

Код безопасности
ГК «Информзащита»

Средство защиты информации

SECRET NET 6



Руководство администратора

Управление. Основные механизмы защиты

RU.88338853.501410.007 91 3



© **Компания "Код Безопасности", 2010. Все права защищены.**

Все авторские права на эксплуатационную документацию защищены.

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

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

| | |
|-----------------|---|
| Почтовый адрес: | 127018, г. Москва, ул. Суцёвский 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 |

Оглавление

| | |
|--|-----------|
| Список сокращений | 6 |
| Введение | 7 |
| Глава 1. Общие принципы управления | 8 |
| Функции администратора безопасности | 8 |
| Организация управления системой защиты | 8 |
| Централизованное и локальное управление | 8 |
| Использование групповых политик | 9 |
| Делегирование административных полномочий | 10 |
| Параметры механизмов защиты и средства управления | 11 |
| Параметры объектов групповой политики | 11 |
| Параметры пользователей | 12 |
| Атрибуты ресурсов | 14 |
| Параметры механизмов КЦ и ЗПС | 14 |
| Контекстное меню пиктограммы Secret Net 6 | 14 |
| Глава 2. Защита входа в систему | 15 |
| Управление персональными идентификаторами | 15 |
| Просмотр сведений об идентификаторах пользователя | 16 |
| Предъявление идентификатора | 16 |
| Инициализация идентификатора | 17 |
| Присвоение идентификатора | 17 |
| Настройка режимов использования идентификаторов | 19 |
| Удаление идентификатора | 21 |
| Проверка принадлежности | 22 |
| Смена пароля | 22 |
| Управление режимами механизма защиты входа в систему | 23 |
| Управление ключами для усиленной аутентификации | 24 |
| Генерация и выдача ключей | 24 |
| Копирование ключей | 26 |
| Настройка параметров смены ключей | 26 |
| Использование ПАК "Соболь" в режиме интеграции с Secret Net 6 | 27 |
| Управление ключами централизованного управления ПАК "Соболь" | 27 |
| Копирование идентификатора администратора ПАК "Соболь" | 29 |
| Предоставление доступа к компьютерам с ПАК "Соболь" | 30 |
| Глава 3. Управление устройствами | 32 |
| Общие принципы | 32 |
| Списки устройств | 32 |
| Режимы работы | 33 |
| Настройки по умолчанию | 33 |
| Способы управления в автономном режиме функционирования | 34 |
| Способы управления в сетевом режиме функционирования | 35 |
| Правила наследования | 36 |
| Особенности применения групповых политик | 36 |
| Задание групповой политики и просмотр списка устройств | 37 |
| Экспорт параметров устройств | 39 |
| Контроль аппаратной конфигурации компьютера | 39 |
| Задание и настройка политики контроля | 39 |
| Изменение перечня регистрируемых событий | 41 |
| Изменение режима работы механизма | 41 |
| Утверждение конфигурации | 41 |
| Добавление устройств в аппаратную конфигурацию | 41 |
| Избирательное разграничение доступа к устройствам | 42 |
| Задание политики и настройка прав доступа к устройствам | 42 |
| Настройка регистрации событий и аудита операций | 44 |
| Изменение режима работы механизма | 44 |
| Глава 4. Контроль целостности и замкнутая программная среда | 45 |

| | |
|---|-----------|
| Модель данных | 45 |
| Способы и средства настройки | 46 |
| Управление работой механизмов..... | 46 |
| Принципы настройки в сетевом режиме функционирования | 46 |
| Настройка механизма | 48 |
| Задачи, возникающие в процессе эксплуатации..... | 48 |
| Этап 1. Подготовка к построению модели данных | 49 |
| Этап 2. Построение фрагмента модели данных по умолчанию..... | 49 |
| Этап 3. Добавление задач в модель данных..... | 50 |
| Этап 4. Добавление заданий и включение в них задач | 52 |
| Этап 5. Подготовка ЗПС к использованию..... | 55 |
| Этап 6. Расчет эталонов | 57 |
| Этап 7. Включение ЗПС в "жестком" режиме | 58 |
| Этап 8. Включение механизма КЦ | 59 |
| Этап 9. Проверка заданий | 59 |
| Хранение и перенос модели данных..... | 59 |
| Сохранение | 59 |
| Оповещение об изменениях..... | 59 |
| Загрузка и восстановление..... | 60 |
| Экспорт..... | 60 |
| Импорт..... | 61 |
| Модификация модели данных..... | 63 |
| Изменение параметров объектов..... | 64 |
| Добавление объектов..... | 66 |
| Удаление объектов..... | 74 |
| Связи между объектами..... | 75 |
| Формирование заданий ЗПС по журналу Secret Net | 75 |
| Подготовка ресурсов для замкнутой программной среды | 77 |
| Расчет эталонов..... | 78 |
| Поиск зависимых модулей | 79 |
| Замена переменных окружения | 79 |
| Настройка задания для ПАК "Соболь"..... | 80 |
| Глава 5. Дополнительные возможности | 81 |
| Затирание файлов..... | 81 |
| Запрет сетевых интерфейсов..... | 81 |
| Контроль печати | 82 |
| Формирование отчетов | 82 |
| Отчет "Паспорт ПО"..... | 83 |
| Отчет "Ресурсы рабочей станции" | 83 |
| Отчет "Допуск пользователей к ПАК "Соболь"" | 85 |
| Отчет "Журнал событий" | 86 |
| Средства экспорта и импорта параметров..... | 86 |
| Экспорт/импорт параметров политик..... | 86 |
| Экспорт/импорт параметров пользователей..... | 87 |
| Экспорт/импорт параметров механизмов КЦ и ЗПС..... | 88 |
| Редактирование учетной информации компьютера | 88 |
| Ввод серийного номера..... | 88 |
| Временное отключение защитных механизмов | 89 |
| Приложение | 90 |
| Интерфейс программы "Контроль программ и данных"..... | 90 |
| Интерфейс программы..... | 90 |
| Настройка элементов интерфейса | 91 |
| Параметры работы программы | 92 |
| Средства для работы со списками объектов..... | 95 |
| Настройка исключений для замкнутой программной среды | 97 |
| Ресурсы, устанавливаемые на контроль целостности..... | 98 |
| Настройка системы для оперативной синхронизации заданий КЦ-ЗПС..... | 99 |
| Централизованное управление списком расширений исполняемых файлов | 100 |
| Создание организационного подразделения | 100 |

| | |
|---|------------|
| Создание групповой политики и добавление шаблона | 100 |
| Включение и настройка административного шаблона | 101 |
| Контролируемые устройства | 103 |
| Использование терминального доступа | 104 |
| Рекомендации по настройке Secret Net 6 на кластере | 105 |
| Применение параметров групповой политики при обновлении | 106 |
| Восстановление системы после сбоев питания компьютера | 108 |
| Восстановление базы данных КЦ-ЗПС | 108 |
| Восстановление локальной базы данных | 108 |
| Терминологический справочник | 109 |
| Документация | 113 |
| Предметный указатель | 114 |

Список сокращений

| | |
|---------------|---|
| AD | Active Directory |
| IEEE | Institute of Electrical and Electronics Engineers |
| MMC | Microsoft Management Console |
| NTFS | New Technology File System |
| PCMCIA | Personal Computer Memory Card International Association |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| RPC | Remote Procedure Call |
| RTF | Rich Text Format |
| TCP | Transmission Control Protocol |
| USB | Universal Serial Bus |
| АРМ | Автоматизированное рабочее место |
| БД | База данных |
| ЗПС | Замкнутая программная среда |
| КЦ | Контроль целостности |
| ЛБД | Локальная база данных |
| МД | Модель данных |
| НСД | Несанкционированный доступ |
| ОС | Операционная система |
| ПАК | Программно-аппаратный комплекс |
| ПО | Программное обеспечение |
| СНК | Серийный номер клиента |
| ЦБД | Центральная база данных |

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 администраторам для настройки и управления основными механизмами защиты.

Перед изучением данного руководства рекомендуется 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).

Глава 1

Общие принципы управления

В системе Secret Net 6 информационная безопасность компьютеров обеспечивается механизмами защиты. Механизм защиты — совокупность настраиваемых программных средств, разграничивающих доступ к информационным ресурсам, а также осуществляющих контроль действий пользователей и регистрацию событий, связанных с информационной безопасностью. Описание механизмов защиты системы Secret Net 6 приведено в документе [1].

Функции администратора безопасности

Функциональные возможности Secret Net 6 позволяют администратору безопасности решать следующие задачи:

- усилить защиту от несанкционированного входа в систему;
- разграничить доступ пользователей к информационным ресурсам на основе принципов избирательного и полномочного разграничения доступа и замкнутой программной среды;
- контролировать и предотвращать несанкционированное изменение целостности ресурсов;
- контролировать вывод на печать конфиденциальной информации;
- контролировать аппаратную конфигурацию защищаемых компьютеров и предотвращать попытки ее несанкционированного изменения;
- загружать системные журналы для просмотра сведений, произошедших на защищаемых компьютерах;
- не допускать восстановление информации, содержащейся в удаленных файлах;
- управлять доступом пользователей к сетевым интерфейсам компьютеров.

Для решения перечисленных и других задач администратор безопасности использует средства системы Secret Net 6 и операционной системы (ОС) Windows.

Основными функциями администратора безопасности являются:

- настройка механизмов защиты, гарантирующая требуемый уровень безопасности ресурсов компьютеров;
- контроль выполняемых пользователями действий с целью предотвращения нарушений информационной безопасности.

Организация управления системой защиты

В автономном режиме функционирования системы Secret Net 6 доступны только локальные функции управления системой.

В сетевом режиме функционирования доступны возможности как локального, так и централизованного управления системой защиты, применяются принципы сетевого администрирования с использованием механизма групповых политик и делегирования административных полномочий.

Централизованное и локальное управление

В сетевом режиме функционирования системы Secret Net 6 для настройки механизмов защиты используются стандартные средства управления компьютерами и доменом, функциональные возможности которых расширяются в результате модификации схемы Active Directory (AD) и установки компонентов Secret Net 6.

Централизованное управление — управление работой системы Secret Net 6, осуществляемое администратором безопасности со своего рабочего места. Рабочим местом администратора безопасности может быть любой компьютер сети с установленными средствами централизованного управления ОС Windows. На контроллере домена средства централизованного управления установлены по

умолчанию. На других компьютерах установку средств необходимо выполнить самостоятельно:

- для ОС Windows 7 — устанавливается компонент "Средства удаленного администрирования сервера для Windows 7". После установки необходимо открыть список компонентов Windows и в папке "Средства удаленного администрирования сервера" включить функции "Средства администрирования возможностей | Средства управления групповыми политиками" и "Средства администрирования ролей | Средства доменных служб Active Directory и служб Active Directory облегченного доступа к каталогам | Средства доменных служб Active Directory | Центр администрирования Active Directory";
- для ОС Windows 2008 — в списке компонентов Windows необходимо включить функции "Управление групповой политикой" и "Средства удаленного администрирования сервера | Средства администрирования ролей | Средства AD DS и AD LDS | Инструменты AD DS | Оснастки AD DS и средства командной строки" (вариант англоязычного названия: "Remote Server Administration Tools | Role Administration Tools | Active Directory Domain Services Tools | Active Directory Domain Controller Tools");
- для ОС Windows Vista — устанавливается компонент "Средства администрирования удаленного сервера для Windows Vista". После установки необходимо открыть список компонентов Windows и в папке "Средства удаленного администрирования сервера" включить функции "Средства администрирования возможностей | Средства управления групповыми политиками" и "Средства администрирования ролей | Средства доменных служб Active Directory | Средства контроллеров доменов Active Directory";
- для ОС Windows XP/2003 — устанавливается компонент "Microsoft Administration Tools Pack" из состава дистрибутива ОС Windows 2003 Server;
- для ОС Windows 2000 — устанавливается компонент "Microsoft Administration Tools Pack" из состава дистрибутива ОС Windows 2000 Server.

Локальное управление — это управление работой механизмов защиты отдельного компьютера, которое осуществляется администратором безопасности непосредственно на каждом компьютере. Локальное управление применяется в тех случаях, когда централизованно настроить механизмы защиты на отдельном компьютере (или компьютерах) по каким-либо причинам невозможно или нецелесообразно. Кроме того, локальное управление применяется для обеспечения требуемого уровня безопасности в работе локальных пользователей.



Для выполнения функций централизованного управления администратор безопасности должен входить в группу администраторов домена. Для локального — в локальную группу администраторов компьютера.

Централизованное управление имеет приоритет перед локальным управлением. Если в групповой политике какие-то параметры для данного компьютера заданы централизованно, то локально их изменить нельзя.

