Код безопасности
ГК «Информзащита»

Средство защиты информации

SECRET NET 6

Руководство администратора

Аудит

RU.88338853.501410.007 91 5

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

Версия: 6.5 Последнее обновление: 14-09-10

Оглавление

Список сокращений

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 6" RU.88338853.501410.007 (далее — система Secret Net 6, система защиты). В руководстве содержатся сведения, необходимые для настройки механизма регистрации, а также для работы с программой просмотра журналов.

Перед изучением руководства необходимо ознакомиться с документом [1].

Условные обозначения

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

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

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

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

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

Другие источники информации

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

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

Основные задачи аудита

Под аудитом системы защиты понимается отслеживание событий, происходивших в системе за определенный период времени.

Основными задачами аудита являются:

- контролирование состояния защищенности системы;
- выявление причин произошедших изменений;
- определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к НСД;
- установление времени изменений.

Аудит системы защиты осуществляет администратор безопасности или другой уполномоченный сотрудник.

В сетевом режиме функционирования системы Secret Net 6 реализована возможность централизованного аудита системы защиты. Помимо администратора безопасности выполнение задач централизованного аудита целесообразно возложить на специально выделенного сотрудника — аудитора. Полномочия для работы с журналами следует распределить таким образом, чтобы администратор безопасности и его помощники могли получать необходимую информацию без возможности удаления содержимого журналов, а аудитор осуществлял анализ защищенности системы и контроль действий пользователей (в том числе административного персонала). В случае нарушения пользователями политики безопасности аудитор должен оповещать об этом соответствующих должностных лиц организации.

Глава 1
Системные журналы

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

Журнал Secret Net

В журнале событий системы Secret Net 6 (далее — журнал Secret Net) накапливается информация о событиях, регистрируемых средствами системы защиты. На каждом компьютере с установленным клиентским ПО Secret Net 6 (далее — защищаемые компьютеры) заполняется отдельный журнал Secret Net.

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 на стр. 41.

Состав регистрируемых в журнале событий определяется заданными параметрами действующей политики безопасности.

В журнале Secret Net используется такой же формат данных и состав полей записей, что и в штатных журналах ОС Windows. Загрузка записей для просмотра осуществляется в программе просмотра журналов системы Secret Net 6.

Штатные журналы ОС Windows

В штатных журналах ОС Windows регистрируются только те события, которые имеют отношение к операционной системе. События системы Secret Net 6 не регистрируются в этих журналах. Информация о событиях сохраняется в следующих штатных журналах:

- 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.

Подробное описание содержимого штатных журналов ОС Windows и процедур настройки регистрации этих событий содержится в документации к операционной системе.

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

Журнал сессий

В сетевом режиме функционирования системы Secret Net 6 на каждом компьютере с установленным ПО "Secret Net 6 — Сервер безопасности" в отдельном журнале протоколируются сессии доступа к серверу безопасности (далее — журнал сессий). Регистрация сессий доступа в журнале сессий происходит при обращениях к серверу безопасности (СБ) следующих компонентов и программ системы защиты:

- клиенты системы Secret Net 6 в сетевом режиме функционирования;
- серверы безопасности, подчиненные данному СБ;
- программа просмотра журналов (в режиме работы с централизованными журналами);
- программа мониторинга.

Кроме того, в журнале сессий могут протоколироваться и некоторые операции, выполняемые самим СБ (старт сервера, соединение с базой данных, архивирование и восстановление журналов и пр.).

Перечень полей, составляющих записи журнала сессий, представлен на стр. 59. Загрузка записей для просмотра осуществляется в программе просмотра журналов (в режиме работы с централизованными журналами).

Организация хранения журналов

Записи журналов могут храниться:

- локально — на компьютере, где они были зарегистрированы;
- централизованно — в БД сервера безопасности;
- в архиве.

В автономном режиме функционирования системы Secret Net 6 журналы могут храниться только локально.

В программе просмотра журналов предусмотрена возможность сохранения записей в файлы.

Хранение локальных 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. Содержимое локальных журналов можно загрузить в программу просмотра в режиме работы с локальными журналами (см. стр. 11).

В сетевом режиме функционирования системы Secret Net 6 локальные журналы хранятся на компьютере до тех пор, пока они не будут переданы на сервер безопасности. После передачи на сервер записи удаляются из журнала.

В программе просмотра в режиме работы с локальными журналами пользователь, наделенный соответствующей привилегией, может выполнять очистку журналов до их передачи на сервер безопасности (см. стр. 29). Необходимо контролировать привилегии пользователей на управление локальными журналами.

Централизованное хранение

Локальные журналы, переданные на сервер безопасности, хранятся в базе данных сервера. Запуск процесса передачи локальных журналов с защищаемого компьютера осуществляется в следующих случаях:

- в моменты времени, заданные параметрами автоматической передачи журналов в программе конфигурирования системы защиты (см. документ [7]);
- по команде пользователя программы просмотра журналов (см. стр. 22).

Для штатных журналов ОС Windows можно отключить передачу записей для централизованного хранения (см. документ [7]). Если для журнала отключена функция централизованного сбора, этот журнал игнорируется при запросе локальных журналов сервером безопасности и содержимое этого журнала остается в локальном хранилище.

Совместно с журналами рабочих станций в базе данных сервера безопасности регистрируются и хранятся записи журнала сессий.

Удаление записей журналов из БД происходит при архивировании журналов.

Просмотр и управление записями журналов, хранящихся в БД сервера безопасности, осуществляется в программе просмотра в режиме работы с централизованными журналами. Описание процедуры запуска программы в этом режиме содержится на стр. 11.

Хранение в архиве

С целью уменьшения объема базы данных сервера безопасности предусмотрена возможность архивирования записей журналов, хранящихся в БД. Архивируются все записи журналов, имеющиеся в базе данных на момент начала процесса архивирования (для журнала сессий — архивируются сведения о завершенных сессиях). Записи, помещенные в архив, удаляются из журналов в базе данных.

Запуск процесса архивирования осуществляется в следующих случаях:

- в моменты времени, заданные параметрами автоматического архивирования журналов в программе конфигурирования (см. документ [7]);
- по команде пользователя программы просмотра журналов (см. стр. 29).

Архивированные записи журналов хранятся в файлах. Для каждого архива создается отдельный файл, в который помещаются записи журналов всех рабочих станций, подчиненных данному серверу безопасности, а также журнал сессий сервера. Файлы архивов базы данных размещаются в подкаталоге \Archive, расположенном в каталоге установки сервера безопасности.

Просмотр записей, помещенных в архив, можно выполнить как с восстановлением записей в базе данных (см. стр. 22), так и без этого (см. стр. 23).

Настройка механизма регистрации событий на компьютерах

Изменение параметров журнала Secret Net

При настройке параметров можно изменить ограничение максимального объема журнала Secret Net и политику перезаписи хранящейся информации.

Данные процедуры описывают последовательность действий при локальном администрировании. Централизованное администрирование осуществляется аналогично в соответствующих оснастках.

Для настройки параметров журнала:

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

   На экране появится окно консоли с загруженной оснасткой для управления параметрами локальной политики безопасности.

2. Перейдите к разделу "Параметры безопасности | Параметры Secret Net | Настройки подсистем".

   В правой части окна появится список параметров.

3. Выберите элемент "Журнал: Максимальный размер журнала системы защиты" и вызовите диалог настройки параметра.

4. В диалоге установите значение максимально допустимого размера журнала в килобайтах. Диапазон значений — от 64 до 4 194 240 Кбайт (с шагом 64).

5. В списке параметров выберите элемент "Журнал: Политика перезаписи событий" и вызовите диалог настройки параметра.

6. В диалоге выберите способ очистки журнала при его переполнении (если размер журнала достигает максимального значения). Для этого установите отметку в одном из полей диалога. Затем нажмите кнопку "ОК".

Затирать события по мере необходимости
При переполнении журнала система защиты автоматически удаляет из журнала необходимое количество самых старых записей
Затирать события старее: <…> дней
При переполнении журнала система защиты автоматически удаляет записи, время хранения которых превысило заданный период. Новые записи не будут добавляться, если журнал достиг максимального размера и не содержит записей старше заданного периода. Диапазон ввода значений — от 1 до 365 дней
Не затирать события
После достижения максимального размера записи хранятся в журнале. Новые события в журнале не регистрируются. Журнал можно очистить только вручную с помощью программы просмотра журналов (см. стр. 28). Очистка должна выполняться периодически по мере накопления записей, чтобы не допустить переполнение журнала, так как это может привести к нарушениям в работе системы и вызвать блокировку компьютера

Выбор событий, регистрируемых в журнале

По умолчанию в журнале Secret Net регистрируются все возможные события, кроме некоторых событий категории "Контроль целостности". Подробное описание регистрируемых событий содержится на стр. 41.

Часть событий регистрируется в обязательном порядке. К таким событиям, например, относятся события категории "Регистрация". Отключить регистрацию таких событий нельзя.

Для настройки списка регистрируемых событий:

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

   На экране появится окно консоли с загруженной оснасткой для управления параметрами локальной политики безопасности.

2. Перейдите к разделу "Параметры безопасности | Параметры Secret Net | Регистрация событий".

   В правой части окна появится список регистрируемых событий.

3. В списке событий выберите элемент с именем события, для которого необходимо изменить режим регистрации, и вызовите диалог настройки параметра.

4. Установите отметку в поле "отключена" (чтобы событие не регистрировалось в журнале) или "включена" (чтобы включить регистрацию) и нажмите кнопку "ОК".

5. При необходимости повторите действия **3**–**4** для других событий в списке.

Глава 2
Начало работы с программой просмотра журналов

Предоставление прав доступа к журналам

Доступ к записям журналов предоставляется сотрудникам, ответственным за управление системой защиты. Права на загрузку записей и управление содержимым журналов определяются привилегиями пользователей:

- привилегии для работы с локальными журналами;
- привилегии для работы с централизованными журналами.

Привилегии для работы с локальными журналами

Для использования программы просмотра в режиме работы с локальными журналами предоставляются следующие привилегии:

- "Просмотр журнала системы защиты" — пользователь может загружать для просмотра записи локального журнала Secret Net;
- "Управление журналом системы защиты" — пользователь может загружать для просмотра записи локального журнала Secret Net, а также осуществлять его очистку.

Примечание. Привилегия "Управление журналом системы защиты" включает в себя разрешение на просмотр журнала Secret Net. Однако во всех случаях, когда пользователям требуется предоставить привилегию на управление журналом, рекомендуется предоставлять обе привилегии.

Для предоставления привилегий:

Данная процедура описывает последовательность действий при локальном администрировании. Централизованное администрирование осуществляется аналогично в соответствующих оснастках.

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

   На экране появится окно консоли с загруженной оснасткой для управления параметрами локальной политики безопасности.
2. Перейдите к разделу "Параметры безопасности | Параметры Secret Net | Привилегии".

   В правой части окна появится список привилегий.
3. Выберите элемент "Журнал: Просмотр журнала системы защиты" и вызовите диалог настройки параметра.
4. В диалоге отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия, и нажмите кнопку "ОК".
5. Выберите элемент "Журнал: Управление журналом системы защиты" и вызовите диалог настройки параметра.
6. В диалоге отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия, и нажмите кнопку "ОК".

Привилегии для работы с централизованными журналами

Для использования программы просмотра в режиме работы с централизованными журналами пользователь должен иметь возможность подключения к серверу (серверам) безопасности. Права на загрузку записей и управление содержимым журналов определяются наличием следующих привилегий:

- "Просмотр информации ОУ" — пользователь может подключиться к определенному серверу безопасности и загружать записи журналов для просмотра;
- "Архивирование журналов" — пользователь может запускать процессы архивирования журналов и восстановления архивов.

Для предоставления привилегий пользователям используется программа конфигурирования (см. документ [7]).

Запуск программы

Программа просмотра журналов может работать в одном из следующих режимов:

- режим работы с локальными журналами — для просмотра содержимого и управления записями локальных журналов компьютера;
- режим работы с централизованными журналами — для просмотра содержимого и управления записями журналов, хранящихся в базе данных СБ;
- режим просмотра архивов — просмотр журналов из файла архива, созданного сервером безопасности.

Для использования программы просмотра в режиме работы с централизованными журналами и в режиме просмотра архивов на компьютере необходимо установить компонент "Secret Net 6 — Средства управления". Для соединения с сервером безопасности на сервере необходимо установить корневой сертификат и сертификат пользователя.

Для запуска программы в режиме работы с локальными журналами:

- Активируйте команду "Пуск | Все программы | Код безопасности | Secret Net | Журналы".

Для запуска программы в режиме работы с централизованными журналами:

1. Активируйте команду "Пуск | Все программы | Код безопасности | Secret Net | Журналы (сетевой режим)".

   Совет. Запуск программы в режиме работы с централизованными журналами можно выполнить из программы мониторинга (см. документ [6]).

   На экране появится окно программы просмотра журналов.

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

   Выбранный сервер безопасности будет корневым элементом иерархии в программе просмотра журналов (см. стр. 13). В программу будут загружены записи журналов только тех компьютеров, которые относятся к данному серверу и к его подчиненным серверам.

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

Для запуска программы в режиме просмотра архивов:

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

   На экране появится окно программы просмотра журналов. Для загрузки архива автоматически открывается стандартный диалог выбора файла.

2. Выберите файл нужного архива.

Интерфейс программы

Внешний вид основного окна программы просмотра журналов в различных режимах работы представлен на Рис. 1 и Рис. 2.

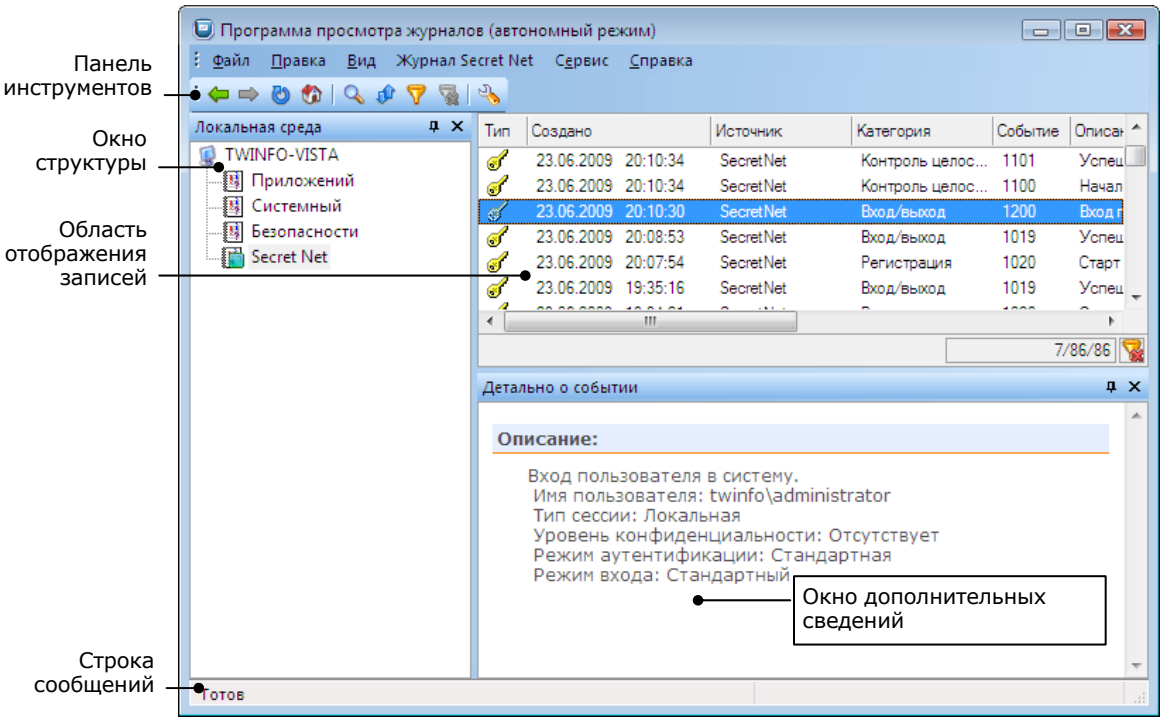


Рис. 1. Окно программы в режиме работы с локальными журналами

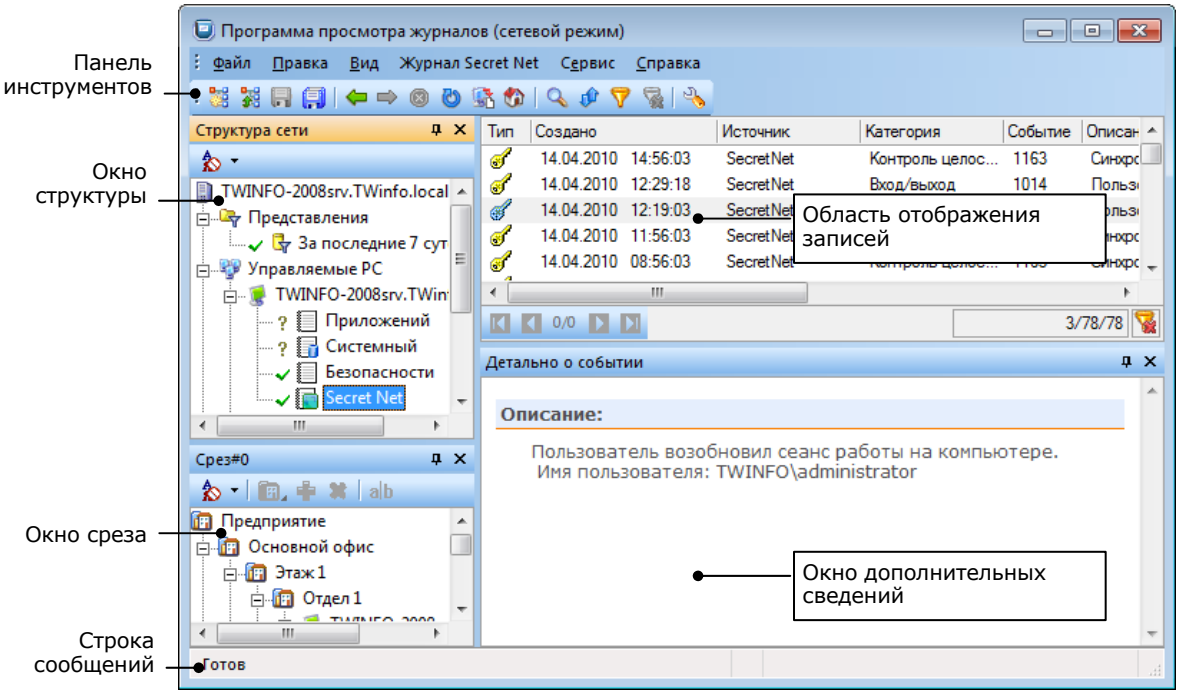


Рис. 2. Окно программы в режиме работы с централизованными журналами

В режиме просмотра архивов окно программы имеет вид, аналогичный режиму работы с централизованными журналами (см. Рис. 2).

Пользователь может изменять состав отображаемых элементов и их расположение на экране (см. стр. 35). 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. 38).

Элементы интерфейса

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 сервера безопасности, имя защищаемого компьютера, название журнала и пр.)
Строка сообщений
Отображает служебные сообщения программы, а также краткие подсказки к командам и кнопкам панели инструментов. В режиме работы с централизованными журналами индикатор  оповещает о том, что выполняется запрос к серверу безопасности
Окно структуры
Предназначено для выбора журнала, объекта структуры или папки. В зависимости от режима работы программы окно содержит: • в режиме работы с локальными журналами — список журналов компьютера, на котором запущена программа просмотра; • в режиме работы с централизованными журналами — в окне представлена иерархия объектов и папок на базе структуры оперативного управления. Корневым элементом иерархии является сервер безопасности, с которым установлено соединение программы. Папка "Управляемые РС" содержит защищаемые компьютеры, относящиеся к данному СБ (включая компьютер самого сервера). Папка "Подчиненные СБ" содержит структуру объектов, относящихся к подчиненному серверу (серверам) безопасности. Каждый компьютер содержит список относящихся к нему журналов. Журнал сессий сервера безопасности представлен в виде структурного элемента "Протоколы сессий", подчиненного СБ. Папка "Представления" содержит список форм запросов к БД СБ (представлений) . Для отображения состояния объектов используются различные пиктограммы (см. стр. 39). Журналы и представления могут быть отмечены знаками: ? — в текущем сеансе не выполнялась загрузка данных в программу просмотра, ✔ — загрузка данных в программу просмотра выполнена успешно, ! — при загрузке данных произошла ошибка. Панель инструментов, расположенная в верхней части окна, содержит кнопку, с помощью которой осуществляется сортировка объектов; • в режиме просмотра архивов — список компьютеров, журналы которых есть в архиве.
Область отображения записей
Отображает записи выбранного журнала/представления 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 (см. следующий раздел). В нижней части области отображения записей могут располагаться следующие элементы: • средства навигации для постраничного просмотра записей (в режиме работы с централизованными журналами или в режиме просмотра архивов) — стандартные кнопки перехода к нужной странице. В центре отображаются номер выбранной страницы и общее число страниц; • сведения о количестве записей в виде: <*номер выбранной записи*> / <*количество отображаемых записей*> / <*общее количество загруженных записей*>; • индикатор включения/отключения фильтрации  (см. стр. 24). 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. 24). При выборе журнала сессий сервера безопасности (в режиме работы с централизованными журналами или в режиме просмотра архивов) область просмотра разделяется на две части. Правую часть области занимает панель выбора сессий для просмотра записей. Список записей отображается в левой части области просмотра

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
Окно среза
Окно может использоваться в режиме работы с централизованными журналами вместо окна структуры объектов. В окне среза можно сгруппировать компьютеры произвольным образом. Панель инструментов окна содержит кнопки, с помощью которых осуществляется формирование списка объектов. Окно появляется при создании или открытии среза

Настройка параметров работы программы

Для настройки параметров:

1. Активируйте команду "Сервис | Настройки…".

   На экране появится диалог "Настройки приложения".

2. Последовательно выбирая названия групп в левой части диалога, задайте в правой части нужные значения параметров. Описание параметров содержится на стр. 35.

Глава 3
Загрузка и просмотр записей журналов

Загрузка записей в режиме работы с локальными журналами

В режиме работы с локальными журналами программа просмотра предоставляет следующие возможности:

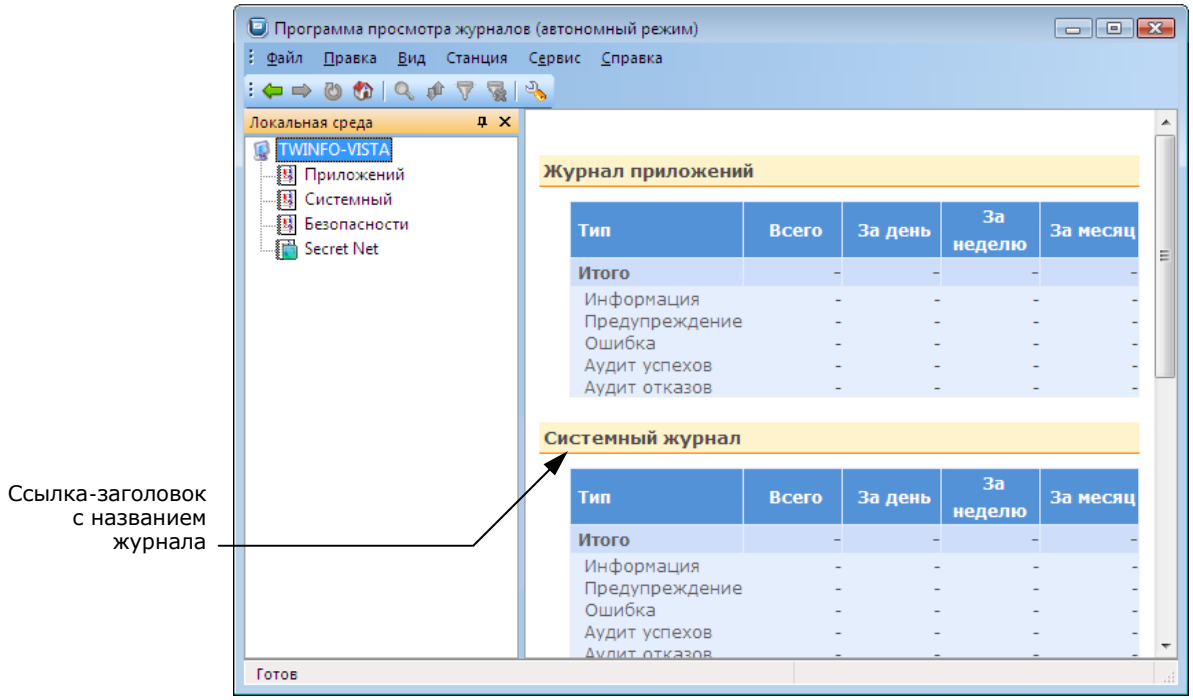
- загрузка записей журналов, хранящихся на компьютере локально;
- загрузка записей из файлов.

Загрузка записей журнала

Для выбора журнала в режиме работы с локальными журналами:

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, активируйте ссылку-заголовок с названием журнала.

Загрузка записей из файла

Программа просмотра в режиме работы с локальными журналами 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. 28).

Для загрузки записей:

1. В режиме работы с локальными журналами выберите журнал (см. стр. 15), 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 активируйте 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 активируйте 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 активируйте команду "Внешний журнал | Закрыть...".

Загрузка записей в режиме работы с централизованными журналами

В режиме работы с централизованными журналами программа просмотра используется для загрузки записей, поступивших на хранение в базу данных сервера безопасности. Загрузку записей из БД можно выполнять с применением различных критериев отбора. Предусмотрены следующие возможности:

- загрузка записей отдельного журнала;
- контекстная загрузка записей о событиях НСД;
- загрузка записей с произвольными критериями отбора.

Загрузка записей журнала

Из базы данных сервера безопасности можно загрузить записи, относящиеся к определенному журналу. Для этого достаточно выбрать нужный журнал в окне структуры или в окне среза. Такая процедура может применяться и для записей журнала сессий.

Для выбора журнала в режиме работы с централизованными журналами:

1. В окне структуры или в окне среза выполните нужное действие:
   - Чтобы загрузить штатный журнал ОС Windows или журнал Secret Net — найдите нужный компьютер, раскройте относящуюся к нему ветвь дерева и выберите журнал.

     Для штатного журнала ОС Windows может быть отключена функция централизованного сбора (см. документ [7]). Такой журнал не поступает на централизованное хранение в базу данных сервера безопасности и хранится только локально. Журнал с отключенной функцией централизованного сбора отображается со специальной пиктограммой (см. стр. 39), а при его выборе в программу будут загружены только записи, поступившие в БД СБ до отключения функции централизованного сбора.

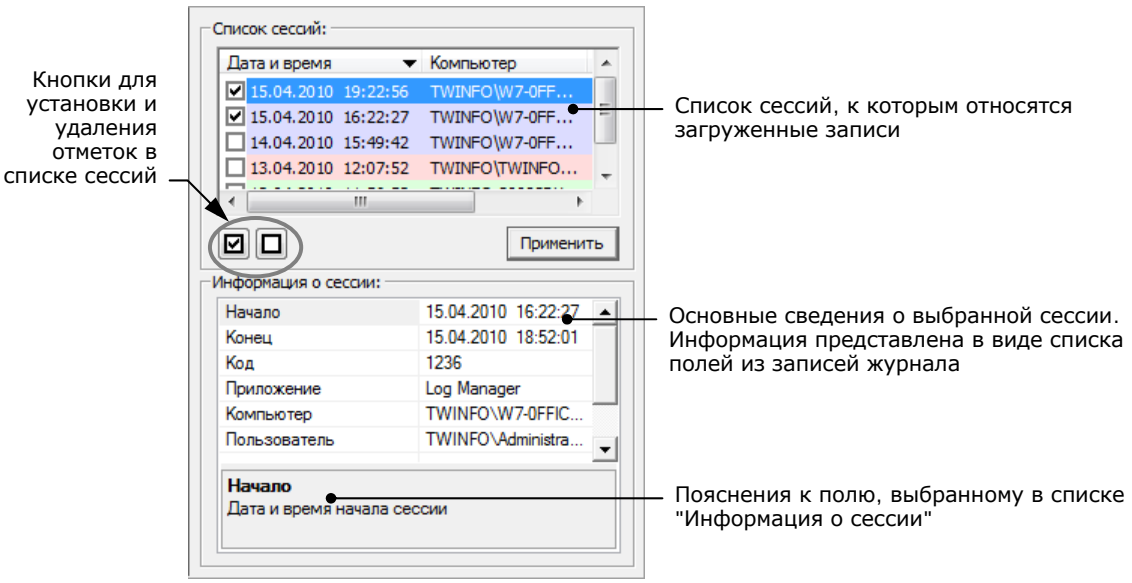
   - Чтобы загрузить журнал сессий — найдите нужный сервер безопасности, раскройте относящуюся к нему ветвь дерева и выберите "Протоколы сессий".

2. При первом обращении к журналу в текущем сеансе на экране может появиться диалог настройки параметров фильтрации записей (если установлено значение "Да" для параметра "Запрос по фильтру" — см. стр. 37). Поля диалога определяют интервал времени для отбора загружаемых записей. При необходимости укажите другие границы интервала времени и нажмите кнопку "ОК".

