пиктограммой в колонке "Разрешения" на экране появляется диалог ОС Windows для настройки прав доступа учетных записей.

Для редактирования списка устройств используются команды контекстного меню. Сведения о предусмотренных возможностях приведены в Приложении на стр. **103**. Описание общих принципов настройки использования устройств и принтеров см. в документе [3].

Устройства могут выделяться в списке следующим образом:

- до сохранения изменений в списке устройств добавленные элементы выделяются зеленым цветом, а удаленные — красным;
- в локальной политике — если устройство не подключено к компьютеру (физически отсутствует), его наименование зачеркнуто.

Настройка параметров, входящих в группу "Принтеры"

В группе "Принтеры" осуществляется управление параметрами контроля и доступа к принтерам и формирование списка принтеров с особыми условиями использования.

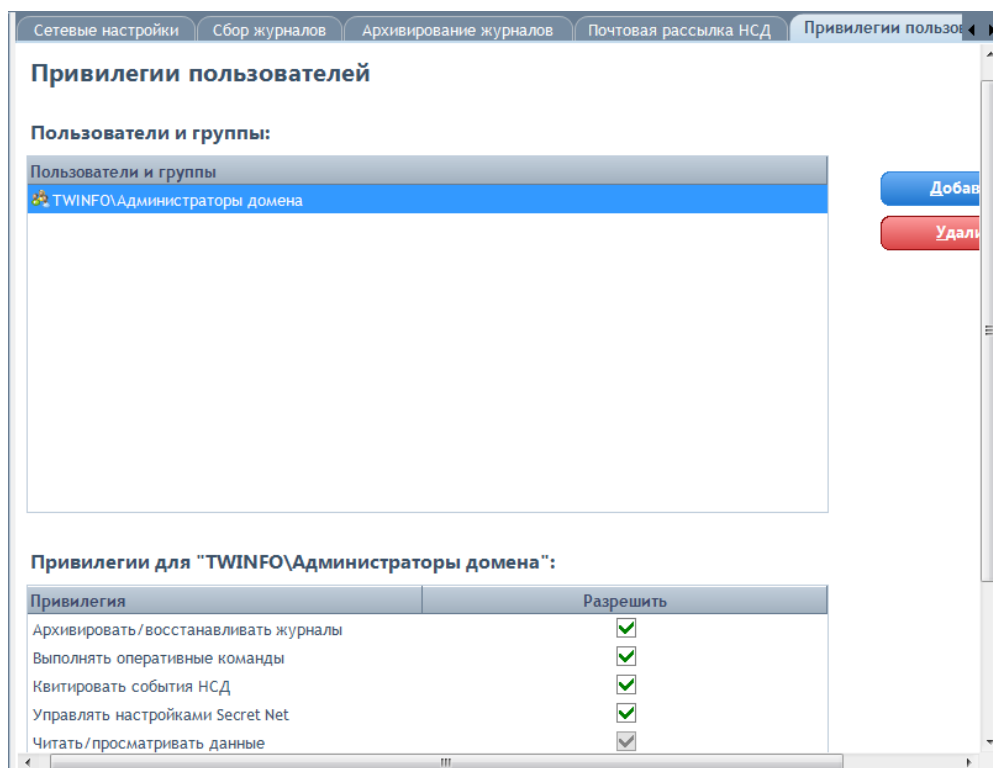
Чтобы централизованно управлять параметрами принтеров в политиках домена, организационного подразделения или сервера безопасности, необходимо задать политику контроля принтеров. Для этого выберите ссылку "Задать политику принтеров" (если отображается предупреждение о том, что политика не определена). Если требуется вернуть политику контроля принтеров в состояние "не задана", вызовите контекстное меню в любом месте списка принтеров и выберите команду "Выключить политику принтеров" (не применяется в локальной политике).

Список принтеров представлен в табличном виде. В группе "Принтеры" используются такие же методы настройки параметров, как и в группе "Устройства" (см. выше).

Для редактирования списка принтеров используются команды контекстного меню. Сведения о предусмотренных возможностях приведены в Приложении на стр. **104**. Описание общих принципов настройки использования устройств и принтеров см. в документе [3].

Привилегии для работы с программой оперативного управления

Для просмотра и предоставления привилегий пользователям программы оперативного управления предназначена вкладка "Привилегии пользователей". Вкладка присутствует при выборе сервера безопасности. Пример содержимого вкладки представлен на следующем рисунке.



Пользователям и группам пользователей могут быть назначены следующие привилегии:

- "Архивировать/восстанавливать журналы" — привилегия на архивирование и восстановление централизованных журналов;
- "Выполнять оперативные команды" — привилегия на выполнение команд оперативного управления;
- "Квитуировать события НСД" — привилегия на выполнение команд квитирования событий НСД;
- "Управлять настройками Secret Net" — привилегия для удаленной настройки параметров Secret Net на рабочих станциях и серверах;
- "Читать/просматривать данные" — привилегия для подключения к серверу безопасности и просмотра информации;
- "Редактировать конфигурацию и свойства объектов" — привилегия для внесения изменений при работе с программой в режиме конфигурирования.

По умолчанию все перечисленные привилегии предоставлены пользователям, входящим в группу администраторов домена безопасности, а также для пользователей группы администраторов Secret Net (SecretNetAdmins), если сервер безопасности установлен в варианте размещения хранилища объектов централизованного управления в Active Directory. При необходимости привилегии можно назначить и другим учетным записям, исключая привилегию "Редактировать конфигурацию и свойства объектов" — данная привилегия в обязательном порядке предоставляется только для указанных групп пользователей.

Назначение привилегий осуществляется только при работе программы в режиме конфигурирования.

Для предоставления привилегий:

1. Сформируйте список пользователей и групп, которым необходимо предоставить привилегии. Для добавления и удаления учетных записей используйте кнопки, расположенные справа от списка.
2. Предоставьте необходимые привилегии учетным записям. Для предоставления привилегии выберите учетную запись и установите отметку

в колонке "Разрешить". Удаление отметки отменяет предоставление привилегии.

Примечание.

Привилегия "Читать/просматривать данные" назначается автоматически для всех учетных записей, представленных в списке "Пользователи и группы".

Привилегия "Редактировать конфигурацию и свойства объектов" не может быть предоставлена другим учетным записям кроме группы (групп) пользователей по умолчанию.

3. Сохраните изменения (см. стр. 22).

Параметры лицензий на использование компонентов

Для просмотра и изменения параметров лицензий на использование компонентов системы Secret Net предназначена вкладка "Лицензии". Вкладка присутствует при выборе сервера безопасности или агента. Пример содержимого вкладки, когда выбран сервер безопасности, представлен на следующем рисунке.

Лицензии

Серийный номер сервера:

Номер: 0000-0000-0000-0000-0000-0000-0000
 Допустимое количество подключений: 18
 Число подключенных клиентов: 8
 Версия продукта: 7.3.545.x

Серийные номера сервера безопасности:

Серийные номера клиентов	Количество лицензий	Продукт	Версия
0000-0000-0000-0000-0000-0000-0000	18	Secret Net 7	
0000-0000-0000-0000-0000-0000-0000	8	Secret Net 7	
0000-0000-0000-0000-0000-0000-0000	18	Secret Net 7	

☐ Показать серийные номера ранних версий

Информация для серийного номера 0000-0000-0000-0000-0000-0000-0000:

Серийный номер предоставляет право подключить к серверу безопасности заданное

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

Для сервера безопасности можно указать следующие типы серийных номеров:

- **Серийный номер сервера безопасности (CHC6)** — содержит лицензию на использование компонента "Secret Net 7 — Сервер безопасности" определенной версии (версий). В CHC6 задано ограничение на максимальное количество клиентов, разрешенных для подчинения серверу безопасности.
- **Серийный номер клиента (CHK)** — содержит лицензию на использование одного или нескольких компонентов "Secret Net 7" определенной версии (версий). CHK определяет разрешенный режим функционирования компонента — сетевой или автономный. Возможности централизованной настройки и оперативного управления доступны на тех компьютерах, на которых зарегистрированы CHK с лицензиями для сетевого режима функционирования. Такие CHK дополнительно задают ограничения на количество

клиентов, для которых можно использовать данный серийный номер. Ограничение действует в рамках глобального каталога, где зарегистрирован СНК. В программе оперативного управления выполняются действия только с СНК с лицензиями для сетевого режима функционирования.

Примечание.

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

- **Серийный номер подсистемы защиты дисков (СНД)** — содержит лицензию на использование механизма защиты дисков на компьютерах с установленным компонентом "Secret Net 7" определенной версии (версий).
- **Серийный номер средств управления (СНУ)** — содержит лицензию на использование одновременно двух или более компонентов "Secret Net 7 — Программа управления" определенной версии (версий). В лицензии заданы ограничения на количество дополнительных компьютеров, с которых возможно одновременное подключение программ оперативного управления к СБ.

В дополнение к серийным номерам СНК и СНД, которые могут регистрироваться на сервере безопасности, для агента отдельно можно зарегистрировать серийный номер следующего типа:

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

Ввод необходимых серийных номеров выполняется при установке компонентов (см. документ [2]). В процессе эксплуатации системы при необходимости можно зарегистрировать новые лицензии, а также заменить или удалить серийные номера лицензий.

Редактирование списка серийных номеров лицензий осуществляется только при работе программы в режиме конфигурирования.

Для редактирования списка серийных номеров лицензий:

- Используйте соответствующие кнопки справа от списка лицензий.

Кнопка	Описание
Добавить	Добавляет новый серийный номер в список
Заменить	Запускает процедуру смены выбранного серийного номера
Удалить	Удаляет выбранный серийный номер из списка

Примечание.

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

Если выбран агент, возможности управления доступны в полном объеме для компьютеров с установленным клиентским ПО Secret Net текущей версии. Для клиентов предыдущих версий управление серийными номерами поддерживается только с версии 6.5 (СНК для версии 6.5).

Учетная информация компьютера

Для просмотра и редактирования учетной информации компьютеров предназначена вкладка "Учетная информация". Вкладка присутствует при выборе агента. Пример содержимого вкладки представлен на следующем рисунке.

Общие	Сетевые настройки	Сбор журналов	Учетная информация	Лицензии	Управление трассировкой
Учетная информация					
Название подразделения:		ОРИТ Secret Net			
Название автоматизированной системы:		SecurityCode			
Рабочее место:		помещение 24			
Номер системного блока:		402480			

Учетная информация используется при построении отчетов со сведениями о компьютере.

Редактирование учетной информации осуществляется только при работе программы в режиме конфигурирования. Также эти сведения можно изменять локально на защищаемом компьютере. Описание процедуры локального редактирования см. в документе [3].

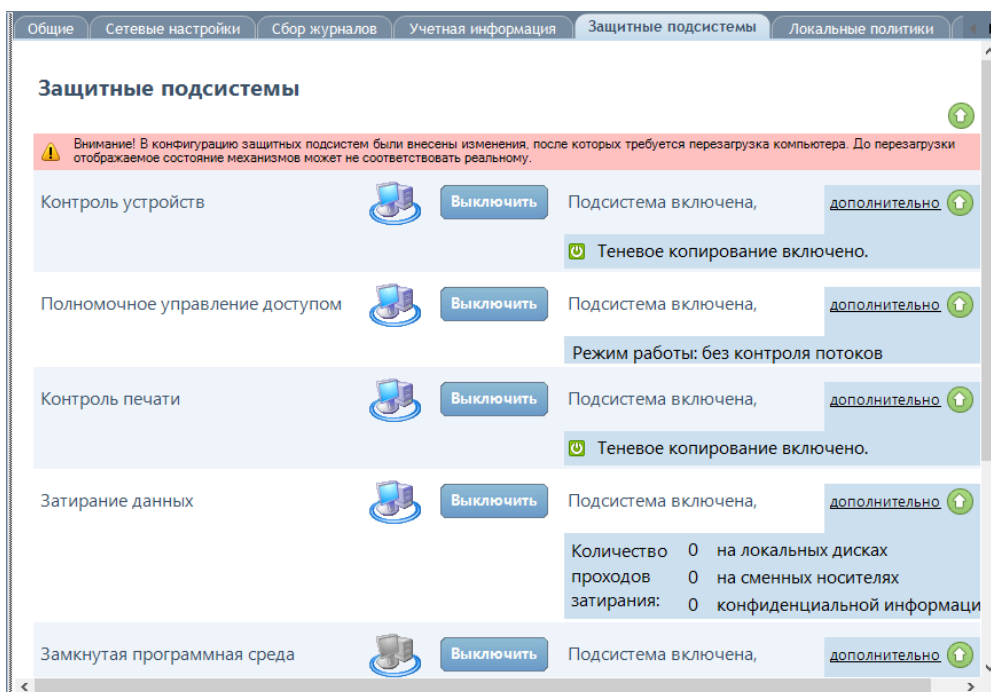
После редактирования сведений в программе сохраните изменения (см. стр. 22).

Примечание.

Редактировать сведения можно как на вкладке "Учетная информация", так и в табличном режиме представления. Учетная информация представлена в следующих колонках (в соответствии с порядком перечисления на вкладке): "Департамент", "Автоматизированная система", "Рабочее место" и "Номер системного блока".

Параметры функционирования механизмов защиты

Для просмотра и настройки параметров функционирования механизмов защиты предназначена вкладка "Защитные подсистемы". Вкладка присутствует при выборе агента. Пример содержимого вкладки представлен на следующем рисунке.



Вкладка содержит сведения о режимах работы механизмов защиты на компьютере. Описание механизмов защиты и предусмотренные для них режимы работы см. в документе [1].

Для отображения состояния функционирования механизмов используются пиктограммы (см. стр. 101). Чтобы скрыть или показать дополнительные сведения о механизмах, используйте соответствующие ссылки "дополнительно" или кнопки справа.

Управление функционированием механизмов защиты осуществляется только для включенных компьютеров при работе программы в режиме мониторинга и централизованного аудита. Также управлять механизмами можно локально на защищаемом компьютере. Описание процедур локального включения, отключения механизмов и настройки параметров см. в документе [3].

Для настройки параметров функционирования механизмов защиты:

1. Чтобы отключить или включить функционирование механизма, нажмите кнопку, которая расположена рядом с его пиктограммой.

Примечание.

Также для включения и отключения функционирования механизмов защиты можно использовать команды оперативного управления в контекстном меню агентов (см. стр. 65).

2. Чтобы настроить дополнительные параметры механизма, используйте следующие предусмотренные возможности:
 - изменение параметра локальной политики безопасности, который определяет режим работы механизма (например, режим теневого копирования) — для этого наведите указатель на ссылку с информацией о режиме и нажмите левую кнопку мыши. Программа выполнит переход на вкладку "Локальные политики" и выделит параметр, который определяет действие режима. Отредактируйте параметр локальной политики и сохраните изменения (см. стр. 41);
 - включение и отключение защиты логических разделов механизмом защиты дисков — для этого отметьте нужные логические разделы в списке "Диски" группы "Защита диска" и нажмите кнопку "Применить".

Примечание.

Возможности управления доступны в полном объеме для компьютеров с установленным клиентским ПО Secret Net текущей версии. Для клиентов предыдущих версий управление работой механизмов защиты поддерживается только с версии 6.5.

В табличном режиме представления отображаются краткие сведения о режимах работы механизмов защиты. Сведения представлены в отдельных колонках для каждого механизма: "Дискреционное управление доступом", "Шифровать управляющий трафик", "Контроль устройств", "Полномочное управление доступом", "Контроль печати", "Затирание данных", "Замкнутая программная среда", "Защита диска". В ячейках таблицы отображаются признаки состояния механизмов. Чтобы получить более подробные сведения, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором. Возможность изменения параметров в ячейке таблицы не предоставляется.

Параметры трассировки ПО системы Secret Net

В программе оперативного управления реализована возможность централизованного включения и настройки параметров трассировки — сервисной функции для сбора информации о работе системы Secret Net. 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 на вкладке "Управление трассировкой". Вкладка присутствует при выборе сервера безопасности или агента. Настройка параметров осуществляется при работе программы в режиме мониторинга и централизованного аудита. 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 данная функция должна быть отключена, чтобы не создавать лишнюю нагрузку для компьютера.

Параметры фильтра уведомлений о НСД для сервера безопасности

Фильтр уведомлений о НСД, заданный для сервера безопасности, позволяет выборочно отслеживать регистрируемые события несанкционированного доступа на агентах подчиненных серверов безопасности. За счет использования фильтра можно сократить сетевой трафик и обеспечить поступление уведомлений только о важных для администратора событиях.

При регистрации удовлетворяющего фильтру события агент отправляет уведомление серверу безопасности. Полученное уведомление обрабатывается сервером и сохраняется в журнале НСД.

На вкладке "Фильтр уведомлений о НСД" осуществляется управление фильтрацией событий НСД для ограничения поступающих уведомлений от агентов тех серверов, которые непосредственно подчинены выбранному серверу безопасности. Аналогичным образом можно применить фильтрацию событий НСД при настройке параметров Secret Net для групповых политик (см. стр. 41).

Для настройки параметров фильтра уведомлений о НСД для серверов непосредственного подчинения:

1. Выберите сервер безопасности и в панели свойств объектов перейдите на вкладку "Фильтр уведомлений о НСД".

2. Сформируйте список правил фильтрации с условиями для содержимого полей в записях журналов. Для формирования списка используйте команды контекстного меню "Добавить правило" и "Удалить" или соответствующие кнопки справа. Для правила можно задать следующие условия, которым должны удовлетворять записи журналов:

- название источника;
- числовой код категории события;
- числовой идентификатор события.



Примечание.

Данные для формирования условий можно получить в области описания событий при просмотре записей журнала НСД. Необходимые сведения представлены в панели журнала НСД на вкладке "Общее" (см. стр. 76). Колонкам списка правил фильтрации соответствуют следующие поля вкладки: колонке "Источник" — поле "Источник", колонке "Категория (код)" — поле "Код категории" и колонке "Идентификаторы (код)" — поле "Событие".

Также правила можно добавлять в список с помощью средств панели событий системы (см. стр. 63) или при работе с журналом НСД в панели "НСД" (см. стр. 94)

3. При необходимости включите режим инверсии правил. В этом режиме фильтр пропускает уведомления только о событиях НСД, соответствующих правилам из списка. Для включения режима установите отметку в поле "Инверсный режим".



Внимание!

Не включайте режим инверсии при пустом списке правил. Иначе после включения фильтр не будет пропускать все события НСД. Режим целесообразно использовать, если требуется пропускать поступающие уведомления об определенных событиях, а остальные — блокировать. Для этого создайте правила, описывающие такие события, и включите режим инверсии.

4. После настройки правил включите действие фильтра. Для этого удалите отметку из поля "Отключить фильтр уведомлений о НСД".
5. Нажмите кнопку "Применить" справа от списка правил.

Возможности работы с параметрами нескольких объектов

В программе оперативного управления предусмотрены следующие возможности просмотра и изменения параметров нескольких объектов:

- сравнение значений параметров;
- одновременная настройка параметров для нескольких объектов;
- копирование значений параметров.

Сравнение параметров

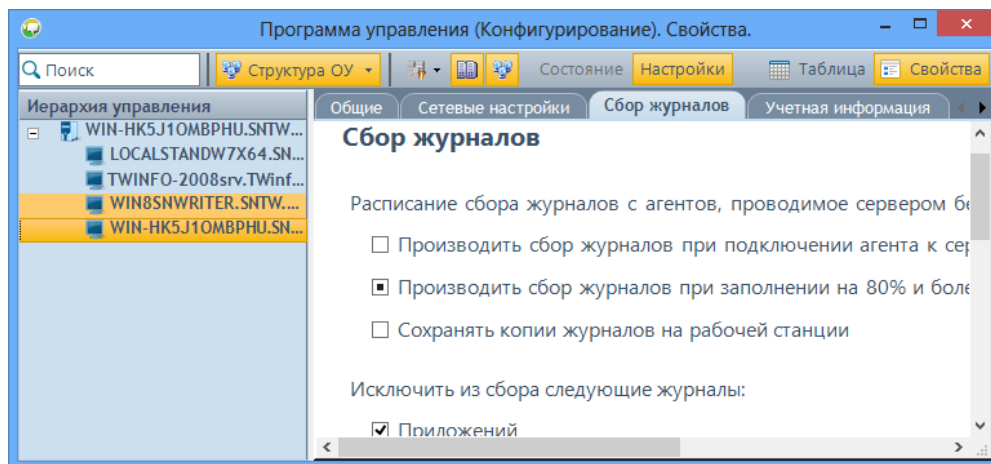
Сравнение параметров нескольких объектов выполняется с помощью вкладок.



Примечание.

Для вкладок "Защитные подсистемы", "Локальные политики" и "Политики Secret Net" сравнение параметров не предусмотрено.

Чтобы сравнить параметры, выберите объекты и в панели свойств перейдите на вкладку, которая содержит нужные параметры. На вкладке будут отображены совпадающие значения. Если значения одних и тех же параметров заданы по-разному, соответствующие поля отображаются пустыми или с признаком различного состояния (в зависимости от типа параметра). Пример отображения параметров нескольких объектов представлен на следующем рисунке.



Настройка параметров нескольких объектов

Возможность одновременной настройки параметров нескольких объектов доступна только при работе с программой в режиме конфигурирования. Настройка выполняется с помощью вкладок.

Для настройки параметров нескольких объектов:

1. Выберите объекты и в панели свойств объектов перейдите на вкладку, которая содержит нужные параметры.
2. Укажите значения параметров. Описания процедур настройки параметров см. выше в соответствующих разделах.
3. Сохраните изменения (см. стр. 22).

Копирование значений параметров

Заданные значения параметров объекта, представленные в табличном режиме, можно копировать (тиражировать) через буфер обмена в параметры других объектов. Возможность копирования значений в табличном режиме доступна только при работе с программой в режиме конфигурирования.

Для копирования значений параметров:

1. В панели свойств объектов включите табличное представление с помощью кнопки "Таблица" на панели выбора режимов отображения.
2. Скопируйте в буфер обмена значения параметров эталонного объекта:
 - чтобы скопировать все значения, — вызовите контекстное меню объекта или любой ячейки в строке с именем объекта и выберите команду "Копировать";

- чтобы скопировать конфигурацию значений, относящихся к определенной колонке, — вызовите контекстное меню ячейки из этой колонки в строке с именем объекта и выберите команду "Копировать свойство".
3. Выберите объекты, в параметры которых требуется скопировать значения параметров эталонного объекта.
 4. Вызовите контекстное меню последнего из выбранных объектов и выберите команду "Вставить".
Значения из буфера обмена будут присвоены параметрам объектов, и после этого обновится информация в ячейках соответствующих колонок.
 5. Сохраните изменения (см. стр. [22](#)).

Глава 4

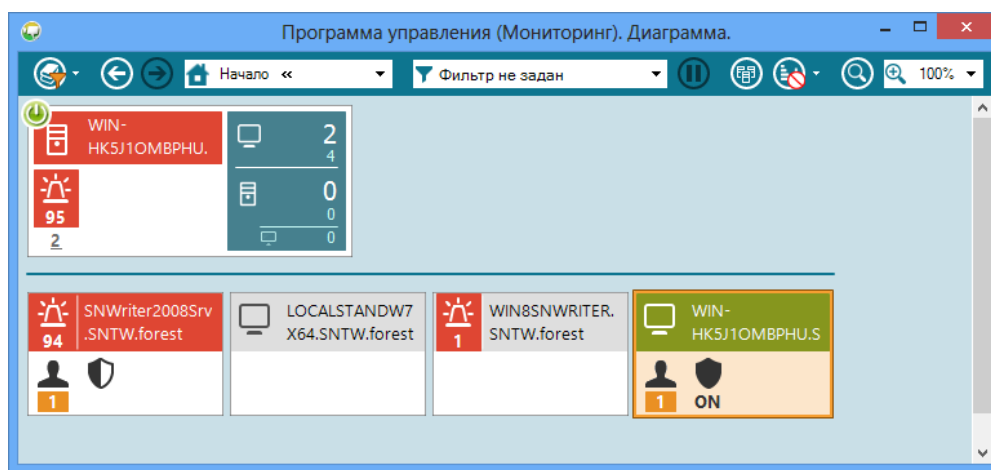
Мониторинг и оперативное управление

Возможности мониторинга и оперативного управления доступны при работе программы в режиме мониторинга и централизованного аудита. Описание процедуры запуска программы в этом режиме см. на стр. 9.

Просмотр сведений

Обозначения объектов на диаграмме управления

При работе с программой в режиме мониторинга и централизованного аудита диаграмма управления имеет вид, подобный представленному на рисунке.



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

Элементы диаграммы управления отображают основные сведения о состоянии объектов. Сведения представлены в виде пиктограмм и расположенных рядом числовых данных (например, количество событий НСД на агенте или количество открытых сессий пользователей). Для серверов безопасности и групп агентов числовые данные приводятся в двух или более строках: верхняя строка содержит общее количество событий/признаков на всех подчиненных агентах (например, сводное количество событий НСД или количество включенных компьютеров), а нижние строки отображают количество агентов или подчиненных серверов безопасности с агентами. Некоторые числовые данные являются ссылками, которые можно использовать для фильтрации списков агентов. Например, чтобы отобразить в диаграмме только агенты с признаками НСД.

Заголовки элементов диаграммы могут выделяться следующими цветами:

- зеленый цвет — компьютер включен;
- красный цвет — компьютер включен, на агенте (агентах) включена блокировка или зафиксированы события НСД;
- голубой цвет — компьютер включен, на агенте (агентах) зафиксировано изменение аппаратной конфигурации;
- оранжевый цвет — зафиксирована ошибка при проверке лицензий на использование компонентов системы Secret Net;
- серый цвет — компьютер отключен.

Кроме того, дополнительные сведения о компьютерах отображаются во всплывающих окнах, которые появляются при наведении указателя мыши на объекты.

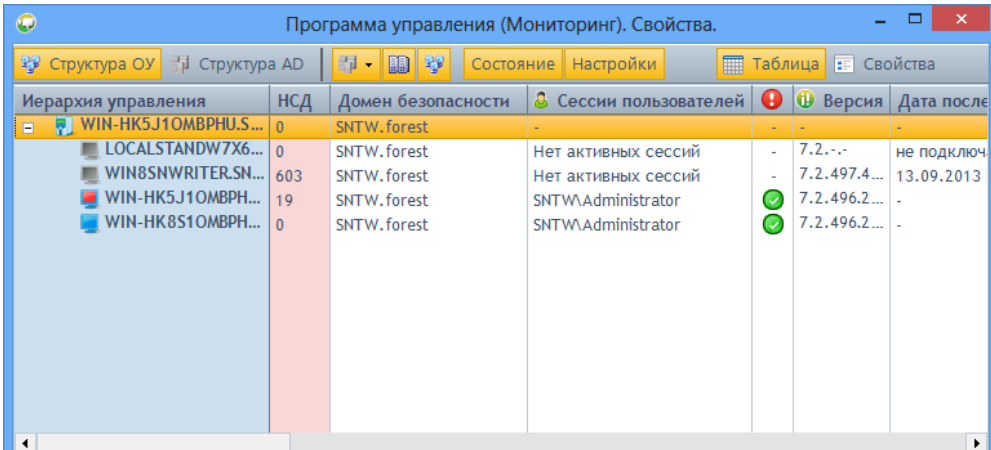
Перечень предусмотренных пиктограмм представлен в следующей таблице:

Пиктограмма	Описание
	На сервере безопасности зафиксирована ошибка при проверке лицензии
	База данных сервера безопасности переполнена
	Включена блокировка агента (агентов). Число соответствует количеству причин блокировки. В приведенном примере — одна причина
	На агенте (агентах) зафиксированы события НСД. Число является счетчиком зарегистрированных событий, ожидающих квитирования (подтверждение приема) администратором безопасности. Максимальное числовое значение счетчика — 999 событий. В случае превышения ограничения, счетчик отображает значение "99+"
	На агенте (агентах) зафиксирована ошибка при проверке лицензий на использование компонентов системы Secret Net
	На агенте (агентах) зафиксировано изменение аппаратной конфигурации
	На агенте (агентах) открыты сессии работы пользователей. Число соответствует количеству открытых сессий. Цветной фон обозначает сессию локального администратора
	На агенте (агентах) действует фильтр событий НСД
	Признак состояния механизмов защиты на агенте: если пиктограмма закрашена целиком — драйверы всех механизмов включены; если заливка отсутствует частично или полностью — отключены соответственно некоторые или все драйверы. В приведенном примере отключены драйверы некоторых механизмов
	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 панели свойств объектов

При работе с программой в режиме мониторинга и централизованного аудита панель свойств объектов имеет вид, подобный представленному на рисунке.



Программа управления (Мониторинг). Свойства.						
Структура ОУ		Структура АД		Состояние		
Иерархия управления		НСД	Домен безопасности	Сессии пользователей	Версия	Дата после
WIN-HK5J1OMBPHU.S...		0	SNTW.forest	-	-	-
LOCALSTANDW7X6...		0	SNTW.forest	Нет активных сессий	7.2.-.-	не подключ
WIN8SNWRITER.SN...		603	SNTW.forest	Нет активных сессий	7.2.497.4...	13.09.2013
WIN-HK5J1OMBPH...		19	SNTW.forest	SNTW\Administrator	7.2.496.2...	-
WIN-HK8S1OMBPH...		0	SNTW.forest	SNTW\Administrator	7.2.496.2...	-

В панели свойств сведения о состоянии объектов представлены в иерархическом списке структуры объектов и в области отображения параметров. В иерархическом списке для отображения состояния объектов используются пиктограммы. Развернутые сведения о состоянии объектов выводятся в таблице области отображения параметров, если включен режим вывода динамически изменяющихся параметров (кнопка "Состояние" в панели выбора режимов отображения).

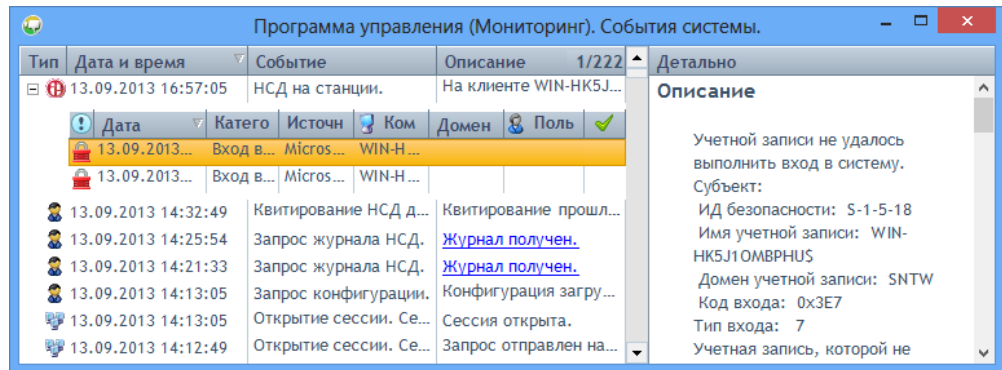
Сведения о компьютерах и серверах безопасности отображаются в колонках:

НСД
Содержит количество событий несанкционированного доступа, произошедших на защищаемом компьютере и ожидающих квитирования (подтверждение приема) администратором безопасности
Домен безопасности
Содержит имя домена безопасности, к которому относится защищаемый компьютер
Сессии пользователей
Содержит краткие сведения об активных сессиях или имя пользователя, открывшего сессию. Чтобы получить более подробные сведения, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором. Кроме того, информация об активных сессиях на агенте представлена на вкладке "Общие" (см. стр. 31)
Статус функционального контроля
Содержит пиктограмму, соответствующую результату проведения функционального контроля при запуске компьютера. Если зафиксирована ошибка функционального контроля, в ячейке отображается та же пиктограмма, что и в заголовке колонки. Чтобы получить более подробные сведения, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором
Версия
Содержит номер версии установленного программного обеспечения (ПО сервера безопасности или клиента)
Дата последнего подключения
Содержит время последнего подключения к серверу безопасности для выключенного агента
Причина блокировки
Содержит краткое описание обстоятельств, из-за которых включена блокировка компьютера
Дискреционное управление доступом
Содержит признак текущего состояния драйвера механизма дискреционного управления доступом к файловым ресурсам. Чтобы получить более подробные сведения, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором. Просмотр и изменение состояния механизмов защиты компьютера можно выполнять на вкладке "Защитные подсистемы" (режим группирования параметров по вкладкам включается с помощью кнопки "Свойства" в панели выбора режимов отображения)
Шифровать управляющий трафик
Содержит сведения о текущем состоянии режима усиленной защиты трафика при обращениях к службам каталогов
Контроль устройств
Содержит признак текущего состояния драйвера механизма контроля устройств. Чтобы получить более подробные сведения, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором. Просмотр и изменение состояния механизмов защиты компьютера можно выполнять на вкладке "Защитные подсистемы" (режим группирования параметров по вкладкам включается с помощью кнопки "Свойства" в панели выбора режимов отображения)

Полномочное управление доступом
Содержит признак текущего состояния драйвера механизма полномочного управления доступом. Чтобы получить более подробные сведения, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором. Просмотр и изменение состояния механизмов защиты компьютера можно выполнять на вкладке "Защитные подсистемы" (режим группирования параметров по вкладкам включается с помощью кнопки "Свойства" в панели выбора режимов отображения)
Контроль печати
Содержит признак текущего состояния драйвера механизма контроля печати. Чтобы получить более подробные сведения, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором. Просмотр и изменение состояния механизмов защиты компьютера можно выполнять на вкладке "Защитные подсистемы" (режим группирования параметров по вкладкам включается с помощью кнопки "Свойства" в панели выбора режимов отображения)
Затирание данных
Содержит признак текущего состояния драйвера механизма затирания. Чтобы получить более подробные сведения, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором. Просмотр и изменение состояния механизмов защиты компьютера можно выполнять на вкладке "Защитные подсистемы" (режим группирования параметров по вкладкам включается с помощью кнопки "Свойства" в панели выбора режимов отображения)
Замкнутая программная среда
Содержит признак текущего состояния драйвера механизма замкнутой программной среды. Чтобы получить более подробные сведения, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором. Просмотр и изменение состояния механизмов защиты компьютера можно выполнять на вкладке "Защитные подсистемы" (режим группирования параметров по вкладкам включается с помощью кнопки "Свойства" в панели выбора режимов отображения)
Защита диска
Содержит признак текущего состояния драйвера механизма защиты локальных дисков. Чтобы получить более подробные сведения, наведите указатель на ячейку — информация будет выведена во всплывающем сообщении рядом с курсором. Просмотр и изменение состояния механизмов защиты компьютера можно выполнять на вкладке "Защитные подсистемы" (режим группирования параметров по вкладкам включается с помощью кнопки "Свойства" в панели выбора режимов отображения)
Контроль аппаратной конфигурации
Содержит сведения о текущем состоянии механизма контроля аппаратной конфигурации для компьютеров с установленным клиентским ПО Secret Net версии 6.5
Разграничение доступа к устройствам
Содержит сведения о текущем состоянии механизма разграничения доступа к устройствам для компьютеров с установленным клиентским ПО Secret Net версии 6.5

Сведения в панели событий системы

При работе с программой в режиме мониторинга и централизованного аудита панель событий системы может использоваться для получения сведений о изменении состояния защищаемых компьютеров. Пример содержимого панели представлен на следующем рисунке.