В соответствии с концепцией Secret Net 6 управление безопасностью в защищаемом домене рекомендуется осуществлять централизованно. Однако следует иметь в виду, что не все параметры защитных механизмов настраиваются централизованно. Некоторые параметры могут настраиваться только локально.

Использование групповых политик

В сетевом режиме функционирования системы Secret Net 6 параметры объектов групповых политик хранятся на контроллерах домена и передаются на защищаемые рабочие станции и серверы, где применяются в соответствии с действием механизма групповых политик.

Если для всех компьютеров домена используется единая политика безопасности, настройку механизмов Secret Net 6 рекомендуется выполнять в политике, применяемой к домену по умолчанию.

С помощью групповых политик для компьютеров отдельных организационных подразделений (Organization Units) домена можно задавать особые параметры механизмов защиты, отличающиеся от общих параметров, применяемых в домене. В общем случае последовательность формирования политик, применяемых к организационным подразделениям, следующая:

1. Настройте механизмы защиты Secret Net 6 в рамках доменной политики.
2. Создайте в домене новые организационные подразделения, для которых должны действовать особые параметры механизмов защиты.
3. Добавьте в созданные подразделения нужные компьютеры домена.
4. Создайте для каждого подразделения свою групповую политику и настройте нужным образом в каждой политике параметры Secret Net 6.
5. Примените созданные политики к соответствующим подразделениям.

Инструменты Groupdate и SecEdit. Эти инструменты командной строки позволяют принудительно обновить групповые политики для компьютера или пользователя. Эти команды могут использоваться для принудительного завершения сеанса пользователя или для перезапуска компьютера после обновления групповой политики, что полезно при обновлении политик, которые применяются только при входе пользователя в систему или при перезапуске компьютера.

Делегирование административных полномочий

В сетевом режиме функционирования системы Secret Net 6 предусмотрено делегирование полномочий администратора безопасности. Это означает, что некоторые функции по настройке и управлению работой механизмов защиты могут быть возложены на пользователей, не являющихся членами доменной группы администраторов. При этом настройка и управление будут осуществляться только в рамках определенных организационных подразделений, созданных внутри домена.

Для делегирования полномочий администратора безопасности необходимо выполнить следующие действия:

1. Создать в Active Directory структуру организационных подразделений, используя стандартные средства операционной системы.
2. Пользователям, уполномоченным настраивать механизмы защиты в рамках организационного подразделения, стандартными средствами ОС предоставить полные права на управление объектами, входящими в подразделение, и групповыми политиками подразделения.

В результате такие пользователи получают возможность:

- управлять объектами "пользователь" и "компьютер", входящими в соответствующее организационное подразделение;
 - редактировать (включая создание и удаление) групповые политики, назначенные для данного подразделения (обязательным условием является включение пользователя в группу Group Policy Creator Owners).
3. Включить пользователя, которому делегированы права на управление объектами организационного подразделения, в группу SecretNetAdmins.

Эта группа создается в домене автоматически при установке Secret Net 6.

В результате пользователь в дополнение к управлению стандартными объектами организационного подразделения получит возможность изменять и настраивать параметры механизмов защиты Secret Net 6:

- управлять параметрами пользователей и выполнять операции с их персональными идентификаторами (кроме доступа к компьютерам с ПАК "Соболь");
- редактировать параметры групповых политик данного организационного подразделения;
- настраивать параметры контроля целостности и замкнутой программной среды для компьютеров организационного подразделения;
- устанавливать клиентское ПО Secret Net 6 в сетевом режиме функционирования на компьютеры, входящие в организационное подразделение, и настраивать параметры их подключения к серверу безопасности.

Для того чтобы пользователь, не входящий в доменную группу администраторов, мог локально выполнять настройку Secret Net 6, он должен входить в локальную группу администраторов компьютера. Кроме того, должны быть выполнены следующие условия:

- пользователю предоставлены полные права на доступ к объектам организационного подразделения, в которое входит данный компьютер;
- пользователь включен в группу SecretNetAdmins.

Полномочия для локального управления предоставляют следующие возможности:

- подключение и отключение ПАК "Соболь";
- изменение учетной записи компьютера;
- установка клиентского ПО Secret Net 6.

Параметры механизмов защиты и средства управления

Параметры механизмов защиты Secret Net 6 в зависимости от места их хранения в системе и способа доступа к ним можно разделить на следующие группы:

- параметры объектов групповой политики;
- параметры пользователей;
- атрибуты ресурсов;
- параметры механизмов контроля целостности (КЦ) и замкнутой программной среды (ЗПС).

Параметры объектов групповой политики

К общим параметрам безопасности ОС Windows добавляются параметры Secret Net 6. Эти параметры применяются на компьютере средствами групповых политик и действуют в рамках локальной политики безопасности (в автономном режиме функционирования системы защиты) или как объединение параметров локальной политики с политикой безопасности домена/организационного подразделения (в сетевом режиме функционирования).

Параметры Secret Net 6 представлены в стандартном узле "Параметры безопасности" иерархии узлов групповой политики. Управление параметрами групповой политики осуществляется в соответствующей оснастке.

Для просмотра и изменения параметров:

1. Вызовите нужную оснастку:
 - чтобы редактировать параметры локальной политики безопасности компьютера — активируйте команду "Пуск | Все программы | Код безопасности | Secret Net | Локальная политика безопасности";
 - чтобы редактировать параметры политики безопасности домена или организационного подразделения на компьютере под управлением ОС Windows Vista/2008/7 — запустите оснастку "Управление групповой политикой", выберите политику домена или нужного организационного подразделения и в контекстном меню политики активируйте команду "Изменить";
 - чтобы редактировать параметры политики безопасности домена или организационного подразделения на компьютере под управлением ОС Windows 2000/XP/2003 — запустите консоль управления Microsoft (MMC) и выполните процедуру добавления оснастки "Редактор объектов групповой политики". В качестве объекта групповой политики для оснастки укажите политику домена или нужного организационного подразделения.

Для централизованного управления параметрами на компьютере, не являющемся контроллером домена, должны быть установлены средства централизованного управления ОС Windows (см. стр. 8).

2. Перейдите к разделу "Конфигурация компьютера | Политики | Конфигурация Windows | Параметры безопасности | Параметры Secret Net".

Примечание. Загруженная оснастка может не содержать узлов "Конфигурация компьютера", "Политики", "Конфигурация Windows".

По умолчанию раздел "Параметры Secret Net" содержит следующие группы параметров:

| Группа | Назначение |
|----------------------------|--|
| Ключи пользователя | Настройка параметров ключей для усиленной аутентификации пользователей (см. стр. 26) |
| Настройки подсистем | Управление режимом работы механизмов контроля устройств и разграничения доступа к устройствам (см. стр. 32). Управление режимами работы механизма защиты входа в систему (см. стр. 23). Управление режимами работы механизма полномочного разграничения доступа и контроля печати (см. документ [4]). Настройка параметров хранения журнала Secret Net (см. документ [5]). Управление механизмом затирания удаляемой информации (см. стр. 81). Управление работой сетевых интерфейсов (см. стр. 81) |
| Привилегии | Назначение пользователям привилегий, связанных с работой следующих механизмов: <ul style="list-style-type: none"> • работа с журналом Secret Net (см. документ [5]); • работа в условиях замкнутой программной среды (см. стр. 45) |
| Регистрация событий | Настройка перечня событий, регистрируемых системой Secret Net 6 (см. документ [5]) |
| Устройства | Управление параметрами механизма контроля устройств и правами доступа к устройствам (см. стр. 32) |

Параметры настройки системы могут быть сгруппированы по принадлежности к защитным механизмам. Переключение режима группировки параметров осуществляется с помощью специальных кнопок панели инструментов или команд в меню "Вид" ("По группам" и "По подсистемам").

Параметры пользователей

Параметры пользователей используются механизмами защиты входа и полномочного разграничения доступа. Параметры пользователя применяются при входе в систему после выполнения процедуры идентификации и аутентификации пользователя.

В сетевом режиме функционирования системы Secret Net 6 параметры доменных и локальных пользователей хранятся, соответственно, в Active Directory и в локальных базах данных защищаемых компьютеров. В автономном режиме функционирования параметры доменных и локальных пользователей хранятся в локальной базе данных компьютера.



При копировании объектов "Пользователь" параметры Secret Net 6 не копируются.

Настройка параметров доменных и локальных пользователей осуществляется в соответствующих оснастках: доменные пользователи представлены в оснастке "Active Directory — пользователи и компьютеры", локальные пользователи — в оснастке "Управление компьютером" (в автономном режиме функционирования параметры системы Secret Net 6 для доменных пользователей настраиваются в оснастке "Управление компьютером").

Для просмотра и изменения параметров:

1. Вызовите нужную оснастку:

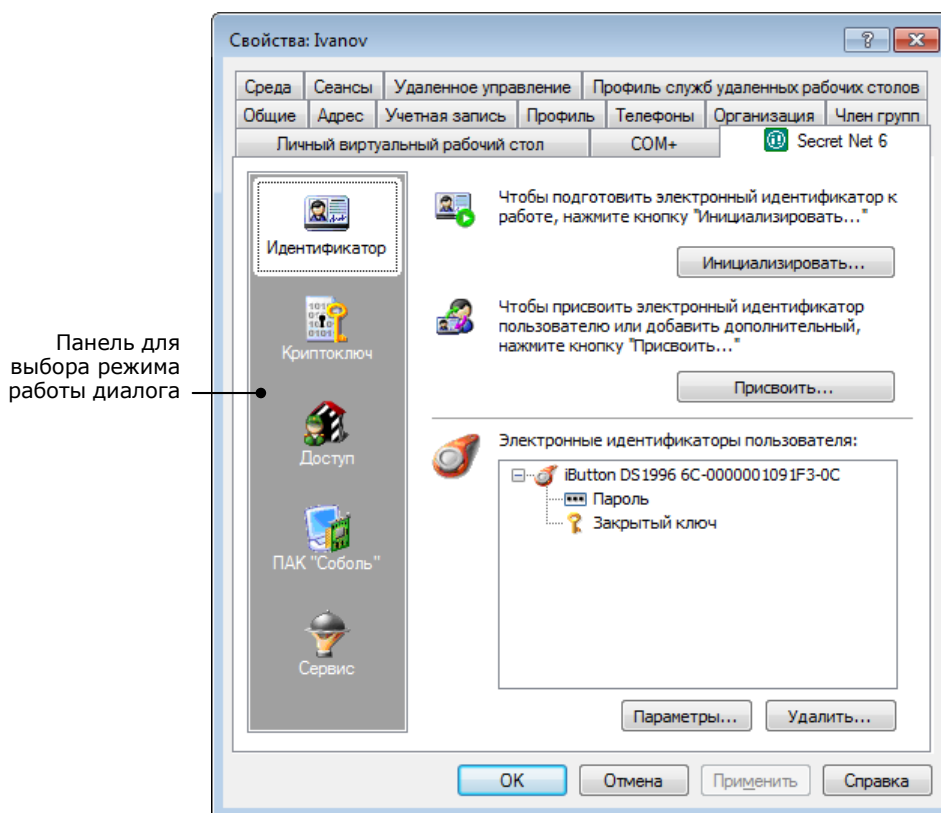
| | |
|---|--|
| Active Directory — пользователи и компьютеры | Активируйте команду "Пуск Все программы Администрирование Active Directory — пользователи и компьютеры". Для управления параметрами доменных пользователей на компьютере, не являющемся контроллером домена, должны быть установлены средства централизованного управления ОС Windows (см. стр. 8). |
| Управление компьютером | Активируйте команду "Пуск Все Программы Код безопасности Secret Net Управление компьютером" |

2. Найдите и выберите папку "Пользователи" (в автономном режиме функционирования выберите папку "Доменные пользователи" для управления па-

раметрами доменных пользователей или папку "Локальные пользователи и группы | Пользователи" — для управления параметрами локальных пользователей компьютера).

В правой части появится список пользователей.

3. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 6".



В левой части диалога расположена панель выбора режима работы. Переключение между режимами осуществляется выбором соответствующей пиктограммы на этой панели. Предусмотрены следующие режимы:

| Режим | Назначение |
|----------------------|--|
| Идентификатор | Управление персональными идентификаторами пользователя (см. стр. 15) |
| Криптоключ | Управление ключами для усиленной аутентификации пользователя (см. стр. 24) |
| Доступ | Управление параметрами полномочного доступа (см. документ [4]) |
| ПАК "Соболь" | Управление доступом пользователя к компьютерам (см. стр. 27). Режим присутствует только для доменных пользователей в сетевом режиме функционирования |
| Сервис | Проверка принадлежности персональных идентификаторов (см. стр. 22) и работа с ключами централизованного управления ПАК "Соболь" (см. стр. 27) |

Список доменных пользователей в автономном режиме функционирования

В папке "Доменные пользователи" отображается список доменных пользователей, зарегистрированных в системе Secret Net 6. Список формируется автоматически при установке клиентского ПО в автономном режиме функционирования (по наличию профилей доменных пользователей, которые уже входили на данный компьютер). Другие доменные пользователи, которым разрешается вход в систему на данном компьютере, должны быть зарегистрированы (добавлены в список) администратором безопасности.



Если во время работы с оснасткой "Управление компьютером" зарегистрированный доменный пользователь был удален средствами администрирования домена, этот пользователь будет отображаться в папке "Доменные пользователи" до закрытия оснастки. Удаление пользователя из списка произойдет при открытии следующего сеанса работы с оснасткой.

Для регистрации доменного пользователя в автономном режиме функционирования:

1. Загрузите оснастку для управления параметрами компьютера и выберите папку "Доменные пользователи" (см. действия 1–2 вышеописанной процедуры).
2. В правой части окна вызовите контекстное меню и активируйте команду "Добавить...".
На экране появится стандартный диалог ОС Windows для выбора объектов.
3. Выберите нужного пользователя и нажмите кнопку "ОК".
Имя выбранного пользователя появится в папке "Доменные пользователи".

Атрибуты ресурсов

Параметры, относящиеся к атрибутам ресурсов (файлов и каталогов), используются в механизме полномочного разграничения доступа. Управление параметрами осуществляется с помощью расширения программы Проводник. Описание процедур изменения параметров см. в документе [9].

Параметры механизмов КЦ и ЗПС

Параметры механизмов контроля целостности и замкнутой программной среды настраиваются в программе "Контроль программ и данных". Описание параметров и порядка их настройки приведено в Главе 4 (см. стр. 45).

Контекстное меню пиктограммы Secret Net 6



После установки клиентского ПО системы защиты в системной области панели задач Windows появляется пиктограмма Secret Net 6. Она предназначена для вызова команд локального управления. Щелчком правой кнопки мыши на пиктограмме можно вызвать меню, содержащее следующие команды:

| Пункт меню | Назначение |
|---|---|
| О системе | Просмотр информации об установленной на компьютере версии клиента Secret Net 6 |
| Справка | Вызов справки системы Secret Net 6 |
| Утвердить аппаратную конфигурацию (Утвердить изменения в конфигурации) | Утверждение новой аппаратной конфигурации компьютера после подключения новых или отключения имеющихся устройств (см. стр. 41) |
| Сменить ключи | Смена ключей для усиленной аутентификации пользователя (см. документ [9]) |
| Уведомления о НСД | Включение и отключение режима локального оповещения о событиях НСД. При включенном режиме в случае возникновения события НСД система оповещает об этом пользователя компьютера посредством подачи звукового сигнала и кратковременным выводом пиктограммы предупреждения в правом верхнем углу экрана |

Глава 2

Защита входа в систему

Основными функциями администратора безопасности по защите входа в систему являются:

- настройка режимов использования персональных идентификаторов пользователей и присвоение идентификаторов пользователям;
- управление режимом входа пользователей в систему;
- управление режимом усиленной аутентификации пользователей;
- настройка параметров блокировки компьютеров.

Управление персональными идентификаторами

Персональный идентификатор — устройство для хранения информации, необходимой при идентификации и аутентификации пользователя. В идентификаторе могут храниться ключи для усиленной аутентификации пользователя.

В Secret Net 6 могут использоваться персональные идентификаторы eToken, iKey, Rutoken или идентификаторы iButton.

Пояснение. Для хранения ключей для усиленной аутентификации могут также использоваться сменные носители, такие как дискеты, Flash-карты, USB Flash-накопители и т. п. В дальнейшем в данном руководстве термин "идентификатор" будет применяться и к сменным носителям.

Персональный идентификатор выдается пользователю администратором. Пользователю можно присвоить неограниченное число идентификаторов. Один и тот же персональный идентификатор не может быть присвоен нескольким пользователям одновременно.

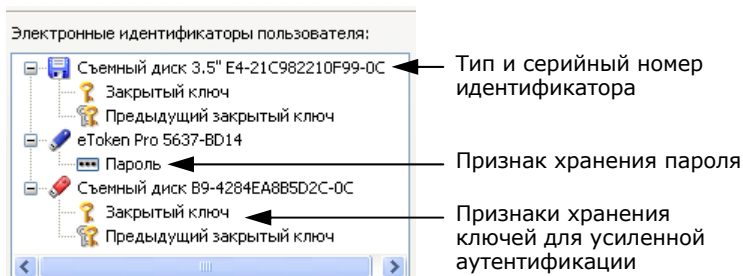
Администратор безопасности может выполнять следующие операции с персональными идентификаторами:

| |
|---|
| Инициализация идентификатора |
| Форматирование, обеспечивающее возможность использования идентификатора в системе Secret Net 6. Инициализация требуется, когда в персональном идентификаторе по каким-либо причинам была нарушена или отсутствует структура данных. Форматированию подлежат также и сменные носители, предназначенные для хранения ключей |
| Присвоение идентификатора |
| Добавление в базу данных Secret Net 6 сведений о том, что пользователю принадлежит персональный идентификатор данного типа с уникальным серийным номером |
| Отмена присвоения идентификатора |
| Удаление из базы данных Secret Net 6 информации о принадлежности данного персонального идентификатора данному пользователю. Далее для простоты эту операцию будем называть "удаление идентификатора" |
| Включение режима хранения пароля в идентификаторе |
| Добавление в базу данных Secret Net 6 сведений о включении для пользователя режима хранения пароля в идентификаторе. Одновременно с этой операцией выполняется запись пароля в идентификатор. После включения режима пароль пользователя при входе в систему не вводится с клавиатуры, а считывается из идентификатора |
| Отключение режима хранения пароля в идентификаторе |
| Операция, противоположная предыдущей. Одновременно с отключением режима хранения выполняется удаление пароля из памяти персонального идентификатора. Идентификатор остается закрепленным за пользователем |
| Включение и отключение режима разрешения входа в ПАК "Соболь" |
| При включенном режиме пользователю разрешено использовать для входа в ПАК "Соболь" идентификатор, присвоенный в системе Secret Net 6 |
| Запись и удаление ключей для усиленной аутентификации |
| Используется для хранения в идентификаторе (или на сменном носителе) ключей для усиленной аутентификации пользователя |
| Проверка принадлежности |
| С помощью этой операции администратор безопасности может проверить, кому из пользователей присвоен данный персональный идентификатор |

Просмотр сведений об идентификаторах пользователя

Сведения о персональных идентификаторах пользователя отображаются в окне свойств пользователя в диалоге "Secret Net 6", работающем в режиме "Идентификатор". Описание процедуры вызова диалогового окна для настройки параметров пользователя см. на стр. 12.

Сведения представлены в виде списка идентификаторов, присвоенных пользователю:



Для каждого идентификатора указаны тип и серийный номер. Дополнительно могут быть указаны следующие признаки хранения служебной информации:

- признак хранения пароля;
- признаки хранения в идентификаторе ключей для усиленной аутентификации;
- признак использования идентификатора для входа в ПАК "Соболь";
- признак использования идентификатора для входа и администрирования ПАК "Соболь";
- признак хранения ключей централизованного управления ПАК "Соболь".

Предъявление идентификатора

При выполнении операций с идентификаторами предъявляется идентификатор для записи или считывания информации. Предъявление идентификатора выполняется по требованию системы.

Для предъявления USB-ключа:

- Если точно известно, какой идентификатор нужно предъявить, вставьте его непосредственно или через удлинитель в разъем USB-порта компьютера.
- Если необходимо выбрать идентификатор из нескольких имеющихся идентификаторов, удалите отметку из поля "Использовать первый предъявленный идентификатор" и поочередно предъявляйте идентификаторы. При этом серийный номер каждого предъявляемого идентификатора будет отображаться в диалоге. Когда нужный идентификатор найден, нажмите кнопку "ОК".

Если предъявлен USB-ключ, который защищен **нестандартным** PIN-кодом (паролем), на экране появится запрос. Введите PIN-код и нажмите кнопку "ОК".

Для предъявления идентификатора iButton:

- Если точно известно, какой идентификатор нужно предъявить, прислоните его к считывателю и удерживайте в таком положении до закрытия диалога "Предъявите идентификатор".
- Если необходимо выбрать идентификатор из нескольких имеющихся идентификаторов, удалите отметку из поля "Использовать первый предъявленный идентификатор" и поочередно предъявляйте идентификаторы. При этом серийный номер каждого предъявляемого идентификатора будет отображаться в диалоге. Когда нужный идентификатор найден, не прерывая контакт этого идентификатора со считывающим устройством, нажмите кнопку "ОК".

Для предъявления дискеты или другого сменного носителя:

1. Вставьте дискету в дисковод или вставьте сменный носитель в разъем USB-порта и нажмите кнопку "Диск".

В диалоге появится наименование сменного носителя.

2. Выберите в списке это наименование и нажмите кнопку "ОК".

Сообщения об ошибках

Если при предъявлении идентификатора произошли ошибки, на экране появится сообщение, поясняющее причину ошибки. В таблице перечислены возможные причины ошибок и действия, которые необходимо предпринять для их устранения.

| Причина | Действие |
|--|--|
| Нарушение контакта идентификатора со считывателем или недостаточная его продолжительность | Предъявите идентификатор повторно с учетом общих требований по использованию идентификаторов |
| Предъявленный идентификатор принадлежит другому пользователю | Процедура будет прервана. Предъявите идентификатор, принадлежащий данному пользователю, или идентификатор, который никому не принадлежит |
| Был предъявлен идентификатор, уже содержащий сведения системы Secret Net 6 или ПАК "Соболь" | Если удаление сведений, содержащихся в идентификаторе, допустимо, можно продолжить выполняемую процедуру |
| Нарушена структура данных в идентификаторе | Выполните инициализацию идентификатора и повторите действие |

Инициализация идентификатора

Инициализацию персонального идентификатора можно выполнять в окне настройки свойств любого пользователя.

Для инициализации идентификатора:

1. Загрузите оснастку для управления параметрами пользователей, вызовите окно настройки свойств любого пользователя и перейдите к диалогу "Secret Net 6" (см. стр. 12).
2. Нажмите кнопку "Инициализировать".
На экране появится диалог "Предъявите идентификатор".
3. Предъявите идентификатор (см. выше).

Для USB-ключа предусмотрена возможность удаления данных, записанных в него вне системы Secret Net 6 (для идентификаторов eToken такая возможность поддерживается только на ОС Windows 2000). Если в идентификаторе записаны такие данные, в момент его предъявления появится сообщение о возможности их удаления. Удаление данных позволяет увеличить доступный объем памяти идентификатора для использования в Secret Net 6.

Произойдет инициализация идентификатора, после чего на экране появится соответствующее сообщение.

Присвоение идентификатора

Процедура присвоения идентификатора пользователю выполняется с помощью программы-мастера. При присвоении можно настроить режимы использования персонального идентификатора.

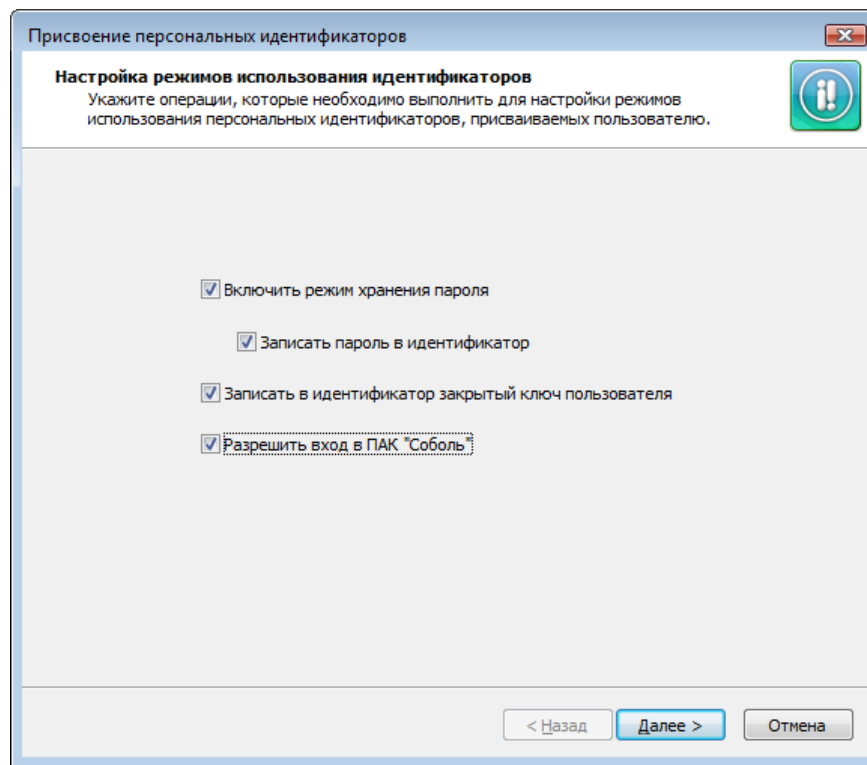
Примечания:

- для записи пароля в идентификатор потребуется ввести пароль данного пользователя;
- для записи в идентификатор уже имеющегося у пользователя ключа для усиленной аутентификации (закрытого ключа) потребуется предъявить идентификатор, на котором этот ключ записан;
- если идентификатор принадлежит администратору ПАК "Соболь", то пароль пользователя Windows и пароль входа в ПАК "Соболь" должны совпадать;
- для включения режима разрешения входа с помощью идентификатора в ПАК "Соболь" необходимо, чтобы ПАК функционировал в режиме интеграции с Secret Net (см. стр. 27).

Для присвоения идентификатора пользователю:

1. Загрузите оснастку для управления параметрами пользователей, вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 6" (см. стр. 12).
2. Нажмите кнопку "Присвоить".

На экране появится стартовый диалог мастера присвоения идентификаторов.



3. Установите отметки в соответствии с выполняемыми операциями и нажмите кнопку "Далее >".

На экране появится диалог мастера, отображающий ход выполнения операций.

4. Если выбрана операция "Записать пароль в идентификатор", "Разрешить вход в ПАК "Соболь" или "Записать в идентификатор закрытый ключ пользователя", выполните действия по запросу программы:
 - При появлении диалога "Ввод пароля" введите пароль пользователя.
 - При появлении диалога "Предъявите идентификатор" предъявите идентификатор пользователя (см. стр. 16), содержащий его закрытый ключ.

Успешно выполненные операции имеют статус "Выполнено". Если при выполнении операции произошла ошибка, в диалоге будет приведено соответствующее сообщение об этом.

5. После успешного выполнения всех операций нажмите кнопку "Далее >".

На экране появится диалог "Предъявите идентификатор".

6. Предъявите идентификатор (см. стр. 16) для присвоения пользователю и записи данных. Не нарушайте контакт идентификатора со считывателем до завершения всех операций.



Если предъявленный идентификатор содержит данные Secret Net 6 или ПАК "Соболь", но не принадлежит никому из доменных пользователей, на экране появится запрос для подтверждения операции. Если вы уверены, что этим идентификатором никто больше не пользуется, нажмите кнопку "Да" и повторно предъявите данный идентификатор.

Ошибки записи данных

В процессе записи данных могут произойти ошибки (например, связанные с идентификатором или БД), которые отображаются в диалоге:

Присвоение персональных идентификаторов

Результат выполнения процедуры
При присвоении персонального идентификатора и выполнении заданных операций получены следующие результаты.

Персональный идентификатор не присвоен пользователю Ivanov.

| | |
|--|-------------------|
| Включение режима хранения пароля | -> Отмена |
| Запись пароля в идентификатор | -> Не выполняется |
| Включение режима входа в ПАК "Соболь" | -> Не выполняется |
| Генерация ключа пользователя | -> Отмена |
| Запись закрытого ключа в идентификатор | -> Отмена |
| Сохранение информации в БД Secret Net | -> Отмена |

Внимание! Не все операции выполнены успешно!
Причина: Электронный идентификатор не предъявлен

Для устранения ошибок нажмите кнопку "< Назад".
Чтобы присвоить пользователю еще один идентификатор с заданными параметрами нажмите кнопку "Повторить...".

Повторить...

< Назад Готово Отмена

Для присвоения пользователю еще одного идентификатора с такими же параметрами

Для устранения ошибок нажмите эту кнопку и повторно предъявите идентификатор

По мере успешного выполнения очередной операции ее статус меняется со значения "Выполняется" на значение "Выполнено". Непредусмотренные операции имеют статус "Не выполняется"

Идентификатор не будет присвоен, если допущена ошибка при выполнении этой операции или эта операция отменена из-за других ошибок

После успешного завершения всех предусмотренных операций статус каждой из них должен иметь значение "Выполнено".

- Для завершения работы нажмите кнопку "Готово".

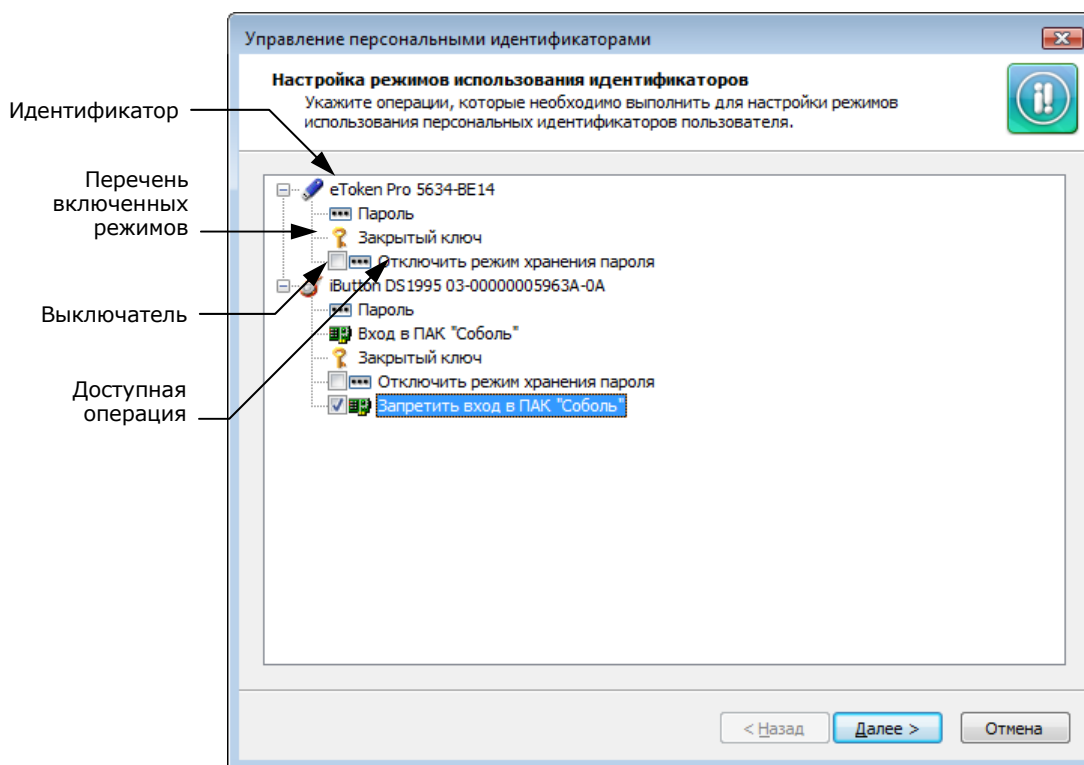
Настройка режимов использования идентификаторов

При необходимости можно изменить действующие режимы использования идентификаторов (кроме сменных носителей), присвоенных пользователю. Процедура настройки режимов выполняется с помощью программы-мастера.

Для настройки режимов идентификаторов пользователя:

- Загрузите оснастку для управления параметрами пользователей, вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 6" (см. стр. 12).
- Нажмите кнопку "Параметры".

На экране появится стартовый диалог мастера настройки режимов.



Диалог содержит список идентификаторов, присвоенных пользователю.

Дискеты и сменные диски, присвоенные пользователю, в списке не отображаются.

Для каждого идентификатора в списке указаны включенные режимы и доступные для выполнения операции. Например, если для идентификатора включен режим хранения пароля, то доступной операцией будет "Отключить режим хранения пароля".

3. Установите отметки в соответствии с выполняемыми операциями и нажмите кнопку "Далее >".
4. Если выбрана операция "Записать пароль в идентификатор" или "Разрешить вход в ПАК "Соболь", на экране появится диалог "Ввод пароля". Введите пароль пользователя и нажмите кнопку "ОК".

После успешного ввода пароля в диалоге справа от названия операции появится запись "Выполнено".

5. Нажмите кнопку "Далее >".

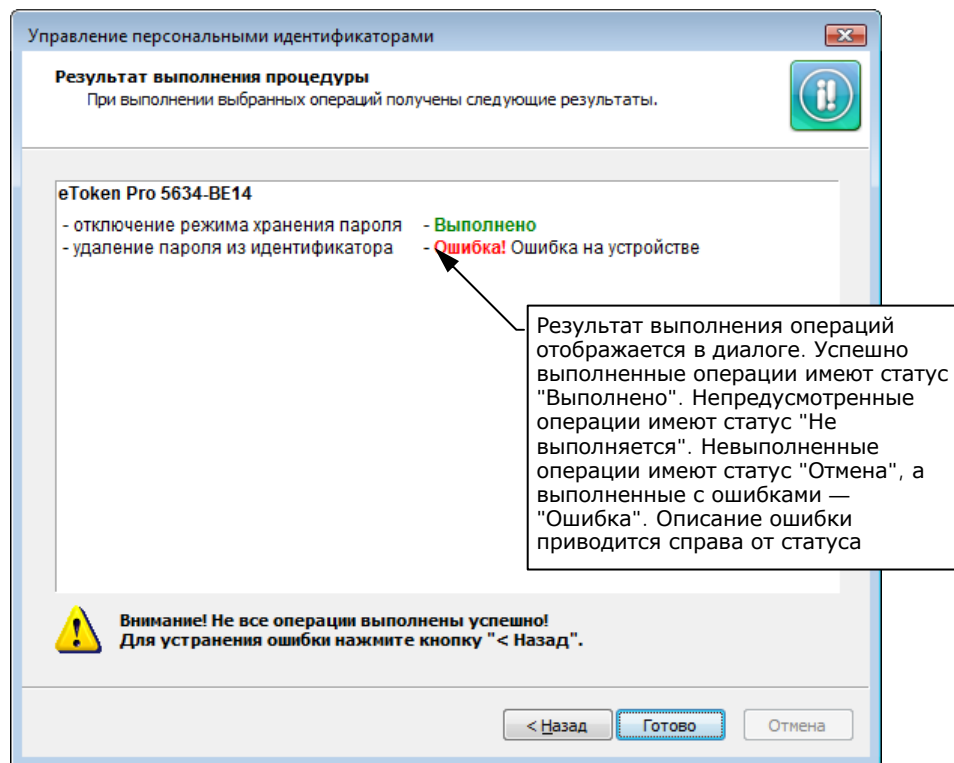
Если была выбрана любая операция, кроме операции "Включить режим хранения пароля", на экране появится диалог "Предъявите идентификатор". В диалоге отображаются наименования идентификаторов, для которых были выбраны операции, и статус их обработки "Не обработан".

6. Предъявите все идентификаторы, указанные в списке (см. стр. 16).

После успешного предъявления идентификатора его статус изменится на "Обработан". Если предъявление идентификатора выполнено с ошибкой, в столбце статуса обработки появится сообщение об ошибке. После предъявления всех идентификаторов кнопка "Отмена" будет заменена кнопкой "Закреть".

7. Нажмите кнопку "Закреть".

На экране появится диалог с результатами выполнения операций. Если операции выполнены с ошибками, в диалоге будет приведено их описание.



После успешного завершения всех предусмотренных операций статус каждой из них должен иметь значение "Выполнено".

8. Для завершения работы нажмите кнопку "Готово".

Удаление идентификатора

После выполнения процедуры удаления идентификатора пользователь теряет возможность использовать идентификатор для входа в систему и хранить в нем пароль и ключи.

Для удаления идентификатора пользователя:

1. Загрузите оснастку для управления параметрами пользователей, вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 6" (см. стр. 12).
2. Выберите в списке идентификатор и нажмите кнопку "Удалить".

Если выбранный идентификатор является единственным идентификатором, в котором хранятся ключи для усиленной аутентификации пользователя, на экране появится запрос на продолжение операции.

3. Нажмите кнопку "Да".
На экране появится запрос на очистку памяти идентификатора.
4. Нажмите кнопку "Да".
На экране появится диалог "Предъявите идентификатор".
5. Предъявите идентификатор (см. стр. 16).
Статус предъявленного идентификатора изменится на "Обработан".

Если при предъявлении идентификатора будут допущены нарушения, сообщение об ошибке появится в таблице диалога в столбце "Статус".

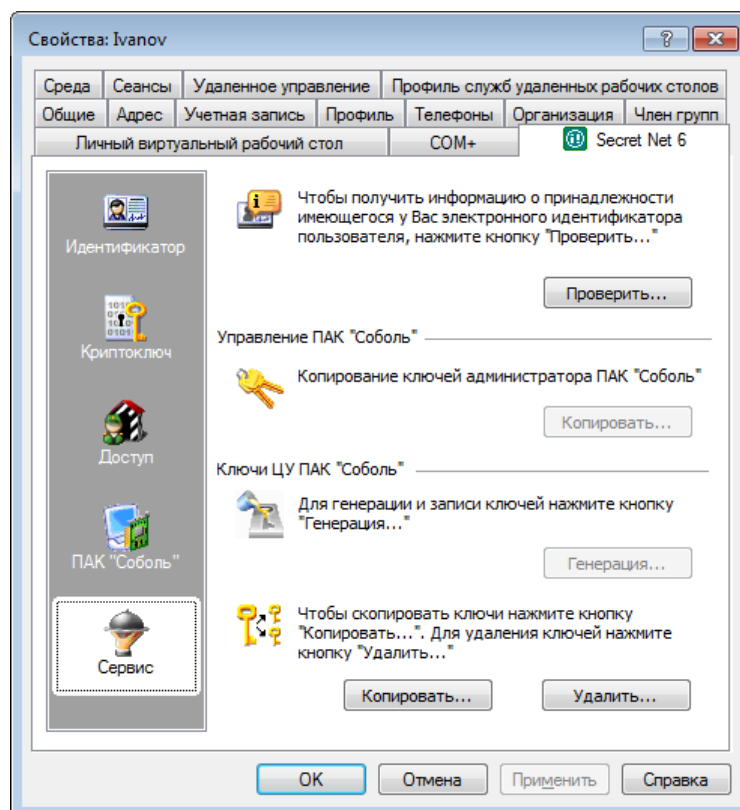
6. Нажмите кнопку "Закреть".
Запись об удаленном идентификаторе исчезнет из списка идентификаторов.

Проверка принадлежности

Проверку принадлежности персонального идентификатора можно выполнять в окне настройки свойств любого пользователя.

Для проверки принадлежности идентификатора:

1. Загрузите оснастку для управления параметрами пользователей, вызовите окно настройки свойств любого пользователя и перейдите к диалогу "Secret Net 6" (см. стр. 12).
2. В панели выбора режима выберите режим "Сервис".



3. Нажмите кнопку "Проверить".
На экране появится диалог "Предъявите идентификатор".
4. Предъявите проверяемый идентификатор (см. стр. 16).
Если в базе данных Secret Net 6 есть сведения о данном идентификаторе, они будут выведены на экран.

Смена пароля

Смена пароля пользователя может быть выполнена самим пользователем или администратором. Смена пароля выполняется стандартными средствами ОС Windows.

Смена пароля самим пользователем описана в документе [9].



Если пользователю присвоен персональный идентификатор и для этого идентификатора включены режимы хранения пароля и использования для входа в ПАК "Соболь", то в этом случае пароль не должен содержать символы кириллицы. Иначе после обработки идентификатора будет утеряна возможность его использования для входа в ПАК "Соболь".

Для смены пароля пользователя администратором:

1. Загрузите оснастку для управления параметрами пользователей (см. стр. 12), в списке пользователей вызовите контекстное меню для ярлыка с именем нужного пользователя и активируйте команду "Смена пароля" ("Задать пароль").

- На экране появится стандартный диалог ОС Windows для ввода пароля.
- Дважды введите новый пароль пользователя и нажмите кнопку "ОК".
Если пароль пользователя хранится в персональных идентификаторах, на экране появится диалог со списком персональных идентификаторов данного пользователя.
 - Предъявите все указанные в списке идентификаторы (см. стр. 16).
Новый пароль будет записан в идентификаторы и их статус изменится на "Обработан", а кнопка "Отмена" изменит название на "Закреть".
- | |
|--|
| Если при предъявлении идентификаторов будут допущены нарушения, сообщение об ошибке появится в таблице диалога в столбце "Статус". |
|--|
- Нажмите кнопку "Закреть".

Управление режимами механизма защиты входа в систему

Для настройки режимов:

- Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
- Выберите папку "Настройки подсистем".
- Вызовите контекстное меню для нужного параметра (см. таблицу ниже) и активируйте в нем команду "Свойства".
На экране появится диалог настройки параметра.
- Настройте действие параметра и нажмите кнопку "ОК".

Вход в систему: Запрет вторичного входа в систему

Если режим включен, блокируется возможность запуска команд и сетевых подключений с вводом учетных данных пользователя, который не выполнил интерактивный вход в систему.

Для компьютеров под управлением ОС Windows XP и выше. После включения режима дополнительно рекомендуется исключить возможность использования ранее сохраненных учетных данных. Для этого раскройте узел "Параметры безопасности | Локальные политики | Параметры безопасности" и включите действие стандартного параметра безопасности ОС Windows "Сетевой доступ: не разрешать хранение паролей или учетных данных для сетевой проверки подлинности" (название параметра может незначительно отличаться в зависимости от версии ОС). Указанный параметр по умолчанию отсутствует в списке параметров групповой политики, если компьютер контроллера домена работает под управлением ОС Windows 2000 Server. В этом случае на компьютерах домена, работающих под управлением ОС Windows XP и выше, настраивать данный параметр можно только в рамках локального администрирования. Для централизованной настройки параметра должны быть установлены средства централизованного управления ОС Windows (см. стр. 8)

Вход в систему: Количество неудачных попыток аутентификации

Устанавливает ограничение на количество неудачных попыток аутентификации пользователя по ключевой информации при входе в систему. При достижении ограничения компьютер блокируется и вход разрешается только для администратора.

Если параметру присвоено значение "0", ограничение не действует

Вход в систему: Максимальный период неактивности до блокировки экрана

Устанавливает максимальное значение интервала неактивности.

Автоматическая блокировка компьютера, включаемая в том случае, если в течение определенного времени не использовались клавиатура и мышь, настраивается каждым пользователем индивидуально. Но пользователь не сможет установить интервал неактивности, превышающий значение, заданное данным параметром

Вход в систему: Разрешить интерактивный вход только доменным пользователям

Если режим включен, интерактивно в систему могут войти только пользователи, зарегистрированные в домене. Интерактивный вход в систему локальных пользователей (включая локальных администраторов) запрещен

Вход в систему: Режим аутентификации пользователя

Стандартная аутентификация. Выполняется по паролю пользователя.

Усиленная аутентификация по ключу. Кроме пароля проверяется подлинность и актуальность (т. е. срок действия) ключевой информации пользователя. Для загрузки ключевой информации пользователь должен предъявить идентификатор. Вход в систему разрешается при подтверждении подлинности и актуальности ключа. Если подлинность ключа не подтверждается, вход запрещается и регистрируется значение ключа (если включен параметр "Регистрировать неверный ключ"). Если срок действия ключа истек, пользователю предлагается выполнить смену ключей для усиленной аутентификации. Включать режим следует после того, как всем пользователям выданы ключи для усиленной аутентификации (см. ниже).

При включенном режиме усиленной аутентификации вход в систему без предъявления ключа возможен только в **административном режиме**. Чтобы войти в систему в административном режиме, выполните следующую последовательность действий:

1. Перезагрузите компьютер.
2. После закрытия стартового окна операционной системы и появления сообщения о запуске системных служб Secret Net 6 нажмите и удерживайте клавишу "Esc". На экране появится сообщение об ошибке функционального контроля.
3. Нажмите <Ctrl> + <Alt> + и введите учетные данные администратора.

Вход в систему: Режим входа пользователя

Стандартный. Для входа в систему пользователь должен ввести свои учетные данные, используя только стандартные средства ОС Windows.

Смешанный. Для входа в систему пользователь может предъявить идентификатор, активированный средствами Secret Net 6, или ввести свои учетные данные, используя стандартные средства ОС Windows.

Только по идентификатору. Для входа в систему пользователь должен предъявить идентификатор, активированный средствами Secret Net 6. Пользователи, не имеющие персонального идентификатора, войти в систему не смогут. Администратор может войти в систему без предъявления идентификатора только в административном режиме (см. ниже).

В стандартном и смешанном режимах входа допускается работа с USB-ключами средствами ОС Windows (см. документацию на ОС Windows). В режиме "Только по идентификатору" используются персональные идентификаторы, активированные средствами Secret Net 6, но не ОС Windows.

При попытках входа пользователей в систему в журнале регистрируются соответствующие события. Состав регистрируемых событий можно изменять. Описание действий для настройки механизма регистрации событий см. в документе [5].

Управление ключами для усиленной аутентификации

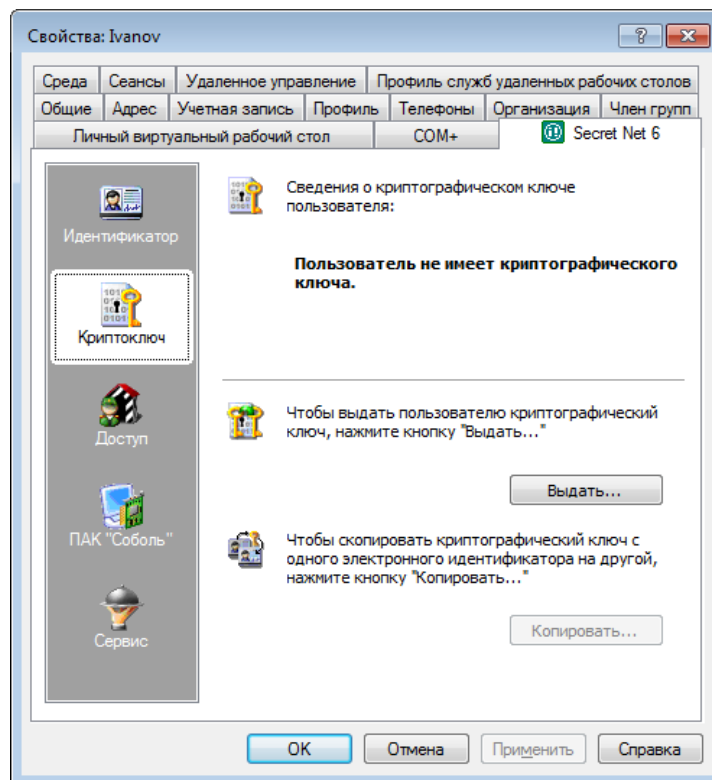
При включенном режиме усиленной аутентификации пользователь при входе в систему должен предъявить носитель, содержащий ключевую информацию. Ключевая информация пользователя может храниться в персональных идентификаторах или сменных носителях, присвоенных пользователю.

Генерация и выдача ключей

Генерация ключевой информации может выполняться средствами системы Secret Net 6 либо при присвоении пользователю персонального идентификатора (см. стр. 17), либо, когда идентификатор уже присвоен пользователю, отдельной процедурой выдачи ключей.

Для выдачи ключей:

1. Загрузите оснастку для управления параметрами пользователей, вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 6" (см. стр. 12).
2. В панели выбора режима выберите режим "Криптоключ".



В этом режиме отображаются сведения о ключах пользователя.

3. Нажмите кнопку "Выдать" (если у пользователя уже есть ключи, эта кнопка называется "Сменить").

Если пользователь уже имеет ключи, на экране появится диалог, предлагающий выбрать один из двух вариантов смены ключей — с сохранением старого ключа пользователя или без его сохранения.

4. Выберите нужный вариант и нажмите кнопку "Далее >".



Вариант без сохранения рекомендуется использовать только в тех случаях, когда невозможно считать текущий ключ с идентификаторов пользователя. Для подтверждения выбора введите в текстовое поле слово "продолжить" (без кавычек) и нажмите кнопку "Далее >". В этом случае программа перейдет к шагу "Запись ключей".

Чтение ключа

Если был выбран вариант с сохранением старого ключа, на экране появится диалог, отображающий ход выполнения операции чтения ключа, и приглашение предъявить идентификатор.

5. Предъявите идентификатор (см. стр. 16), содержащий старый закрытый ключ данного пользователя.

После успешного выполнения операции в диалоге справа от названия операции появится запись "Выполнено". Если при выполнении операции была допущена ошибка, в диалоге будет приведено сообщение об ошибке.

Продолжение процедуры без устранения ошибки невозможно.

6. Устраните ошибку, если она есть, нажав кнопку "Повторить" и повторно выполнив операцию. Нажмите кнопку "Далее >".

Запись ключей

На экране появится диалог, отображающий ход выполнения операций, и приглашение предъявить идентификаторы.

7. Предъявите все идентификаторы, указанные в списке.

При успешном предъявлении идентификатора его статус изменится на "Обработан". Если предъявление идентификатора выполнено с ошибкой, в столбце статуса обработки появится сообщение об ошибке. После предъявления всех идентификаторов кнопка "Отмена" будет заменена кнопкой "Закреть".

8. Нажмите кнопку "Закреть".

На экране появится диалог с результатами выполнения операций. Если операции выполнены с ошибками, в диалоге будет приведено их описание.



- Устраните ошибки, если они есть, нажав кнопку "< Назад" и повторно выполнив операцию, после чего нажмите кнопку "Готово".

Внимание! Настоятельно рекомендуется исправлять ошибки, произошедшие при записи ключей в идентификаторы. После успешного завершения всех предусмотренных операций статус каждой из них должен иметь значение "Выполнено".

Копирование ключей

Ключи пользователя, сгенерированные средствами системы Secret Net 6, можно скопировать с одного идентификатора пользователя на другой. Процедура копирования выполняется администратором безопасности.

Для копирования ключей:

- Загрузите оснастку для управления параметрами пользователей, вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 6" (см. стр. 12).
- В панели выбора режима выберите режим "Криптоключ".
- Нажмите кнопку "Копировать".
На экране появится диалог "Предъявите идентификатор".
- Предъявите идентификатор (см. стр. 16), содержащий копируемые ключи пользователя.
Произойдет считывание ключей и на экране появится диалог со списком идентификаторов пользователя.
- Предъявите идентификатор, на который требуется записать ключи.
При успешной записи ключей в идентификатор его статус изменится на "Обработан".
- Нажмите кнопку "Закреть".

Настройка параметров смены ключей

Администратор может настраивать следующие параметры смены ключей, сгенерированных средствами системы Secret Net 6:

- максимальный срок действия;
- минимальный срок действия;
- время предупреждения об истечении срока действия ключа.

Действие параметров распространяется на всех пользователей. По истечении максимального срока действия ключевая информация пользователя становится недействительной. В этом случае пользователь должен сменить ключевую информацию (описание процедуры смены ключевой информации пользователем см. в документе [9]). Смена ключевой информации самим пользователем возможна только по истечении минимального срока действия ключа.

Данные параметры взаимосвязаны. Минимальный срок действия и время предупреждения об истечении срока действия не могут быть равны или превышать максимальный срок действия ключа.

Для настройки параметров:

- Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
- Выберите папку "Ключи пользователя".
В правой части окна появится список параметров смены ключей.
- Вызовите контекстное меню нужного параметра и выберите в нем команду "Свойства".
На экране появится диалог настройки параметра.
- Настройте действие параметра и нажмите кнопку "ОК".

Примечание. Если параметру присвоено значение "0", он перестает оказывать действие на порядок смены ключей.

Использование ПАК "Соболь" в режиме интеграции с Secret Net 6

В Secret Net 6 предусмотрен режим интеграции с ПАК "Соболь", обеспечивающий реализацию следующих возможностей:

- вход доменных или локальных пользователей в систему на компьютерах с ПАК "Соболь" с помощью персонального идентификатора, инициализированного и присвоенного пользователю средствами Secret Net 6;
- формирование заданий на контроль целостности для ПАК "Соболь" средствами управления Secret Net 6 (см. Главу 4);
- автоматическая передача записей журнала регистрации событий ПАК "Соболь" в журнал Secret Net с последующей возможностью централизованного сбора журналов с локальных компьютеров в базу данных сервера безопасности (см. документ [8]).

Режим интеграции включается администратором безопасности на этапе установки ПАК "Соболь" (описание процедуры установки и включения режима см. в документе [8]). Следует обратить внимание на следующие особенности включения режима интеграции в сетевом режиме функционирования системы:

1. После установки ПАК "Соболь" на АРМ администратора безопасности и перевода его в режим совместного использования администратор безопасности должен сгенерировать ключи централизованного управления и записать их в идентификатор.
2. После подключения ПАК "Соболь" к системе Secret Net 6 администратор безопасности должен включить для своего персонального идентификатора режим разрешения входа в ПАК "Соболь". Включение режима осуществляется при настройке режимов использования идентификатора. Описание процедуры настройки режимов см. на стр. 19.

Управление ключами централизованного управления ПАК "Соболь"

В сетевом режиме функционирования системы Secret Net 6 при выполнении операций, связанных с организацией доступа пользователей к компьютерам, и операций с ключами администратора ПАК "Соболь" необходимо загрузить ключи централизованного управления ПАК "Соболь". Общие сведения о ключах и описание процедуры генерации см. в документе [8].

Загрузка ключей

Процедура загрузки ключей выполняется в оснастке "Active Directory — пользователи и компьютеры". После загрузки ключи сохраняются в системе до закрытия оснастки.

Для загрузки ключей:

1. Загрузите оснастку "Active Directory — пользователи и компьютеры" (см. стр. 12), вызовите контекстное меню для ярлыка любого пользователя и активируйте в нем команду "Загрузить ключи ЦУ".

Если команда недоступна, это означает, что ключи уже загружены.

На экране появится диалог "Предъявите идентификатор".

2. Предъявите носитель (см. стр. 16), на котором хранятся ключи централизованного управления ПАК "Соболь".

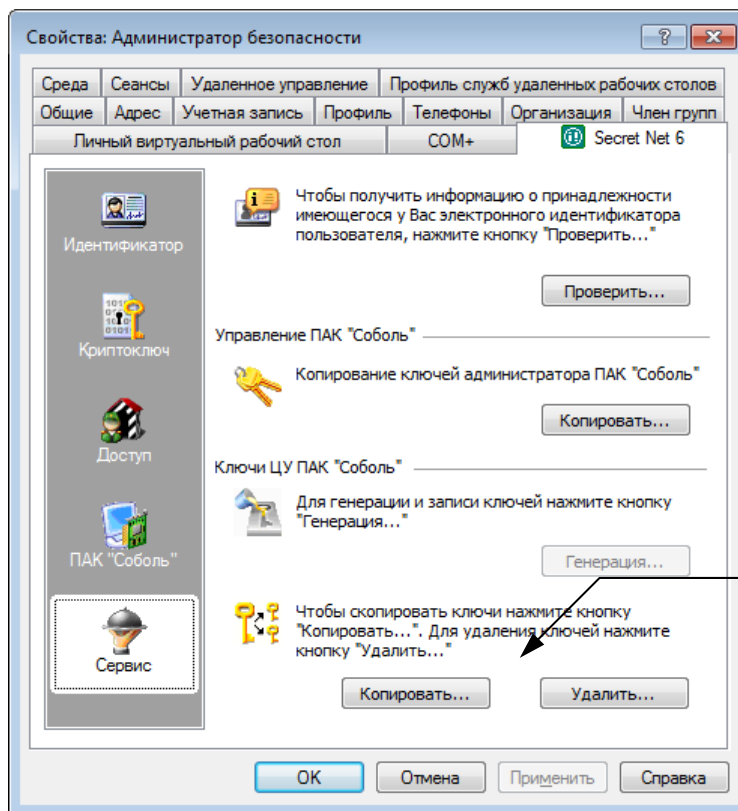
После успешной загрузки ключей на экране появится сообщение об этом.

Копирование и удаление ключей

При необходимости ключи централизованного управления ПАК "Соболь" могут быть скопированы с одного ключевого носителя на другой или удалены.

Для копирования ключей:

1. Загрузите оснастку "Active Directory — пользователи и компьютеры", вызовите окно настройки свойств любого пользователя и перейдите к диалогу "Secret Net 6" (см. стр. 12).
2. В панели выбора режима выберите режим "Сервис".



3. Нажмите кнопку "Копировать".
На экране появится диалог "Предъявите идентификатор".
4. Предъявите идентификатор (см. стр. 16), содержащий копируемые ключи централизованного управления ПАК "Соболь".
Произойдет считывание ключей, после чего на экране появится следующий диалог для предъявления идентификатора.
5. Предъявите идентификатор, на который требуется записать ключи.
При успешной записи ключей в идентификатор его статус изменится на "Обработан".
6. Нажмите кнопку "Закреть".

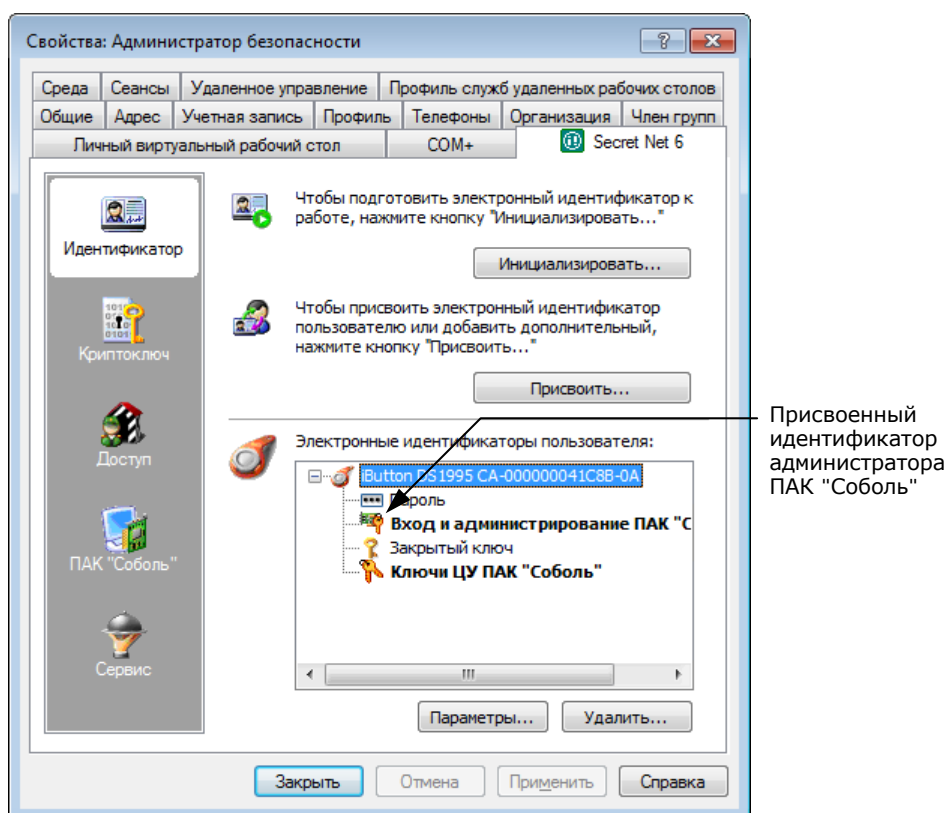
Для удаления ключей:

1. Загрузите оснастку "Active Directory — пользователи и компьютеры", вызовите окно настройки свойств любого пользователя и перейдите к диалогу "Secret Net 6" (см. стр. 12).
2. В панели выбора режима выберите режим "Сервис".
3. Нажмите кнопку "Удалить".
На экране появится запрос на продолжение операции.
4. Нажмите кнопку "Да" в диалоге запроса.
Произойдет удаление ключей из системы и на экране появится диалог для предъявления идентификатора, с которого будут удалены ключи.

5. Выполните нужное действие:
 - Если удалять ключи с идентификатора не требуется, нажмите кнопку "Отмена". На этом процедура удаления завершается.
 - Чтобы удалить ключи с идентификатора, предъявите его и подтвердите решение в появившемся диалоге запроса.
При успешном удалении ключей из идентификатора его статус изменится на "Обработан".
6. Закройте диалог предъявления идентификатора.
На экране появится запрос на удаление ключей со следующего носителя.
7. Если требуется удалить ключи с другого носителя, нажмите кнопку "Да" и предъявите следующий идентификатор. Для завершения процедуры нажмите кнопку "Нет".

Копирование идентификатора администратора ПАК "Соболь"

В Secret Net 6 идентификатор администратора ПАК "Соболь" может быть присвоен пользователю системы. После присвоения такой идентификатор отображается в списке идентификаторов пользователя со специальной пиктограммой:

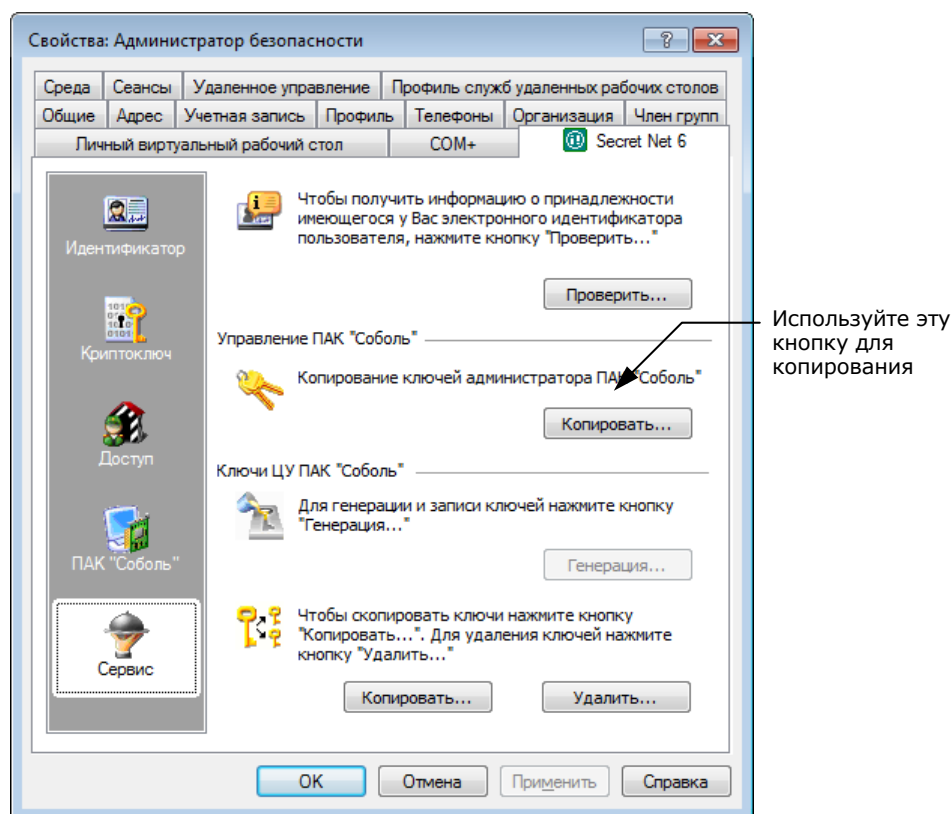


Если при инициализации ПАК "Соболь" не было создано достаточное количество резервных копий идентификаторов, можно скопировать содержимое идентификатора администратора ПАК "Соболь" на другой носитель. Новый идентификатор также можно будет использовать для администрирования комплексов "Соболь".

Для копирования идентификатора администратора ПАК "Соболь":

1. Если необходимо выполнить процедуру для доменного пользователя в сетевом режиме функционирования, загрузите ключи централизованного управления ПАК "Соболь" (см. стр. 27).
2. Загрузите оснастку для управления параметрами пользователей, вызовите окно настройки свойств любого пользователя и перейдите к диалогу "Secret Net 6" (см. стр. 12).

3. В панели выбора режима выберите режим "Сервис".



4. В разделе "Управление ПАК "Соболь" нажмите кнопку "Копировать".
На экране появится диалог "Предъявите идентификатор".
5. Предъявите идентификатор (см. стр. 16) администратора ПАК "Соболь".
На экране появится диалог запроса пароля.
6. Введите пароль администратора ПАК "Соболь" и нажмите кнопку "ОК".
На экране появится следующий диалог для предъявления идентификатора.
7. Предъявите идентификатор, в который должны быть скопированы сведения из идентификатора администратора ПАК "Соболь".
После успешной записи сведений в идентификатор его статус примет значение "Обработан".
8. Нажмите кнопку "ОК".

Предоставление доступа к компьютерам с ПАК "Соболь"

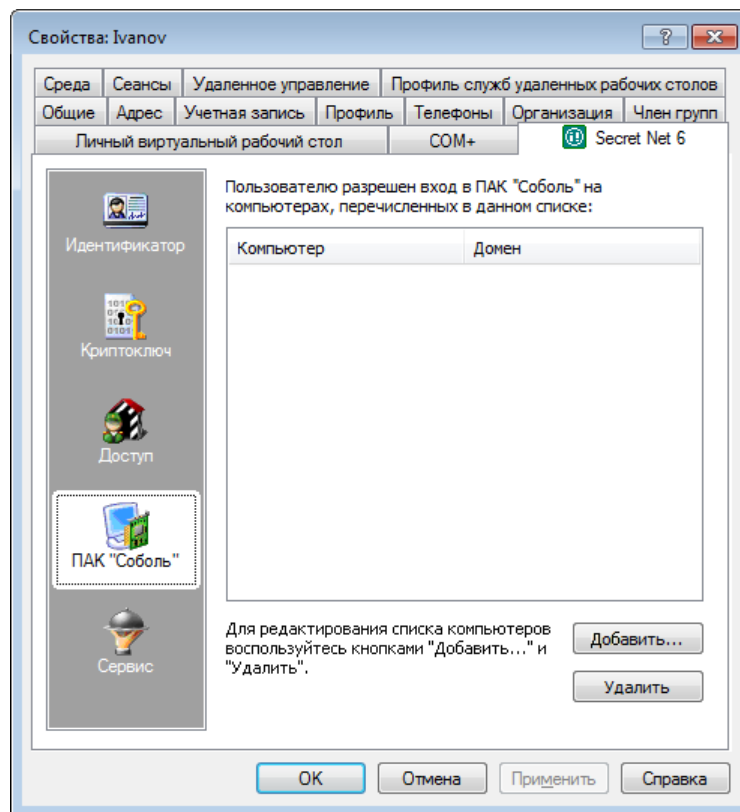
В сетевом режиме функционирования системы Secret Net 6 на компьютерах с ПАК "Соболь" при включенном режиме интеграции с Secret Net 6 (см. документ [8]) пользователи имеют возможность выполнять вход в ПАК "Соболь" и далее в систему с использованием персональных идентификаторов, инициализированных и присвоенных пользователям средствами системы защиты. То есть для входа в ПАК "Соболь" и для входа в систему пользователь может использовать один идентификатор.

Чтобы предоставить такую возможность доменному пользователю, необходимо выполнить следующие действия:

- присвоить пользователю идентификатор с включенным режимом разрешения входа в ПАК "Соболь" (см. стр. 17). Для идентификаторов, присвоенных пользователю ранее, включить режим можно при настройке режимов использования идентификатора (см. стр. 19);
- сформировать список компьютеров, на которых пользователю разрешается выполнять вход в ПАК "Соболь" (см. процедуру ниже).

Для формирования списка компьютеров:

1. Загрузите ключи централизованного управления ПАК "Соболь" (см. стр. 27).
2. В оснастке "Active Directory — пользователи и компьютеры" вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 6".
3. В панели выбора режима выберите режим "ПАК "Соболь"".



4. Нажмите кнопку "Добавить".
На экране появится стандартный диалог ОС Windows для выбора объектов.
5. Выберите компьютеры, к которым пользователь должен иметь доступ, и добавьте их в список.
6. Если требуется удалить компьютер из списка, выберите его и нажмите кнопку "Удалить".
7. Завершив формирование списка компьютеров, нажмите кнопку "ОК" или "Применить" в окне настройки свойств пользователя.

Глава 3

Управление устройствами

Общие принципы

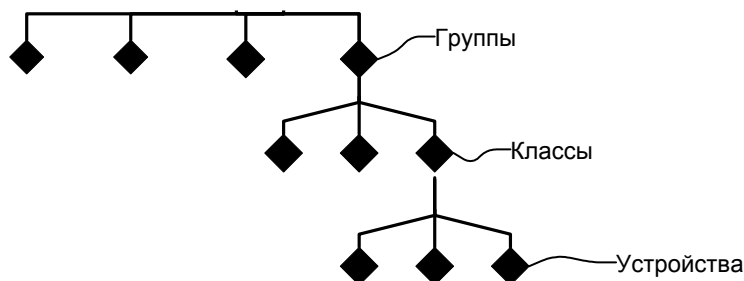
В этой главе описывается настройка двух механизмов защиты: механизма контроля аппаратной конфигурации и механизма разграничения доступа к устройствам. Работа этих механизмов взаимосвязана. Механизм контроля аппаратной конфигурации предназначен для обнаружения и реагирования на изменения аппаратной конфигурации компьютера, а также для поддержания в актуальном состоянии списка устройств компьютера. На основании списков устройств с помощью второго механизма выполняется разграничение доступа пользователей к устройствам.

Списки устройств

Для описания устройств, входящих в состав или подключаемых к защищаемым компьютерам в Secret Net 6, используется иерархическая схема. Все устройства разделены на **классы**, а классы принадлежат **группам**. Предусмотрены следующие группы:

- локальные устройства;
- устройства USB;
- устройства PCMCIA;
- устройства IEEE1394;
- устройства Secure Digital.

Контролируемые устройства



Для объектов каждого уровня определен набор параметров, с помощью которых настраиваются механизмы контроля аппаратной конфигурации и разграничения доступа к устройствам. Иерархия списка устройств позволяет выполнять настройку как на уровне отдельного устройства, так и на уровне классов и групп.

Полный список групп и классов устройств приведен в Приложении на стр. 103.

На компьютере список устройств создается сразу после установки клиентского ПО системы Secret Net 6 при первой загрузке ОС. Этот список устройств принимается как эталонная конфигурация компьютера. Список устройств отображается в локальной политике безопасности и хранится в локальной базе данных системы Secret Net 6.

В сетевом режиме функционирования системы защиты при создании групповой политики также создается список устройств. В него входят группы и классы устройств. Параметры доступа к группам и классам устройств хранятся и распространяются в домене в составе доменных (групповых) политик.

Режимы работы

Механизм контроля аппаратной конфигурации может работать в следующих режимах:

| Режим | Описание |
|-------------------|---|
| Прозрачный | Изменения аппаратной конфигурации автоматически фиксируются в локальной базе данных Secret Net 6. События в журнале не регистрируются. Реакция системы на изменения в конфигурации отсутствует |
| Мягкий | События регистрируются в журнале. Блокировка не применяется. Изменения эталонной аппаратной конфигурации фиксируются в локальной базе данных Secret Net 6 только после утверждения изменений администратором безопасности |
| Жесткий | События регистрируются в журнале. При изменении конфигурации работа пользователя блокируется. Снять блокировку и утвердить новую конфигурацию в качестве эталонной может только администратор безопасности |

Для надежной защиты компьютера рекомендуется использовать "жесткий" режим. При этом на практике требование контролировать все устройства, входящие в конфигурацию компьютера, не является обязательным. Также не является обязательной регистрацией всех событий, связанных с изменениями в аппаратной конфигурации. Поэтому администратору безопасности необходимо определить, какие устройства подлежат обязательному контролю и какие события следует регистрировать в журнале.

Механизм разграничения доступа к устройствам может работать в следующих режимах:

| Режим | Описание |
|------------------|--|
| Отключено | Доступ к устройствам не контролируется. События, связанные с доступом пользователей к устройствам, в журнале Secret Net не регистрируются |
| Мягкий | Доступ к устройствам контролируется. Попытки несанкционированного доступа к устройствам регистрируются в журнале Secret Net. При этом запрет доступа не осуществляется |
| Жесткий | Доступ к устройствам контролируется в полном объеме. Попытки несанкционированного доступа к устройствам запрещаются и регистрируются в журнале Secret Net |

Если в процессе работы в системе появляется новое устройство, система защиты определяет его и относит к соответствующей группе и классу. Права доступа пользователей к этому устройству устанавливаются автоматически в соответствии с правами, установленными для класса или группы устройств. По умолчанию каждому новому устройству назначаются (наследуются) права, установленные для его класса, и после этого функция наследования прав для устройства отключается.

Настройки по умолчанию

По умолчанию для механизма контроля аппаратной конфигурации задан "мягкий" режим работы, который распространяется на всех пользователей компьютера (в сетевом режиме функционирования параметры контроля аппаратной конфигурации по умолчанию не определены в групповых политиках, поэтому на всех компьютерах действуют параметры локальной политики).

Права доступа к устройствам по умолчанию сводятся к предоставлению полного доступа трем стандартным группам пользователей (SYSTEM, Администраторы, Все) к устройствам только данного компьютера. Права доступа складываются из разрешений и запретов на выполнение определенных операций. Набор операций зависит от типа устройства, например:

| Тип устройства | Операции |
|--|---|
| Локальные устройства Логические диски | <ul style="list-style-type: none"> • Использование устройства • Чтение • Запись • Выполнение • Особые разрешения |

| Тип устройства | Операции |
|-----------------------------------|--|
| Устройства USB Прочие | <ul style="list-style-type: none"> • Подключение устройства • Отключение устройства |
| Устройства USB Хранение данных | <ul style="list-style-type: none"> • Подключение устройства • Отключение устройства • Использование устройства • Чтение • Запись • Выполнение • Особые разрешения |

По умолчанию после установки системы защиты действуют следующие правила, которые распространяются на всех пользователей:

- Контролируются все устройства, входящие в группу "Локальные устройства".
- Режим работы механизма — "мягкий" (см. ниже в этом разделе).
- Регистрируются все события категорий "Контроль аппаратной конфигурации" и "Разграничение доступа к устройствам" (см. документ [5]).

Чтобы пользователь мог подключать к компьютеру только устройства, разрешенные к использованию администратором безопасности, настройку системы можно выполнить следующим образом:

1. После установки системы защиты администратор последовательно подключает к компьютеру все необходимые устройства. На этом этапе устройства регистрируются в системе и для них копируются разрешающие права доступа (от классов), после чего система отключает наследование прав на эти устройства.
2. По завершении регистрации устройств администратор отключает разрешающие права для соответствующих классов или групп (например, для группы "Устройства USB"). Это приведет к тому, что пользователь сможет подключать только устройства, зарегистрированные на шаге 1. Подключение других устройств (в приведенном примере — USB-устройств) будет запрещено.
3. В дальнейшем при необходимости разрешить подключение дополнительного устройства администратор сначала включает разрешающие права для соответствующего класса или группы, подключает устройство и после его регистрации снова отключает разрешающие права для класса (группы).

Способы управления в автономном режиме функционирования

Настраивать параметры контроля и права доступа можно непосредственно для каждого конкретного устройства. Этот способ управления рекомендуется использовать тогда, когда в отдельных случаях требуется предоставить особые права доступа к конкретным устройствам.

Если же для всех устройств данного класса или группы должны действовать типовые параметры контроля и права доступа, рекомендуется выполнять настройку этих параметров для класса или группы устройств, а для конкретных устройств, входящих в класс или группу, включать режим наследования параметров контроля и прав доступа.

В этом случае после назначения прав доступа для группы (или класса) эти права автоматически распространяются на все устройства, относящиеся к данной группе (классу). Причем это относится как к устройствам, присутствующим в системе (при условии, что права доступа для этих устройств наследуются от групп и классов), так и к вновь подключаемым устройствам.

Способы управления в сетевом режиме функционирования

В сетевом режиме функционирования системы Secret Net 6 применение локальных и групповых политик обеспечивает гибкое управление механизмами контроля аппаратной конфигурации и разграничения доступа к устройствам. Существует несколько подходов к организации управления. Администратор безопасности в зависимости от стоящих перед ним задач может выбрать один из вариантов:

- смешанное централизованное и локальное управление — централизованное управление только на уровне групп и классов и локальное управление на уровне отдельных устройств;
- централизованное управление на всех уровнях.

Централизованное управление

Администратор безопасности может управлять параметрами контроля и правами доступа доменных пользователей применительно к группам и классам устройств, используя редактор групповой политики. Выполненные настройки сохраняются в объектах групповых политик и вступают в силу после успешного их применения. После назначения параметров применительно к группе (классу) они автоматически распространяются на все устройства, относящиеся к данной группе (классу). Причем это относится как к устройствам, присутствующим в системе (при условии, что параметры для этих устройств наследуются от групп и классов), так и к вновь подключаемым устройствам.

Этот вариант управления является предпочтительным, когда управление осуществляется на уровне групп, т. е. нет необходимости устанавливать особые настройки для отдельных устройств.

Локальное управление на уровне отдельных устройств

Если в отдельных случаях требуется установить особые настройки для конкретных устройств, то можно выполнить настройку локальной политики доступа. С ее помощью администратор безопасности может настроить на компьютере параметры контроля и доступ пользователей и групп пользователей как к группам и классам устройств, так и к отдельным устройствам (если настройки объектов не определены в групповой политике). Настройки локальной политики сохраняются в локальной базе данных.

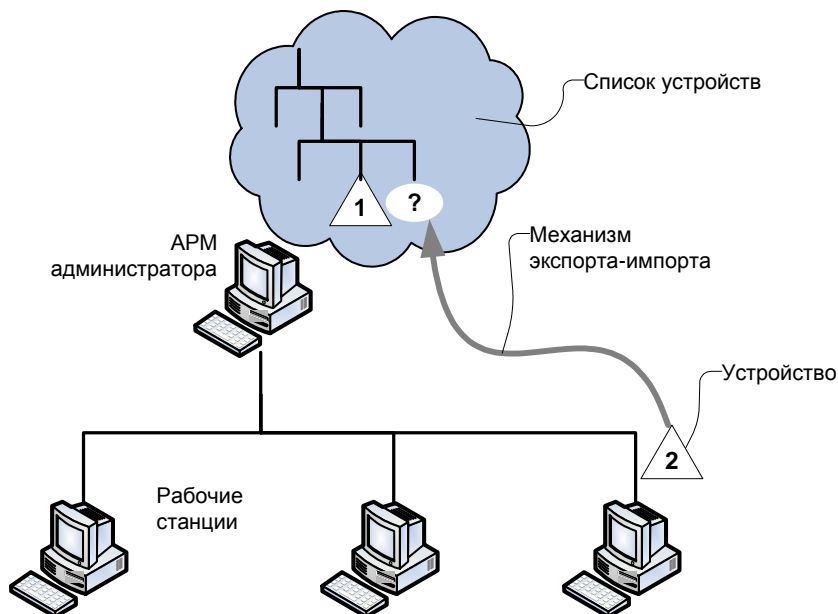
Централизованное управление на уровне отдельных устройств

Если на компьютерах требуется использовать особые настройки для отдельных устройств, то можно управлять контролем и доступом к таким устройствам централизованными средствами управления групповой политикой. Для этого такие устройства необходимо включить в список устройств групповой политики.

Добавление устройств в список устройств политики осуществляется посредством экспорта-импорта параметров устройств. Сначала для нужных устройств выполняется экспорт параметров. Экспорт осуществляется с компьютеров, к которым подключены устройства. Экспорт можно выполнить:

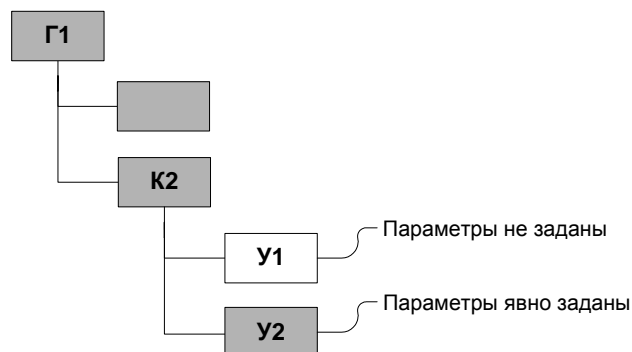
- централизованно в программе "Монитор" (см. документ [6]);
- локально на компьютере, где установлено устройство (см. стр. 39).

Далее полученный файл (файлы) со сведениями об устройствах импортируется в групповую политику для добавления в список устройств групповой политики (см. стр. 41).



Правила наследования

В рамках групповой или локальной политики права доступа к каждому объекту (группе, классу, устройству), а также политика контроля устройств определяются в соответствии с правилами наследования или явного задания параметров. Параметры могут быть заданы для групп (Г), классов (К) или отдельных устройств (У). В задании параметров может использоваться принцип наследования от групп к классам и от классов к устройствам. При этом явно заданные параметры имеют приоритет перед наследуемыми параметрами старших элементов иерархии. Например, если для устройства явно заданы особые параметры доступа, они будут применяться независимо от того, какие параметры заданы для класса и группы.



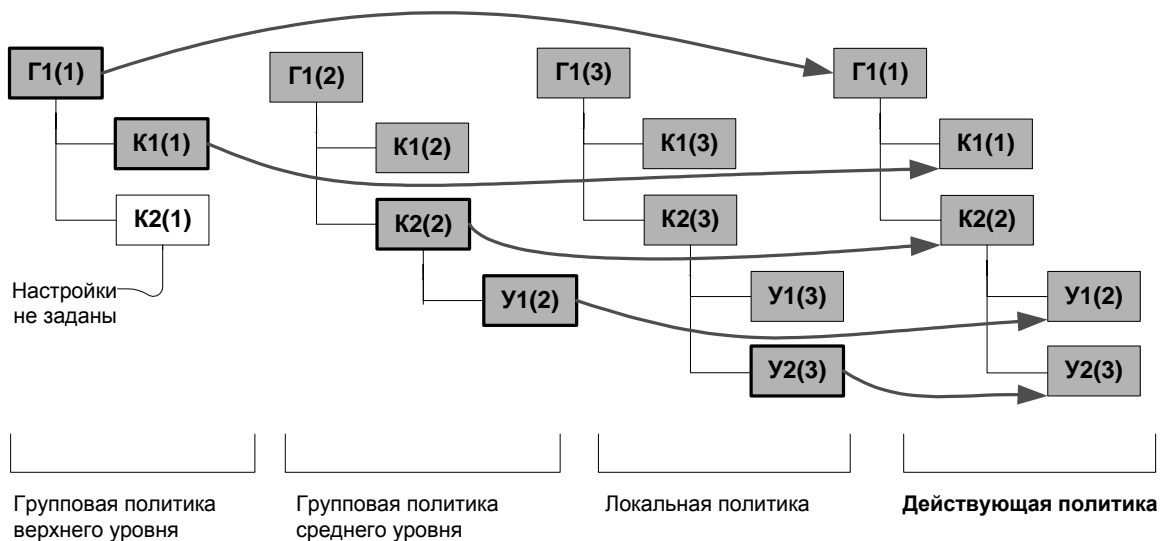
В приведенном на рисунке примере устройство "У1" наследует параметры, заданные для класса "К2". А для устройства "У2" действуют явно заданные параметры, которые могут отличаться от параметров, заданных для класса "К2".

Особенности применения групповых политик

В сетевом режиме функционирования системы Secret Net 6 администратор безопасности имеет возможность создавать политики разграничения доступа к устройствам, которые могут применяться в домене в составе групповых политик. Разграничение можно осуществлять как на уровне домена, так и на уровне организационных подразделений. При создании политики формируется список групп и входящих в них классов устройств, а также устанавливаются права доступа к группам и классам.

При входе пользователя в систему значения параметров доступа устанавливаются в соответствии с действующей политикой. Действующая политика определяется по стандартному для Windows правилу применения политик и их приоритет) с учетом прав доступа, настроенных в групповых и локальных политиках. Если

групповая политика не определена, вступают в силу параметры, настроенные в политике, имеющей более низкий приоритет. Частный пример применения групповых политик показан на рисунке:



Задание групповой политики и просмотр списка устройств

Для централизованного управления механизмами контроля аппаратной конфигурации и разграничения доступа должна быть задана групповая политика контроля устройств. Политика включает в себя список групп и классов устройств, а также параметры этих объектов.

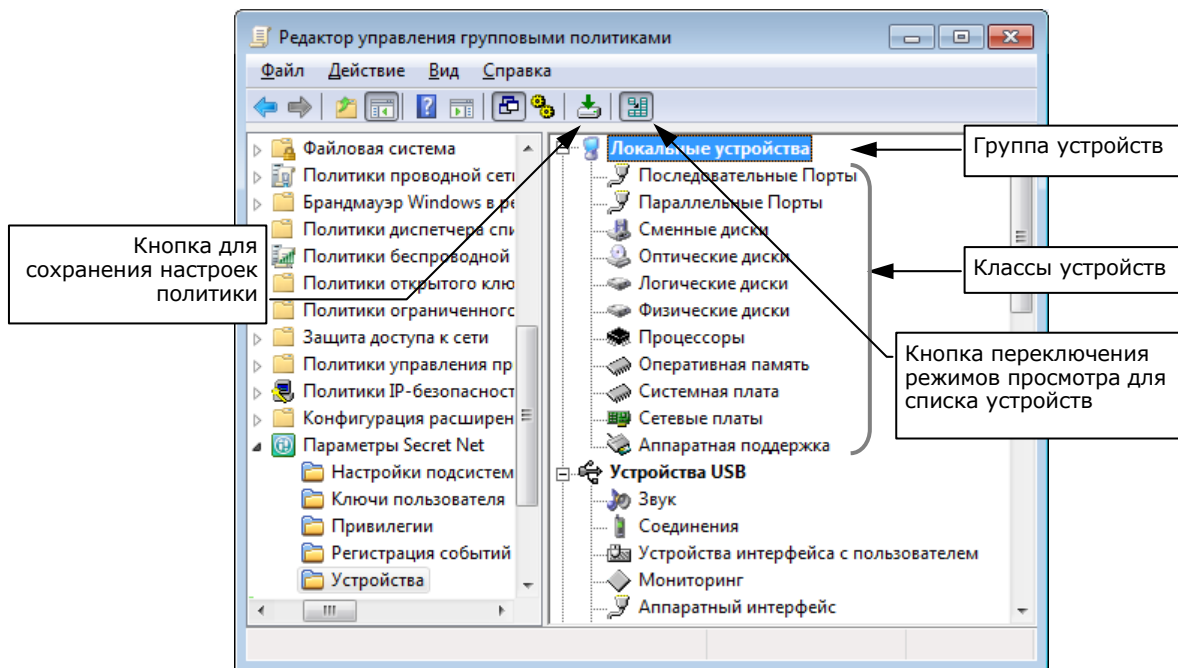
После установки системы групповая политика не определена. Поэтому независимо от того, какой механизм настраивается, ее необходимо задать.

Для задания групповой политики контроля устройств:

1. