Код Безопасности

Средство защиты информации

SECRET NET 7

Руководство администратора

Локальная работа с журналами регистрации

RU.88338853.501410.015 91 5

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

Оглавление

Список сокращений

CRC	Cyclic Redundancy Check
DNS	Domain Name System
RTF	Reach Text Format
SID	Security Identifier
USB	Universal Serial Bus
БД	База данных
ЗПС	Замкнутая программная среда
КЦ	Контроль целостности
НСД	Несанкционированный доступ
ОС	Операционная система
ОУ	Оперативное управление
ПО	Программное обеспечение
РС	Рабочая станция
СБ	Сервер безопасности
СЗИ	Средство или система защиты информации
ЭЦП	Электронная цифровая подпись

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 возможностях использования программы просмотра локальных журналов.

Перед изучением данного руководства необходимо ознакомиться с документами [**1**] и [**3**].

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 в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training-courses/. Связаться по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Глава 1
Общие сведения о регистрации событий на рабочей станции

Локальные журналы регистрации событий

События, происходящие в системе, регистрируются в соответствующих журналах. Сведения о событиях сохраняются в виде записей, содержащих подробную информацию для анализа событий.

Журнал Secret Net

В журнале событий системы Secret Net (далее — журнал Secret Net) накапливается информация о событиях, регистрируемых на компьютере средствами системы защиты.

Сведения, содержащиеся в журнале Secret Net, позволяют контролировать работу механизмов защиты (защита входа в систему, контроль аппаратной конфигурации, контроль целостности и др.). Подробное описание регистрируемых событий приведено в документе [**3**].

Состав регистрируемых событий определяется заданными параметрами действующей политики безопасности.

В журнале Secret Net используется такой же формат данных и состав полей записей, как и в штатных журналах ОС Windows. Для локальной работы с записями журнала используется программа просмотра локальных журналов системы Secret Net.

Штатные журналы ОС Windows

В штатных журналах ОС Windows регистрируются только те события, которые имеют отношение к операционной системе. Под "штатными журналами" понимаются следующие журналы:

- журнал приложений — содержит сведения об ошибках, предупреждениях и других событиях, возникающих при работе приложений;
- системный журнал — содержит сведения об ошибках, предупреждениях и других событиях, возникающих в операционной системе;
- журнал безопасности — хранит информацию о доступе пользователей к компьютеру, применении групповых политик и изменении прав доступа, а также о событиях, связанных с использованием системных ресурсов.

Примечание.
Описание содержимого штатных журналов ОС Windows и процедур настройки регистрации событий см. в документации к операционной системе.

Компоненты системы Secret Net не осуществляют регистрацию событий в штатных журналах (за исключением журнала приложений, в котором могут регистрироваться некоторые специфические ошибки, связанные с функционированием ОС).

Программа просмотра локальных журналов позволяет осуществлять загрузку и просмотр записей штатных журналов, хранящихся на компьютере локально. При этом сохраняется возможность загрузки записей в другие средства работы с журналами ОС Windows.

Хранилище теневого копирования

В хранилище теневого копирования помещаются дубликаты (копии) данных, выводимых на отчуждаемые носители информации. Хранилище дубликатов представляет собой специально организованное место в системной папке на локальном диске компьютера. Средства работы с хранилищем обеспечивают бесперебойную запись информации и выполнение различных служебных операций с содержимым (например, поиск, очистка хранилища и др.).

Доступ к хранилищу теневого копирования осуществляется в программе просмотра локальных журналов. При этом учитываются права доступа пользователя: если предоставлены привилегии для просмотра журналов — пользователь получит доступ к хранилищу только для чтения. При наличии привилегий на управление журналами можно совершать административные операции с хранилищем.

Размер хранилища и методы его заполнения определяются заданными параметрами действующей политики безопасности.

Реализация поиска в хранилище

В программе просмотра журналов предусмотрена возможность поиска в хранилище теневого копирования. Функция поиска реализована с использованием компонента Windows Search, в котором для ускорения процесса поиска применяется индекс — база с подробными сведениями о файлах на компьютере. Формирование актуального индекса происходит при периодическом индексировании файлов. Запуск индексирования хранилища теневого копирования осуществляется автоматически в определенные моменты времени.

Новые файлы, поступившие в хранилище теневого копирования, могут отсутствовать в индексе на момент поиска. Поэтому если поиск не дал результатов, это может быть связано с отсутствием новых файлов в индексе. В программе просмотра журналов предусмотрена возможность принудительного запуска процесса индексирования хранилища.

Особенности поиска по именам файлов

При сохранении дубликата в хранилище теневого копирования для файла генерируется новое внутреннее имя на основе его контрольной суммы и метки времени. Расширение файла не меняется, но оно может быть удалено при достижении ограничения на максимальную длину имени файла.

Имя файла дубликата в хранилище теневого копирования и исходное имя файла сопоставляются в записи о событии теневого копирования. Таким образом, с помощью записи журнала можно восстановить файл в том виде, в каком был осуществлен его вывод на отчуждаемый носитель.

При поиске по именам файлов в хранилище теневого копирования рассматриваются внутренние, а не исходные имена файлов. Если требуется выполнить поиск по исходным именам файлов, для этого следует воспользоваться средствами поиска по записям журнала Secret Net — исходные имена файлов указаны в описаниях событий категории "Теневое копирование".

Особенности поиска по содержимому файлов

Компонент Windows Search, на базе которого реализован поиск в хранилище теневого копирования, по умолчанию поддерживает широкий спектр типов файлов для поиска по содержимому. Например, поиск по наличию слова или фразы выполняется в файлах с расширениями txt, htm, html, xml, а также в документах, сохраненных в приложениях пакета Microsoft Office (до версии Microsoft Office 2003 включительно).

Примечание.
Полный перечень типов и форматов файлов, поддерживаемых компонентом Windows Search, приведен на сайте компании Microsoft.

Список типов и форматов файлов, поддерживаемых компонентом Windows Search для поиска по содержимому, расширяется при установке клиентского ПО системы Secret Net. Кроме того, в состав установочного компакт-диска системы включены программы установки некоторых дополнительных системных фильтров Microsoft для встраивания в компонент (в частности, фильтры для документов пакета Microsoft Office 2010). Программы установки размещены в каталоге \Tools\Microsoft\WinSearch Filters.

Другие производители программного обеспечения также распространяют на платной или бесплатной основе собственные системные фильтры, обеспечивающие поиск по содержимому в файлах специфических форматов. Дополнительные системные фильтры могут встраиваться и при установке некоторых приложений. Например, при установке программы Adobe Acrobat Reader в системе регистрируется фильтр, позволяющий выполнять поиск по содержимому PDF-файлов.

Хранение и очистка локальных журналов

При регистрации событий записи о них помещаются в соответствующие локальные журналы (штатные журналы ОС Windows и журнал Secret Net) и хранятся на компьютере локально. 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).

В сетевом режиме функционирования системы Secret Net 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.

В автономном режиме функционирования журналы могут храниться только в локальном хранилище.

По мере регистрации событий записи журналов в локальном хранилище могут замещаться новыми записями. Перезапись информации в журналах осуществляется в соответствии с заданными параметрами регистрации событий. Описание процедур настройки параметров регистрации событий в журнале Secret Net см. в документе [**3**].

В программе просмотра локальных журналов пользователь может выполнять экспорт записей журналов в файлы. При этом также осуществляется и экспорт файлов из хранилища теневого копирования, относящихся к экспортируемым записям. Если пользователю предоставлена соответствующая привилегия, он может выполнять и очистку журналов. При очистке журнала из локального хранилища удаляются все записи или выбранная часть записей.

Одновременно с удалением записей журнала Secret Net происходит очистка хранилища теневого копирования — из хранилища удаляются файлы, которые были помещены туда при регистрации соответствующих событий.

Глава 2
Начало работы с программой просмотра локальных журналов

Запуск программы

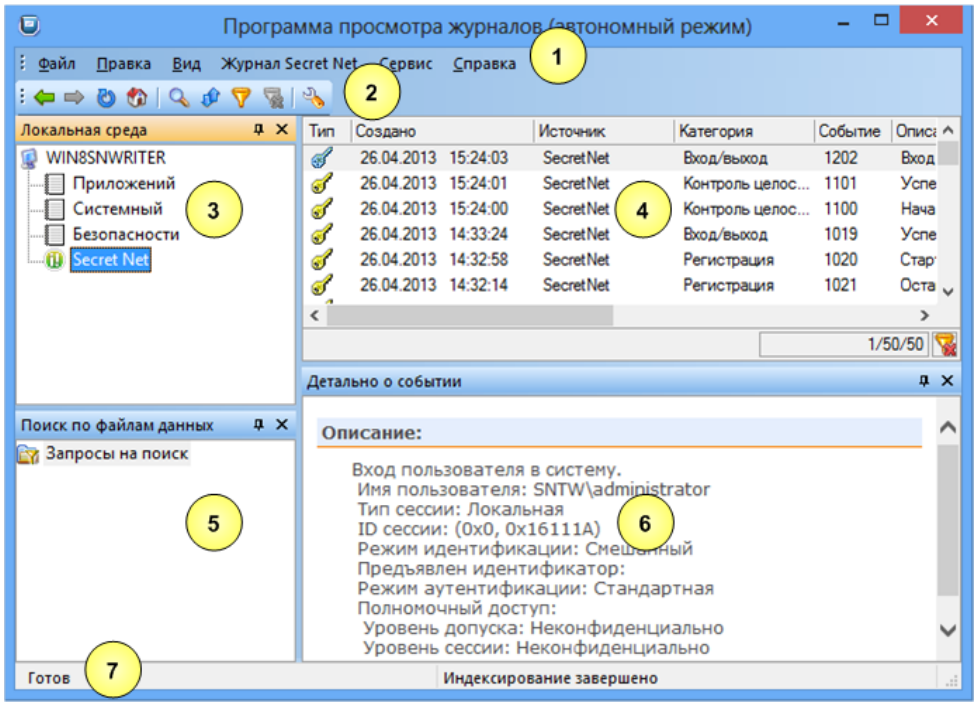
Программа просмотра локальных журналов устанавливается на компьютере при установке клиентского ПО системы Secret Net. Для работы с программой пользователю должны быть предоставлены соответствующие привилегии (описание процедуры предоставления привилегий см. в документе [**3**]).

Для запуска программы:

- 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 "Журналы" (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 | Журналы".

Интерфейс программы

Пример внешнего вида основного окна программы просмотра локальных журналов представлен на следующем рисунке.



Пояснение.
На рисунке обозначены: 1 — меню; 2 — панель инструментов; 3 — окно структуры; 4 — область отображения записей; 5 — окно запросов на поиск по файлам данных; 6 — окно дополнительных сведений; 7 — строка сообщений.

Пользователь может изменять состав отображаемых элементов и их расположение на экране (см. стр.**10**). Параметры внешнего вида основного окна

сохраняются в системном реестре компьютера и используются в следующих сеансах работы пользователя с программой.

При работе с большими объемами данных можно использовать средства навигации по структурам и средства настройки отображения таблиц (см. стр.**13**).

Основное окно программы может содержать следующие элементы интерфейса:

Меню
Содержит команды управления программой
Панель инструментов
Содержит кнопки быстрого вызова команд управления и программных средств
Информационный заголовок
Отображает название программы и имя выбранного элемента структуры (имя защищаемого компьютера, название журнала и пр.)
Окно структуры
Содержит список, состоящий из журналов компьютера и журналов, загруженных в программу из файлов. Окно используется для выбора журнала
Область отображения записей
Отображает записи выбранного журнала или запроса в табличной форме. Строки таблицы можно скопировать в буфер обмена, используя стандартные способы. Для отображения сведений о записи в виде списка полей наведите указатель мыши на нужную строку таблицы — через 1–2 секунды появится всплывающее окно. В зависимости от характеристик событий записи могут выделяться различными цветами. Настройка цветового оформления записей осуществляется при настройке параметров программы. В нижней части области отображения записей могут располагаться следующие элементы: • сведения о количестве записей в виде <*номер выбранной записи*>/ <*количество отображаемых записей*>/<*общее количество загруженных записей*>; • индикатор включения/отключения фильтрации  (см. стр.**16**). Красный крестик на пиктограмме означает, что фильтрация отключена. При выборе в окне структуры защищаемого компьютера в области просмотра отображается сводная информация о журналах этого компьютера, которые уже загружались в текущем сеансе работы с программой. Специальные ссылки позволяют выбрать журнал для загрузки записей или выполнить оперативную фильтрацию загруженных записей (см. стр.**16**)
Окно запросов на поиск
Содержит список запросов для поиска по файлам данных в хранилище теневого копирования. Результатом поиска являются записи журнала Secret Net, относящиеся к найденным файлам. Список записей выводится в области отображения записей при выборе запроса
Окно дополнительных сведений
Содержит подробную информацию о событии. Отображаемые сведения относятся к текущей выбранной записи. Содержимое окна можно скопировать в буфер обмена, используя стандартные способы
Строка сообщений
Отображает служебные сообщения программы, состояние индексирования хранилища теневого копирования, а также краткие подсказки к командам и кнопкам панели инструментов

Настройка элементов интерфейса

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

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

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

Состав отображаемых элементов интерфейса настраивается командами меню "Вид", которые перечислены в следующей таблице.

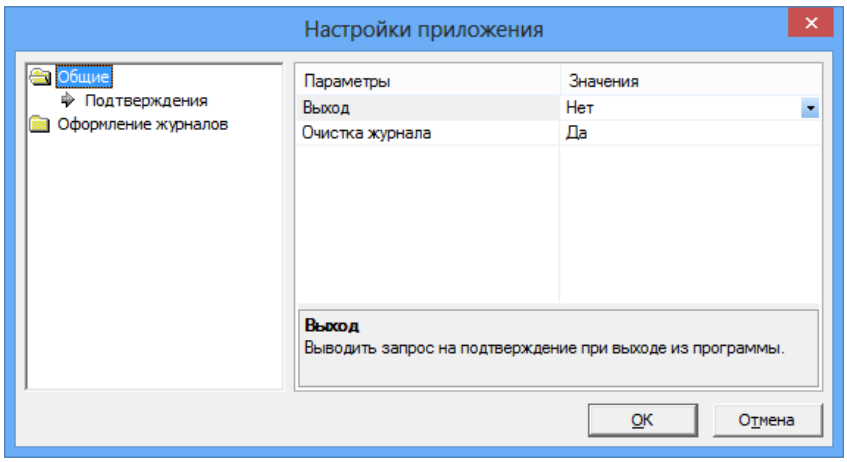
Команда	Описание
Вид | Строка статуса	Включает или отключает отображение строки сообщений
Вид | Панели | Кнопки	Включает или отключает отображение панели инструментов
Вид | Панели | Заголовок	Включает или отключает отображение информационного заголовка
Вид | Панели | Структура	Включает или отключает отображение окна структуры
Вид | Панели | Запросы на поиск	Включает или отключает отображение окна запросов на поиск по файлам данных
Вид | Панели | Детально о событии	Включает или отключает отображение окна дополнительных сведений

Настройка параметров работы программы

Для настройки параметров:

1. Выберите команду "Сервис | Настройки…".

   На экране появится диалог "Настройки приложения".



2. Последовательно выбирая названия групп из списка в левой части диалога, укажите необходимые значения параметров (параметры представлены в правой части).

Группа параметров "Общие | Подтверждения"

Содержит параметры подтверждения выполняемых операций. Если установлено значение "Да", при выполнении данной операции будет выводиться диалог запроса для подтверждения операции.

Группа параметров "Оформление журналов | Общие"

Содержит общие параметры оформления записей. Для параметров цветового оформления таблиц текущий выбранный цвет представлен в ячейке со значением параметра. Изменение цвета осуществляется стандартными средствами, для вызова которых используется кнопка в правой части ячейки.

Текст
Определяет цвет текста записей
Фон
Определяет цвет фона записей. Заданный фон используется, если отключены режимы цветового оформления записей. Для удобства просмотра четные строки в таблице будут отображаться на более светлом фоне по сравнению с заданным цветом
Тип текстом
Если установлено значение "Да", в поле "Тип" отображаются названия типов событий ("Аудит успехов" и пр.). Перечень предусмотренных пиктограмм и названий типов событий приведен на стр.**27**
Раскраска по типам
Определяет режим цветового оформления фона записей в зависимости от типов событий. Если установлено значение "Да", фон записей соответствует цветам, которые заданы для расположенных ниже параметров с названиями "Информация", "Предупреждение" и т. п. Для журнала Secret Net данный режим действует, если параметру "Раскраска по категориям" группы "Оформление журналов | Secret Net" присвоено значение "Нет". Для оперативного переключения режима цветового оформления записей в зависимости от типов событий используйте команду "Сервис | Типы событий"
Порядок отображения
Если установлено значение "С конца списка", новые записи добавляются в конец (нижнюю часть) списка записей. При необходимости можно включить отображение новых записей в верхней части списка — для этого установите значение "С начала списка". Для оперативного переключения режима используйте соответствующую команду в меню "Сервис | Порядок отображения"

Группа параметров "Оформление журналов | Secret Net"

Содержит параметры цветового оформления фона записей журнала Secret Net. Для параметров цветового оформления таблиц текущий выбранный цвет представлен в ячейке со значением параметра. Изменение цвета осуществляется стандартными средствами, для вызова которых используется кнопка в правой части ячейки.

Раскраска по категориям
Определяет режим цветового оформления фона записей в зависимости от категорий событий. Если установлено значение "Да", фон записей журнала соответствует цветам, которые заданы для параметров с названиями категорий (все остальные параметры группы). Если установлено значение "Нет", то действует режим цветового оформления записей, заданный параметром "Раскраска по типам" группы "Оформление журналов | Общие". Для оперативного переключения режима цветового оформления записей в зависимости от типов событий используйте команду "Сервис | Категории Secret Net"

Средства для работы со списками объектов

Навигация при работе со структурами объектов

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

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

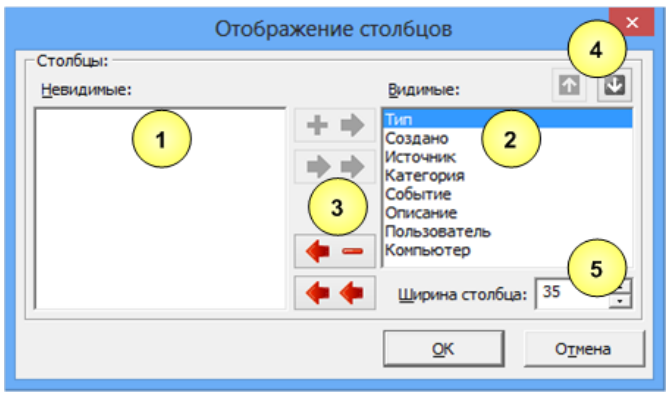
Настройка отображения колонок в таблицах

В программе просмотра локальных журналов можно настраивать отображение таблиц со списками записей, устанавливая ширину колонок, их порядок и состав. Управление колонками можно осуществлять с использованием заголовков колонок или в диалоге настройки.

Для управления колонками с помощью диалога настройки:

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

   На экране появится диалог настройки параметров отображения колонок:



Пояснение.
На рисунке обозначены: 1 — список колонок, не отображаемых в таблице; 2 — список отображаемых колонок; 3 — кнопки перемещения из списка в список; 4 — кнопки формирования порядка следования колонок; 5 — поле ввода ширины выбранной колонки (в пикселях).

2. Настройте параметры отображения колонок.

Для восстановления исходного состояния таблицы:

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

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

Глава 3
Загрузка и просмотр записей журналов

Загрузка записей в программу

Для работы с записями журналов необходимо выполнить загрузку записей в программу. Предусмотрены следующие способы загрузки записей:

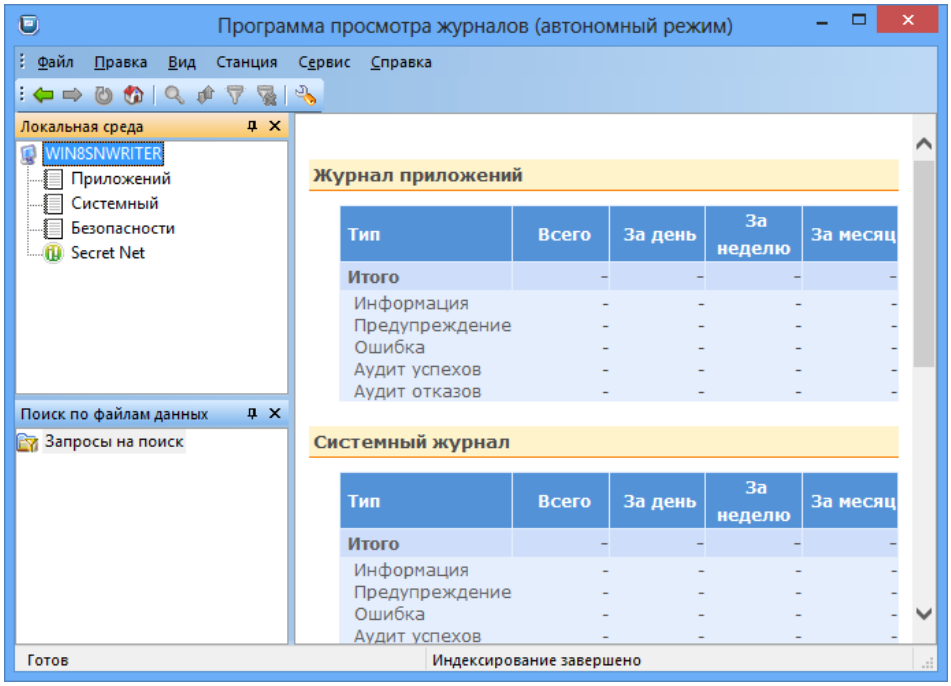
- загрузка записей журналов, хранящихся на компьютере локально;
- загрузка записей из файлов;
- загрузка результатов поиска по файлам данных в хранилище теневого копирования.

Загрузка записей журнала

Для выбора журнала:

1. В окне структуры выберите корневой элемент (имя компьютера).

   В области отображения записей появится сводная информация о журналах:



2. Выберите нужный журнал одним из следующих способов:
   - в окне структуры выберите название журнала;
   - в области отображения записей, где представлена сводная информация о журналах, выберите ссылку-заголовок с названием журнала.

Загрузка записей из файла

Программа просмотра локальных журналов позволяет выполнять загрузку записей из файлов следующих форматов:

- стандартный формат журналов событий ОС Windows (файлы *.evt*);
- формат декодированного хранения записей (файлы *.dvt).

Файлы указанных форматов могут быть созданы в программе просмотра журналов (см. стр.22).

Для загрузки записей:

1. Выберите журнал (см. стр.14), тип которого соответствует записям, хранящимся в файле.

   Пример.
   Если в файле хранятся записи журнала Secret Net, выберите журнал Secret Net.

2. В окне структуры вызовите контекстное меню выбранного журнала и выберите команду "Открыть файл журнала...".

   На экране появится диалог настройки параметров загрузки.

3. В поле "Путь к файлу" введите полное имя файла, при необходимости укажите дополнительные параметры загрузки и нажмите кнопку "ОК".

Отображаемое имя
Определяет имя, под которым группа загруженных записей будет представлена в списке журналов
Тип журнала
Определяет тип журнала, записи которого сохранены в файле: один из штатных журналов ОС Windows (журнал приложений, системный или журнал безопасности) или журнал Secret Net. Тип журнала должен соответствовать хранящимся в файле записям, иначе после загрузки записей возможно некорректное отображение данных. По умолчанию указан тип выбранного журнала

По завершении процесса загрузки записи появятся в окне программы. Заданное имя группы загруженных записей будет представлено в виде отдельного элемента в списке журналов компьютера. Для вызова диалога с основными сведениями о файле выберите добавленный элемент и в меню программы выберите команду "Внешний журнал | Свойства...".

Записи, загруженные из файла, не выгружаются из программы просмотра до окончания сеанса работы с ней. Чтобы выгрузить записи, выберите в окне структуры эту группу записей и в меню программы выберите команду "Внешний журнал | Закрыть...".

Загрузка результатов поиска по файлам данных

Программа просмотра позволяет выполнять поиск по файлам данных в хранилище теневого копирования. Поиск осуществляется с помощью запросов, настроенных с нужными критериями отбора.

Если в хранилище найдены файлы, удовлетворяющие заданным критериям, программа загружает из журнала Secret Net записи о событиях теневого копирования, которые относятся к найденным файлам.

Настройка параметров запроса осуществляется в специальном диалоговом окне.

Внимание!
Перед поиском рекомендуется проверить состояние индексирования хранилища теневого копирования. Текущий статус индексирования отображается в строке сообщений. Если требуется выполнить индексирование для актуализации с содержимым хранилища (при поступлении новых файлов в хранилище), выберите в меню "Сервис" команду "Индексировать хранилище".

Для создания нового запроса на поиск:

1. В окне "Поиск по файлам данных" вызовите контекстное меню любого элемента и выберите команду "Новый...".

   На экране появится диалоговое окно настройки параметров запроса.

2. Настройте параметры запроса (см. стр.19) и нажмите кнопку "ОК".

Для созданных запросов вызов диалогового окна настройки осуществляется с помощью команд "Изменить и обновить" или "Свойства" в контекстном меню запроса.

Фильтрация записей

Программа позволяет фильтровать загруженные записи для отображения нужной информации.

Оперативная фильтрация

Из загруженных записей журнала можно исключить ненужные сведения и оперативно отобразить записи о событиях, имеющих определенный тип и зарегистрированных в течение некоторого промежутка времени (за день, неделю или месяц).

Для оперативной фильтрации записей:

1. После загрузки записей журнала в окне структуры выберите корневой элемент (имя компьютера).

   В области отображения записей появится сводная информация о журналах. Конкретные сведения (количество событий) указаны для тех журналов, которые были загружены в текущем сеансе работы с программой.

2. Перейдите к сведениям о нужном журнале.

   Сводная информация о записях журнала представлена в виде таблицы. В строках указаны типы событий, а в столбцах — интервалы времени: за текущий день, за текущую неделю (начиная с понедельника) и за текущий месяц (начиная с первого числа). Ячейки содержат количество событий. Значения в ячейках являются ссылками, с помощью которых осуществляется отбор записей по соответствующим условиям.

3. Выберите ссылку в ячейке, определяющей нужные условия отбора.

В области отображения записей появятся записи, удовлетворяющие условию отбора. Параметры действуют до выполнения следующей фильтрации или до отключения режима фильтрации (см. стр.**17**).

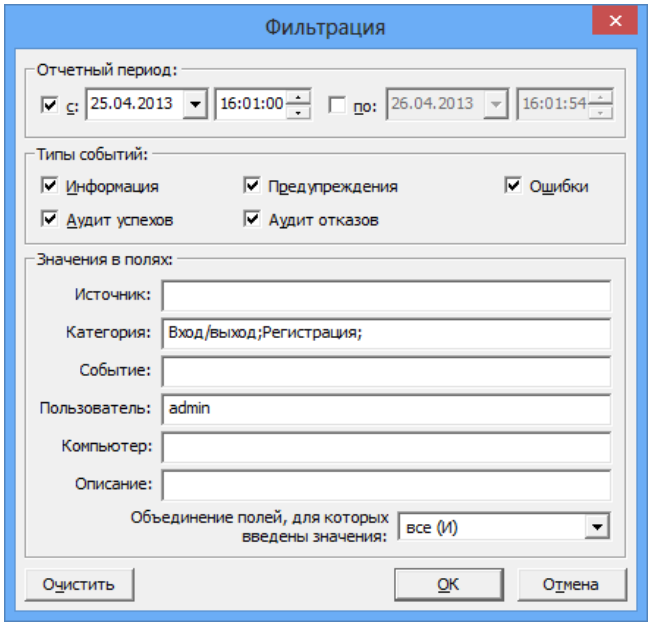
Фильтрация по заданным параметрам

Настроить параметры фильтрации можно в специальном диалоге программы. Заданные параметры применяются к записям текущего выбранного журнала или запроса на поиск по файлам данных.

Для фильтрации записей:

1. Выберите нужный журнал или запрос на поиск по файлам данных.
2. Выберите команду "Правка | Фильтр".

   На экране появится диалог настройки параметров фильтрации.



3. Настройте параметры фильтрации и нажмите кнопку "ОК".

Группа полей "Отчетный период"
Поля группы определяют интервал времени. Фильтру будут удовлетворять записи, которые были зарегистрированы в указанных границах временного интервала
Группа полей "Типы событий"
Поля группы определяют типы событий, которые будут удовлетворять фильтру
Группа полей "Значения в полях"
Поля группы определяют искомое текстовое содержимое. Фильтрация осуществляется по наличию или отсутствию заданных строк в соответствующих полях без учета регистра. Полю "Описание" соответствуют сведения о событии, отображаемые в окне дополнительных сведений. При вводе нескольких строк в одном поле их необходимо разделять символом ";" (только символ, без пробела). Заданная строка может являться частью содержимого поля записи. Например, если в поле "Пользователь" введено значение "admin", при фильтрации будут учитываться имена пользователей admin и administrator. Фильтру будут удовлетворять записи в зависимости от выбранного условия в поле "Объединение полей, для которых введены значения": • "все (И)" — все поля в записях должны включать заданные строки; • "хотя бы один из (ИЛИ)" — хотя бы одна из заданных строк должна присутствовать в записях; • "ни одного из (ИЛИ-НЕ)" — все заданные строки должны отсутствовать в записях

После применения параметров фильтрации в области отображения записей появятся записи, удовлетворяющие заданным условиям отбора.

Пример.

В соответствии с представленным примером настройки параметров будут загружены записи, удовлетворяющие следующим условиям фильтрации:

- поле "Пользователь" содержит подстроку "admin";
- поле "Категория" содержит название категории "Вход/выход" или "Регистрация".

Отключение режима фильтрации

Режим фильтрации отключается отдельно для каждого журнала или запроса на поиск по файлам данных. Чтобы отключить фильтрацию записей, выберите команду "Правка | Все события".

Сортировка отображаемых записей

Отображаемые записи сортируются по значениям, содержащимся в колонках таблицы записей. В заголовке колонки, по которой отсортирована таблица, указывается соответствующее направление сортировки.

В дополнение к стандартным методам сортировки таблиц можно выполнять сортировку по заданным параметрам.

Для сортировки по заданным параметрам:

1. Выберите нужный журнал или запрос на поиск по файлам данных и выберите команду "Правка | Сортировка...".

   На экране появится диалог настройки параметров сортировки.
2. В группе полей "Сортировать" выберите в поле "По столбцу" название колонки, по содержимому которой необходимо выполнить сортировку (названия колонок упорядочены по алфавиту). Отметьте нужное направление сортировки.
3. Если требуется дополнительная сортировка по содержимому другой колонки, настройте параметры в группе полей "Затем".
4. Нажмите кнопку "ОК".

Примечание.
При сортировке по двум колонкам сначала сортируются значения первой колонки, затем записи с одинаковыми значениями в этой колонке сортируются по второй выбранной колонке.

Поиск в отображаемых записях

Программа позволяет выполнить поиск записей, удовлетворяющих заданным параметрам. Поиск осуществляется только среди отображаемых записей.

Для поиска записей:

1. Выберите нужный журнал или запрос на поиск по файлам данных.
2. Выберите в меню команду "Правка | Поиск...".

   На экране появится диалог для настройки параметров поиска.
3. Настройте параметры поиска. Параметры настраиваются аналогично, как при настройке параметров фильтрации — см. стр.**16**.
4. Определите направление поиска. По умолчанию поиск осуществляется в сторону последней (нижней) записи. Для поиска в обратном направлении отметьте поле "Искать вверх".
5. Нажмите одну из кнопок для запуска процесса поиска:

Кнопка	Описание
Найти	Выполняет переход к следующей записи, удовлетворяющей заданным параметрам поиска
Пометить все	Выделяет все записи, удовлетворяющие заданным параметрам поиска

Обновление записей

При обновлении записей происходит новая загрузка записей из журнала (журналов) в программу просмотра. Это позволяет загрузить для просмотра записи, помещенные в журналы после предыдущей загрузки, или применить другие критерии после их изменения в запросе на поиск по файлам данных.

Чтобы обновить записи, выберите команду "Обновить" в контекстном меню журнала или запроса на поиск по файлам данных.

Использование запросов на поиск по файлам данных

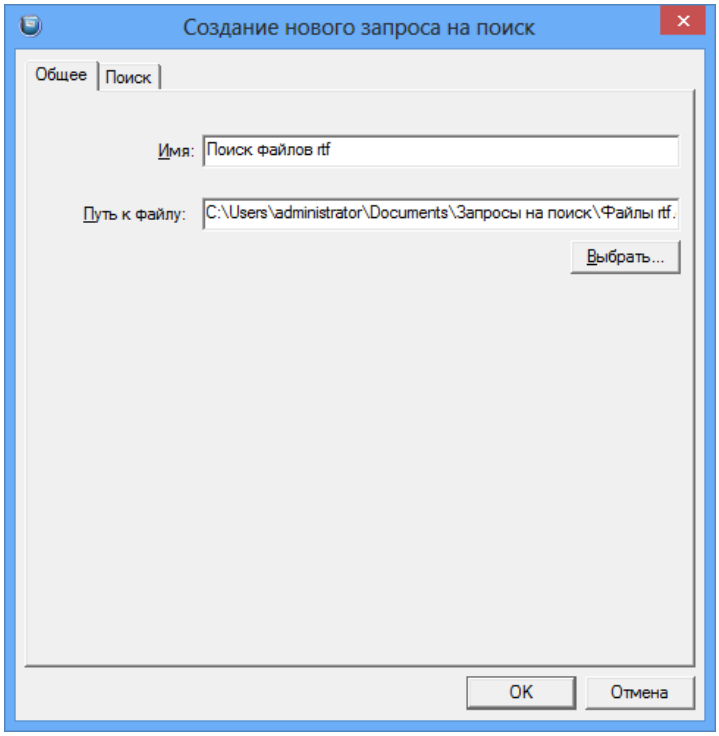
В программе просмотра локальных журналов для загрузки записей с особыми критериями отбора могут использоваться запросы на поиск по файлам данных. Такие запросы предназначены для поиска файлов в хранилище теневого копирования и загрузки записей журнала Secret Net, относящихся к найденным файлам.

Запросы можно сохранять в файлы и загружать в следующих сеансах работы с программой.

Настройка параметров запроса на поиск по файлам данных

Настройка параметров запроса осуществляется в следующих диалогах:

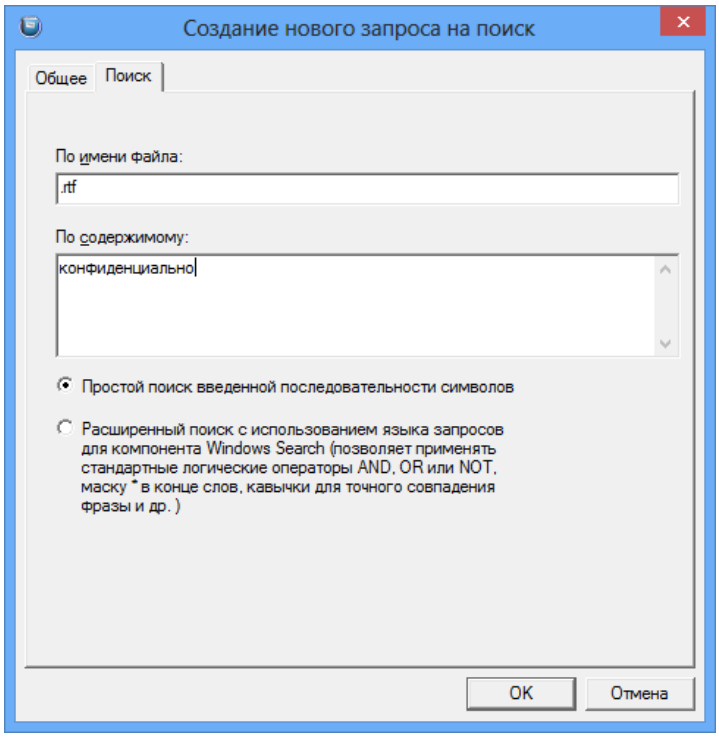
- Диалог "Общее".



В диалоге настройте следующие параметры:

Имя
Содержит имя запроса, отображаемое в окне запросов на поиск
Путь к файлу
Содержит имя файла для сохранения параметров запроса. Если поле пустое, параметры не сохраняются и запрос будет отсутствовать в следующих сеансах работы программы. Имя файла можно указать вручную или в стандартном диалоге выбора файла, вызов которого осуществляется с помощью кнопки "Выбрать". Параметры запроса автоматически сохраняются в указанном файле при закрытии диалогового окна настройки с помощью кнопки "OK"

- Диалог "Поиск".

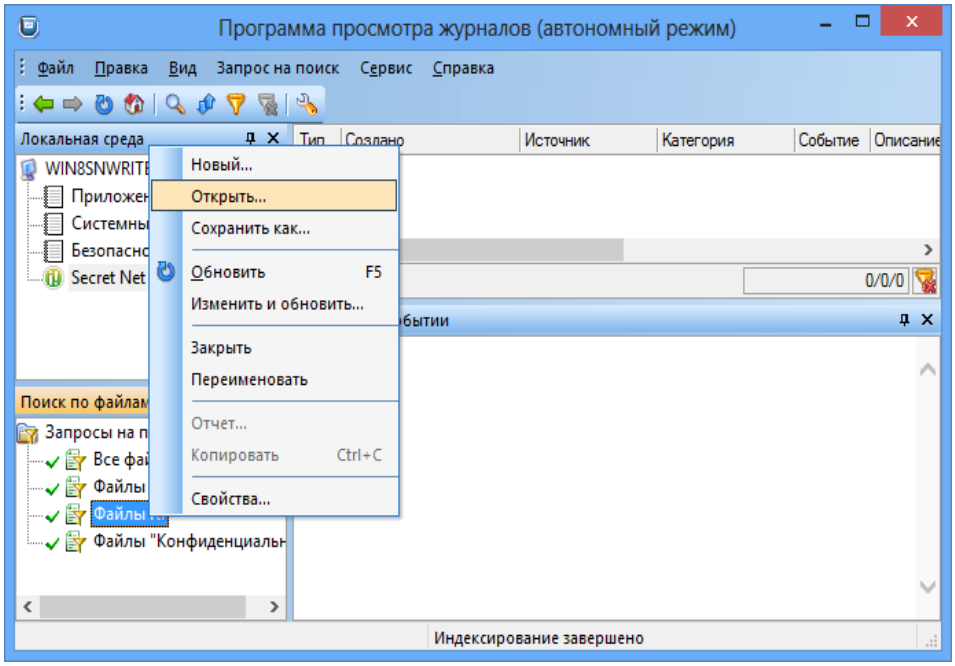


В диалоге настройте следующие параметры:

По имени файла
Определяет строку поиска в именах файлов. При поиске рассматриваются внутренние имена файлов, под которыми они помещены в хранилище теневого копирования (см. стр.**7**). Поиск по исходным именам файлов следует осуществлять в записях журнала Secret Net. Описание процедуры поиска по записям журнала см. на стр.**18**
По содержимому
Определяет строку поиска в содержимом файлов. Поиск по содержимому выполняется в файлах определенных типов и форматов, которые поддерживаются компонентом Windows Search (см. стр.**7**)
Переключатель для выбора простого или расширенного поиска
Если выбран простой поиск, введенные строки в полях "По имени файла" и "По содержимому" рассматриваются в том виде, как они указаны. То есть будут найдены файлы, в которых имя и/или содержимое включают указанный текст. В режиме простого поиска регистр символов не учитывается. В одном поле можно указать несколько строковых значений, разделенных запятой или символом ";". Если выбран расширенный поиск, введенные строки анализируются, и при наличии в них логических операторов или специальных символов поиск осуществляется в соответствии с правилами языка запросов для компонента Windows Search. В этом случае могут применяться логические операторы "И", "ИЛИ", "НЕ" (соответственно "AND", "OR" или "NOT"), маски для указания любых символов и другие средства. При расширенном поиске поисковые строки следует заключать в кавычки. Например, если требуется найти файлы, содержащие слова "секретный", "секретное", "секретные" и т. п. или фразу "конфиденциальный документ", в строке поиска можно указать: "секретн*" OR "конфиденциальный документ". Полный перечень возможностей языка запросов с примерами использования приводится на сайте компании Microsoft: http://msdn.microsoft.com/en-us/library/bb231270(v=VS.85).aspx

Управление списком запросов

Список запросов выводится в окне "Поиск по файлам данных". Пример списка запросов представлен на следующем рисунке:



Для управления списком могут использоваться команды контекстного меню запросов.

Команда	Описание
Новый	Запускает процедуру создания нового запроса с предварительной настройкой параметров
Открыть	Выполняет загрузку запроса из файла. Имя файла и его местоположение указываются в стандартном диалоге открытия файла ОС Windows
Сохранить как	Сохраняет запрос в новом файле. Имя файла и его местоположение указываются в стандартном диалоге сохранения файла ОС Windows
Изменить и обновить	Выполняет новую загрузку записей с предварительной настройкой параметров запроса
Закрыть	Выгружает запрос из программы. Заданное имя запроса не сохраняется при закрытии. Невыгруженные запросы автоматически загружаются в следующем сеансе работы программы, если они были сохранены
Переименовать	Включает режим редактирования названия запроса
Свойства	Вызывает диалоговое окно настройки параметров запроса

Глава 4
Дополнительные возможности программы

Экспорт записей журналов

Программа позволяет сохранять (экспортировать) в файлы записи выбранного журнала. Поддерживаемые форматы сохранения перечислены в следующей таблице.

Имя	Формат	Описание
***.mdb**	Формат баз данных Microsoft Jet 4.0	Экспорт поддерживается на компьютерах с 32-разрядными версиями ОС Windows. Загруженные в программу записи можно сохранить полностью или выборочно. Для просмотра содержимого mdb-файлов необходимо использовать другие приложения, например, программу Microsoft Access
***.dvt**	Формат декодированного хранения записей	Загруженные в программу записи можно сохранить полностью или выборочно. Загрузка содержимого dvt-файлов может осуществляться в программе просмотра журналов (см. стр.**14**), а также в следующих случаях: • при работе в программе "Контроль программ и данных" (см. документ [**3**]); • при работе со списком устройств групповой политики (см. документ [**3**])
.evt (*.evt или *.evtx)	Стандартный формат журналов событий ОС Windows	В файле сохраняется все содержимое выбранного журнала (включая те записи, которые не загружены в программу просмотра). При экспорте журнала Secret Net в отдельном подкаталоге создается копия хранилища теневого копирования. Загрузка содержимого evt-файлов может осуществляться в программе просмотра локальных журналов (см. стр.**14**) или в других приложениях, поддерживающих данный формат (при этом будут недоступны некоторые функции, реализованные в программе просмотра локальных журналов). Например, файлы указанного формата можно загрузить в оснастке "Просмотр событий" ОС Windows. При загрузке записей журнала Secret Net в сторонних приложениях необходимо указать тип журнала безопасности ОС Windows

Для экспорта записей:

1. Выберите нужный журнал.
2. Если требуется экспортировать часть загруженных записей (при экспорте в mdb- или dvt-файл), выделите нужные записи в таблице или выполните фильтрацию с нужными параметрами (см. стр.**16**).
3. В контекстном меню журнала выберите команду "Экспорт...".

   На экране появится диалог настройки параметров экспорта.
4. В поле "Тип выходного файла" выберите нужный формат экспорта.
5. В поле "Путь к файлу" введите полное имя файла для сохранения или нажмите кнопку "Выбрать", чтобы указать файл в диалоге сохранения файла ОС Windows.

Примечание.
При экспорте записей, к которым относятся файлы в хранилище теневого копирования, эти файлы также экспортируются и помещаются в отдельном подкаталоге в месте размещения файла с записями журнала. Каталогу будет присвоено такое же имя, которое указано для файла с записями.

6. Настройте параметры экспорта, перечисленные ниже. После настройки нажмите кнопку "ОК".

Экспортировать
Определяет, какие записи будут экспортированы в mdb- или dvt-файл: • "Все" — выполняется экспорт всех записей, загруженных в программу просмотра (в том числе тех, которые не удовлетворяют текущим параметрам фильтрации); • "Видимые" — выполняется экспорт записей, соответствующих параметрам 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
Удалить после экспорта
Если установлена отметка, автоматически будет выполнена очистка журнала после экспорта записей в evt-файл. При очистке журнала Secret Net удаляется и содержимое хранилища теневого копирования. Для очистки журнала Secret Net пользователю должна быть предоставлена привилегия "Журнал: Управление журналом системы защиты" (см. документ [**3**])

Получение сведений об устройствах из записей журнала

Программа просмотра локальных журналов позволяет скопировать в буфер обмена или сохранить в отдельном файле сведения об устройстве, хранящиеся в журнале Secret Net. Получение сведений осуществляется из записей, содержащих описание устройства. Например, данные об устройстве сохраняются в журнале при регистрации события "Подключение устройства".

Копирование сведений об устройствах

Сведения об устройстве можно скопировать в буфер обмена и вставить в список устройств групповой политики. Вставка содержимого буфера обмена осуществляется стандартным для ОС Windows способом. Подробные сведения о работе со списками устройств в групповых политиках см. в документе [**3**].

Для копирования сведений об устройстве в буфер обмена:

1. Выберите журнал Secret Net для загрузки записей о событиях подключения устройств.
2. Выделите запись, содержащую данные о нужном устройстве.
3. Вызовите контекстное меню записи и выберите команду "Копировать данные" (команда недоступна при отсутствии в записи сведений об устройстве).

Сохранение сведений об устройствах

Сведения об устройстве можно сохранить в файл для последующего импорта в список устройств групповой политики. Экспорт осуществляется в файл специального формата описания устройств системы Secret Net (*.sndev). Содержимое файла в дальнейшем можно импортировать в список устройств. Подробные сведения о работе со списками устройств в групповых политиках см. в документе [**3**].

Для сохранения сведений об устройстве в файл:

1. Выберите журнал Secret Net для загрузки записей о событиях подключения устройств.
2. Выделите запись, содержащую данные о нужном устройстве.
3. Вызовите контекстное меню записи и выберите команду "Сохранить данные в файл" (команда недоступна, если запись не содержит сведений об устройстве).

   На экране появится стандартный диалог сохранения файла ОС Windows.
4. Укажите имя файла для сохранения сведений.

Очистка локального журнала и хранилища теневого копирования

Очистку (удаление записей) локального журнала можно выполнить при экспорте в evt-файл (см. стр. 22) или с помощью команды "Очистить" в контекстном меню журнала (команда "Очистить" может применяться только для штатных журналов ОС Windows). Удаление содержимого хранилища теневого копирования осуществляется при очистке журнала Secret Net.

Просмотр хранилища теневого копирования

Для просмотра содержимого хранилища теневого копирования и выполнения стандартных операций с файлами (копирование, запуск, открытие и др.) используется программа "Проводник" ОС Windows. Вызов окна программы "Проводник" можно выполнить из программы просмотра локальных журналов.

Внимание!
При работе в программе "Проводник" блокируются все операции, связанные с удалением файлов из хранилища.

Предусмотрены следующие возможности для просмотра файлов в хранилище теневого копирования:

- открытие основной папки хранилища;
- открытие папки временных файлов, в которой предварительно создана копия выбранного файла с исходным именем.

Открытие основной папки хранилища

Основной папкой хранилища теневого копирования является корневая папка файловой структуры хранилища.

Для открытия окна с основной папкой хранилища:

- В меню "Сервис" выберите команду "Просмотр хранилища".

  На экране появится окно программы "Проводник" с содержимым основной папки хранилища.

Создание временной копии файла

При регистрации событий теневого копирования дубликаты файлов, выводимых на отчуждаемые носители информации, помещаются в хранилище в особых служебных папках. Файлам дубликатов присваиваются внутренние имена, сгенерированные на основе контрольных сумм файлов и меток времени. В связи с этим переход к нужному файлу при просмотре содержимого хранилища может оказаться затруднительным.

Программа просмотра локальных журналов предоставляет возможность создать нужный файл с исходным именем и выполнить быстрый переход к этому файлу. Такой файл создается во временной папке хранилища на основе файла дубликата. Для создания используется запись журнала Secret Net, содержащая

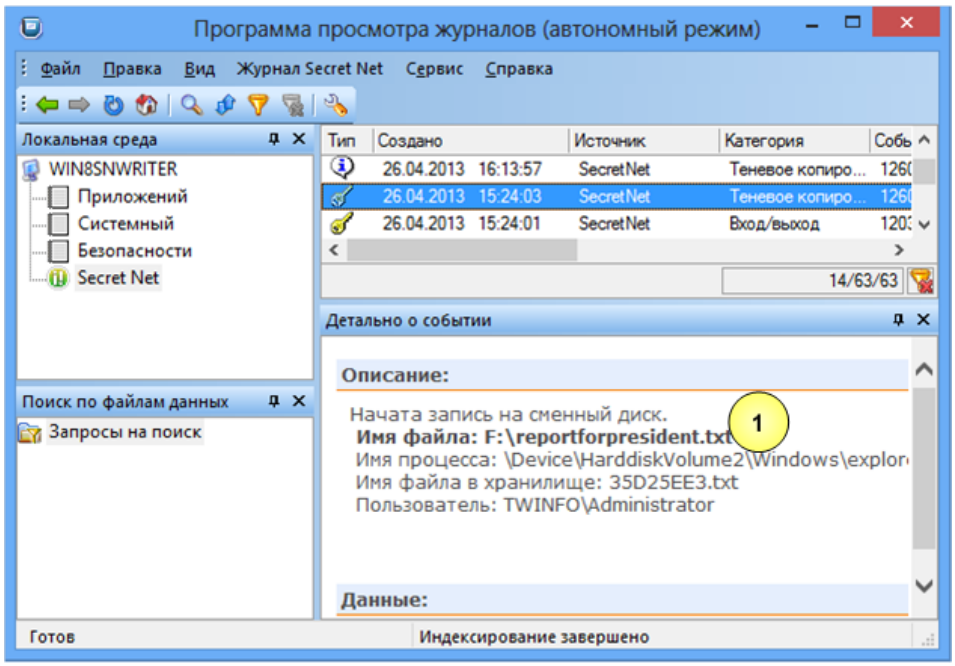
сведения о событии теневого копирования с указанным исходным именем файла.

Внимание!
Папка с временными файлами хранилища автоматически очищается при каждом запуске программы просмотра журналов.

Для открытия окна с временной копией файла в хранилище:

1. Выберите журнал Secret Net или запрос для загрузки записей о событиях теневого копирования.
2. Выделите нужную запись, содержащую данные о выводе файла на отчуждаемый носитель.

   В окне дополнительных сведений появится подробная информация о событии.



Пояснение.
На рисунке обозначены: 1 — команда-ссылка для перехода к копии файла.

3. В окне дополнительных сведений выберите команду-ссылку, которая представлена в виде исходного имени файла в разделе "Описание".

   Программа создаст копию файла с исходным именем во временной папке хранилища, после чего на экране появится окно программы "Проводник". В окне будет отображен список файлов временной папки, в котором выделен нужный файл.

Формирование отчета по записям журнала

Программа просмотра локальных журналов позволяет создавать отчеты, содержащие сведения о записях журналов.

Отчеты сохраняются в файлы формата RTF. Для работы с RTF-файлами необходимы соответствующие приложения, 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

В отчете сохраняются следующие сведения:

- тип журнала и имя компьютера, к которому относится журнал;
- список записей в табличной форме.

Для формирования отчета:

1. Выберите нужный журнал или запрос.
2. Если требуется сохранить часть загруженных записей, выделите нужные записи в таблице или выполните фильтрацию с необходимыми параметрами (см. стр.**16**).
3. В контекстном меню журнала или запроса выберите команду "Отчет...".

   На экране появится стартовый диалог мастера формирования отчета.

   Совет.
   Для настройки нумерации страниц отчета нажмите кнопку "Дополнительно".

4. Укажите сохраняемые в отчете сведения и нажмите кнопку "Далее >".

Все записи журнала
Сохраняются все записи журнала или запроса, загруженные в программу просмотра (в том числе те, которые не удовлетворяют текущим параметрам фильтрации)
Записи, удовлетворяющие фильтру (отображаемые)
Сохраняются только записи, соответствующие параметрам фильтрации
Записи из диапазона
Сохраняются записи из заданного диапазона в соответствии с текущими параметрами сортировки. Границы диапазона определяются в полях "от:" и "до:". Первая и последняя записи диапазона также будут сохранены
Выбранные записи
Сохраняются только те записи, которые выделены в таблице
Добавить в отчет детальную информацию о событиях
Если установлена отметка, в отчете будут сохранены подробные сведения о зарегистрированных событиях

5. В следующем диалоге в поле "Сохранить файл отчета как" укажите имя файла отчета и нажмите кнопку "Построить".

Приложение

Пиктограммы объектов

В программе просмотра локальных журналов используются пиктограммы журналов, перечисленные в следующей таблице.

Пиктограмма	Описание
	Штатный журнал ОС Windows (журнал приложений, системный журнал или журнал безопасности)
	Журнал Secret Net

В программе просмотра локальных журналов используются пиктограммы запросов, перечисленные в следующей таблице.

Пиктограмма	Описание
	Несохраненный запрос
	Сохраненный запрос

Типы регистрируемых событий

Пиктограммы и названия типов событий, регистрируемых в журналах Windows и журнале Secret Net, перечислены в следующей таблице.

Пиктограмма, название типа	Описание
 Информация	Обозначает события, информирующие об успешном выполнении операций
 Предупреждение	Обозначает события, предупреждающие об изменении состояния объектов или о создавшихся угрозах для безопасности системы
 Ошибка	Обозначает события, предупреждающие о возникших неполадках при выполнении действий
 Аудит успехов	Обозначает события, информирующие об успешном доступе
 Аудит отказов	Обозначает события, информирующие об отказе в доступе

Загрузка архивов, созданных сервером безопасности версий 6.X, 5.X

Программа просмотра журналов текущей версии предоставляет возможность загрузки записей из файлов архивов, созданных сервером безопасности версий 6.X или 5.X (файлы формата *.oma). Для загрузки таких файлов программа должна функционировать в специальном режиме просмотра архивов.

Для загрузки файлов архивов формата *.oma:

1. Запустите консоль командной строки (cmd.exe).
2. Перейдите в каталог установки клиента (по умолчанию \Program Files\Secret Net\Client).
3. Введите команду: OMSLogManager.exe /browse

   На экране появится окно программы просмотра журналов с диалогом выбора файла для загрузки архива.
4. Выберите нужный файл.

> **Примечание.**
> Имя файла архива можно указать в качестве дополнительного параметра в команде запуска программы: OMSLogManager.exe /browse <*имя_файла*>. В этом случае архив будет загружен сразу при запуске и диалог выбора файла не появится.

В режиме просмотра архивов можно поочередно загружать разные архивы в одном сеансе работы программы (при этом предыдущий архив выгружается). Для загрузки другого архива используйте команду "Открыть" в меню "Файл ".

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