В панели событий системы могут выводиться сведения следующих типов:




- "События сети" — уведомления о 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 НСД для агентов..." и др.);
- "События НСД" — уведомления о фактах регистрации событий НСД на защищаемых компьютерах (например, "НСД 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. 12).

Управление отображением сведений

Панель событий системы можно настроить на отображение сведений определенных типов, перечисленных выше. Выбор отображаемых типов сведений осуществляется с помощью кнопок, расположенных в правой части панели навигации по функциям программы. Описание кнопок представлено в следующей таблице.

Кнопка	Описание
	Включает или отключает отображение сведений, относящихся к типу "События сети"
	Включает или отключает отображение сведений, относящихся к типу "Действия пользователя". Некоторые сведения (например, о запуске программы оперативного управления) отображаются всегда
	Включает или отключает отображение сведений, относящихся к типу "События НСД"

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 НСД. Расширенная информация выводится в виде табличного блока, для отображения которого используется кнопка раскрытия иерархии в левой части строки.

Табличный блок уведомления о изменении политики содержит список политик и их измененных значений. Для событий НСД информация выводится в виде записей журнала с описанием событий. В колонках табличного блока представлено содержимое полей в записях журнала. 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 НСД

Программа оперативного управления в режиме мониторинга и централизованного аудита информирует о событиях НСД, произошедших на защищаемых компьютерах. Событиями НСД считаются события, которые имеют тип "Аудит отказов" и регистрируются локально в журнале Secret Net или штатном журнале безопасности ОС Windows.

Сервер безопасности протоколирует события НСД в отдельном журнале. Журнал НСД формируется из уведомлений, направляемых серверу от агентов.

Оповещение о событиях НСД

При возникновении события НСД на защищаемом компьютере пользователь программы оперативного управления оповещается следующим образом:

- в диаграмме управления на элементах, к которым относится агент, увеличивается счетчик событий НСД. Сами элементы выделяются красным цветом (см. стр. [56](#));
- в панели свойств объектов изменяется пиктограмма агента, а в колонке "НСД" отображается количество зарегистрированных событий (см. стр. [57](#));
- в панели событий системы появляется уведомление "НСД на станции" (см. стр. [59](#));
- воспроизводится звуковой сигнал, заданный при настройке параметров работы программы (см. стр. [12](#));

Возвращение обычного вида объектов происходит после квитирования всех событий НСД, относящихся к агенту (агентам).



Внимание!

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

Квитирование событий НСД

Под квитированием событий НСД понимается подтверждение о получении информации администратором безопасности с описанием принятых мер. Как правило, каждое событие НСД 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 НСД, 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 НСД не удаляется из журнала. В дальнейшем по журналу НСД можно определить, кто, когда и как отреагировал на произошедшие события. После квитирования всех событий, полученных от агента, этому объекту возвращается нормальный вид отображения.



Примечание.

Помимо квитирования событий НСД с обязательным вводом комментария администратором безопасности, в программе предусмотрена возможность сброса счетчиков событий (см. стр. 62). Процедура сброса счетчиков предназначена только для случаев, связанных с настройкой системы защиты, и не должна применяться в штатном режиме функционирования.

Квитирование событий НСД выполняется при работе с журналом НСД в панели "НСД" или при просмотре сведений в панели событий системы. Процедура квитирования применяется для событий, произошедших на агентах, которые находятся в непосредственном подчинении серверу подключения (сервер безопасности, с которым установлено соединение программы).

Для квитирования событий НСД в панели событий системы:

1. В панели событий системы перейдите к уведомлению о событиях НСД 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. 59.

2. В блоке с расширенной информацией вызовите контекстное меню событий и выберите команду "Квитировать НСД".

На экране появится диалог для ввода текстового комментария.

3. Введите текстовый комментарий с описанием причин и принятых мер по факту НСД и нажмите кнопку "Квитировать".

В табличном блоке расширенной информации в колонке "Квитировано" появится отметка, свидетельствующая о присвоении признака квитирования событиям НСД.

Сброс счетчиков событий НСД

При получении от агентов уведомлений о зарегистрированных событиях НСД счетчики событий отображаются в диаграмме управления и в панели свойств объектов (см. стр. 56 и стр. 57). Счетчики и измененные пиктограммы объектов отображаются до тех пор, пока не будут обнулены значения счетчиков для этих объектов.

Уменьшение значений счетчиков происходит при квитировании событий НСД (см. стр. 62). 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 НСД для оперативного возврата к нормальному виду отображения объектов. При сбросе счетчиков система воспринимает в качестве принятых к сведению все события НСД, произошедшие на агенте (агентах) на момент поступления команды. Однако в отличие от процедуры квитиования 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 НСД.

Для сброса счетчиков событий НСД на определенных агентах:

1. В диаграмме управления или в панели свойств объектов выберите нужные объекты. Для сброса счетчиков событий НСД можно выбрать следующие объекты:
 - агенты с ненулевыми счетчиками;
 - серверы безопасности — если требуется сбросить счетчики на всех агентах, подчиненных выбранным СБ;
 - группы — если требуется сбросить счетчики на всех агентах, включенных в выбранные группы (только в диаграмме управления).
2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Команды" и в разделе "Квитиовать события НСД" выберите команду "Все для агента (ов)". 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.

Для сброса всех счетчиков событий НСД:

- В диаграмме управления или в панели свойств объектов вызовите контекстное меню любого объекта, раскройте подменю "Команды" и в разделе "Квитиовать события НСД" выберите команду "Все в системе". При появлении диалога запроса на продолжение действия подтвердите выполнение операции.

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

Создание правил фильтрации на основе уведомлений о НСД

Для выборочного отслеживания событий можно настроить фильтр, который будет определять, какие уведомления о НСД должны поступать на сервер безопасности. Фильтр НСД 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. Настройка фильтра НСД для агентов осуществляется на вкладке управления групповыми политиками (см. стр. 41), настройка фильтра для серверов непосредственного подчинения — на вкладке "Фильтр уведомлений о НСД" (см. стр. 52).

Правила для фильтра НСД можно создавать при работе с журналом НСД в панели "НСД" (см. стр. 94) или при просмотре сведений в панели событий системы. В создаваемых правилах автоматически добавляются условия фильтрации на основе выбранных сведений. Создание правил в панели событий предусмотрено для уведомлений о событиях НСД, 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 НСД 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. 59.

2. В блоке с расширенной информацией вызовите контекстное меню события и раскройте подменю "Фильтр НСД".
3. Выберите подменю с нужным типом и размещением фильтра. Фильтр НСД может быть задан в групповых политиках (при наличии возможности изменения политик) и/или в параметрах сервера безопасности.
4. Для выбранного фильтра в открывшемся подменю "Фильтровать по" укажите нужные условия, которые будут добавлены в правило фильтрации. Для правила можно задать следующие условия на основе сведений о выбранном событии:
 - название источника;
 - название источника и числовой код категории события;
 - название источника, числовой код категории события и числовой идентификатор события.

После выбора команды в панели свойств объектов будет открыта соответствующая вкладка, и в списке правил фильтра НСД 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 агентам сервера подключения (сервер безопасности, с которым установлено соединение программы) и к агентам 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 не активна.

Блокировка и разблокирование компьютеров

Включенные компьютеры можно удаленно заблокировать или снять блокировку (разблокировать).

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

Если компьютер заблокирован системой защиты, соответствующие объекты в программе оперативного управления отображаются с измененными пиктограммами (см. стр. 56). Для такого агента 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 панели свойств объектов выберите нужные агенты или серверы безопасности.
2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Команды" и в разделе "Оперативные команды" выберите команду

"Заблокировать". При появлении диалога запроса на продолжение действия подтвердите выполнение операции.

Для разблокирования компьютеров:

1. В диаграмме управления или в панели свойств объектов выберите заблокированные агенты или серверы безопасности.
2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Команды" и в разделе "Оперативные команды" 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.

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 панели свойств объектов выберите нужные агенты или серверы безопасности.
2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Команды" и в разделе "Оперативные команды" выберите команду "Перезагрузить" или "Выключить" соответственно для перезагрузки или выключения компьютера. 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 агентам, серверам безопасности и группам агентов. Если выбран сервер безопасности или группа, обновление групповых политик выполняется на всех компьютерах, 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 панели свойств объектов выберите нужные объекты.
2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Команды" и в разделе "Оперативные команды" выберите команду "Применить групповые политики".

Команды управления механизмами защиты

Для включенных компьютеров можно использовать команды оперативного включения и отключения функционирования механизмов защиты. Команды применяются к отдельным агентам или к нескольким выбранным агентам.

Включение и отключение механизмов защиты можно выполнять и при настройке параметров функционирования механизмов на вкладке "Защитные подсистемы" (см. стр. 50). Однако с помощью команд оперативного управления можно изменять состояние механизмов одновременно для нескольких агентов.

Для включения и отключения механизмов защиты на компьютерах:

1. В панели свойств объектов выберите нужные агенты.

2. Вызовите контекстное меню одного из выбранных агентов, раскройте подменю "Защитные подсистемы" и выберите команду включения или отключения в разделе с названием механизма, для которого требуется изменить состояние.

Утверждение изменений аппаратной конфигурации

Для включенных компьютеров можно удаленно утвердить изменения аппаратной конфигурации. Команда утверждения конфигурации применяется только к отдельным агентам.

Агент, на котором зафиксировано изменение аппаратной конфигурации, обозначается в диаграмме управления специальной пиктограммой (см. стр.56).

Для утверждения аппаратной конфигурации на компьютере:

1. Вызовите контекстное меню агента 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_агента> 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.34).

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



Внимание!

Не осуществляется передача локального журнала, если для этого журнала отключена функция централизованного сбора.

Для запуска процесса передачи локальных журналов:

1. В диаграмме управления или в панели свойств объектов выберите нужные объекты.
2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Команды" и в разделе "Оперативные команды" раскройте подменю "Собрать журналы".
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".

Формирование отчетов

В программе оперативного управления можно формировать следующие отчеты:

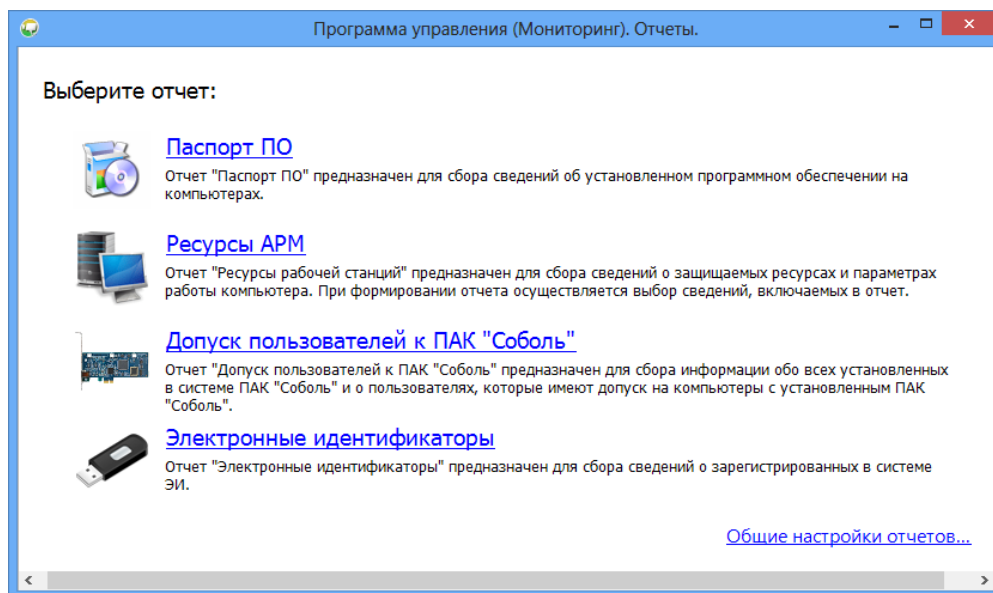
- "Паспорт ПО" — содержит сведения о программном обеспечении, установленном на компьютерах;

- "Ресурсы АРМ" — содержит сведения о ресурсах, объектах и параметрах компьютеров;
- "Допуск пользователей к ПАК "Соболь"" — содержит сведения о установленных ПАК "Соболь" и список пользователей, имеющих допуск к компьютерам с ПАК "Соболь";
- "Электронные идентификаторы" — содержит сведения о электронных идентификаторах, зарегистрированных в системе Secret Net.

Дополнительные сведения о назначении и содержании отчетов приведены в документе [3].

Создание запросов для построения отчетов выполняется в панели "Отчеты". Во время работы с программой переход к панели осуществляется с помощью ярлыка "Отчеты" в панели навигации.

В режиме ожидания запроса панель содержит экран выбора типа отчета со списком ссылок. Внешний вид панели в этом режиме представлен на следующем рисунке.



Запуск процедур формирования отчетов осуществляется с помощью соответствующих ссылок.

Для отчетов могут быть заданы общие параметры оформления: реквизиты организации и параметры нумерации страниц. Чтобы изменить общие параметры, выберите ссылку "Общие настройки отчетов" и укажите нужные значения в появившемся диалоге.

Отчеты сохраняются 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 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>.

Некоторые отчеты также можно сформировать с помощью программы "Контроль программ и данных" (см. документ [3]).

Отчет "Паспорт ПО"

Отчет со сведениями о программном обеспечении, установленном на компьютерах, формируется только для включенных агентов.

Для формирования отчета "Паспорт ПО":

1. Перейдите к панели "Отчеты". Если панель находится в режиме создания запроса на построение другого отчета, нажмите кнопку "Новый", чтобы перейти к экрану выбора типа отчета.
2. Выберите ссылку "Паспорт ПО".

Панель будет переведена в режим создания запроса на построение отчета "Паспорт ПО" и примет вид, подобный представленному на следующем рисунке.

В левой части панели содержится список агентов, сведения о которых можно добавить в отчет. Список состоит из включенных компьютеров.

Примечание.

Список агентов может быть представлен в табличной форме или в виде иерархии. При отображении списка в табличной форме выводятся имена компьютеров с указанием сетевого пути LDAP. Иерархический список формируется аналогично иерархии управления в панели свойств объектов. Переключение вида осуществляется с помощью кнопки "Список/дерево", расположенной слева на панели инструментов над списком.

В табличной форме отображения список можно отфильтровать по именам агентов. Чтобы отобразить в списке нужные компьютеры, введите в правом поле панели инструментов строку символов, которая должна присутствовать в именах компьютеров.

3. Отметьте компьютеры, сведения о которых требуется получить в отчете. Чтобы установить или удалить отметки одновременно для всех компьютеров, используйте соответствующие кнопки на панели инструментов над списком.

Примечание.

Предварительный выбор агентов для формирования отчета можно сделать в диаграмме управления или в панели свойств объектов. Действия выполняются аналогично командам оперативного управления. Чтобы перейти к формированию запроса на построение отчета для нужных агентов, используйте команду "Паспорт ПО" в подменю "Отчеты" контекстного меню объектов.

4. В правой части панели "Отчеты" введите в соответствующих полях ФИО сотрудников, ответственных за эксплуатацию выбранных компьютеров.
5. В поле "Сохранить файл отчета как" введите полное имя файла отчета или нажмите кнопку в правой части поля, чтобы указать файл в диалоге сохранения файла ОС Windows.
6. Нажмите кнопку "Построить".

Программа начнет процесс получения и обработки данных. По завершении подготовки отчета на экране появится соответствующее сообщение. Чтобы загрузить полученный файл отчета, нажмите кнопку "Просмотр".

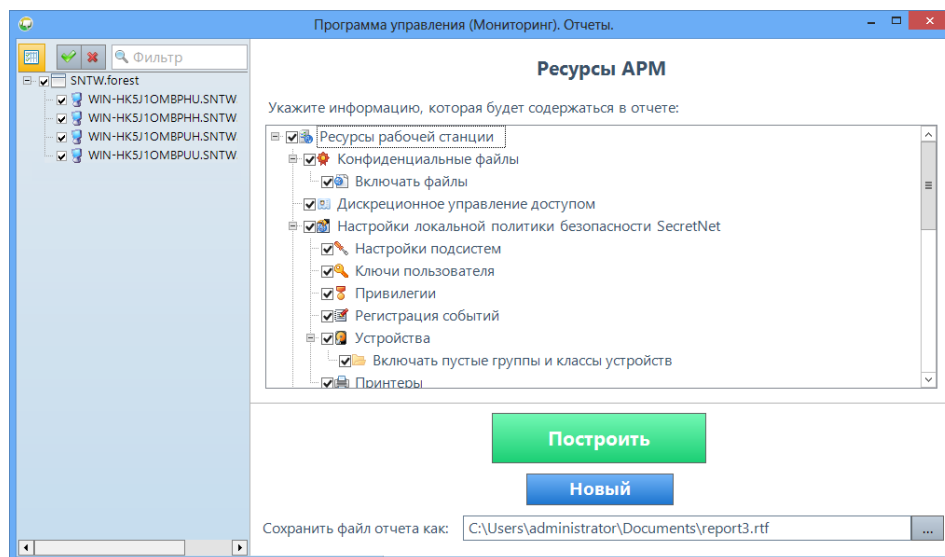
Отчет "Ресурсы АРМ"

Отчет со сведениями о ресурсах, объектах и параметрах компьютеров формируется только для включенных агентов.

Для формирования отчета "Ресурсы АРМ":

1. Перейдите к панели "Отчеты". Если панель находится в режиме создания запроса на построение другого отчета, нажмите кнопку "Новый", чтобы перейти к экрану выбора типа отчета.
2. Выберите ссылку "Ресурсы АРМ".

Панель будет переведена в режим создания запроса на построение отчета "Ресурсы АРМ" и примет вид, подобный представленному на следующем рисунке.



В левой части панели содержится список агентов, сведения о которых можно добавить в отчет. Список состоит из включенных компьютеров.

Примечание.

Список агентов может быть представлен в табличной форме или в виде иерархии. При отображении списка в табличной форме выводятся имена компьютеров с указанием сетевого пути LDAP. Иерархический список формируется аналогично иерархии управления в панели свойств объектов. Переключение вида осуществляется с помощью кнопки "Список/дерево", расположенной слева на панели инструментов над списком.

В табличной форме отображения список можно отфильтровать по именам агентов. Чтобы отобразить в списке нужные компьютеры, введите в правом поле панели инструментов строку символов, которая должна присутствовать в именах компьютеров.

3. Отметьте компьютеры, сведения о которых требуется получить в отчете. Чтобы установить или удалить отметки одновременно для всех компьютеров, используйте соответствующие кнопки на панели инструментов над списком.

Примечание.

Предварительный выбор агентов для формирования отчета можно сделать в диаграмме управления или в панели свойств объектов. Действия выполняются аналогично командам оперативного управления. Чтобы перейти к формированию запроса на построение отчета для нужных агентов, используйте команду "Ресурсы АРМ" в подменю "Отчеты" контекстного меню объектов.

4. В правой части панели "Отчеты" отметьте разделы сведений, которые необходимо включить в отчет. Разделы представлены в виде иерархического списка, элементы которого соответствуют следующим сведениям:

- **Список конфиденциальных ресурсов.** Если установлена отметка у элемента "Конфиденциальные файлы" — отчет будет содержать 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, действующей на компьютере.** Чтобы поместить список в отчет, отметьте элемент "Настройки локальной политики безопасности Secret Net". Для получения отдельных 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 поместить список в отчет, 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 поместить сведения в отчет, 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 поместить список в отчет, отметьте элемент "Локальные пользователи".
 - **Список локальных групп пользователей.** Чтобы поместить список в отчет, отметьте элемент "Локальные группы".
 - **Список доменных пользователей.** Чтобы поместить список в отчет, отметьте элемент "Доменные пользователи" (присутствует, если процедура формирования отчета выполняется на контроллере домена).
 - **Список файловых ресурсов с явно заданными правами доступа.** Чтобы поместить список в отчет, отметьте элемент "Дискреционное управление доступом".
5. В поле "Сохранить файл отчета как" введите полное имя файла отчета или нажмите кнопку в правой части поля, чтобы указать файл в диалоге сохранения файла ОС Windows.
6. Нажмите кнопку "Построить".
- Программа начнет процесс получения и обработки данных. По завершении подготовки отчета на экране появится соответствующее сообщение. Чтобы загрузить полученный файл отчета, нажмите кнопку "Просмотр".

Отчет "Допуск пользователей к ПАК "Соболь""

Отчет со сведениями о установленных ПАК "Соболь" и списком пользователей, имеющих допуск к компьютерам с ПАК "Соболь", формируется по информации, которая хранится на сервере безопасности.

Для формирования отчета "Допуск пользователей к ПАК "Соболь"":

1. Перейдите к панели "Отчеты". Если панель находится в режиме создания запроса на построение другого отчета, нажмите кнопку "Новый", чтобы перейти к экрану выбора типа отчета.
 2. Выберите ссылку "Допуск пользователей к ПАК "Соболь"".
- Панель будет переведена в режим создания запроса на построение отчета "Допуск пользователей к ПАК "Соболь"" и примет вид, подобный представленному на следующем рисунке.

Примечание.

При работе с объектами в диаграмме управления или в панели свойств объектов можно перейти к формированию отчета "Допуск пользователей к ПАК "Соболь"" с помощью команды "Соболь" в подменю "Отчеты" контекстного меню объектов.

3. Выберите нужный вариант группировки сведений в отчете. Сведения могут быть представлены по компьютерам или по пользователям. Для выбора варианта группировки установите отметку в соответствующем поле.
4. Если требуется, чтобы в отчете дополнительно были представлены сведения о компьютерах, на которых не установлен ПАК "Соболь", установите отметку в поле "Добавить в отчет рабочие станции без ПАК "Соболь"".
5. Если требуется добавить в отчет учетную информацию для каждого компьютера (сведения о рабочем месте, номер системного блока и др.), установите отметку в поле "Добавить в отчет регистрационную информацию о рабочих станциях".
6. В поле "Сохранить файл отчета как" введите полное имя файла отчета или нажмите кнопку в правой части поля, чтобы указать файл в диалоге сохранения файла ОС Windows.
7. Нажмите кнопку "Построить".

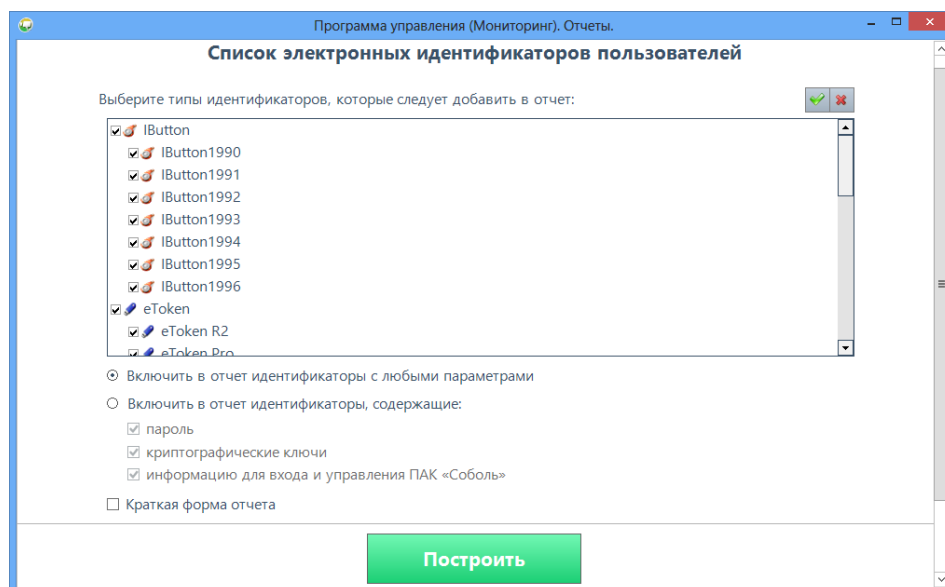
Программа начнет процесс получения и обработки данных. По завершении подготовки отчета на экране появится соответствующее сообщение. Чтобы загрузить полученный файл отчета, нажмите кнопку "Просмотр".

Отчет "Электронные идентификаторы"

Отчет со сведениями о электронных идентификаторах, зарегистрированных в системе Secret Net, формируется по информации, которая хранится на сервере безопасности.

Для формирования отчета "Электронные идентификаторы":

1. Перейдите к панели "Отчеты". Если панель находится в режиме создания запроса на построение другого отчета, нажмите кнопку "Новый", чтобы перейти к экрану выбора типа отчета.
2. Выберите ссылку "Электронные идентификаторы".
Панель будет переведена в режим создания запроса на построение отчета "Электронные идентификаторы" и примет вид, подобный представленному на следующем рисунке.



Примечание.

При работе с объектами в диаграмме управления или в панели свойств объектов можно перейти к формированию отчета "Электронные идентификаторы" с помощью одноименной команды в подменю "Отчеты" контекстного меню объектов.

3. В списке поддерживаемых идентификаторов отметьте типы устройств, сведения о которых требуется получить в отчете. Чтобы установить или удалить отметки одновременно для всех элементов списка, используйте соответствующие кнопки над списком.
4. Если требуется отфильтровать идентификаторы в зависимости от содержащихся в них данных (паролей пользователей, криптографических ключей или данных для работы с ПАК "Соболь"), установите отметку в поле "Включить в отчет идентификаторы, содержащие" и отметьте нужные типы данных. В отчете будут представлены те идентификаторы, которые содержат данные любого типа из числа отмеченных.
5. По умолчанию для каждого идентификатора в отчете представлен перечень всех типов данных, которые могут быть записаны. При необходимости сохранить в отчете только сведения о имеющихся данных установите отметку в поле "Краткая форма отчета".
6. В поле "Сохранить файл отчета как" введите полное имя файла отчета или нажмите кнопку в правой части поля, чтобы указать файл в диалоге сохранения файла ОС Windows.
7. Нажмите кнопку "Построить".

Программа начнет процесс получения и обработки данных. По завершении подготовки отчета на экране появится соответствующее сообщение. Чтобы загрузить полученный файл отчета, нажмите кнопку "Просмотр".

Глава 5

Работа с централизованными журналами

Возможности загрузки централизованных журналов из базы данных сервера безопасности доступны при работе программы оперативного управления в режиме мониторинга и централизованного аудита. Загрузку записей из архивов, хранящихся в файлах, можно выполнять при работе программы как в режиме мониторинга и централизованного аудита, так и в автономном режиме. Описание процедуры запуска программы в различных режимах см. на стр.9.

Централизованные журналы

В базе данных сервера безопасности накапливаются следующие журналы:

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

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

Журнал НСД

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

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

Для агентов может действовать фильтр событий НСД, который определяет критерии выборочного отслеживания событий. Сведения о настройке параметров фильтра см. на стр.41. Если правила фильтрации не заданы, в журнал НСД поступает информация о каждом событии НСД на агенте.

Сведения о событиях сохраняются в журнале в виде записей в базе данных. Каждая запись состоит из набора полей с полученными данными о событии. Общие данные о событии представлены в тех же полях, как и в штатном журнале безопасности ОС Windows или в журнале Secret Net. Дополнительная информация о событиях сохраняется в поле с детальным описанием события и в полях, перечисленных в следующей таблице.

Поле	Описание
Журнал	Тип локального журнала, в котором зарегистрировано событие. События НСД регистрируются в журнале безопасности или в журнале Secret Net
Агент	Тип агента оперативного управления, установленного на защищаемом компьютере
Код категории	Числовой код категории события

Поле	Описание
Домен	Тип домена безопасности (указывается для событий, регистрируемых в журнале Secret Net)
Квитировано	Признак квитирования (подтверждение приема) события НСД

Объединенный журнал агентов

Объединенный журнал агентов (называемый также журнал станций) предназначен для централизованного хранения содержимого локальных журналов, поступивших с защищаемых компьютеров. К локальным журналам относятся: журнал Secret Net и штатные журналы ОС Windows (журнал приложений, системный журнал и журнал безопасности). Описание назначения локальных журналов см. в документе [5].

Передача локальных журналов для централизованного хранения в базу данных сервера безопасности осуществляется в соответствии с заданными параметрами (см. стр.34).

Сведения, полученные из локальных журналов, сохраняются в полном объеме в объединенном журнале агентов. Вместе с этими сведениями сервер безопасности получает от агентов и фиксирует в объединенном журнале дополнительную информацию о событиях. Эта информация сохраняется в поле с детальным описанием события и в полях, перечисленных в следующей таблице.

Поле	Описание
Журнал	Тип локального журнала, в котором зарегистрировано событие
Агент	Тип агента оперативного управления, установленного на защищаемом компьютере

Журнал сервера безопасности

В журнале сервера безопасности протоколируются сессии доступа к серверу безопасности и операции, выполняемые сервером. Регистрация сессий доступа происходит при обращениях к серверу безопасности компонентов и программ системы защиты.

Перечень полей, составляющих записи журнала сессий, представлен в следующей таблице.

Поле	Описание
Результат	Признак успешного завершения операции (нулевое значение — операция завершена успешно, ненулевое — отказ при выполнении операции)
Действие	Краткое описание (название) выполненной операции
SID компьютера	Системный идентификатор безопасности компьютера
Время действия	Дата и время выполнения операции
Класс клиента	Обозначение компонента системы Secret Net, открывшего сессию доступа к серверу безопасности
Тип клиента	Тип или режим использования компонента системы Secret Net, открывшего сессию доступа к серверу безопасности
SID пользователя	Системный идентификатор безопасности пользователя, открывшего сессию доступа к серверу безопасности
Имя компьютера	Имя компьютера, с которого поступил запрос на открытие сессии доступа к серверу безопасности
Имя пользователя	Имя пользователя, открывшего сессию доступа к серверу безопасности

Поле	Описание
Время открытия сессии	Дата и время открытия сессии доступа к серверу безопасности
Код завершения	Код, возвращенный системой при закрытии сессии доступа к серверу безопасности. При нормальном завершении сессии поле содержит нулевое значение. Другие значения соответствуют ошибкам закрытия сессии. Если на момент запроса журнала сессия продолжается, поле пустое
Время закрытия сессии	Дата и время закрытия сессии доступа к серверу безопасности. Если на момент запроса журнала сессия продолжается, поле пустое
Код действия	Кодовое обозначение выполненной операции

Хранение журналов в сетевом режиме функционирования

В сетевом режиме функционирования системы Secret Net журналы с записями о событиях могут храниться в следующих хранилищах:

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

В программе оперативного 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 (штатные журналы ОС Windows и журнал Secret Net) и хранятся на защищаемом компьютере. Пока записи хранятся в локальном хранилище, их можно загрузить в программу просмотра локальных журналов или в другие программы, позволяющие осуществлять загрузку журналов (кроме журнала Secret Net). Сведения о работе с программой просмотра локальных журналов, входящей в состав ПО системы Secret Net, см. в документе [5].

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



Внимание!

В программе просмотра локальных журналов пользователь, наделенный соответствующей привилегией, может выполнять очистку журналов до их передачи на сервер безопасности. Чтобы исключить возможность несанкционированного удаления информации, необходимо предоставлять привилегии на управление локальными журналами только доверенным пользователям.

Централизованное хранилище

В централизованном хранилище сервера безопасности хранится содержимое централизованных журналов. Сведения о событиях, регистрируемых в журнале НСД или в журнале сервера безопасности, поступают непосредственно в централизованное хранилище без промежуточного размещения в других хранилищах. В объединенном журнале агентов 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. 34);
- по команде пользователя программы оперативного управления (см. стр. 66).

**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 оперативного управления при работе в режиме мониторинга и централизованного аудита.

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. [36](#));
- по команде пользователя программы просмотра журналов (см. стр. [100](#)).

Архивированные записи журналов хранятся в файлах. Для каждого архива создается отдельный файл. Файлы архивов базы данных размещаются в каталоге, заданном при настройке параметров сервера безопасности (см. стр. [31](#)). По умолчанию для размещения архивов используется подкаталог \Archive, расположенный в каталоге установки сервера безопасности.

Просмотр записей, помещенных в архив, осуществляется в программе оперативного управления при работе в режиме мониторинга и централизованного аудита или в автономном режиме.

Панели для работы с записями журналов

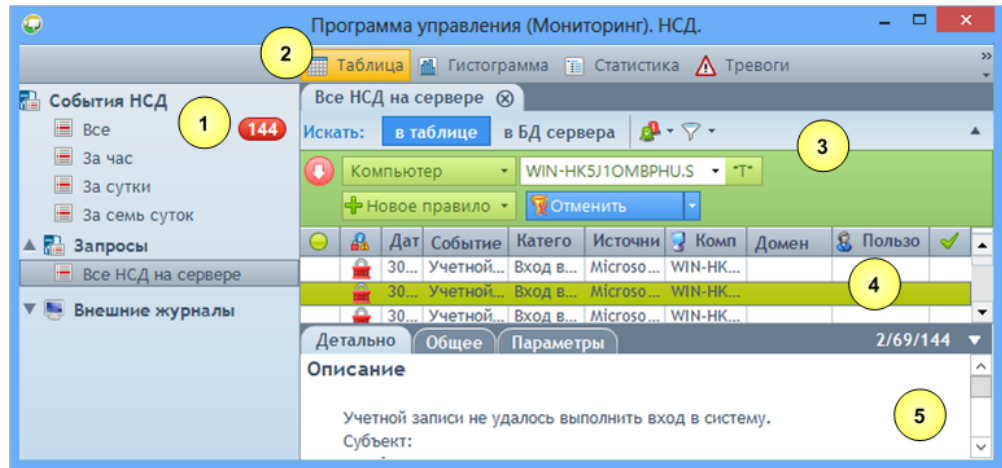
Вывод записей централизованных журналов осуществляется в следующих панелях:

- панель журнала НСД — открывается по умолчанию, если при запуске программы оперативного управления в диалоге выбора режима работы (см. стр. [9](#)) выбрана одна из команд для загрузки записей журнала НСД: "Журналы НСД", "Новый запрос" справа от команды "Журналы НСД" или команда запуска в автономном режиме "Журналы" с последующим открытием файла с записями журнала НСД. Во время работы с программой переход к панели журнала НСД осуществляется с помощью ярлыка "НСД" в панели навигации или по ссылке "Журнал получен" в уведомлении о запросе журнала НСД в панели событий системы;
- панель журналов станций и сервера безопасности — открывается по умолчанию, если при запуске программы оперативного управления в диалоге выбора режима работы выбрана одна из команд для загрузки записей журнала станций или журнала сервера безопасности: "Журналы", "Новый запрос" справа от команды "Журналы" или команда запуска в автономном режиме "Журналы" с последующим открытием файла с записями любых журналов, кроме журнала НСД. Во время работы с программой переход к панели журналов осуществляется с помощью ярлыка "Журналы" в панели навигации или по ссылке "Журнал получен" в уведомлении о запросе журнала событий или журнала сервера в панели событий системы;
- панель архивов журналов — открывается по умолчанию, если при запуске программы оперативного 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 с помощью закладок с названиями запросов.

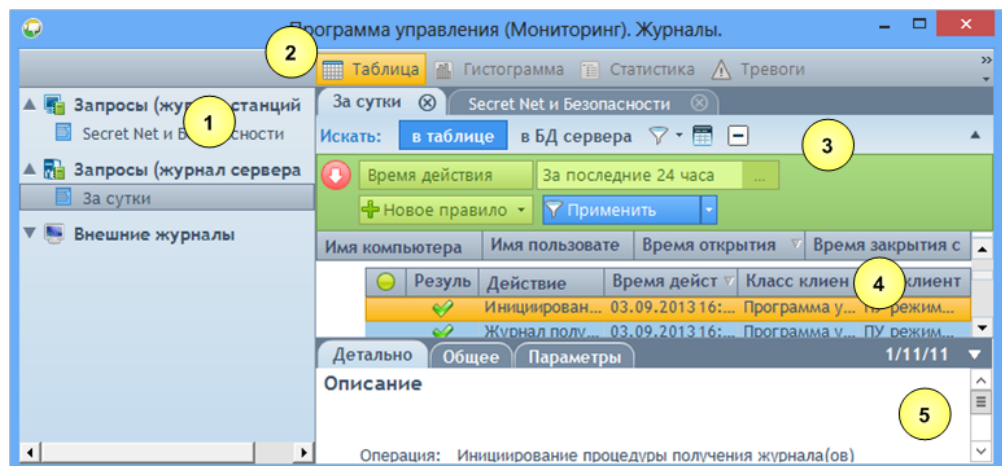
Панель журнала НСД имеет вид, подобный представленному на следующем рисунке.



Пояснение.

На рисунке выносками обозначены элементы: 1 — панель управления запросами; 2 — панель выбора режимов отображения и поиска; 3 — заголовок вкладки запроса; 4 — область отображения сведений; 5 — область описания событий.

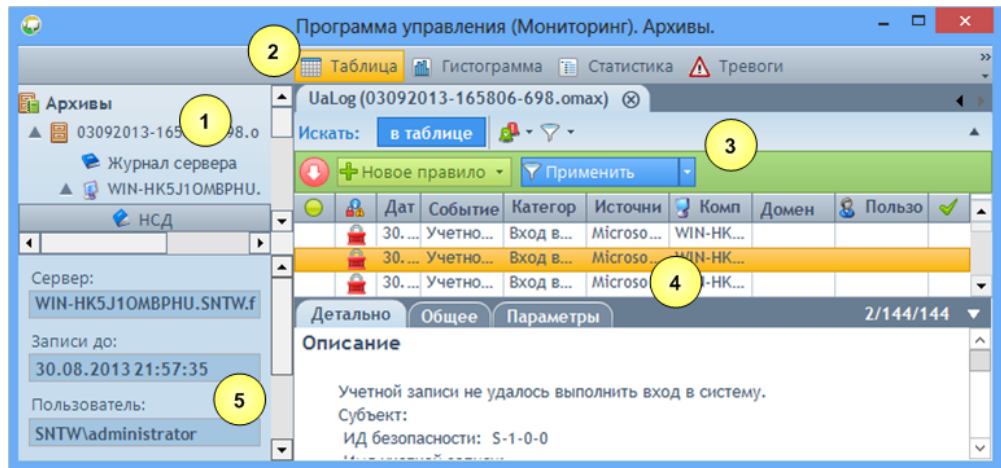
Панель журналов станций и сервера безопасности имеет вид, подобный представленному на следующем рисунке.



Пояснение.

На рисунке выносками обозначены элементы: 1 — панель управления запросами; 2 — панель выбора режимов отображения и поиска; 3 — заголовок вкладки запроса; 4 — область отображения сведений; 5 — область описания событий.

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



Пояснение.

На рисунке выносками обозначены элементы: 1 — панель управления запросами; 2 — панель выбора режимов отображения и поиска; 3 — заголовок вкладки запроса; 4 — область отображения сведений; 5 — область основных сведений об архиве.

Элементы интерфейса панелей:

Панель управления запросами

Содержит списки запросов для загрузки записей.

В панели журнала НСД запросы группируются в следующих разделах:

- "События НСД" — запросы с predetermined критериями отбора записей, загружаемых из журнала НСД;
- "Запросы" — запросы, созданные пользователем для загрузки записей из журнала НСД;
- "Внешние журналы" — запросы, созданные при загрузке записей из файлов.

В панели журналов станций и сервера безопасности запросы группируются в следующих разделах:

- "Запросы (журнал станций)" — запросы, созданные пользователем для загрузки записей из объединенного журнала агентов;
- "Запросы (журнал сервера)" — запросы, созданные пользователем для загрузки записей из журнала сервера безопасности;
- "Внешние журналы" — запросы, созданные при загрузке записей из файлов.

В панели архивов журналов запросы группируются в следующих разделах:

- "Архивы" — запросы, полученные по результатам анализа содержимого загруженных архивов;
- "Поиск" — запросы, созданные пользователем для загрузки записей из нескольких загруженных архивов

Панель выбора режимов отображения и поиска

Содержит кнопки переключения вида отображаемых данных в области отображения сведений и средства для поиска записей (действуют при отображении в виде простой таблицы)

Заголовок вкладки запроса

Предназначен для управления загрузкой и отображением записей. Верхняя часть заголовка содержит панель с элементами управления для выбора источника загружаемых записей и настройки общих параметров запроса. В нижней части заголовка представлены элементы управления параметрами фильтрации. Включение и отключение нижней части заголовка осуществляется с помощью кнопки "Показать/скрыть фильтр", расположенной справа в панели с элементами управления

Область отображения сведений

Содержит сведения о событиях в соответствии с выбранным видом отображения данных. Сведения могут быть представлены в следующих режимах:

- режим отображения в виде простой таблицы со списком записей журнала (режим является основным и включен по умолчанию);
- режим отображения в виде гистограммы с графиками распределения событий;
- режим отображения в виде таблицы статистических данных со сводной информацией по всем журналам;
- режим отображения в виде таблицы со списком зафиксированных событий тревоги.

Переключение режимов осуществляется в панели выбора режимов отображения и поиска с помощью соответствующих кнопок: "Таблица", "Гистограмма", "Статистика" и "Тревоги". Описание возможностей для вывода сведений в различных режимах см. на стр. **88**

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, полученных из детального описания события. Список представлен в табличной форме;
- "Квотирование НСД" — содержит сведения о том, кто и когда выполнил процедуру квотирования (подтверждение приема) для выбранной записи и текстовый комментарий с описанием действий. Вкладка отображается только для журнала НСД при выборе записи с признаком квотирования;
- "Правила" — содержит список основных параметров события тревоги (название, описание, отслеживаемые журналы и др.). Вкладка отображается только при выборе события тревоги.

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

Область основных сведений об архиве

Используется только в панели архивов журналов. Содержит основные сведения о выбранном архиве, сохраненные при его создании: имя сервера безопасности, граница интервала времени для записей, имя создавшего архив пользователя, описание архива

Загрузка записей журналов

Запросы для журнала НСД

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

- контекстное создание запросов;
- создание запросов с предопределенными критериями отбора записей;
- создание общих запросов;
- создание запросов на загрузку записей журнала НСД из файлов.

Контекстное создание запросов

Запросы на загрузку записей журнала НСД можно создавать применительно к объектам, выбранным в панели диаграммы управления или в панели свойств 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 панели свойств объектов выберите нужные объекты. Для создания запроса на загрузку записей журнала НСД можно выбрать следующие объекты:
 - агенты, подчиненные одному серверу безопасности;

- сервер безопасности — если требуется создать запрос для загрузки записей, поступивших от всех подчиненных серверу агентов;
- группу агентов — если требуется создать запрос для загрузки записей, поступивших от всех агентов в группе.

Примечание.

О наличии зарегистрированных событий НСД, ожидающих квитирования (подтверждения приема) администратором безопасности, оповещают счетчики событий НСД, которые отображаются рядом с объектами (см. стр. 56 и стр. 57).

2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Запросы" и в нем подменю "Журнал НСД".
3. Выберите команду, соответствующую нужным критериям отбора записей. В разделе "Неквитированные НСД" представлены команды для загрузки записей о событиях, которые не прошли процедуру квитирования. В разделе "НСД всех типов" представлены команды для загрузки любых записей журнала НСД. С использованием соответствующих команд можно загрузить записи о событиях, зарегистрированных в течение последнего часа, последних суток, или все записи. По команде "Новый запрос" выполняется создание запроса с переходом в панель журнала НСД для настройки параметров запроса (см. стр. 86).

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. 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 predeterminedенными критериями отбора записей

Запросы журнала НСД с predeterminedенными критериями отбора позволяют оперативно загрузить в программу неквитированные записи о событиях НСД, которые были зарегистрированы в следующие периоды времени:

- весь период регистрации событий (при наличии в системе записей о событиях, которые не прошли процедуру квитирования);
- в течение последнего часа;
- в течение последних суток;
- в течение последних семи суток.

Создание запросов с predeterminedенными критериями отбора выполняется в панели журнала НСД. Такие запросы целесообразно создавать при наличии в системе неквитированных записей о событиях НСД. О наличии неквитированных записей сигнализирует, в частности, элемент "Все" со счетчиком событий в списке запросов раздела "События НСД" панели управления запросами.

Для создания запроса с predeterminedенными критериями отбора:

- В разделе "События НСД" панели управления запросами наведите указатель на элемент списка, соответствующий нужному периоду времени регистрации событий. Справа от названия элемента нажмите кнопку создания запроса.

Примечание.

Для элемента "Все" кнопкой создания запроса является сам счетчик событий НСД. Кнопки рядом с остальными элементами списка ("За час", "За сутки", "За семь суток") появляются при наведении указателя на строку элемента.

В панели журнала НСД 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 общих запросов

Общие запросы на загрузку записей журнала НСД создаются для последующей настройки параметров и запуска процесса получения записей вручную. Для таких запросов предоставляются возможности переименования и сохранения в файлы, чтобы использовать их в дальнейшем.

Создание общих запросов выполняется в панели журнала НСД.

Для создания общего запроса:

1. В панели управления запросами наведите указатель на раздел "Запросы". Справа от названия раздела нажмите кнопку создания запроса.

Примечание.

Кнопка рядом с названием раздела появляется при наведении указателя на строку раздела.

В панели журнала НСД будет создан новый запрос с параметрами по умолчанию.

2. Настройте параметры нового запроса (см. стр. 86) и нажмите кнопку "Применить" в заголовке вкладки 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 НСД из файлов

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

Файл для загрузки можно указать при запуске программы в автономном режиме (см. стр. 9) или во время работы с программой в панели журнала НСД.

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

1. В панели управления запросами наведите указатель на раздел "Внешние журналы". Справа от названия раздела нажмите кнопку создания запроса.

Примечание.

Кнопка рядом с названием раздела появляется при наведении указателя на строку раздела.

На экране появится диалог открытия файла ОС Windows.

2. Выберите нужный файл.

В панели журнала НСД 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;
- создание общих запросов;
- создание запросов на загрузку записей журнала станций или локальных журналов из файлов.

Контекстное создание запросов

Запросы на загрузку записей журнала станций можно создавать применительно к объектам, выбранным в панели диаграммы управления или в панели свойств 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 панели свойств объектов выберите нужные объекты. Для создания запроса на загрузку записей журнала станций можно выбрать следующие объекты:
 - агенты, подчиненные одному серверу безопасности;
 - сервер безопасности — если требуется создать запрос для загрузки записей, поступивших от всех подчиненных серверу агентов;
 - группу агентов — если требуется создать запрос для загрузки записей, поступивших от всех агентов в группе.
2. Вызовите контекстное меню одного из выбранных объектов, раскройте подменю "Запросы" и в нем подменю "Журналы станций".
3. Выберите команду, соответствующую нужным критериям отбора записей. С использованием соответствующих команд можно загрузить записи о событиях, поступившие из определенных локальных журналов по отдельности или журнала Secret Net совместно с журналом безопасности. По команде "Новый запрос" выполняется создание запроса с переходом в панель "Журналы" для настройки параметров запроса (см. стр. 86).

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 общих запросов

Общие запросы на загрузку записей журнала станций создаются для последующей настройки параметров и запуска процесса получения записей вручную.

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

Для создания общего запроса:

1. В панели управления запросами наведите указатель на раздел "Запросы (журнал станций)". Справа от названия раздела нажмите кнопку создания запроса.

Примечание.

Кнопка рядом с названием раздела появляется при наведении указателя на строку раздела.

В панели "Журналы" будет создан новый запрос с параметрами по умолчанию.

2. Настройте параметры нового запроса (см. стр. 86) и нажмите кнопку "Применить" в заголовке вкладки 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" 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*. Возможность обработки таких файлов доступна на компьютерах под управлением ОС Windows Vista и выше.

Файл для загрузки можно указать при запуске программы в автономном режиме (см. стр. 9) или во время работы с программой в панели "Журналы".

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

1. В панели управления запросами наведите указатель на раздел "Внешние журналы". Справа от названия раздела нажмите кнопку создания запроса.

Примечание.

Кнопка рядом с названием раздела появляется при наведении указателя на строку раздела.

На экране появится диалог открытия файла ОС Windows.

2. Выберите нужный файл.

В панели "Журналы" 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 общих запросов;
- 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 панели свойств 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 панели свойств объектов вызовите контекстное меню сервера безопасности, журнал которого требуется загрузить. В контекстном меню раскройте подменю "Запросы" и в нем подменю "Журнал сервера".
2. Выберите команду, соответствующую нужным критериям отбора записей. С использованием соответствующих команд можно загрузить записи о событиях, зарегистрированных в течение последнего часа, последних суток, или все записи. По команде "Новый запрос" выполняется создание запроса с переходом в панель "Журналы" для настройки параметров запроса (см. стр. 86).

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 общих запросов

Общие запросы на загрузку записей журнала сервера безопасности создаются для последующей настройки параметров и запуска процесса получения записей вручную.

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

Для создания общего запроса:

1. В панели управления запросами наведите указатель на раздел "Запросы (журнал сервера)". Справа от названия раздела нажмите кнопку создания запроса.

Примечание.

Кнопка рядом с названием раздела появляется при наведении указателя на строку раздела.

В панели "Журналы" будет создан новый запрос с параметрами по умолчанию.

2. Настройте параметры нового запроса (см. стр. 86) и нажмите кнопку "Применить" в заголовке вкладки 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 *.snsv. Загрузка записей из таких файлов в панель "Журналы" осуществляется путем создания отдельных запросов для каждого файла.

Файл для загрузки можно указать при запуске программы в автономном режиме (см. стр. 9) или во время работы с программой в панели "Журналы".

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

1. В панели управления запросами наведите указатель на раздел "Внешние журналы". Справа от названия раздела нажмите кнопку создания запроса.

Примечание.

Кнопка рядом с названием раздела появляется при наведении указателя на строку раздела.

На экране появится диалог открытия файла ОС Windows.

2. Выберите нужный файл.

В панели "Журналы" 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. Загрузку файлов архивов можно выполнять при работе программы в режиме мониторинга и централизованного аудита или в автономном режиме.

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 НСД 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. 9) или во время работы с программой в панели "Архивы".

**Примечание.**

В программе оперативного управления поддерживается загрузка файлов архивов, созданных сервером безопасности версии 7.0 и выше. Для работы с архивами, созданными СБ предыдущих версий, необходимо использовать программу просмотра локальных журналов (см. документ [5]).

Для загрузки файлов архивов в панели "Архивы":

1. В панели управления запросами наведите указатель на раздел "Архивы". Справа от названия раздела нажмите кнопку добавления архива.

Примечание.

Кнопка рядом с названием раздела появляется при наведении указателя на строку раздела.

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. В списке подраздела с названием архива изменится пиктограмма выбранного журнала.

Создание запроса для отбора записей журнала НСД или журнала станций в загруженных архивах

Среди загруженных архивов можно сделать выборку из всех записей журнала НСД или журнала 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 НСД или журнала станций:

1. В панели управления запросами наведите указатель на раздел "Поиск". Справа от названия раздела появится кнопка создания запроса.
2. Вызовите контекстное меню кнопки создания запроса и выберите команду, соответствующую нужному журналу: "В журналах НСД" или "В журналах станций".

Примечание.

Аналогичным образом можно создать запрос, относящийся к одному из загруженных архивов. Для этого вызовите контекстное меню подраздела с названием нужного архива и выберите соответствующую команду.

В панели "Архивы" будет создан новый запрос с параметрами по умолчанию.

3. Настройте параметры нового запроса и нажмите кнопку "Применить" в заголовке вкладки запроса.

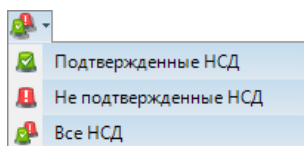
После отбора записей сведения будут отображены на вкладке запроса.

Настройка параметров запроса

С целью получения нужных сведений в запросе записей журнала можно изменять параметры загрузки и фильтрации записей. Настройка параметров осуществляется в заголовке вкладки запроса. Примеры содержимого заголовка представлены на рисунках с изображением панелей для работы с журналами (см. стр. 76).

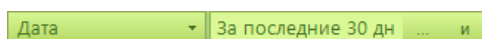
Для настройки параметров запроса:

1. Укажите источник получения сведений. Для выбора источника используйте соответствующие кнопки в группе "Искать", которая размещается в левой части заголовка вкладки запроса:
 - Чтобы выполнить отбор (фильтрацию) записей из числа уже загруженных в данном запросе, нажмите кнопку "в таблице". Этот режим включается по умолчанию после предыдущей загрузки записей.
 - Чтобы сделать новую выборку записей журнала из базы данных сервера безопасности, нажмите кнопку "в БД сервера". Справа от кнопки появятся средства для уточнения параметров загрузки. Укажите объем загружаемых сведений: для загрузки неограниченного количества записей нажмите кнопку "все события", для загрузки определенного количества — нажмите кнопку "последние <число> событий" (чтобы ввести другое число, выделите текущее значение). В поле "Сервер" укажите сервер безопасности, из базы данных которого необходимо загрузить записи журнала. Список поля содержит имена серверов безопасности, с которых возможно получение журналов в текущей сессии подключения.
 - Чтобы выполнить отбор записей из загруженных архивов (в панели "Архивы"), нажмите кнопку "В архивах" и отметьте файлы нужных архивов в раскрывающемся списке.
2. Если запрос создан для загрузки записей журнала НСД, выберите режим фильтрации по признаку квитирования событий. Для этого раскройте список кнопки "НСД", которая размещается справа от средств выбора источника получения сведений.



В списке режимов укажите нужное условие:

- "Подтвержденные НСД" — в запросе будут рассматриваться записи, для которых выполнялась процедура квитирования;
 - "Неподтвержденные НСД" — в запросе будут рассматриваться записи, для которых процедура квитирования не выполнялась;
 - "Все НСД" — признак квитирования событий не учитывается.
3. В нижней части заголовка вкладки запроса сформируйте список правил фильтрации. Правила фильтрации определяют условия для содержимого колонок таблицы записей журнала. Каждое правило состоит из двух элементов: поле с названием колонки (слева) и поле с условием для содержимого колонки (справа). Пример правила фильтрации представлен на следующем рисунке.

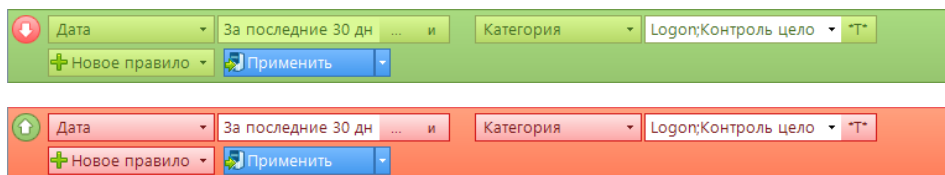


Добавление правил осуществляется с помощью кнопки "Новое правило" в конце списка правил или по команде "Фильтр: <название_колонки> <условие> <текущее_значение>" в контекстном меню ячеек таблицы с записями. Для правила можно изменить колонку, к которой оно относится, или условие фильтрации содержимого колонки. Чтобы изменить

правило, нажмите кнопку в правой части соответствующего поля или отредактируйте его текстовое содержимое (если это допускается). Возможность изменения отсутствует для правил, сформированных автоматически при создании запроса. При наличии в списке нескольких правил указываются условия их совместного или отдельного применения: чтобы правило применялось совместно со следующим правилом, для него устанавливается логический оператор "И" (указан по умолчанию); если правила должны применяться отдельно, необходимо использовать оператор "ИЛИ".

4. При необходимости включите режим инверсии параметров фильтрации. В этом режиме фильтру будут удовлетворять записи, которые не соответствуют заданным условиям. Для включения и отключения режима используйте кнопку "Инверсия" слева от списка правил фильтрации.

После включения или отключения режима инверсии изменяется фон списка правил фильтрации и изображение самой кнопки "Инверсия". Примеры списка правил при отключенном и включенном режиме инверсии представлены на следующих рисунках:



5. Чтобы применить заданные параметры и заново выполнить отбор или выборку записей в запросе, нажмите кнопку "Применить" в конце списка правил. Кнопка имеет название "Отменить", если получение сведений в соответствии с заданными параметрами уже выполнено.

Примечание.

Кнопку "Отменить" можно использовать для отмены фильтрации по заданным параметрам и отображения всех загруженных записей в данном запросе.

Управление запросами

В панелях "НСД" и "Журналы" операции по управлению запросами выполняются с помощью команд контекстного меню в панели управления запросами. Команды управления перечислены в следующей таблице.

Команда	Описание
Переименовать	Включает режим редактирования для переименования выбранного запроса. Не применяется для запросов журнала НСД с predetermined критериями отбора записей (в разделе "События НСД")
Заккрыть	Закрывает вкладку выбранного запроса. Для закрытия можно также использовать кнопку справа от названия запроса, которая появляется при наведении указателя на запрос (кроме запросов в разделе "События НСД"), или кнопку закрытия на закладке запроса
Удалить	Выгружает из программы файл выбранного запроса, если запрос был сохранен в файле или загружен из файла. Если файл сохраненного запроса не был выгружен из программы, при следующем запуске он загружается автоматически
Сохранить	Сохраняет выбранный запрос в файле. Не применяется для запросов журнала НСД с predetermined критериями отбора записей (в разделе "События НСД") и для запросов на загрузку записей из файлов (в разделах "Внешние журналы")

Команда	Описание
Сохранить как	Сохраняет выбранный запрос в другом файле. Не применяется для запросов журнала НСД с предопределенными критериями отбора записей (в разделе "События НСД") и для запросов на загрузку записей из файлов (в разделах "Внешние журналы")
Открыть	Открывает запрос из файла. Открытый запрос помещается в тот раздел, к которому он относится
Свойства	Вызывает диалог "Свойства пользовательского запроса" для выбранного запроса, если запрос был сохранен в файле или загружен из файла

В панели "Архивы" команды управления запросами не применяются. Для закрытия созданных запросов можно использовать кнопку справа от названия запроса, которая появляется при наведении указателя на запрос, или кнопку закрытия на закладке запроса.

Созданные запросы для загрузки записей выгружаются из программы при окончании сеанса работы с ней. Чтобы использовать созданный запрос в следующих сеансах, его следует сохранить в файле. Сохраненные запросы отображаются в панелях "НСД" и "Журналы" с измененной пиктограммой.

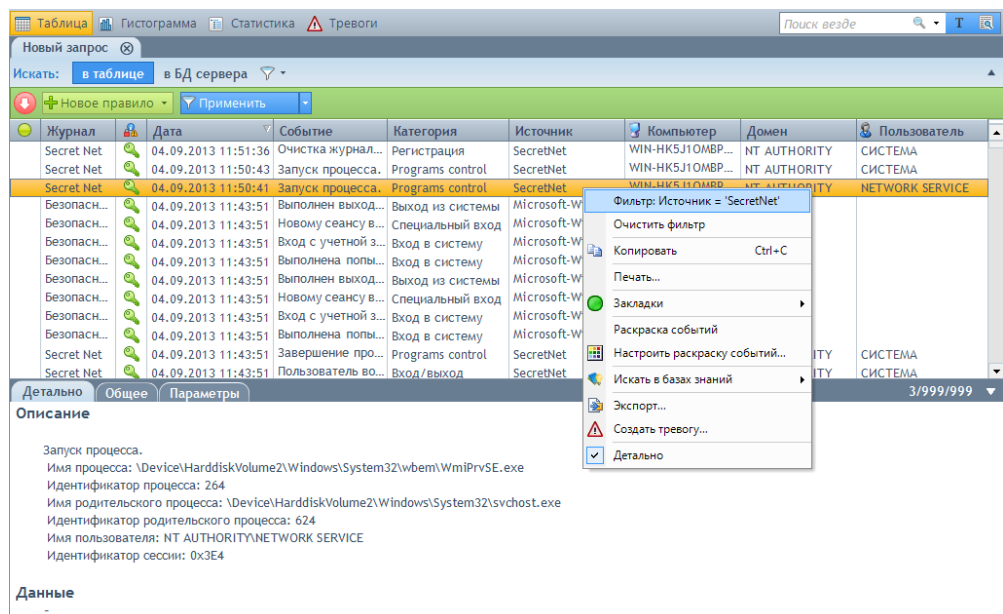
Возможности при просмотре записей

Режимы отображения сведений о событиях

Загруженная информация о событиях выводится в области отображения сведений соответствующей панели (см. стр. 76). Для анализа содержимого журналов предусмотрены различные режимы отображения сведений (кроме журнала сервера безопасности). Помимо вывода информации в виде обычного списка записей программа предоставляет возможности для просмотра сведений в виде графиков гистограмм, сводных таблиц статистики или как списки важных событий тревоги.

Режим "Таблица"

В режиме "Таблица" 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.

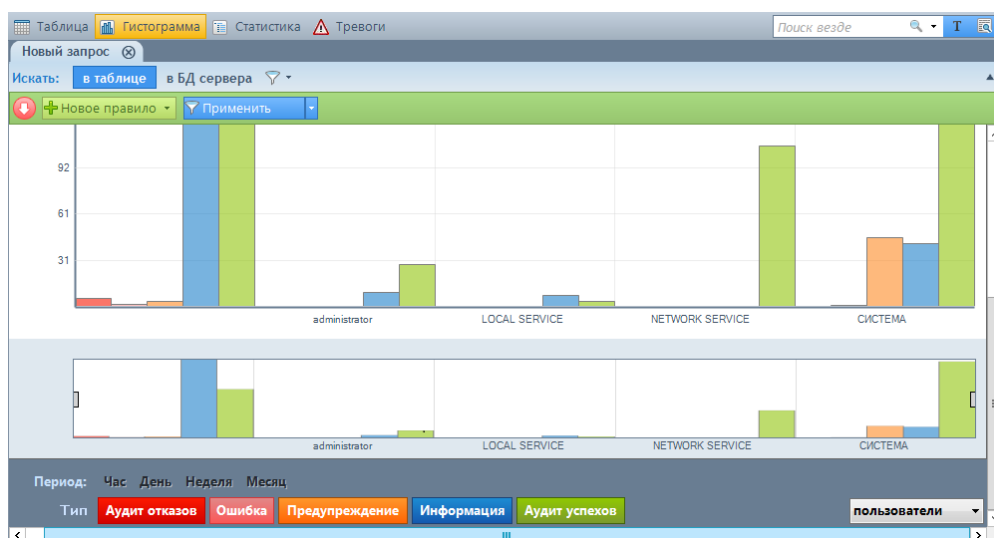


С помощью контекстного меню записей (на рисунке показано меню для одной из записей в ячейке колонки "Источник") выполняются необходимые действия: фильтрация, печать, сохранение, создание закладок и др. Описания действий представлены далее в соответствующих разделах.

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

Режим "Гистограмма"

В режиме "Гистограмма" выводятся графики распределения событий в зависимости от их типов и выбранных характеристик. Графики показывают количественное соотношение событий. Режим предназначен для визуализации представления информации, касающейся объема и характера зарегистрированных событий. Пример содержимого окна с графиками представлен на следующем рисунке:



Графики выводятся в верхней части области отображения сведений. В нижней части содержится полоса масштабирования горизонтальной оси гистограммы и элементы управления, с помощью которых осуществляются выбор и уточнение характеристик событий для построения графиков.

По умолчанию графики строятся по всем типам событий: "Аудит отказов", "Ошибки", "Предупреждения", "Информация" и "Аудит успехов". Расцветка столбцов соответствует цветам кнопок с названиями типов событий в строке "Тип". Подсчет количества событий осуществляется среди записей, которые были зарегистрированы в течение последних 30 дней.

Наибольшую высоту имеет столбец, который соответствует максимальному количеству событий. Высота остальных столбцов пропорциональна количеству событий каждого типа. Определить количество событий можно путем сопоставления высоты столбца с вертикальной шкалой или, для получения точного значения, наведите указатель на нужный столбец — число появится под курсором. Кроме того, столбцы могут использоваться для переключения в режим "Таблица" с автоматической фильтрацией отображаемых записей. Чтобы применить фильтр и вывести список записей, наведите указатель на нужный столбец и дважды нажмите левую кнопку мыши.

При необходимости можно изменить масштаб гистограммы или отключить отображение столбцов определенных типов событий. Для изменения масштаба используйте боковые границы полосы масштабирования или ссылки в строке "Период". Выбор отображаемых столбцов осуществляется с помощью кнопок в строке "Тип".

Предусмотрены возможности построения гистограммы не только по времени регистрации событий, но и по компьютерам или пользователям, к которым отно-

сятся события. Для выбора нужных параметров используйте раскрывающийся список под полосой масштабирования справа.

Режим "Статистика"

В режиме "Статистика" выводится сводная информация по всем журналам с указанием основных характеристик и количества зарегистрированных событий в различные промежутки времени. Режим предназначен для наглядного представления информации о распределении загруженных записей. Пример содержимого окна со сведениями о зарегистрированных событиях представлен на следующем рисунке.

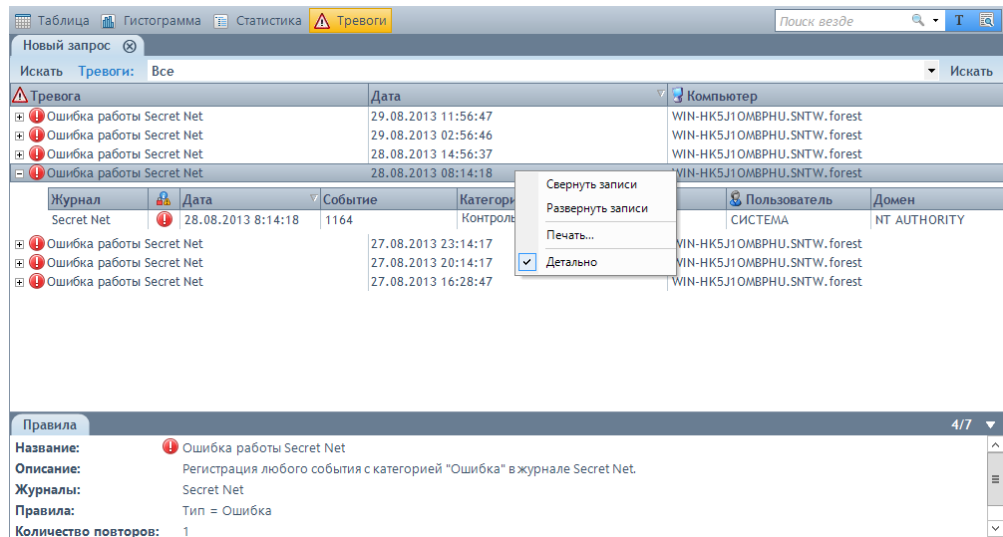
Тип журнала	Тип события	Событие	Источник	Час	День	Неделя	Всего
Безопасности				23	154	195	195
	Аудит отказов			6	6	6	6
	Ошибка	Учетной	Microsoft-Windows-Security-	6	6	6	6
	Предупреждение						
	Информация						
	Аудит успехов			17	148	189	189
Системный				3	41	196	196
	Аудит отказов						
	Ошибка	1054	Microsoft-Windows-GroupPolicy		1	1	1
	Предупреждение				13	17	17
	Информация			3	27	178	178
	Аудит успехов						
Приложений				95	197	197	197
	Аудит отказов						
	Ошибка				1	2	2
	Предупреждение				15	17	17
	Информация				79	178	178
	Аудит успехов						

Информация выводится в табличной форме с возможностью раскрытия и сворачивания блоков, относящихся к одному журналу или к одному типу событий в журнале. Внутри этих уровней иерархии можно выполнять сортировку по колонкам таблицы.

Количественные значения в ячейках таблицы могут использоваться для переключения в режим "Таблица" с автоматической фильтрацией отображаемых записей. Чтобы применить фильтр и вывести список записей, наведите указатель на нужную ячейку и дважды нажмите левую кнопку мыши.

Режим "Тревоги"

В режиме "Тревоги" выводится список событий тревоги, полученных в результате анализа загруженных записей. События тревоги представляют собой сжатые или разъясняющие сведения о зарегистрированных событиях (например, событие тревоги 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.



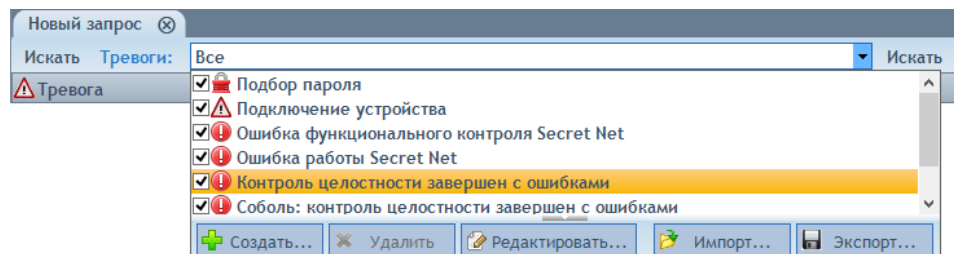
Информация выводится в табличной форме с возможностью раскрытия списков зарегистрированных событий, относящихся к событиям тревоги. При просмотре табличных блоков с записями журналов могут использоваться те же функции настройки отображения, как и в основной таблице с записями журнала (сортировка, группировка, выбор колонок и др.).

С помощью команд контекстного меню событий тревоги (такое меню показано на рисунке) можно свернуть или развернуть табличные блоки с записями журналов одновременно для всех событий, отправить список на печать или включить/отключить отображение области описания событий.

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

Для настройки анализа записей и поиска событий тревоги:

1. Загрузите записи журнала (см. стр. 79).
2. Переключите область отображения сведений в режим "Тревоги" с помощью кнопки на панели выбора режимов отображения и поиска.
3. В заголовке вкладки запроса раскройте список для выбора искомых событий тревоги:



В списке представлены события тревоги, поиск которых может выполняться среди загруженных записей. По умолчанию список содержит предустановленные события тревоги общего характера. Такие события нельзя удалить.

4. Сформируйте нужный список событий для поиска. Управление списком осуществляется с помощью инструментов (кнопок) на панели под списком.

Примечание.

Чтобы включить или отключить отображение панели инструментов управления списком, наведите указатель на середину нижней границы списка и нажмите левую кнопку мыши.

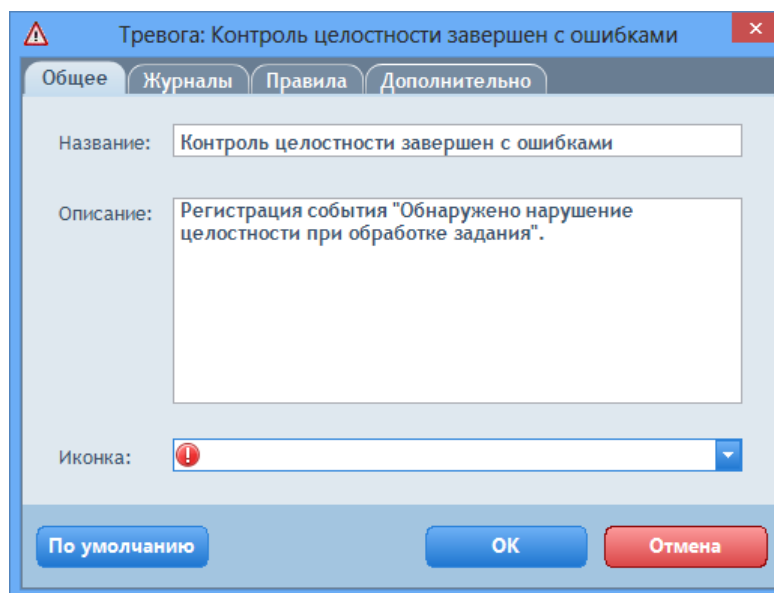
Для формирования списка предусмотрены следующие возможности:

- добавление и удаление событий (с помощью кнопок "Создать" и "Удалить");

- загрузка списка событий, сохраненного в файле (с помощью кнопки "Импорт").
5. Настройте параметры поиска событий. Настройка осуществляется для каждого события в отдельном диалоговом окне. При создании нового события вызов диалогового окна настройки происходит автоматически. Чтобы настроить параметры имеющегося события, выберите его в списке и нажмите кнопку "Редактировать".

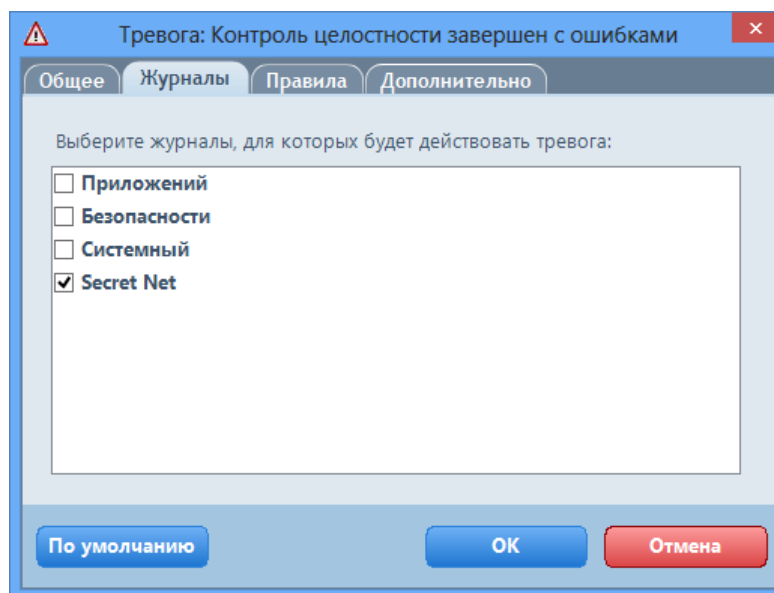
Настройка параметров события осуществляется в следующих вкладках:

- Вкладка "Общее". Пример содержимого вкладки представлен на следующем рисунке.



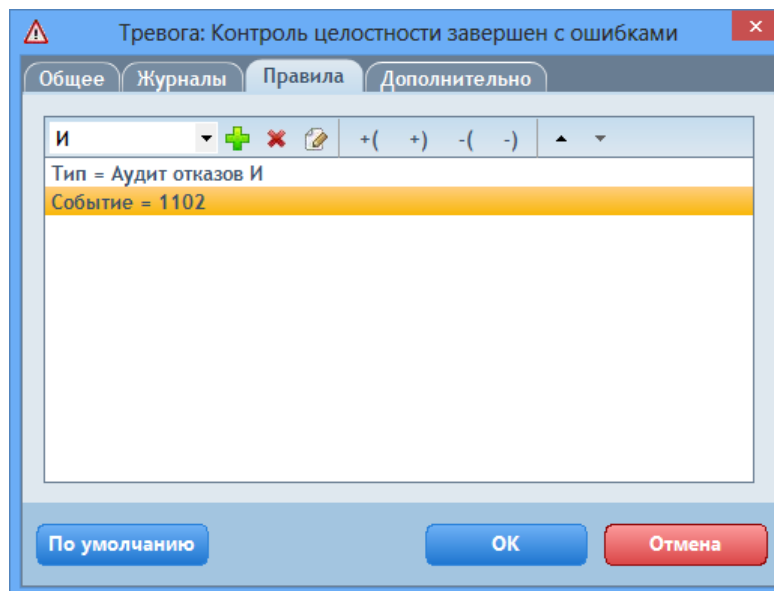
В соответствующих полях укажите название, дополнительные сведения и пиктограмму для события тревоги.

- Вкладка "Журналы". Пример содержимого вкладки представлен на следующем рисунке.



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

- Вкладка "Правила". Пример содержимого вкладки представлен на следующем рисунке.

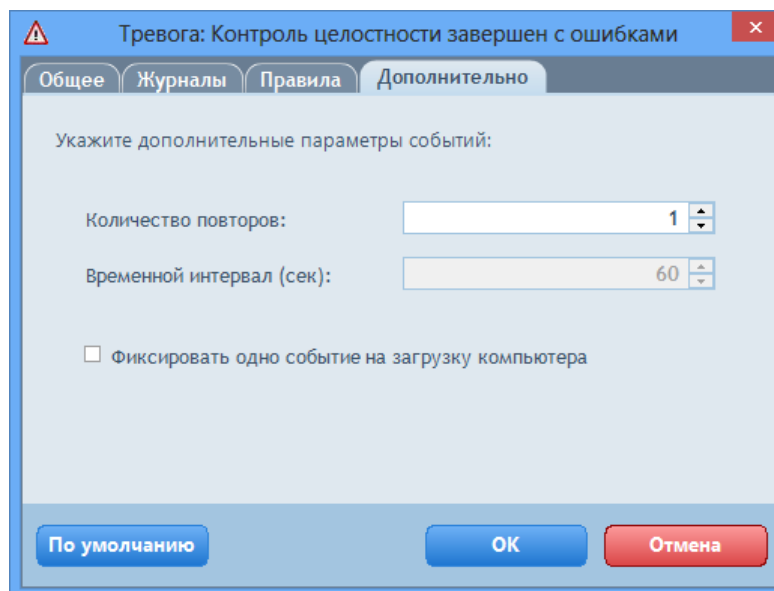


Составьте список условий, которым должны удовлетворять записи для соответствия данному событию тревоги. Условия определяют содержимое полей в записях о событиях или параметров в описаниях событий. Для контроля содержимого поля или параметра в списке должно присутствовать выражение, задающее допустимые значения. Например, для поля "Тип события" 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 события", "Источник" и "Компьютер", чтобы при анализе не рассматривались записи, у которых хотя бы одно из значений в указанных полях не совпадает с заданным.

Для управления списком условий используйте средства панели инструментов в верхней части вкладки. При добавлении или редактировании выражения на экране появляется диалог, в котором необходимо выбрать поле или параметр, указать условие для содержимого и задать значение.

- Вкладка "Дополнительно". Пример содержимого вкладки представлен на следующем рисунке.



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 тревоги для случаев, если при анализе выявляется несколько таких событий за время одного сеанса работы компьютера (к которому относятся записи). За счет этого сокращается список событий тревоги. Данный режим следует использовать, если последовательность событий тревоги в масштабе одной загрузки компьютера не важна. Для включения режима сжатия установите отметку в поле "Фиксировать одно событие на загрузку компьютера".

6. После настройки параметров поиска событий при необходимости сохраните этот список в файл для дальнейшего использования (с помощью кнопки "Экспорт").
7. Отметьте в списке события тревоги, которые следует найти, и нажмите кнопку "Искать" в заголовке вкладки запроса.
После анализа загруженных записей появится список полученных событий тревоги.

Квитирование событий НСД в журнале НСД

Квитирование событий НСД можно выполнять при просмотре сведений в панели событий системы (см. стр. 62) или при работе с журналом НСД в панели "НСД".

Для квитирования событий НСД в запросе с записями журнала НСД:

1. Загрузите записи журнала НСД из БД сервера безопасности (см. стр. 79).
2. В списке записей журнала выделите записи о событиях, которые необходимо квитировать.
3. Вызовите контекстное меню одной из выбранных записей и выберите команду "Квитировать НСД".

На экране появится диалог для ввода текстового комментария.

4. Введите текстовый комментарий с описанием причин и принятых мер по факту НСД и нажмите кнопку "Квитировать".

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

Создание правил фильтрации на основе записей о НСД

При работе с записями журнала НСД можно создавать правила для фильтра НСД аналогично, как при просмотре сведений в панели событий системы (см. стр. 63). В создаваемых правилах автоматически добавляются условия фильтрации на основе сведений о зарегистрированных событиях.

Настройка фильтра НСД для агентов осуществляется на вкладке управления групповыми политиками (см. стр. 41), настройка фильтра для серверов непосредственного подчинения — на вкладке "Фильтр уведомлений о НСД" (см. стр. 52).

Для добавления правила в запросе с записями журнала НСД:

1. Загрузите записи журнала НСД из БД сервера безопасности (см. стр. 79).
2. В списке записей журнала вызовите контекстное меню нужной записи и раскройте подменю "Фильтр НСД".
3. Выберите подменю с нужным типом и размещением фильтра. Фильтр НСД может быть задан в групповых политиках (при наличии возможности изменения политик) и/или в параметрах сервера безопасности.
4. Для выбранного фильтра в открывшемся подменю "Фильтровать по" укажите нужные условия, которые будут добавлены в правило фильтрации. Для

правила можно задать следующие условия на основе сведений о выбранном событии:

- название источника;
- название источника и числовой код категории события;
- название источника, числовой код категории события и числовой идентификатор события.

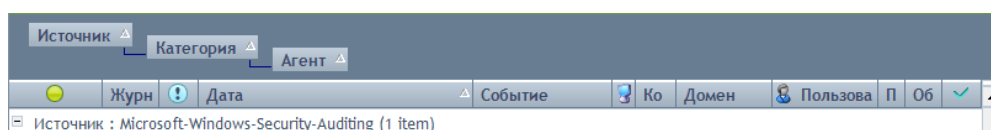
После выбора команды в панели свойств объектов будет открыта соответствующая вкладка, и в списке правил фильтра НСД появится новое правило. Если добавляемое правило может повлиять на применение ранее заданных параметров, перед добавлением на экране появится запрос на выполнение дальнейших действий. В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

Сортировка записей

Отображаемые записи сортируются по значениям, содержащимся в определенных колонках таблицы записей. Сортировка выполняется с использованием команд контекстного меню в строке заголовков колонок.

Записи можно сортировать по значениям отдельных колонок (команды "По возрастанию", "По убыванию") или посредством включения записей в группы с одинаковыми значениями колонок (команда "Группировать по этому полю"). При группировке записей используется комбинированный вид отображения таблицы и иерархических списков с возможностью сворачивания групп. Для управления списком колонок, по которым выполняется группировка, используется область группировки, включение и отключение которой осуществляется с помощью команды "Область группировки".

Пример строки заголовков колонок с областью группировки представлен на следующем рисунке.



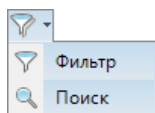
При просмотре записей журнала сервера безопасности сведения о сессиях могут быть представлены отдельными табличными блоками для каждой сессии (по умолчанию) или как единая таблица записей. Переключение вида отображения осуществляется с помощью кнопки "Плоский/сгруппированный вид" в заголовке вкладки запроса. Если сведения представлены отдельными табличными блоками, записи сортируются в группы, соответствующие сессиям. Группы можно сворачивать и раскрывать по отдельности или одновременно (с помощью кнопки "Раскрыть/скрыть записи" в заголовке вкладки запроса).

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, удовлетворяющих заданным параметрам:

1. Загрузите записи журнала и настройте параметры запроса (см. стр. 79).
2. Выберите режим поиска. Для этого раскройте список кнопки "Режим фильтра" в заголовке вкладки запроса и выберите команду "Поиск".

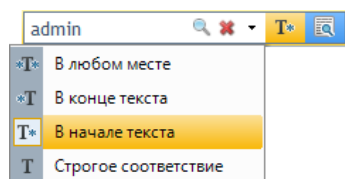


В таблице записей будут выделены все записи, удовлетворяющие заданным параметрам в запросе.

3. Для выполнения переходов между выделенными записями используйте кнопки с изображением стрелок ("Предыдущая" и "Следующая") в заголовке вкладки запроса. Кнопки появляются при наличии записей, удовлетворяющих заданным параметрам в запросе.

Для поиска записей, содержащих текстовую строку:

1. Загрузите записи журнала (см. стр. 79).
2. В панели выбора режимов отображения и поиска введите текстовую строку и укажите условия поиска.



Условия поиска указываются с использованием средств, расположенных справа от раскрывающегося списка введенных строк поиска. Для поиска можно задать следующие условия:

- наличие в искомых словах символов до или после строки поиска — определяется выбранной маской;
- наличие строки поиска в таблице записей или на вкладке с детальным описанием событий — определяется в меню поиска.

В таблице записей будут выделены все записи, содержащие текстовую строку и удовлетворяющие заданным условиям.

3. Для переходов между выделенными записями или снятия выделения используйте кнопки в раскрывающемся списке введенных строк поиска.

Цветовое оформление записей

Для наглядного представления информации предусмотрено цветовое оформление отображаемых записей. Методы цветового оформления различаются в зависимости от типов журналов.

В таблице записей журнала сервера безопасности применяется метод попеременного выделения записей различными цветами по сессиям подключения к серверу. Записи каждой сессии выделяются особым цветом, который отличается от цвета записей других сессий.

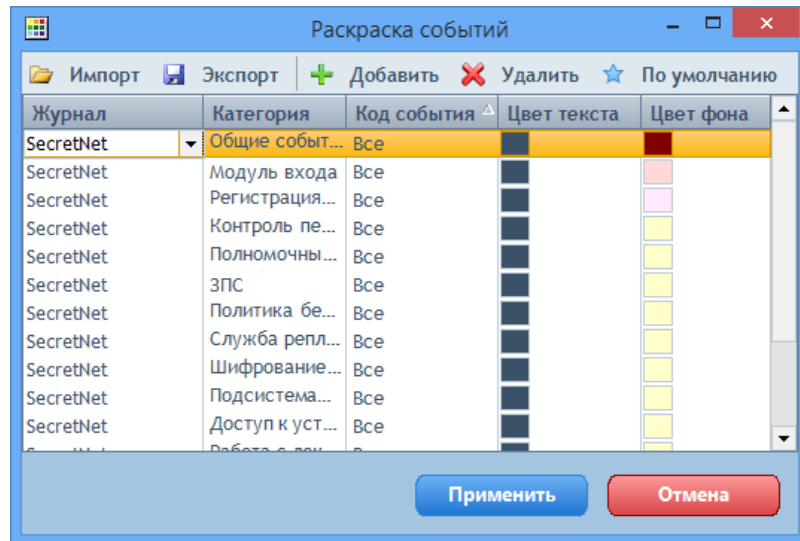
Цветовое оформление записей журналов НСД и журналов станций можно настраивать, устанавливая соответствие цвета текста и фона записей определенным характеристикам событий. При включенном режиме цветового оформления записи выделяются теми цветами, которые заданы при настройке параметров программы.

Для включения режима цветового оформления:

1. Загрузите записи журнала НСД или журнала станций (см. стр. 79).
2. Вызовите контекстное меню любой записи и выберите команду "Раскраска событий".
Записи будут выделены цветами, соответствующими характеристикам событий.
Отключение режима цветового оформления выполняется аналогично.

Для настройки параметров цветового оформления записей:

1. Загрузите записи журнала НСД или журнала станций (см. стр. 79).
2. Вызовите контекстное меню любой записи и выберите команду "Настроить раскраску событий".
На экране появится диалог для настройки параметров.



Диалог содержит список правил цветового оформления записей. Каждое правило определяет цвета для текста и фона, которыми выделяются записи, удовлетворяющие условиям правила.

3. Сформируйте список правил цветового оформления. Для формирования списка предусмотрены следующие возможности:
 - добавление и удаление отдельных элементов (кнопки "Добавить" и "Удалить" в верхней части диалога);
 - загрузка исходного списка правил программы (кнопка "По умолчанию");
 - загрузка списка правил, сохраненного в файле (кнопка "Импорт").
4. В списке правил укажите в соответствующих колонках нужные условия и цвета оформления записей. Для правила могут быть заданы следующие условия:
 - события были зарегистрированы в определенном локальном журнале;
 - события относятся к определенной категории;
 - в записях указан определенный код события.
5. При необходимости сохраните список правил в файл для дальнейшего использования (кнопка "Экспорт").
6. Нажмите кнопку "Применить".

Использование закладок

При просмотре записей можно использовать закладки для быстрого перехода (возврата) к определенным записям в таблице. Закладки представляют собой маркеры, которыми отмечаются нужные записи. Маркеры закладок отображаются в отдельной колонке таблицы записей.

Команды управления закладками сгруппированы в подменю "Закладки" контекстного меню записей. Описание команд представлено в следующей таблице.

Команда	Описание
Поставить	Помечает выбранную запись маркером закладки
Снять	Удаляет закладку для выбранной записи
Следующая	Выполняет переход к следующей записи с закладкой (ниже по списку относительно текущей выбранной записи)
Предыдущая	Выполняет переход к предыдущей записи с закладкой (выше по списку относительно текущей выбранной записи)
Снять все	Удаляет закладки для всех отображаемых записей

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 НСД или журнала станций (см. стр.79).
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

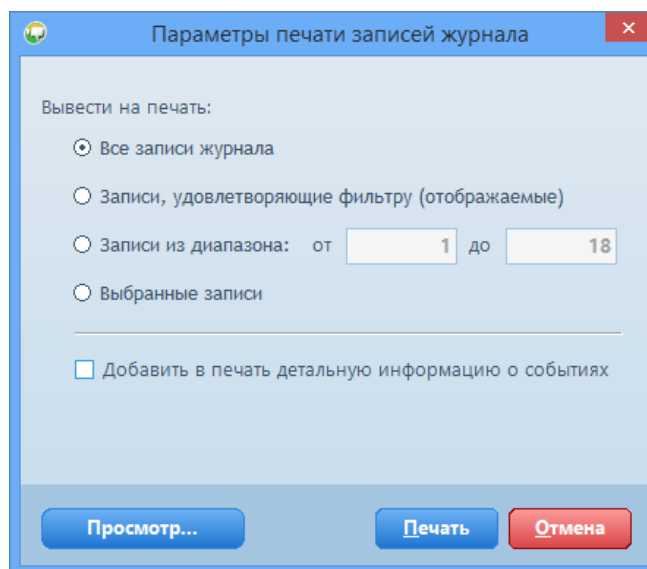
Программа позволяет отправлять на печать записи текущего запроса.

Возможность печати не предусмотрена для записей журнала сервера безопасности.

Для печати записей:

1. Загрузите записи журнала НСД или журнала станций (см. стр.79).
2. Если требуется распечатать часть загруженных записей, выделите нужные записи в таблице или выполните фильтрацию с нужными параметрами (см. стр.86).
3. Вызовите контекстное меню записи (группы выбранных записей) и выберите команду "Печать".

На экране появится диалог настройки параметров.



4. Настройте параметры печати.

Группа полей "Вывести на печать"

Определяет, какие записи будут распечатаны:

- "Все" — выполняется печать всех записей, загруженных в запрос (в том числе тех, которые не удовлетворяют текущим параметрам фильтрации);
- "Записи, удовлетворяющие фильтру (отображаемые)" — выполняется печать записей, отображаемых в соответствии с текущими параметрами фильтрации;
- "Записи из диапазона" — 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;
- "Выбранные записи" — выполняется печать только тех записей, которые выделены в таблице

Поле "Добавить в печать детальную информацию о событиях"

Если установлена отметка, будет распечатано содержимое полей с детальным описанием событий

5. Чтобы открыть окно предварительного просмотра страниц, нажмите кнопку "Просмотр". После просмотра закройте окно.
6. Нажмите кнопку "Печать".
На экране появится диалог ОС Windows для выбора принтера и настройки общих параметров печати.
7. Выберите принтер и нажмите кнопку "ОК".

Экспорт записей

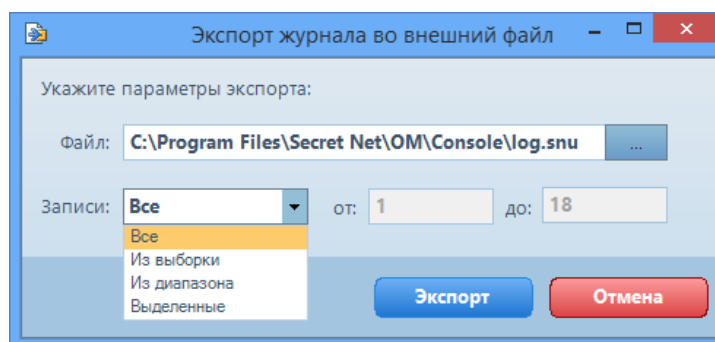
Программа позволяет экспортировать (сохранять) в файлы записи текущего запроса. Экспорт осуществляется в файлы специальных форматов:

- записи журнала НСД — экспортируются в файлы формата *.snu;
- 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. 79).
2. Если требуется экспортировать часть загруженных записей, выделите нужные записи в таблице или выполните фильтрацию с нужными параметрами (см. стр. 86).
3. Вызовите контекстное меню записи (группы выбранных записей) и выберите команду "Экспорт".

На экране появится диалог настройки параметров.



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

Группа полей "Записи"

Определяет, какие записи будут экспортированы:

- "Все" — выполняется экспорт всех записей, загруженных в запрос (в том числе тех, которые не удовлетворяют текущим параметрам фильтрации);
- "Из выборки" — выполняется экспорт записей, отображаемых в соответствии с текущими параметрами фильтрации;
- "Из диапазона" — 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;
- "Выделенные" — выполняется экспорт только тех записей, которые выделены в таблице

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. 36).

При работе с программой в режиме мониторинга и централизованного аудита можно выполнить запуск процесса внеочередного архивирования централизованных журналов. Команда архивирования применяется к серверу безопасности, с которым установлено соединение программы.



Внимание!

Чтобы выполнять архивирование и очистку журналов, пользователю должна быть предоставлена привилегия "Архивировать/восстанавливать журналы".

Для запуска процесса архивирования журналов:

1. В диаграмме управления или в панели свойств 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

Приложение

Пиктограммы защитных механизмов

Пиктограмма	Описание
 (затененное изображение)	Драйвер механизма отключен
 (затененное изображение компьютера)	Драйвер механизма включен, но механизм не функционирует — требуется включить механизм и установить "жесткий" или "мягкий" режим работы
 (синяя подсветка экрана и контура)	Механизм защиты функционирует
	Механизм защиты не активирован (требуется регистрация лицензии) или обнаружен сбой в работе защитного механизма

Параметры сетевого взаимодействия

Наименование параметра, пояснение	Диапазон
Время ожидания разрешения имен DNS Значение "0" соответствует бесконечному времени ожидания	30–1000 с
Время ожидания соединения с сервером	30–1000 с
Время ожидания отправки запроса на сервер	30–1000 с
Время ожидания 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
Время ожидания события 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
Время ожидания сервером ответа на контрольный запрос Определяет максимальное время ожидания ответа на отправленный контрольный запрос. Параметр предназначен для контроля установленного соединения	30–1000 с
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
Размер блока 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

Редактирование списков устройств и принтеров в групповых политиках

Управление списком устройств

В списке устройств групповой политики можно добавлять сведения о конкретных устройствах. Это позволяет задать параметры для устройства централизованно или локально, если устройство ранее не подключалось к компьютеру или по каким-либо причинам отсутствует в списке.

Предусмотрены следующие способы добавления устройств:

- добавление с помощью мастера импорта устройств;
- вставка из буфера обмена.



Внимание!

При добавлении устройства копируются заданные для него параметры контроля и доступа. Однако в некоторых случаях параметрам могут быть присвоены значения по умолчанию, если получение прежних значений технически невозможно. После добавления устройства обязательно проверьте заданные для него параметры и при необходимости откорректируйте их.

Использование мастера импорта устройств

Мастер импорта предоставляет следующие возможности:

- импорт устройства из файла, в котором сохранены (экспортированы) сведения об устройстве. Экспорт сведений об устройствах можно выполнить в стандартных оснастках управления групповыми политиками (см. документ [3]), в программе просмотра локальных журналов (см. документ [5]) или в списке устройств групповой политики другого уровня (см. ниже);
- добавление стандартного устройства из предопределенного списка (например, порт ввода/вывода).

Для импорта устройств в список групповой политики:

1. Вызовите контекстное меню в любом месте списка устройств групповой политики и выберите команду "Добавить устройство".
На экране появится стартовый диалог мастера импорта устройств.
2. Выберите вариант добавления устройства, нажмите кнопку "Далее >" и следуйте инструкциям мастера.

Экспорт сведений об устройствах из списка устройств

Сведения об устройствах, присутствующих в списке групповой политики, можно экспортировать в файлы. Экспорт осуществляется в файлы специального формата описания устройств системы Secret Net (*.sndev). Содержимое файлов в дальнейшем можно импортировать с помощью мастера импорта (см. выше).

Примечание.

Экспорт в файл формата *.sndev поддерживается только для устройств и моделей.

Для экспорта сведений:

1. Вызовите контекстное меню нужного устройства или модели и выберите команду "Экспорт".
На экране появится стандартный диалог сохранения файла ОС Windows.
2. Укажите имя файла для сохранения сведений.

Использование буфера обмена для добавления устройств

Сведения об устройстве можно скопировать в буфер обмена из следующих источников:

- список устройств групповой политики другого уровня;

- запись журнала Secret Net о событии подключения или запрета подключения устройства.

Методы использования буфера обмена для копирования и добавления устройств в список групповой политики являются стандартными для ОС Windows.

Копирование сведений об устройстве в буфер обмена из записи журнала Secret Net выполняется с помощью команды в контекстном меню записи журнала.

Удаление устройств

При необходимости удалить устройство из списка групповой политики вызовите контекстное меню устройства и выберите команду "Удалить".

Управление списком принтеров

В список принтеров групповой политики можно добавлять элементы, соответствующие конкретным принтерам. Добавление осуществляется с помощью специальной программы-мастера.

Использование мастера добавления принтеров

Мастер добавления предоставляет следующие возможности:

- добавление принтера, подключенного к выбранному компьютеру;
- добавление принтера, подключение к которому осуществляется по сети (сетевой принтер);
- добавление принтера по введенным именам компьютера и принтера.

Для добавления принтера в список групповой политики:

1. Вызовите контекстное меню в любом месте списка принтеров групповой политики и выберите команду "Добавить принтер".

На экране появится стартовый диалог мастера добавления принтеров.

2. Выберите вариант добавления принтера, нажмите кнопку "Далее >" и следуйте инструкциям мастера.

Удаление принтеров

При необходимости удалить принтер из списка групповой политики вызовите контекстное меню принтера и выберите команду "Удалить".

Восстановление журналов из архивов

Записи централизованных журналов, помещенные в архив из БД сервера безопасности, могут быть снова восстановлены в базе данных сервера. Процедура восстановления выполняется при работе с программой в режиме мониторинга и централизованного аудита. 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 "Архивировать/восстанавливать журналы".

Для восстановления записей из архива:

1. В диаграмме управления или в панели свойств 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".

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 | 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.

Документация

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