   Загрузка записей осуществляется при первом обращении к журналу в текущем сеансе работы программы. При следующих обращениях к данному журналу в текущем сеансе программа выводит ранее загруженные записи.

   Если программа не сможет загрузить записи журнала в полном объеме, осуществляется постраничная загрузка записей. Постраничный просмотр записей выполняется средствами навигации, находящимися в левом нижнем углу области отображения записей. Количество записей, включаемых в страницу, определяется при настройке параметров программы (см. описание параметра "Записей на страницу" на стр. 37).

3. Если выбран журнал сессий, справа от области отображения записей появится панель выбора сессий:



   Отметьте нужные сессии и нажмите кнопку "Применить". В области отображения записей появятся записи о событиях, которые были зарегистрированы во время выбранных сессий.

Контекстная загрузка записей о событиях НСД

События несанкционированного доступа (НСД) считаются события, которые имеют тип "Аудит отказов" и регистрируются в журнале Secret Net или штатном журнале безопасности ОС Windows. Загрузка таких записей может осуществляться в виде отдельных групп, для чего используются специальные формы запросов (представления).

Представления можно создавать контекстно в окне структуры. Элементы структуры в иерархии оперативного управления для контекстного создания представлений перечислены в следующей таблице.

Табл. 1. Элементы структуры для контекстного создания представлений

Элементы структуры	Описание создаваемых представлений
Сервер безопасности, папки "Управляемые PC", "Представления"	В представление будут загружены записи, поступившие от подчиненных компьютеров сервера безопасности. Причем загружаются записи не только компьютеров, подчиненных в текущий момент, но и тех, которые были подчинены СБ в указанный период времени
Защищаемый компьютер	В представление будут загружены записи, поступившие с выбранного компьютера

Элементы структуры	Описание создаваемых представлений
Группа выбранных компьютеров	В представление будут загружены записи, поступившие со всех выбранных компьютеров — при условии, что эти компьютеры подчинены одному СБ. При выборе компьютеров, подчиненных различным СБ, в представление загружаются записи последних выбранных компьютеров

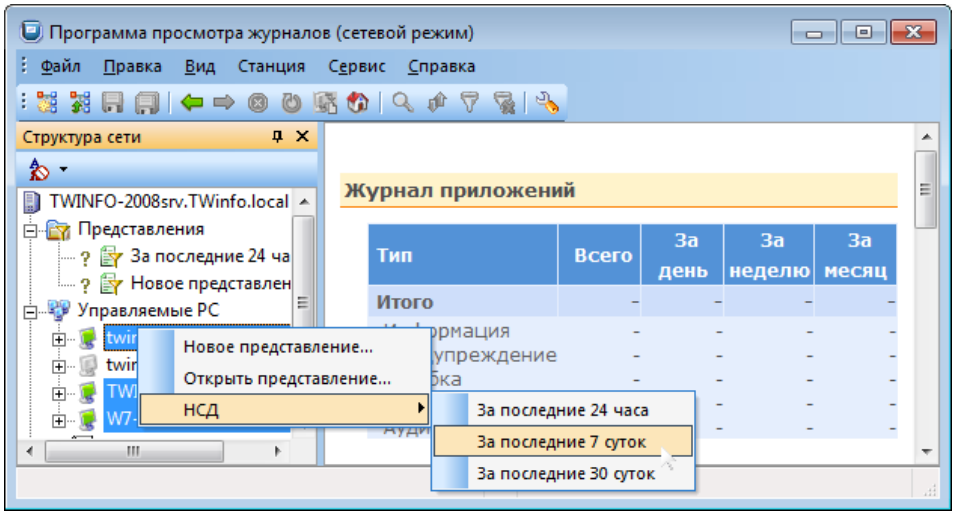
Предусмотрены следующие периоды времени для контекстной загрузки записей:

- за последние 24 часа;
- за последние 7 суток;
- за последние 30 суток.

Записи о событиях НСД загружаются из БД сервера безопасности. Следует иметь в виду, что сведения о событиях поступают в БД СБ с некоторой задержкой, обусловленной периодичностью сбора локальных журналов. Поэтому на момент запроса в БД могут отсутствовать записи о недавно произошедших событиях. Для гарантированного получения актуальных сведений о событиях НСД используйте программу мониторинга (см. документ [6]) или выполните запрос нужных локальных журналов (см. стр. 22).

Для контекстной загрузки записей о событиях НСД:

1. В окне структуры выберите нужный объект, папку или группу компьютеров (для выбора нескольких компьютеров используйте клавиши <Ctrl> или <Shift>).
2. Вызовите контекстное меню выбранного элемента, откройте подменю "НСД" и активируйте команду, соответствующую нужному периоду времени. Например, для загрузки записей, поступивших в БД сервера безопасности в течение предыдущих 7 дней, активируйте команду "За последние 7 суток".



В папке "Представления" появится новая форма запроса, в которую будут загружены записи.

При необходимости можно изменить параметры созданного представления и осуществить загрузку записей с другими критериями отбора. Представление можно сохранить в файле, чтобы использовать данную форму запроса в других сеансах работы. Описание действий для управления представлениями см. на стр. 19.

Загрузка записей с произвольными критериями отбора

Загрузка записей, поступивших в БД СБ из штатных журналов ОС Windows и журналов Secret Net, может выполняться с помощью представлений, настроенных с нужными критериями отбора. Настройка параметров представления осуществляется в специальном диалоговом окне.

Для созданных представлений, имеющихся в папке "Представления", вызов диалогового окна настройки осуществляется с помощью команд "Изменить и обновить" или "Свойства" в контекстном меню представления.

Новое представление можно создать с использованием элементов структуры, перечисленных в Табл. 1.

Для создания нового представления:

1. В окне структуры выберите нужный объект, папку, имеющееся представление или группу компьютеров (для выбора нескольких компьютеров используйте клавиши <Ctrl> или <Shift>).
2. Вызовите контекстное меню выбранного элемента и активируйте соответствующую команду:
   - "Новое...", если выбрано представление или папка "Представления";
   - "Новое представление...", если выбран другой элемент.

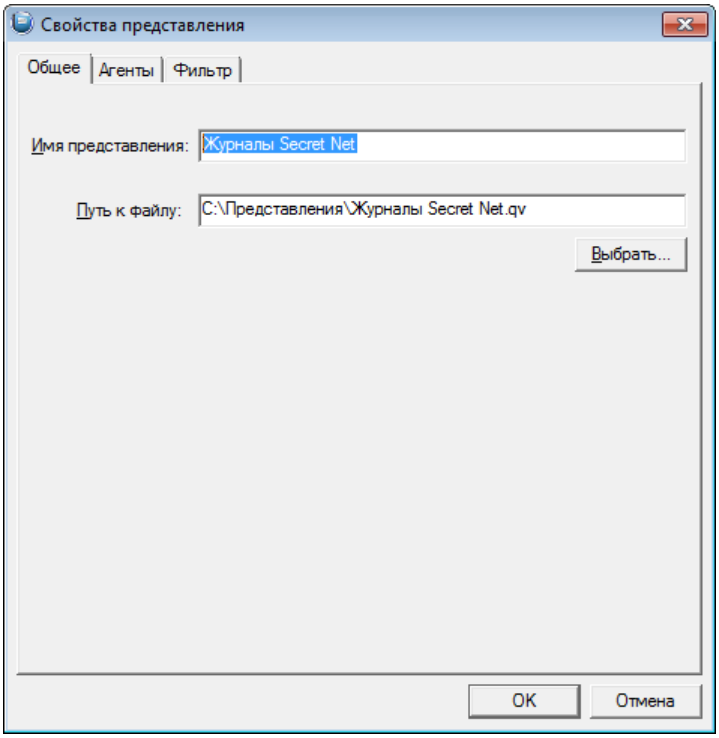
   На экране появится диалоговое окно настройки параметров представления.
3. Настройте параметры представления (см. ниже) и нажмите кнопку "OK".

Управление представлениями

Настройка параметров представления

Настройка параметров представления осуществляется в следующих диалогах:

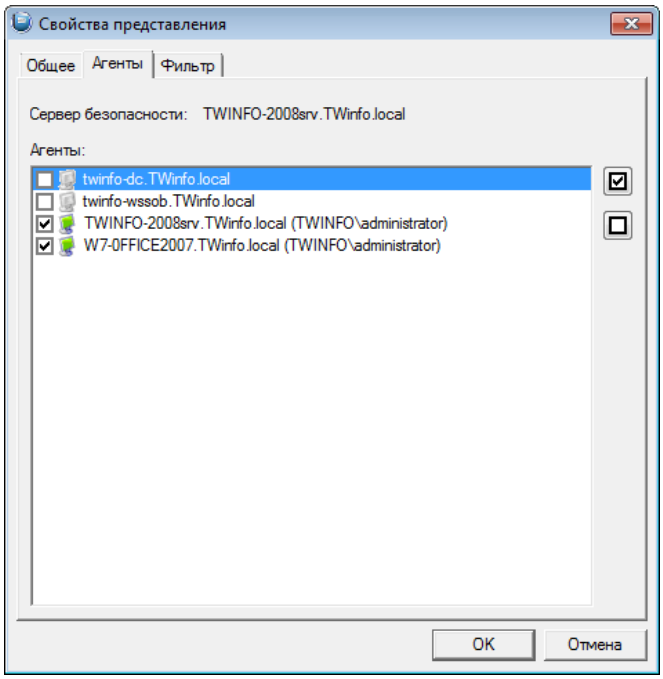
- Диалог "Общее".



В диалоге настройте следующие параметры:

Имя представления
Содержит имя представления, отображаемое в папке "Представления"
Путь к файлу
Содержит имя файла для сохранения параметров представления. Если поле пустое, параметры представления не сохраняются, и оно 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 представления автоматически сохраняются в указанном файле при закрытии диалогового окна настройки с помощью кнопки "OK"

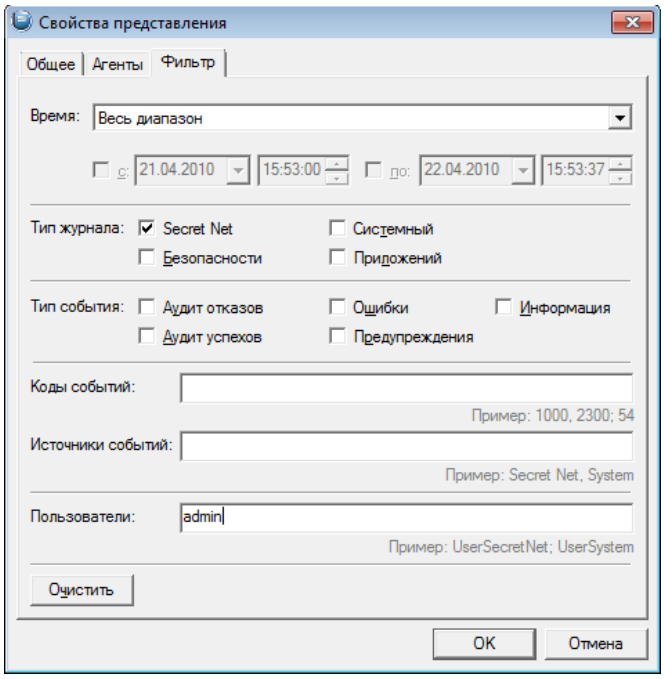
- Диалог "Агенты".



Диалог содержит список компьютеров, подчиненных серверу безопасности. Отметьте компьютеры, записи которых необходимо загрузить в представление. Чтобы установить или удалить отметки для всех элементов, используйте кнопки справа от списка.

Если в списке не отмечен ни один элемент, это равносильно выбору всех компьютеров, включая те, которые были выведены из подчинения данному СБ и поэтому не отображаются в списке. Это позволяет загрузить записи, поступившие в БД сервера безопасности до вывода компьютеров из подчинения.

- Диалог "Фильтр".



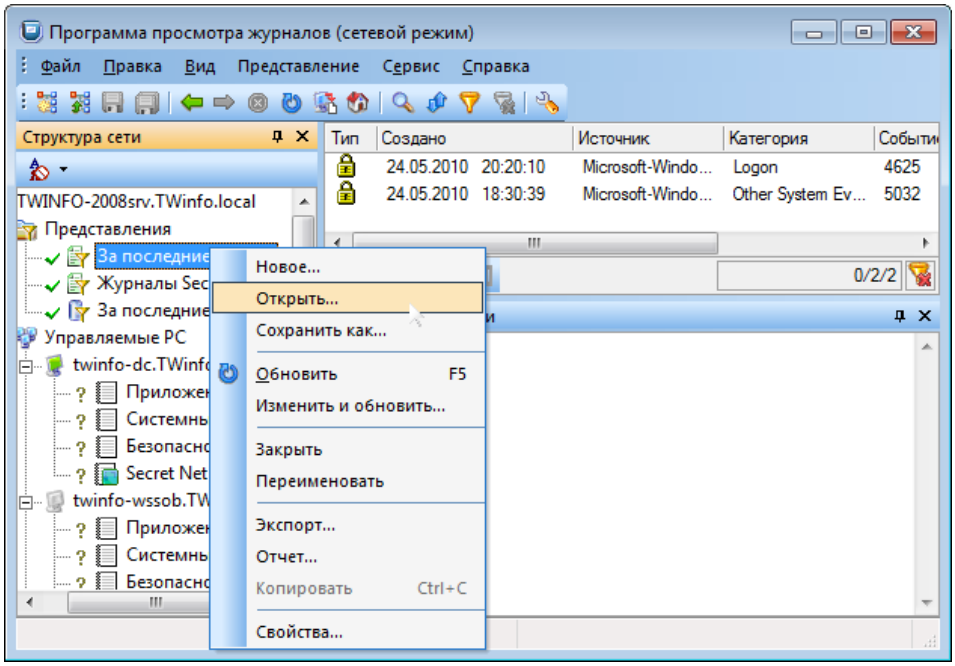
В диалоге настройте следующие параметры:

Группа полей "Время"
Поля группы предназначены для определения интервала времени. В представление будут загружены только те записи, которые были помещены в базу данных в указанное время. Предусмотрены различные временные диапазоны. Предоставляется возможность указать произвольный диапазон в виде фиксированных границ интервала
Группа полей "Тип журнала"
Поля группы предназначены для выбора журналов, записи которых необходимо загрузить в представление. Если в группе не отмечен ни один элемент, типы журналов не учитываются
Группа полей "Тип события"
Поля группы предназначены для выбора типов событий, записи которых необходимо загрузить в представление. Если в группе не отмечен ни один элемент, типы событий не учитываются
Поля "Коды событий", "Источники событий", "Пользователи"
Поля определяют искомое текстовое содержимое. В представление будут загружены только те записи, которые содержат в соответствующих полях указанный текст. Регистр символов не учитывается. В одном поле можно указать несколько строковых значений, разделенных запятой или символом ";"

По окончании настройки параметров нажмите кнопку "ОК".

Управление списком представлений

Список представлений, применяемых для запросов записей из БД сервера безопасности, содержится в папке "Представления".



Для управления списком могут использоваться команды контекстного меню представлений. Команды перечислены в следующей таблице:

Табл. 2. Команды меню для управления представлениями

Команда	Описание
Новое	Запускает процедуру создания нового представления. Для нового представления осуществляется настройка параметров
Открыть	Выполняет загрузку представления из файла. Имя файла и его местоположение указываются в стандартном диалоге открытия файла ОС Windows
Сохранить как	Сохраняет представление в новом файле. Имя файла и его местоположение указываются в стандартном диалоге сохранения файла ОС Windows

Команда	Описание
Изменить и обновить	Выполняет новую загрузку записей в представление с предварительной настройкой параметров представления
Закрыть	Выгружает представление из программы. Заданное имя представления не сохраняется при его закрытии. Невыгруженные представления автоматически загружаются в следующем сеансе работы программы, если эти представления были сохранены
Переименовать	Включает режим редактирования названия представления
Свойства	Вызывает диалоговое окно настройки параметров представления

Принудительная остановка процесса загрузки

В режиме работы с централизованными журналами процесс загрузки записей из базы данных может занять продолжительное время. Длительность процесса зависит от скорости обработки данных в локальной сети и от количества загружаемых записей.

Остановка процесса загрузки записей выполняется командой "Вид | Стоп".

Запрос локального журнала

В программе просмотра в режиме работы с централизованными журналами можно выполнить запрос текущего содержимого локального журнала компьютера. При выполнении запроса осуществляется внеочередная передача записей локального журнала в базу данных сервера безопасности, после чего эти записи могут быть загружены в программу просмотра. Для выполнения процедуры запроса локального журнала выбранный компьютер должен быть включен.

Не осуществляется загрузка локального журнала, если для этого журнала отключена функция централизованного сбора (см. документ [7]).

Для запроса локального журнала:

- В окне структуры или окне среза найдите нужный компьютер, раскройте относящуюся к нему ветвь дерева, вызовите контекстное меню журнала и активируйте команду "Собрать".

Через некоторое время, необходимое для передачи содержимого локального журнала, записи будут переданы в БД сервера безопасности и загружены в программу просмотра.

Восстановление архивированных записей

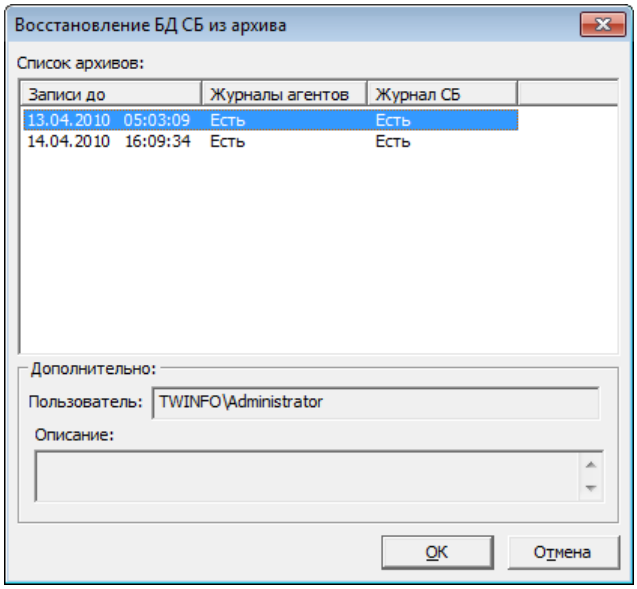
Записи журналов, помещенные в архив из БД сервера безопасности, могут быть снова восстановлены в базе данных сервера. Процедура восстановления выполняется в режиме работы с централизованными журналами. Восстановленные записи могут быть загружены для просмотра так же, как и другие записи, хранящиеся в БД.

Выполнять восстановление архивов может только пользователь, которому предоставлена привилегия "Архивирование журналов" (см. стр. 11).

Для восстановления записей из архива:

1. Выберите в окне структуры сервер безопасности и активируйте команду "Сервер безопасности | Восстановить...".

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



Информация об архивах выводится в следующих колонках:

Записи до
Архив содержит записи, зарегистрированные до указанного момента времени
Журналы агентов
Определяет наличие в архиве записей из локальных журналов компьютеров
Журнал СБ
Определяет наличие в архиве записей журналов сессий

2. Выберите нужный архив и нажмите кнопку "OK".

Для выбранного архива в группе полей "Дополнительно" содержатся сведения о пользователе, создавшем архив, и уточняющая информация.

Загрузка записей в режиме просмотра архивов

Записи журналов, помещенные в архив из БД сервера безопасности, можно загрузить из архива в программу просмотра. Восстановление архива в базе данных сервера безопасности при этом не осуществляется. Для этого программа должна работать в режиме просмотра архивов.

Для загрузки архива:

1. Запустите программу в режиме просмотра архивов (см. стр. 11). При запуске программы на экране автоматически появляется стандартный диалог выбора файла для загрузки архива.

Совет. Чтобы вызвать диалог выбора файла в процессе работы с программой, используйте команду "Файл | Открыть...".

Диалог выбора файла дополнен в нижней части специальными полями. Если в общем списке файлов выбран файл архива, в этих полях отображаются основные сведения об архиве.

2. Выберите нужный файл архива и нажмите кнопку "Открыть".

Архив будет загружен в программу просмотра, и в области отображения записей появятся основные сведения об архиве. При этом предыдущий архив (если он был загружен в текущем сеансе работы с программой) будет выгружен.

Для вызова диалога с основными сведениями о файле активируйте команду "Файл | Информация по архиву...".

Загрузка записей журнала

Для выбора журнала в режиме просмотра архивов:

- В окне структуры выполните нужное действие:
  - Чтобы загрузить штатный журнал ОС Windows или журнал Secret Net — найдите нужный компьютер, раскройте относящуюся к нему ветвь дерева и выберите журнал.
  - Чтобы загрузить журнал сессий — выберите элемент "Протоколы сессий" и выполните действия, описанные в процедуре выбора журнала в режиме работы с централизованными журналами (см. стр. 16).

Если программа не сможет загрузить записи журнала в полном объеме, осуществляется постраничная загрузка записей. Постраничный просмотр записей выполняется средствами навигации, находящимися в левом нижнем углу области отображения записей. Количество записей, включаемых в страницу, определяется при настройке параметров программы аналогично как для режима работы с централизованными журналами.

Фильтрация записей

Программа позволяет фильтровать загруженные записи для отображения нужной информации.

В режиме работы с централизованными журналами или в режиме просмотра архивов программа может осуществлять постраничную загрузку записей. Если в программу загружена отдельная страница (часть записей журнала/представления), фильтрация осуществляется только для записей текущей страницы. Изменение количества записей, включаемых в страницу, осуществляется при настройке параметров программы (см. описание параметра "Записей на страницу" на стр. 37).

Оперативная фильтрация

Из загруженных записей журнала можно оперативно исключить ненужные сведения и отобразить для просмотра записи о событиях, имеющих определенный тип и зарегистрированных в течение некоторого промежутка времени (за день, за неделю или за месяц). Оперативная фильтрация может применяться к записям штатных журналов ОС Windows и журнала Secret Net.

Для оперативной фильтрации записей:

1. После загрузки записей журнала в окне структуры выберите компьютер, к которому относится журнал.

   В области отображения записей появится сводная информация о журналах выбранного компьютера. 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. Назначение строк и столбцов таблицы разъясняется в выносках к рисунку. Значения в ячейках являются ссылками, с помощью которых осуществляется отбор записей по соответствующим условиям.

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

В области отображения записей появятся записи, удовлетворяющие условию отбора. Выбранные параметры фильтрации действуют до выполнения следующей фильтрации или до отключения режима фильтрации (см. стр. 26).

Фильтрация по заданным параметрам

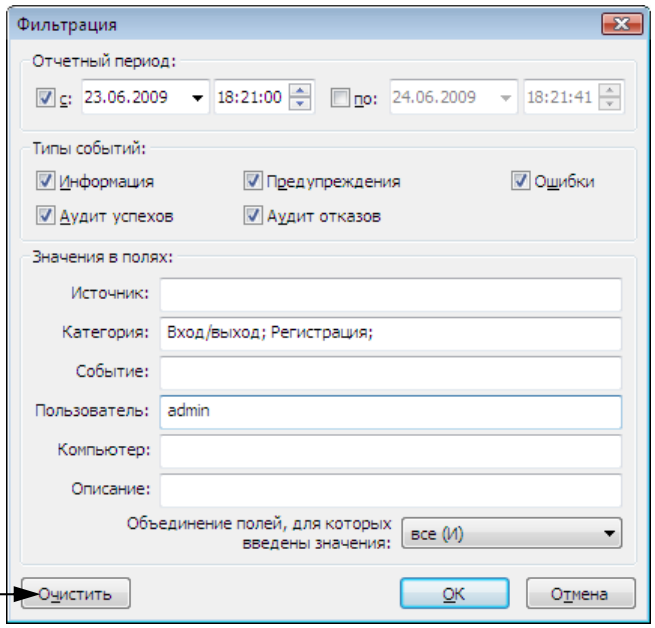
Настроить параметры фильтрации можно в специальном диалоге программы. Заданные параметры применяются к записям текущего выбранного журнала/представления.

Для режима работы с централизованными журналами. В отличие от параметров фильтра, настраиваемых для представления (см. стр. 19), параметры фильтрации записей действуют после загрузки этих записей в программу просмотра. То есть они не влияют на отбор записей из базы данных сервера и действуют независимо от параметров фильтра, заданных в представлении.

Для фильтрации записей:

1. Выберите нужный журнал или представление.
2. Активируйте команду "Правка | Фильтр".

   На экране появится диалог, набор полей которого зависит от выбранного журнала. Если выбран журнал ОС Windows, журнал Secret Net или представление, диалог имеет вид:



Кнопка сброса заданных параметров

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

Группа полей "Отчетный период" (для журнала сессий — "Отчетный период по выполнению операций в сессиях")
Поля группы определяют интервал времени. Фильтру будут удовлетворять записи, которые поступили в базу данных сервера безопасности в указанных границах временного интервала. При фильтрации записей журнала сессий учитывается время выполнения операций
Группа полей "Типы событий" (для журнала сессий — "Тип")
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. Несколько строк в одном поле разделяйте символом ";".

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 параметрами, настроенными так, как это показано на рисунке, 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 представления. Чтобы отключить фильтрацию записей, активируйте команду "Правка | Все события".

Сортировка отображаемых записей

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

В программе просмотра журналов используются стандартные для приложений Windows методы сортировки таблиц и сортировка по заданным параметрам.

Для сортировки по заданным параметрам:

1. Выберите нужный журнал или представление и активируйте 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 выполняется сортировка (названия колонок упорядочены по алфавиту). Отметьте нужное направление сортировки.
3. Если требуется дополнительная сортировка по содержимому другой колонки, настройте параметры в группе полей "Затем". Нажмите кнопку "ОК".

При сортировке по двум колонкам вначале 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 представление.
2. Активируйте команду "Правка | Поиск…".

   На экране появится диалог для настройки параметров поиска.
3. Настройте параметры поиска. Параметры настраиваются аналогично тому, как это выполняется при настройке параметров фильтрации — см. стр. 25.

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

Обновление записей может выполняться в следующих режимах работы программы просмотра:

- режим работы с локальными журналами;
- режим работы с централизованными журналами.

При обновлении записей происходит новая загрузка из БД в программу просмотра. Это позволяет загрузить для просмотра записи, помещенные в БД после предыдущей загрузки.

Чтобы обновить записи, активируйте команду "Обновить" в контекстном меню журнала или представления.

Глава 4
Работа с записями и управление журналами

Экспорт записей журналов

Программа позволяет сохранять (экспортировать) в файлы записи выбранного журнала или представления. Поддерживается несколько форматов сохранения.

Табл. 3. Форматы экспорта записей

Имя	Формат	Описание
***.mdb**	Формат баз данных Microsoft Jet 4.0	Экспорт поддерживается для любого журнала или представления, выбранного в программе просмотра. 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	Экспорт поддерживается для штатных журналов ОС Windows, журнала Secret Net или представления. Загруженные в программу записи можно сохранить полностью или выборочно. Загрузка содержимого dvt-файлов может осуществляться: • в программе просмотра журналов (см. стр. 15); • в программе "Контроль программ и данных" (см. документ [3]).
.evt (*.evt или *.evtx)	Стандартный формат журналов событий ОС Windows	Экспорт поддерживается для любого журнала, но только в режиме работы с локальными журналами. В файле сохраняется все содержимое выбранного журнала (включая те записи, которые не загружены в программу просмотра). Загрузка содержимого evt-файлов может осуществляться в программе просмотра журналов (см. стр. 15) или в других приложениях, поддерживающих данный формат. Например, в оснастке "Просмотр событий" ОС Windows. При загрузке записей журнала Secret Net укажите тип журнала безопасности ОС Windows

Для экспорта записей:

1. Выберите нужный журнал или представление.
2. Если требуется сохранить записи выборочно (при экспорте в mdb- или dvt-файл) — подготовьте список записей, используя следующие процедуры:
   - фильтрация загруженных записей (см. стр. 24);
   - выделение фрагмента записей.
3. В контекстном меню журнала или представления активируйте 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, при необходимости настройте дополнительные параметры экспорта и нажмите кнопку "ОК".

Экспортировать
Определяет, какие записи будут сохранены в mdb- или dvt-файле: • "Все" — сохраняются все записи, загруженные в программу просмотра (в том числе те, которые не удовлетворяют текущим параметрам фильтрации); • "Видимые" — сохраняются записи, соответствующие параметрам фильтрации; • "Из диапазона" — позволяет задать диапазон сохраняемых записей 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 сохранены; • "Выделенные" — сохраняются только те записи, которые выделены в таблице.
Удалить после просмотра
Если установлена отметка, будет выполнена автоматическая очистка журнала после экспорта записей в evt-файл. Для очистки журнала Secret Net пользователю должна быть предоставлена привилегия "Журнал: Управление журналом системы защиты" (см. стр. 10)

Очистка локального журнала

В режиме работы с локальными журналами программа просмотра позволяет выполнить очистку локальных журналов компьютера. Записи можно удалить из журнала при экспорте в evt-файл (см. стр. 28) или с помощью команды "Очистить" в контекстном меню папки журнала (команда "Очистить" может применяться только для штатных журналов ОС Windows).

В сетевом режиме функционирования системы Secret Net 6 очистка локальных журналов защищаемых компьютеров выполняется автоматически при передаче журналов на сервер безопасности. Процедура передачи локальных журналов запускается по заданному расписанию (см. документ [7]) или по команде пользователя в программе просмотра в режиме работы с централизованными журналами (см. стр. 22).

Архивирование централизованных журналов

В сетевом режиме функционирования системы Secret Net 6 в соответствии с заданным расписанием осуществляется автоматическое архивирование журналов, хранящихся в базе данных сервера безопасности (см. документ [7]). В режиме работы с централизованными журналами пользователь программы просмотра может использовать команду принудительного запуска процесса архивирования. Команда применима только для СБ, с которым установлено соединение программы.

Чтобы выполнять архивирование и очистку журналов, пользователю должна быть предоставлена привилегия "Архивирование журналов" (см. стр. 11).

Для архивирования и очистки журналов:

1. Запустите программу просмотра в режиме работы с централизованными журналами (см. стр. 11). При запуске программы установите соединение с тем СБ, журналы которого требуется архивировать.
2. В окне структуры выберите этот СБ и в меню "Сервер безопасности" активируйте команду "Архивировать...".

   На экране появится диалог для настройки параметров архивирования.
3. Настройте параметры архивирования и нажмите кнопку "ОК".

Группа полей "Дата и время"
Поля группы определяют границу интервала времени. В архив будут помещены записи, которые были зарегистрированы до указанного момента времени
Группа полей "Типы журналов"
Поля группы определяют типы журналов, записи которых должны архивироваться
Поле "Описание"
Введите в этом поле краткое описание создаваемого архива

Глава 5
Дополнительные средства программы

Использование срезов

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

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

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

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

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

Управление файлами срезов

Операции выполняются с помощью команд меню и кнопок панели инструментов.

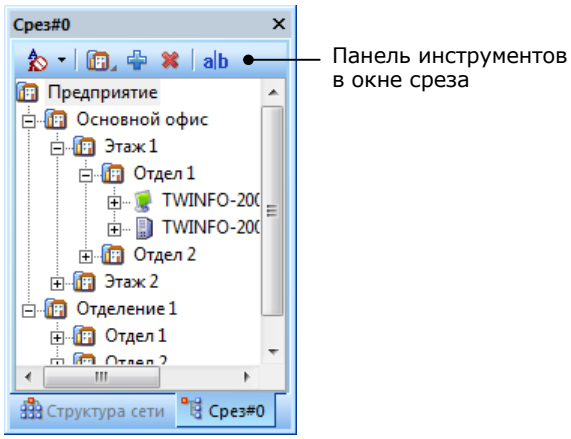
Табл. 4. Команды меню и кнопки для управления файлами срезов

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

Формирование содержимого среза

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

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



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

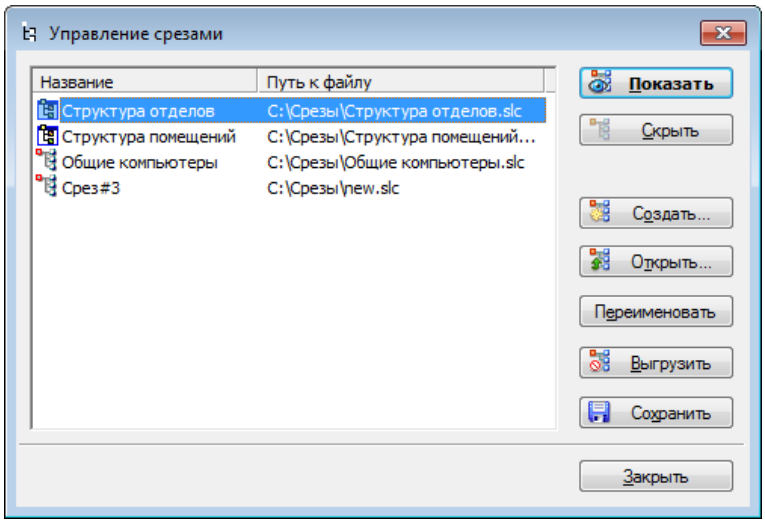
Табл. 5. Команды меню и кнопки для формирования содержимого среза

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

Местоположение элементов структуры можно изменять. Перемещение элементов осуществляется стандартным способом с помощью мыши. Кроме того, предусмотрена возможность сортировки объектов в окне среза (см. стр. 33).

Управление срезами в специальном диалоге

Диалог управления срезами предназначен для работы со списком загруженных срезов. Для вызова диалога активируйте команду "Сервис | Срезы...".



Список срезов в диалоге представлен в табличной форме. Колонка "Путь к файлу" содержит полные имена файлов, в которых сохранены срезы.

Для управления срезами используются кнопки диалога.

Табл. 6. Кнопки для управления срезами

Кнопка	Описание
Показать	Открывает окно среза. Окно выбранного среза добавится к отображаемым окнам программы. Если окно уже открыто, оно будет активировано (станет текущим окном)
Скрыть	Отключает отображение окна выбранного среза
Создать	Создает новый файл среза (команда "Файл | Добавить срез | Новый" в Табл. 4 на стр. 30)
Открыть	Выполняет загрузку среза из файла (команда "Файл | Добавить срез | Существующий" в Табл. 4 на стр. 30)
Переименовать	Включает режим редактирования для переименования выбранного среза
Выгрузить	Выгружает срез из программы без сохранения изменений (команда "Файл | Выгрузить срез" в Табл. 4 на стр. 30)
Сохранить	Сохраняет изменения в выбранном срезе (команда "Файл | Сохранить срез" в Табл. 4 на стр. 30)

Обновление структуры объектов

Обновление структуры объектов может выполняться только в режиме работы с централизованными журналами. Данная процедура позволяет заново загрузить в окно структуры иерархический список защищаемых компьютеров и серверов безопасности.

Для обновления структуры объектов:

1. Активируйте команду "Вид | Обновить структуру".

   На экране появится диалог запроса, содержащий предупреждение о последующей выгрузке всех загруженных записей из программы просмотра.
2. Нажмите кнопку "Да".

Формирование отчета по записям журнала

Программа просмотра 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.

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 представление.
2. Если требуется сохранить записи выборочно, подготовьте список записей, используя следующие процедуры:
   - фильтрация загруженных записей (см. стр. 24);
   - выделение фрагмента записей.
3. В контекстном меню журнала или представления активируйте 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/представления, 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 полное имя файла отчета и нажмите кнопку "Построить".

Сортировка компьютеров в иерархических списках

В режиме работы с централизованными журналами или в режиме просмотра архивов можно выполнять сортировку иерархических списков компьютеров, представленных в окне структуры объектов и в окнах срезов. Сортировка осуществляется в алфавитном порядке имен компьютеров (и папок среза) на каждом уровне иерархии. Можно применить прямой или обратный порядок сортировки. Если сортировка отключена, объекты располагаются в том порядке, в каком они были добавлены в структуру.

Для сортировки иерархических списков:

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

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

Приложение

Настройка элементов интерфейса

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

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

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

Состав отображаемых элементов интерфейса настраивается командами меню "Вид".

Табл. 7. Команды меню для управления элементами интерфейса

Команда	Описание
Вид | Строка статуса (Вид | Строка состояния)	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 | Детально о событии	Включает или отключает отображение окна дополнительных сведений

Параметры работы программы

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

Группа параметров "Общие | Подтверждения"

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

Группа параметров "Оформление журналов | Общие"

Группа 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" кроме пиктограмм типов событий будут показаны их названия ("Аудит успехов" и пр.). Перечень пиктограмм и названий типов событий приведен на стр. 40
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"

Группа содержит параметры цветового оформления фона записей для 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"

Группа параметров "Оформление журналов | Протоколы сессий"

Группа содержит параметры цветового оформления фона записей для журнала сессий (в режиме работы с локальными журналами эта группа отсутствует). 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 сессиям
Определяет режим цветового оформления фона записей в зависимости от типов сессий, во время которых регистрировались события: если установлено значение "Да", записи журнала окрашены в соответствии с цветами, которые заданы для параметров с названиями типов (все остальные параметры группы). Тип сессии определяется в зависимости от компонентов (приложений), выполнявших обращения к серверу безопасности: • "Собственные" — внутренние сессии сервера безопасности; • "Подчиненные" — сессии подчиненных серверов безопасности; • "Рабочие станции" — сессии клиентов системы защиты; • "Монитор" — сессии программы мониторинга; • "Программа просмотра журналов" — сессии программы просмотра журналов.

Группа параметров "Сетевой режим | Основные"

Группа присутствует только в режиме работы с централизованными журналами и содержит следующие параметры:

Запрос по фильтру
Если установлено значение "Да", при выборе журнала для загрузки записей или при обновлении записей (см. стр. 27) на экране будет появляться специальный диалог, позволяющий настроить параметры фильтрации записей по времени регистрации событий. Если установлено значение "Нет" — фильтрация не осуществляется
Отчетный период
Определяет интервал времени по умолчанию для диалога настройки параметров фильтрации. (Фильтрация записей при загрузке осуществляется, если для параметра "Запрос по фильтру" установлено значение "Да".) Параметр может принимать значения: • "за сутки" — 24-часовой интервал; • "за неделю" — 7-дневный интервал; • "за месяц" — 30-дневный интервал. Программа автоматически вычисляет интервал относительно текущего времени
Число журналов
Определяет максимальное количество журналов, загруженные записи которых хранятся в оперативной памяти при работе с программой просмотра. Если количество журналов, записи которых загружены в программу, больше указанного — программа высвобождает оперативную память от содержимого ранее загруженных журналов (выполняется перемещение соответствующих данных во временный файл). Хранение записей в оперативной памяти позволяет сократить время переходов между записями различных журналов. Параметр может принимать значения от 1 до 10
Записей на страницу
Определяет количество записей, отображаемых в программе при постраничной загрузке. Режим постраничной загрузки используется в тех случаях, когда программе не удается загрузить все необходимые записи по причине заполнения оперативной памяти. При загрузке каждой следующей страницы (группы записей) осуществляется высвобождение оперативной памяти от содержимого ранее загруженной страницы. Параметр может принимать значения от 10 000 до 100 000
Доменные имена
Если установлено значение "Да", в окне структуры и в окнах срезов отображаются полные имена компьютеров (в формате <*имя_компьютера*>.<*имя_домена*>). При отключенном режиме имена доменов в иерархических списках не указываются

Группа параметров "Сетевой режим | Транспорт"

Группа содержит параметры сетевого взаимодействия программы с сервером безопасности.

Тип соединения
Определяет шаблон настроек сетевого взаимодействия. Выберите нужный шаблон или настройте параметры вручную, раскрыв список "Ручные настройки" (описание параметров содержится на стр. 60)

Группа параметров "Сетевой режим | Привилегии"

Группа содержит список привилегий для работы с программой мониторинга и программой просмотра журналов. Список предназначен для ознакомления с текущим набором привилегий пользователя программы. Значение "Да" соответствует предоставленной привилегии. Предоставление привилегий пользователям осуществляется в программе конфигурирования (см. документ [7]).

Группа параметров "Просмотр архивов | Основные"

Группа присутствует только при работе программы в режиме просмотра архивов и содержит параметры, назначение которых аналогично одноименным параметрам в группе "Сетевой режим | Основные".

Средства для работы со списками объектов

Навигация при работе со структурами объектов

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

Табл. 8. Команды меню и кнопки для навигации в структуре объектов

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

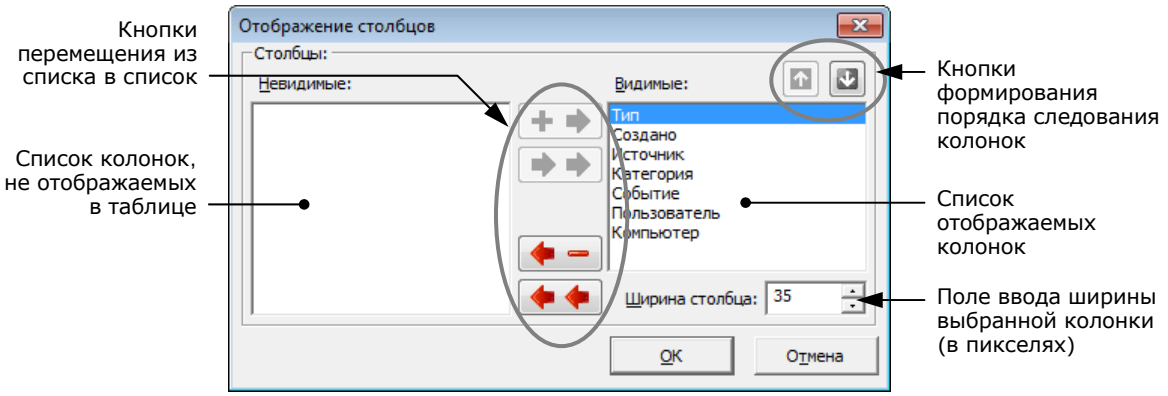
Настройка отображения колонок в таблицах

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

Для управления колонками с помощью диалога настройки:

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

   На экране появится диалог настройки параметров отображения колонок:



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

Для восстановления исходного состояния таблицы:

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

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

Пиктограммы объектов в сетевом режиме работы

Табл. 9. Пиктограммы компьютеров

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

Табл. 10. Пиктограммы журналов

Пиктограмма	Описание
	Штатный журнал ОС Windows (журнал приложений, системный журнал или журнал безопасности)
	Штатный журнал ОС Windows, для которого отключена функция централизованного сбора
	Журнал Secret Net
	Журнал сессий

Табл. 11. Пиктограммы представлений

Пиктограмма	Описание
	Несохраненное представление
	Сохраненное представление

Типы регистрируемых событий

Табл. 12. Типы событий, регистрируемых в журналах Windows и журнале Secret Net

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

Табл. 13. Типы событий, регистрируемых в журнале сессий

Пиктограмма, название типа	Описание
 Успех	Обозначает события, информирующие об успешном завершении операции
 Ошибка	Обозначает события, информирующие о возникшей ошибке при выполнении операции
	Обозначает события, информирующие о незавершенной операции или о том, что сессия была прекращена до завершения операции

События, регистрируемые в журнале Secret Net

Табл. 14. События категории "Вход/выход"

Название	ID	Тип	Описание
Завершение работы пользователя	1011	Аудит успехов	Сеанс работы пользователя в системе завершен. Имя пользователя и тип входа (локальный или терминальный) указаны в поле "Описание"
Электронный идентификатор не зарегистрирован	1013	Аудит отказов	Предъявленный персональный идентификатор (при входе пользователя в систему или при разблокировании компьютера) не сопоставлен ни с одним пользователем. В поле "Описание" указываются: • тип идентификатора ("iButton", "eToken" и пр.); • номер идентификатора.
Пользователь приостановил сеанс работы на компьютере	1014	Аудит успехов	Пользователь прервал работу, не завершая сеанс. Событие регистрируется, например, при смене пользователя или при закрытии окна терминальной сессии без завершения сеанса
Пользователь возобновил сеанс работы на компьютере	1015	Аудит успехов	Пользователь продолжил работу в текущем сеансе (ранее приостановленном)
Компьютер заблокирован системой защиты	1016	Аудит отказов	Блокировка компьютера была автоматически включена по одной из следующих причин: • нарушена аппаратная конфигурация компьютера; • нарушена целостность объектов контроля. Причина блокировки указана в поле "Описание"
Компьютер разблокирован	1017	Аудит успехов	Блокировка компьютера отключена администратором безопасности
Ошибка выполнения функционального контроля	1018	Аудит отказов	При загрузке компьютера обнаружены сбои в работе функциональных модулей системы защиты. Причины сбоев указаны в поле "Описание"
Успешное завершение функционального контроля	1019	Аудит успехов	Выполнена проверка работы функциональных модулей системы защиты. Сбои не обнаружены
Вход пользователя в систему	1200	Аудит успехов	В систему успешно вошел пользователь. В поле "Описание" указываются: • имя пользователя; • тип входа (локальный или терминальный); • назначенный уровень конфиденциальности для сессии работы пользователя (неконфиденциально, конфиденциально или строго конфиденциально); • режим аутентификации при входе (стандартная или усиленная); • режим входа (стандартный или по идентификатору).
Запрет входа пользователя	1201	Аудит отказов	Пользователю отказано во входе в систему. Причина запрета указывается в поле "Описание"

Табл. 15. События категории "Регистрация"

Название	ID	Тип	Описание
Старт службы регистрации	1020	Аудит успехов	Выполнен автоматический запуск службы регистрации событий при загрузке компьютера
Остановка службы регистрации	1021	Аудит успехов	Выполнена автоматическая остановка службы регистрации событий при выключении компьютера
Переполнение журнала регистрации	1024	Ошибки	Попытка регистрации новых записей привела к превышению максимально разрешенного объема журнала Secret Net
Очистка журнала регистрации	1025	Аудит успехов	На компьютере выполнена очистка журнала Secret Net. Имя evt-файла, в котором сохранены записи журнала перед выполнением очистки, указывается в поле "Описание"
Журнал регистрации отправлен на сервер	1026	Аудит успехов	Выполнена передача локального журнала Secret Net в базу данных на сервере безопасности. Имя evt-файла, временно созданного для передачи содержимого журнала, указывается в поле "Описание"

Табл. 16. События категории "Контроль печати"

Название	ID	Тип	Описание
Печать документа	1030	Аудит успехов	Выполнена печать неконфиденциального документа. В поле "Описание" указываются: • название документа; • имя процесса, осуществившего печать; • имя принтера; • имя временного файла, созданного при печати; • формат временного файла.
Печать конфиденциального документа	1031	Аудит успехов	Выполнена печать конфиденциального документа. В поле "Описание" указываются: • название документа; • имя файла, в котором хранится документ; • категория конфиденциальности файла; • число страниц в документе; • число копий документа; • регистрационный номер документа; • имя процесса, осуществившего печать; • имя принтера.
Прямое обращение к принтеру	1033	Аудит успехов	Выполнена печать документа посредством прямого обращения к порту принтера (например, из командной строки или с помощью DOS-программы). Данный способ печати возможен при отключенном режиме контроля печати конфиденциальных документов. В поле "Описание" указываются: • имя принтера или порта; • имя процесса, осуществившего печать.
Запрет прямого обращения к принтеру	1034	Аудит отказов	Пользователю отказано в печати документа посредством прямого обращения к порту принтера (например, из командной строки или с помощью DOS-программы). Причина запрета — включен режим контроля печати конфиденциальных документов. В поле "Описание" указываются: • имя принтера или порта; • имя процесса, осуществившего печать.
Запрет печати конфиденциального документа	1035	Аудит отказов	Пользователю отказано в выводе конфиденциального документа на печать (например, если пользователь не имеет привилегии на печать конфиденциальных документов или произошла попытка вывода документа без грифа конфиденциальности). В поле "Описание" указываются: • название документа; • имя процесса, осуществившего печать; • категория конфиденциальности файла (конфиденциально или строго конфиденциально); • имя принтера; • имя временного файла, созданного при печати; • формат временного файла; • причина запрета.

Табл. 17. События категории "Полномочное управление доступом"

Название	ID	Тип	Описание
Изменение категории конфиденциальности	1040	Аудит успехов	Изменена категория конфиденциальности файла или каталога. В поле "Описание" указываются: • имя файла (каталога); • имя процесса, выполнившего действие; • название новой категории конфиденциальности; • название старой категории конфиденциальности.

Название	ID	Тип	Описание
Запрет изменения параметров конфиденциальности ресурса	1041	Аудит отказов	Пользователю отказано в изменении категории конфиденциальности файла или каталога (например, если пользователь не имеет соответствующей привилегии или файлу присваивается более высокая категория, чем у каталога). В поле "Описание" указываются: • имя файла (каталога); • имя процесса, выполнявшего действие; • причина запрета.
Изменение признака наследования	1044	Аудит отказов	Для конфиденциального каталога установлен или отменен признак наследования. В поле "Описание" указываются: • имя каталога; • имя процесса, выполнившего действие; • значение признака (установлен/отменен).
Вывод конфиденциальной информации	1045	Аудит успехов	Выполнено сохранение конфиденциального файла на внешний носитель. В поле "Описание" указываются: • имя файла, указанного при сохранении (с полным путем к файлу на внешнем носителе); • имя процесса, выполнившего действие; • название категории конфиденциальности файла.
Запрет вывода конфиденциальной информации	1046	Аудит отказов	Выполнена попытка сохранения конфиденциального файла на внешний носитель. Из-за отсутствия соответствующей привилегии пользователю отказано в сохранении файла. В поле "Описание" указываются: • имя файла, указанного при сохранении (с полным путем к файлу на внешнем носителе); • имя процесса, выполнившего действие; • название категории конфиденциальности файла.
Доступ к конфиденциальному документу	1047	Аудит успехов	Выполнено открытие конфиденциального файла. В поле "Описание" указываются: • имя файла; • имя процесса, выполнившего действие; • название категории конфиденциальности файла; • текущий режим контроля потоков (включен/отключен); • вид запрошенного доступа к файлу (чтение/запись).
Запрет доступа к конфиденциальному документу	1048	Аудит отказов	Выполнена попытка открытия конфиденциального файла. Из-за недостаточного уровня допуска к конфиденциальной информации пользователю отказано в открытии файла. В поле "Описание" указываются: • имя файла; • имя процесса, выполнившего действие; • название категории конфиденциальности файла; • текущий режим контроля потоков (включен/отключен); • вид запрошенного доступа к файлу (чтение/запись).

Табл. 18. События категории "Замкнутая программная среда"

Название	ID	Тип	Описание
Запрет запуска программы	1050	Аудит отказов	Произошла попытка запуска программы, которая не входит в список разрешенных для запуска программ, или нарушена целостность исполняемого файла программы. Если используется "мягкий" режим замкнутой программной среды, запуск программы разрешается, несмотря на это событие. В "жестком" режиме пользователю будет отказано в запуске программы. В поле "Описание" указываются: • имя программы; • имя процесса, выполнившего действие; • режим работы механизма замкнутой программной среды; • причины запрета.

Название	ID	Тип	Описание
Запуск программы	1051	Аудит успехов	Выполнен запуск программы, которая удовлетворяет заданным условиям механизма замкнутой программной среды — программа входит в список разрешенных для запуска программ и целостность исполняемого файла программы не нарушена. В поле "Описание" указываются: • имя программы; • имя процесса, выполнившего действие; • режим работы механизма замкнутой программной среды.
Запрет загрузки библиотеки	1052	Аудит отказов	Произошла попытка загрузки динамической библиотеки (DLL), файл которой не входит в список разрешенных для запуска программ, или нарушена целостность файла библиотеки. Если используется "мягкий" режим замкнутой программной среды, загрузка разрешается, несмотря на это событие. В "жестком" режиме процессу будет отказано в загрузке библиотеки. В поле "Описание" указываются: • имя файла библиотеки; • имя процесса, выполнившего действие; • режим работы механизма замкнутой программной среды; • причины запрета. Событие регистрируется, если включен режим "Контроль заголовков" для механизма замкнутой программной среды. При выключенном режиме в таких случаях регистрируется событие "Запрет запуска программы"
Загрузка библиотеки	1053	Аудит успехов	Выполнена загрузка динамической библиотеки (DLL), которая удовлетворяет заданным условиям механизма замкнутой программной среды — файл библиотеки входит в список разрешенных для запуска программ и его целостность не нарушена. В поле "Описание" указываются: • имя файла библиотеки; • имя процесса, выполнившего действие; • режим работы механизма замкнутой программной среды. Событие регистрируется, если включен режим "Контроль заголовков" для механизма замкнутой программной среды. При выключенном режиме в таких случаях регистрируется событие "Запуск программы"
Исполнение скрипта	1054	Аудит успехов	Разрешено выполнение сценария (последовательность исполняемых команд и/или действий в текстовом виде, скрипт), который удовлетворяет заданным условиям механизма замкнутой программной среды — сценарий зарегистрирован в БД КЦ-ЗПС и его исполнение разрешено (сценарий включен в задание ЗПС). В поле "Описание" указываются: • имя файла сценария (если есть) или название сценария; • сведения о сценарии, хранящиеся в БД; • имя файла сценария, сохраненного в хранилище системы защиты; • имя процесса, выполнившего действие; • режим работы механизма замкнутой программной среды.

Название	ID	Тип	Описание
Запрет исполнения неизвестного скрипта	1055	Аудит отказов	Произошла попытка выполнения сценария (последовательность исполняемых команд и/или действий в текстовом виде, скрипт), который не зарегистрирован в БД КЦ-ЗПС. Если используется "мягкий" режим замкнутой программной среды, выполнение сценария разрешается, несмотря на это событие. В "жестком" режиме процессу будет отказано в исполнении сценария. В поле "Описание" указываются: • имя файла сценария (если есть) или название сценария; • имя файла сценария, сохраненного в хранилище системы защиты; • имя процесса, выполнившего действие; • режим работы механизма замкнутой программной среды; • причины запрета.
Запрет исполнения скрипта	1056	Аудит отказов	Произошла попытка выполнения сценария (последовательность исполняемых команд и/или действий в текстовом виде, скрипт), который зарегистрирован в БД КЦ-ЗПС, но его исполнение запрещено (сценарий не включен в задание ЗПС). Если используется "мягкий" режим замкнутой программной среды, выполнение сценария разрешается, несмотря на это событие. В "жестком" режиме процессу будет отказано в исполнении сценария. В поле "Описание" указываются: • имя файла сценария (если есть) или название сценария; • сведения о сценарии, хранящиеся в БД; • имя файла сценария, сохраненного в хранилище системы защиты; • имя процесса, выполнившего действие; • режим работы механизма замкнутой программной среды; • причины запрета.

Табл. 19. События категории "Расширение групповой политики"

Название	ID	Тип	Описание
Групповые политики успешно применены	1060	Аудит успехов	Новые заданные параметры групповых политик вступили в силу
Ошибка применения групповых политик	1061	Ошибки	При попытке применения параметров групповых политик произошла ошибка. Код ошибки указан в поле "Описание"
Предупреждение при применении групповых политик	1062	Предупреждения	При попытке применения параметров групповых политик обнаружено несоответствие версий шаблона групповой политики безопасности и клиента системы защиты. Для устранения несоответствия требуется синхронизировать версии (в зависимости от ситуации обновить шаблон на контроллере домена или обновить ПО клиента). В поле "Описание" указываются: • код предупреждения; • имя групповой политики.

Табл. 20. События категории "Служба репликации"

Название	ID	Тип	Описание
Ошибка создания контекста пользователя	1065	Ошибки	При входе пользователя в систему произошла ошибка формирования контекста пользователя для работы в системе защиты. В текущем сеансе работы пользователю предоставляются минимальные права или привилегии на работу в системе (в зависимости от того, при чтении каких данных произошла ошибка). В поле "Описание" указываются: • имя пользователя; • раздел данных контекста, при получении которых произошла ошибка (параметры полномочного доступа, открытый ключ пользователя, привилегии пользователя); • код ошибки.

Табл. 21. События категории "Контроль целостности"

Название	ID	Тип	Описание
Начало обработки задания на контроль целостности	1100	Аудит успехов	На компьютере началась проверка целостности ресурсов, входящих в задание на контроль целостности. Имя задания указано в поле "Описание"
Завершение обработки задания на контроль целостности	1101	Аудит успехов	На компьютере завершена проверка целостности ресурсов, входящих в задание на контроль целостности. Целостность всех проверенных ресурсов не нарушена. Имя задания указано в поле "Описание"
Обнаружено нарушение целостности при обработке задания	1102	Аудит отказов	На компьютере завершена проверка целостности ресурсов, входящих в задание на контроль целостности. В процессе проверки обнаружено нарушение целостности одного или нескольких ресурсов, входящих в задание. В поле "Описание" указываются: • имя задания; • тип реакции на отказ при контроле целостности, заданный для задания (блокировка компьютера, восстановление ресурса, принятие нового значения объекта в качестве эталонного).
Завершение проверки целостности ресурса	1103	Аудит успехов	При проверке целостности ресурса не обнаружено нарушений. В поле "Описание" указываются: • тип ресурса (файл, каталог, ключ реестра и пр.); • имя ресурса; • имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; • название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); • название алгоритма расчета контрольных сумм (CRC7, ЭЦП, Хеш и пр.), если в качестве метода контроля используется проверка содержимого; • имя связанной с заданием задачи, к которой относится ресурс; • имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием; • дополнительное описание процедуры проверки целостности (в случае необходимости). Например, параметры использованного эталонного значения для контроля целостности ресурса, если имеется несколько эталонов.

Название	ID	Тип	Описание
Нарушение целостности ресурса	1104	Аудит отказов	При проверке целостности ресурса обнаружено нарушение целостности. В поле "Описание" указываются: • тип ресурса (файл, каталог, ключ реестра и пр.); • имя ресурса; • имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; • название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); • название алгоритма расчета контрольных сумм (CRC7, ЭЦП, Хеш и пр.), если в качестве метода контроля используется проверка содержимого; • имя связанной с заданием задачи, к которой относится ресурс; • имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием; • дополнительное описание процедуры проверки целостности (в случае необходимости). Например, текущие и предыдущие параметры ресурса, когда это возможно отследить.
Для ресурса отсутствует эталонное значение	1105	Аудит отказов	Проверка целостности ресурса не была выполнена из-за отсутствия эталонного значения для контроля (например, если после формирования задания не были рассчитаны эталонные значения контролируемых параметров). В поле "Описание" указываются: • тип ресурса (файл, каталог, ключ реестра и пр.); • имя ресурса; • имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; • название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); • название алгоритма расчета контрольных сумм (CRC7, ЭЦП, Хеш и пр.), если в качестве метода контроля используется проверка содержимого; • имя связанной с заданием задачи, к которой относится ресурс; • имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием.
Удаление устаревших эталонных значений	1106	Аудит успехов	Системой автоматически удалены "устаревшие" эталонные значения для контроля целостности ресурса. Под устаревшими подразумеваются значения, имеющие более раннее время создания, чем то эталонное значение, с которым совпал результат проверки целостности ресурса. В поле "Описание" указываются: • тип ресурса (файл, каталог, ключ реестра и пр.); • имя ресурса; • имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; • название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); • название алгоритма расчета контрольных сумм (CRC7, ЭЦП, Хеш и пр.), если в качестве метода контроля используется проверка содержимого; • имя связанной с заданием задачи, к которой относится ресурс; • имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием; • время создания эталонного значения, с которым совпал полученный результат проверки целостности ресурса.

Название	ID	Тип	Описание
Текущее значение ресурса принято в качестве эталонного	1107	Аудит успехов	Полученное при контроле целостности значение контролируемого параметра ресурса сохранено в качестве эталонного значения. Событие происходит, если в параметрах задания, в состав которого входит ресурс, определена реакция принятия новых значений контролируемых параметров в качестве эталонных. В поле "Описание" указываются: • тип ресурса (файл, каталог, ключ реестра и пр.); • имя ресурса; • имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; • название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); • название алгоритма расчета контрольных сумм (CRC7, ЭЦП, Хеш и пр.), если в качестве метода контроля используется проверка содержимого; • имя связанной с заданием задачи, к которой относится ресурс; • имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием.
Восстановление ресурса	1108	Аудит успехов	Ресурс, у которого обнаружено нарушение целостности, был восстановлен с использованием эталонного значения. Событие происходит при условии физической возможности операции восстановления (например, невозможно восстановить файл, если контроль целостности осуществляется методом проверки существования). В поле "Описание" указываются: • тип ресурса (файл, каталог, ключ реестра и пр.); • имя ресурса; • имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; • название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); • название алгоритма расчета контрольных сумм (CRC7, ЭЦП, Хеш и пр.), если в качестве метода контроля используется проверка содержимого; • имя связанной с заданием задачи, к которой относится ресурс; • имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием; • дополнительное описание процедуры восстановления (в случае необходимости).
Ошибка при восстановлении ресурса по эталонному значению	1109	Ошибки	При попытке восстановления ресурса с использованием эталонного значения произошла ошибка (например, если у пользователя отсутствуют необходимые права). В поле "Описание" указываются: • тип ресурса (файл, каталог, ключ реестра и пр.); • имя ресурса; • имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; • название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); • название алгоритма расчета контрольных сумм (CRC7, ЭЦП, Хеш и пр.), если в качестве метода контроля используется проверка содержимого; • имя связанной с заданием задачи, к которой относится ресурс; • имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием; • дополнительное описание процедуры восстановления (в случае необходимости).

Название	ID	Тип	Описание
Ошибка при открытии базы данных контроля целостности	1110	Ошибки	При попытке обращения к локальной базе данных контроля целостности произошла ошибка (например, если база данных повреждена). Место нахождения базы данных указано в поле "Описание"
Ошибка принятия текущего значения ресурса в качестве эталонного	1112	Ошибки	При попытке принять полученное значение контролируемого параметра ресурса в качестве эталонного значения произошла ошибка (например, если ресурс отсутствует). Событие регистрируется при контроле целостности, если в параметрах задания, в состав которого входит ресурс, определена реакция принятия новых значений объектов в качестве эталонных. В поле "Описание" указываются: • тип ресурса (файл, каталог, ключ реестра и пр.); • имя ресурса; • имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; • название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); • название алгоритма расчета контрольных сумм (CRC7, ЭЦП, Хеш и пр.), если в качестве метода контроля используется проверка содержимого; • имя связанной с заданием задачи, к которой относится ресурс; • имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием; • дополнительное описание процедуры проверки целостности (в случае необходимости).
Исправление ошибок в базе данных	1113	Предупреждения	Обнаружены и автоматически исправлены ошибки в базе данных подсистемы контроля целостности и замкнутой программной среды (например, если обнаружены связи с отсутствующими объектами, эти связи удаляются). Место нахождения базы данных указано в поле "Описание"
Установка задания КЦ на контроль	1150	Аудит успехов	В программе управления (в режиме работы с локальной БД) установлена связь между заданием на контроль целостности и субъектом (компьютером). Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: • имя задания; • параметры расписания выполнения задания.
Снятие задания КЦ с контроля	1151	Аудит успехов	В программе управления (в режиме работы с локальной БД) удалена связь между заданием на контроль целостности и субъектом (компьютером). Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: • имя задания; • параметры расписания выполнения задания.
Добавление учетной записи к заданию ЗПС	1152	Аудит успехов	В программе управления (в режиме работы с локальной БД) установлена связь между заданием замкнутой программной среды и субъектом (пользователем). Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: • имя задания; • имя учетной записи, с которой связано задание.
Удаление учетной записи из задания ЗПС	1153	Аудит успехов	В программе управления (в режиме работы с локальной БД) удалена связь между заданием замкнутой программной среды и субъектом (пользователем). Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: • имя задания; • имя учетной записи, с которой было связано задание.

Название	ID	Тип	Описание
Создание задания	1154	Аудит успехов	В программе управления (в режиме работы с локальной БД) создан объект "Задание". Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: • имя задания; • название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); • название алгоритма расчета контрольных сумм (CRC7, ЭЦП, Хеш и пр.), если в качестве метода контроля используется проверка содержимого; • параметры расписания выполнения задания; • тип реакции при успешном выполнении контроля целостности (включена или нет регистрация событий); • тип реакции на отказ при контроле целостности (блокировка компьютера, восстановление ресурса и т. п.).
Удаление задания	1155	Аудит успехов	В программе управления (в режиме работы с локальной БД) удален объект "Задание". Событие регистрируется после сохранения модели данных программы. Имя задания указано в поле "Описание"
Изменение задания	1156	Аудит успехов	В программе управления (в режиме работы с локальной БД) изменены параметры объекта "Задание". Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: • имя задания (то, которое было до изменения параметров); • перечень измененных параметров; • новое имя задания (если имя было изменено).
Создание задачи	1157	Аудит успехов	В программе управления (в режиме работы с локальной БД) создан объект "Задача". Событие регистрируется после сохранения модели данных программы. Имя задачи указано в поле "Описание"
Удаление задачи	1158	Аудит успехов	В программе управления (в режиме работы с локальной БД) удален объект "Задача". Событие регистрируется после сохранения модели данных программы. Имя задачи указано в поле "Описание"
Изменение задачи	1159	Аудит успехов	В программе управления (в режиме работы с локальной БД) изменены параметры объекта "Задача". Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: • имя задачи (то, которое было до изменения параметров); • перечень измененных параметров; • новое имя задачи (если имя было изменено).
Создание группы ресурсов	1160	Аудит успехов	В программе управления (в режиме работы с локальной БД) создан объект "Группа ресурсов". Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: • имя группы ресурсов; • какие типы ресурсов могут включаться в группу (файлы/каталоги или объекты реестра).
Удаление группы ресурсов	1161	Аудит успехов	В программе управления (в режиме работы с локальной БД) удален объект "Группа ресурсов". Событие регистрируется после сохранения модели данных программы. Имя группы ресурсов указано в поле "Описание"
Изменение группы ресурсов	1162	Аудит успехов	В программе управления (в режиме работы с локальной БД) изменены параметры объекта "Группа ресурсов". Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: • имя группы ресурсов (то, которое было до изменения параметров); • перечень измененных параметров; • новое имя группы ресурсов (если имя было изменено).
Синхронизация локальной базы данных с центральной	1163	Аудит успехов	Выполнена синхронизация локальной и центральной базы данных контроля целостности и замкнутой программной среды (КЦ–ЗПС)

Название	ID	Тип	Описание
Ошибка синхронизации локальной базы данных с центральной	1164	Ошибки	При попытке синхронизации локальной и центральной базы данных КЦ-ЗПС произошла ошибка. Сведения об ошибке указаны в поле "Описание"

Табл. 22. События категории "ЦУ КЦ-ЗПС"

Название	ID	Тип	Описание
Установка задания КЦ на контроль	1210	Аудит успехов	В программе управления (в режиме работы с центральной БД) установлена связь между заданием на контроль целостности и субъектом. В поле "Описание" указываются: • имя задания; • тип субъекта (компьютер или группа, включающая компьютеры); • SID учетной записи субъекта; • параметры расписания выполнения задания.
Снятие задания КЦ с контроля	1211	Аудит успехов	В программе управления (в режиме работы с центральной БД) удалена связь между заданием на контроль целостности и субъектом. В поле "Описание" указываются: • имя задания; • тип субъекта (компьютер или группа, включающая компьютеры); • SID учетной записи субъекта; • параметры расписания выполнения задания.
Добавление учетной записи к заданию ЗПС	1212	Аудит успехов	В программе управления (в режиме работы с центральной БД) установлена связь между заданием замкнутой программной среды и субъектом. В поле "Описание" указываются: • имя задания; • тип субъекта (компьютер или группа, включающая компьютеры); • SID учетной записи субъекта.
Удаление учетной записи из задания ЗПС	1213	Аудит успехов	В программе управления (в режиме работы с центральной БД) удалена связь между заданием замкнутой программной среды и субъектом. В поле "Описание" указываются: • имя задания; • тип субъекта (компьютер или группа, включающая компьютеры); • SID учетной записи субъекта.
Создание задания	1214	Аудит успехов	В программе управления (в режиме работы с центральной БД) создан объект "Задание". В поле "Описание" указываются: • имя задания; • тип задания (тиражируемое/нетиражируемое); • название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); • название алгоритма расчета контрольных сумм (CRC7, ЭЦП, Хеш и пр.), если в качестве метода контроля используется проверка содержимого; • параметры расписания выполнения задания; • тип реакции при успешном выполнении контроля целостности (включена или нет регистрация событий); • тип реакции на отказ при контроле целостности (блокировка компьютера, восстановление ресурса, принятие нового значения объекта в качестве эталонного).
Удаление задания	1215	Аудит успехов	В программе управления (в режиме работы с центральной БД) удален объект "Задание". Имя задания указано в поле "Описание"

Название	ID	Тип	Описание
Изменение задания	1216	Аудит успехов	В программе управления (в режиме работы с центральной БД) изменены параметры объекта "Задание". В поле "Описание" указываются: • имя задания (то, которое было до изменения параметров); • перечень измененных параметров; • новое имя задания (если имя было изменено).
Создание задачи	1217	Аудит успехов	В программе управления (в режиме работы с центральной БД) создан объект "Задача". Имя задачи указано в поле "Описание"
Удаление задачи	1218	Аудит успехов	В программе управления (в режиме работы с центральной БД) удален объект "Задача". Имя задачи указано в поле "Описание"
Изменение задачи	1219	Аудит успехов	В программе управления (в режиме работы с центральной БД) изменены параметры объекта "Задача". В поле "Описание" указываются: • имя задачи (то, которое было до изменения параметров); • перечень измененных параметров; • новое имя задачи (если имя было изменено).
Создание группы ресурсов	1220	Аудит успехов	В программе управления (в режиме работы с центральной БД) создан объект "Группа ресурсов". В поле "Описание" указываются: • имя группы ресурсов; • какие типы ресурсов могут включаться в группу (файлы/каталоги или объекты реестра).
Удаление группы ресурсов	1221	Аудит успехов	В программе управления (в режиме работы с центральной БД) удален объект "Группа ресурсов". Имя группы ресурсов указано в поле "Описание"
Изменение группы ресурсов	1222	Аудит успехов	В программе управления (в режиме работы с центральной БД) изменены параметры объекта "Группа ресурсов". В поле "Описание" указываются: • имя группы ресурсов (то, которое было до изменения параметров); • перечень измененных параметров; • новое имя группы ресурсов (если имя было изменено).
Добавление субъекта	1223	Аудит успехов	В программе управления (в режиме работы с центральной БД) добавлен субъект управления. В поле "Описание" указываются: • SID учетной записи субъекта; • тип субъекта (компьютер или группа, включающая компьютеры); • заданные параметры субъекта.
Удаление субъекта	1224	Аудит успехов	В программе управления (в режиме работы с центральной БД) удален субъект управления. В поле "Описание" указываются: • SID учетной записи субъекта; • тип субъекта (компьютер или группа, включающая компьютеры).
Изменение субъекта	1225	Аудит успехов	В программе управления (в режиме работы с центральной БД) изменены параметры субъекта управления. В поле "Описание" указываются: • SID учетной записи субъекта; • тип субъекта (компьютер или группа, включающая компьютеры); • перечень измененных параметров.

Табл. 23. События категории "Контроль конфигурации"

Название	ID	Тип	Описание
Успешное завершение контроля аппаратной конфигурации	1120	Аудит успехов	Завершена процедура контроля аппаратной конфигурации при загрузке компьютера. Состояние контролируемых устройств не изменилось. Новые устройства не обнаружены. Текущий режим работы подсистемы контроля аппаратной конфигурации ("мягкий" или "жесткий") указан в поле "Описание"

Название	ID	Тип	Описание
Ошибка при контроле аппаратной конфигурации	1121	Аудит отказов	Завершена процедура контроля аппаратной конфигурации при загрузке компьютера. Текущая конфигурация не соответствует сохраненному списку устройств компьютера (т. е. обнаружены факты изменения состояния устройств или добавления новых). Если используется "мягкий" режим контроля, загрузка компьютера не прерывается, несмотря на это событие. В "жестком" режиме компьютер блокируется. Режим, в котором работает подсистема контроля аппаратной конфигурации, указан в поле "Описание"
Обнаружено новое устройство	1122	Аудит отказов	При контроле аппаратной конфигурации компьютера обнаружено новое подключенное устройство. Если используется "мягкий" режим контроля, загрузка компьютера или работа пользователя не прерывается, несмотря на это событие. В "жестком" режиме компьютер блокируется. В поле "Описание" указываются: • название группы, к которой относится устройство (USB-устройство, локальное устройство и пр.); • название класса, к которому относится устройство (принтер, локальный диск и пр.); • описание устройства; • режим, в котором работает подсистема контроля аппаратной конфигурации.
Устройство удалено из системы	1123	Аудит отказов	При контроле аппаратной конфигурации не было найдено устройство, входящее в список устройств компьютера. Если используется "мягкий" режим контроля, загрузка компьютера или работа пользователя не прерывается, несмотря на это событие. В "жестком" режиме компьютер блокируется. В поле "Описание" указываются: • название группы, к которой относится устройство (USB-устройство, локальное устройство и пр.); • название класса, к которому относится устройство (принтер, локальный диск и пр.); • описание устройства; • режим, в котором работает подсистема контроля аппаратной конфигурации.
Изменение параметров устройства	1124	Аудит отказов	При контроле аппаратной конфигурации при загрузке компьютера обнаружено изменение физического параметра устройства (например, объем памяти). Если используется "мягкий" режим контроля, загрузка компьютера или работа пользователя не прерывается, несмотря на это событие. В "жестком" режиме компьютер блокируется. В поле "Описание" указываются: • название группы, к которой относится устройство (USB-устройство, локальное устройство и пр.); • название класса, к которому относится устройство (принтер, локальный диск и пр.); • описание устройства; • режим, в котором работает подсистема контроля аппаратной конфигурации; • название измененного параметра; • текущее значение параметра; • предыдущее значение параметра.
Утверждение аппаратной конфигурации	1131	Аудит успехов	Текущая аппаратная конфигурация компьютера утверждена администратором. С этого момента данная аппаратная конфигурация считается эталонной

Табл. 24. События категории "Разграничение доступа к устройствам"

Название	ID	Тип	Описание
Подключение устройства	1125	Аудит успехов	Во время работы пользователя на компьютере произошло подключение устройства. Пользователь обладает разрешением на подключение данного устройства. В поле "Описание" указываются: • название группы, к которой относится устройство (USB-устройство, локальное устройство и пр.); • название класса, к которому относится устройство (принтер, локальный диск и пр.); • описание устройства; • режим, в котором работает подсистема разграничения доступа к устройствам.
Отключение устройства	1126	Аудит успехов	Во время работы пользователя на компьютере произошло отключение устройства. Пользователь обладает разрешением на отключение данного устройства. В поле "Описание" указываются: • название группы, к которой относится устройство (USB-устройство, локальное устройство и пр.); • название класса, к которому относится устройство (принтер, локальный диск и пр.); • описание устройства; • режим, в котором работает подсистема разграничения доступа к устройствам.
Запрет подключения устройства	1127	Аудит отказов	Во время работы пользователя на компьютере произошла попытка подключения устройства. Пользователь не обладает разрешением на подключение данного устройства. Если используется "мягкий" режим работы подсистемы разграничения доступа, устройство функционирует без ограничений, несмотря на это событие. В "жестком" режиме работа устройства блокируется. В поле "Описание" указываются: • название группы, к которой относится устройство (USB-устройство, локальное устройство и пр.); • название класса, к которому относится устройство (принтер, локальный диск и пр.); • описание устройства; • режим, в котором работает подсистема разграничения доступа к устройствам.
Несанкционированное отключение устройства	1128	Аудит отказов	Во время работы пользователя на компьютере произошло отключение устройства. Пользователь не обладает разрешением на отключение данного устройства. В поле "Описание" указываются: • название группы, к которой относится устройство (USB-устройство, локальное устройство и пр.); • название класса, к которому относится устройство (принтер, локальный диск и пр.); • описание устройства; • режим, в котором работает подсистема разграничения доступа к устройствам.
Доступ к устройству	1132	Аудит успехов	Во время работы пользователя на компьютере было использовано устройство. Пользователь обладает разрешением на доступ к данному устройству. В поле "Описание" указываются: • название группы, к которой относится устройство (USB-устройство, локальное устройство и пр.); • название класса, к которому относится устройство (принтер, локальный диск и пр.); • описание устройства; • имя процесса, выполнившего обращение; • режим, в котором работает подсистема разграничения доступа к устройствам; • описание запрошенного доступа.

Название	ID	Тип	Описание
Запрет доступа к устройству	1133	Аудит отказов	Во время работы пользователя на компьютере произошла попытка использования устройства. Пользователь не обладает разрешением на доступ к данному устройству. Если используется "мягкий" режим работы подсистемы разграничения доступа, доступ к устройству разрешается, несмотря на это событие. В "жестком" режиме доступ к устройству блокируется. В поле "Описание" указываются: • название группы, к которой относится устройство (USB-устройство, локальное устройство и пр.); • название класса, к которому относится устройство (принтер, локальный диск и пр.); • описание устройства; • имя процесса, выполнившего обращение; • режим, в котором работает подсистема разграничения доступа к устройствам; • описание запрошенного доступа; • описание прав пользователя на доступ к устройству.

Табл. 25. События категории "Сетевые подключения"

Название	ID	Тип	Описание
Запрет использования сетевого интерфейса	1240	Информация	Сетевой интерфейс отключен системой защиты. Событие регистрируется при загрузке ОС или при попытке подключения сетевого интерфейса, для которого установлен запрет использования. В поле "Описание" указываются: • название интерфейса; • код выполнения операции.
Запрет сетевого подключения под другим именем	1242	Аудит отказов	Произошла попытка запуска команды или сетевого подключения с вводом учетных данных пользователя, который не выполнил интерактивный вход в систему. Действие блокировано системой защиты. В поле "Описание" указываются: • сведения о сессии пользователя, ресурсе, имени подключаемого диска; • имя пользователя.

Табл. 26. События категории "Администрирование"

Название	ID	Тип	Описание
Добавлен пользователь	1140	Аудит успехов	Пользователь добавлен в локальную базу данных системы защиты. Имя или SID пользователя указывается в поле "Описание"
Удален пользователь	1141	Аудит успехов	Пользователь удален из локальной базы данных системы защиты. Имя или SID пользователя указывается в поле "Описание"
Изменены параметры пользователя	1142	Аудит успехов	Изменены параметры или привилегии пользователя: В поле "Описание" указываются: • имя или SID пользователя; • разделы параметров пользователя, в которых сделаны изменения (параметры полномочного доступа, привилегии пользователя, параметры электронных идентификаторов).
Изменен ключ пользователя	1143	Аудит успехов	Выполнена смена закрытого ключа пользователя. В поле "Описание" указываются: • имя или SID пользователя; • инициатор смены ключа (администратор безопасности или сам пользователь); • сведения о предыдущем закрытом ключе.

Название	ID	Тип	Описание
Изменены параметры действующей политики безопасности	1144	Аудит успехов	Изменены параметры системы защиты в консоли локальной политики безопасности. В поле "Описание" указываются названия разделов, в которых сделаны изменения (настройки подсистемы контроля печати, настройки подсистемы полномочного управления доступом, привилегии пользователей и групп, настройки политики аудита и др.)
Удален ключ пользователя	1145	Аудит успехов	Закрытый ключ пользователя удален. В поле "Описание" указываются: • имя или SID пользователя; • сведения о закрытом ключе.

Табл. 27. События категории "ПАК "Соболь"[1]

Название	ID	Тип	Описание
Соболь: вход пользователя	1170	Аудит успехов	Программно-аппаратным комплексом (ПАК) "Соболь" успешно выполнены идентификация и аутентификация пользователя. Вход пользователя в систему разрешен. В поле "Описание" указываются: • номер предъявленного персонального идентификатора; • имя пользователя.
Соболь: не рассчитаны контрольные суммы	1171	Аудит отказов	После инициализации ПАК "Соболь" для контролируемых объектов не были рассчитаны эталонные значения контрольных сумм при настройке подсистемы контроля целостности. Если используется "мягкий" режим контроля целостности, загрузка компьютера разрешается, несмотря на это событие. В "жестком" режиме вход пользователя в систему будет заблокирован. В поле "Описание" указываются: • номер предъявленного персонального идентификатора; • имя пользователя.
Соболь: изменение режима работы	1172	Аудит успехов	ПАК "Соболь" переведен пользователем в другой режим работы (автономный или сетевой). В автономном режиме управление работой ПАК "Соболь" осуществляется только средствами администрирования программно-аппаратного комплекса. При этом регистрация событий категории "ПАК "Соболь" в журнале Secret Net прекращается. В сетевом режиме ПАК "Соболь" функционирует совместно с СЗИ Secret Net 6 и часть функций управления передается средствам управления системы защиты. В поле "Описание" указываются: • номер предъявленного персонального идентификатора; • имя пользователя; • название включенного режима работы.
Соболь: очистка журнала	1173	Аудит успехов	Пользователем выполнена очистка системного журнала ПАК "Соболь" В поле "Описание" указываются: • номер предъявленного персонального идентификатора; • имя пользователя.
Соболь: ошибка синхронизации параметров	1174	Ошибки	Обнаружена ошибка при обработке запроса, поступившего к ПАК "Соболь". Запрос не был обработан. Ошибка может быть вызвана тем, что запрос поступил от внешней программы, не относящейся к СЗИ Secret Net 6
Соболь: перерасчет контрольных сумм	1175	Аудит успехов	Выполнен расчет эталонных значений контрольных сумм для контролируемых объектов. Запуск процедуры расчета может быть выполнен по команде администратора ПАК "Соболь" или по запросу, поступившему от СЗИ Secret Net 6. В поле "Описание" указываются: • номер предъявленного персонального идентификатора; • имя пользователя.

[1] В связи с особенностями регистрации записи о событиях категории "ПАК "Соболь" содержат в поле "Пользователь" значение "SYSTEM". Для большинства зарегистрированных событий правильное имя пользователя, действия которого привели к возникновению события, указано в поле "Описание".

Название	ID	Тип	Описание
Соболь: смена аутентификатора	1176	Аудит успехов	Выполнена смена аутентификатора пользователя. В поле "Описание" указываются: • номер предъявленного персонального идентификатора; • имя пользователя.
Соболь: запрет входа пользователя	1177	Аудит отказов	Пользователю отказано во входе в систему. В поле "Описание" указываются: • номер предъявленного персонального идентификатора; • имя пользователя; • причина запрета (предъявлен незарегистрированный идентификатор, введен неправильный пароль, пользователь заблокирован).
Соболь: нарушена целостность ресурса	1178	Аудит отказов	При проверке целостности контролируемого объекта средствами ПАК "Соболь" обнаружено несовпадение полученных и эталонных значений контрольных сумм или не найдены файлы шаблонов для контроля целостности. В поле "Описание" указываются: • номер предъявленного персонального идентификатора; • имя пользователя; • тип ресурса (сектор диска или файл); • имя ресурса; • дополнительные сведения.
Соболь: синхронизация параметров	1179	Аудит успехов	Обработан запрос, поступивший к ПАК "Соболь", или изменен список пользователей программно-аппаратного комплекса (добавлены или удалены пользователи). Сведения о выполненном действии указаны в поле "Описание"
Соболь: смена пароля	1180	Аудит успехов	Пароль пользователя был изменен. В поле "Описание" указываются: • номер персонального идентификатора, принадлежащего пользователю, которому сменили пароль; • имя пользователя, сменившего пароль; • имя пользователя, пароль которого изменен.
Соболь: включен режим совместной работы с Secret Net	1181	Аудит успехов	Средствами администрирования системы Secret Net 6 включен режим интеграции с ПАК "Соболь"
Соболь: ошибка при включении режима совместной работы с Secret Net	1182	Ошибки	При попытке включения режима интеграции ПАК "Соболь" и системы Secret Net 6 произошла ошибка. Сведения об ошибке указаны в поле "Описание"
Соболь: выключен режим совместной работы с Secret Net	1183	Аудит успехов	Средствами администрирования системы Secret Net 6 отключен режим интеграции с ПАК "Соболь"
Соболь: ошибка при выключении режима совместной работы с Secret Net	1184	Ошибки	При попытке отключения режима интеграции ПАК "Соболь" и системы Secret Net 6 произошла ошибка. Сведения об ошибке указаны в поле "Описание"
Соболь: ошибка КС в памяти идентификатора	1185	Ошибки	Обнаружена ошибка при проверке контрольной суммы содержимого персонального идентификатора (например, из-за неисправности идентификатора). В поле "Описание" указываются: • номер предъявленного персонального идентификатора; • имя пользователя.
Соболь: изменены параметры загрузочного диска	1186	Аудит успехов	На компьютере произошла смена основного загрузочного диска (например, если выполнена загрузка с внешнего носителя)

Табл. 28. События категории "Общие события"

Название	ID	Тип	Описание
Событие	1000	Аудит успехов	Некоторое событие, зарегистрированное системой, которое означает успешное выполнение определенного действия. В поле "Описание" указывается информация о процессе, зарегистрировавшем событие, и другие необходимые данные. Включение режима регистрации таких событий осуществляется отдельно
Несанкционированное действие	1001	Аудит отказов	Некоторое событие, зарегистрированное системой, которое означает отказ в выполнении определенного действия. В поле "Описание" указывается информация о процессе, зарегистрировавшем событие, и другие необходимые данные. Включение режима регистрации таких событий осуществляется отдельно
Ошибка	1002	Ошибки	Некоторое событие, зарегистрированное системой, которое означает возникшие неполадки при выполнении определенного действия. В поле "Описание" указывается информация о процессе, зарегистрировавшем событие, и другие необходимые данные. Включение режима регистрации таких событий осуществляется отдельно
Предупреждение	1003	Предупреждения	Некоторое событие, зарегистрированное системой, которое предупреждает о создавшейся угрозе для безопасности системы. В поле "Описание" указывается информация о процессе, зарегистрировавшем событие, и другие необходимые данные. Включение режима регистрации таких событий осуществляется отдельно
Отладочное событие	1004	Информация	Некоторое событие, зарегистрированное системой, которое относится к событиям отладки программ. В поле "Описание" указывается информация о процессе, зарегистрировавшем событие, и другие необходимые данные. Включение режима регистрации таких событий осуществляется отдельно
Нарушение лицензионной политики	1005	Ошибки	Обнаружено несоответствие перечня используемых функций и текущего варианта применения системы Secret Net 6, определенного лицензией

Поля записей журнала сессий

Табл. 29. Перечень полей, составляющих запись журнала сессий

Поле	Описание
Тип	Тип зарегистрированного события. Перечень пиктограмм и названий типов событий, регистрируемых в журнале сессий, см. в Табл. 13 на стр. 40
Время операции	Дата и время выполнения операции
Операция	Название операции, например, "Инициирование процедуры получения журнала"
Начало сессии	Дата и время открытия сессии
Конец сессии	Дата и время закрытия сессии. Если на момент запроса журнала сессия продолжается, поле пустое
Код завершения сессии	Код, возвращенный системой при закрытии сессии. При нормальном завершении сессии поле содержит нулевое значение. Все остальные значения являются кодами ошибок. Если на момент запроса журнала сессия продолжается, поле пустое
Приложение	Имя программы, открывшей сессию. Поле может содержать значения: • "Agent" — клиент системы защиты; • "Monitor" — программа мониторинга; • "Log Manager" — программа просмотра журналов; • "OMS Service" — сервер безопасности.
Компьютер	Имя компьютера, с которого поступил запрос на открытие сессии
Пользователь	Имя пользователя, использовавшего программу для открытия сессии

Параметры сетевого взаимодействия

Табл. 30. Перечень параметров сетевого взаимодействия компонентов

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

Терминологический справочник

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

Документация

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

Предметный указатель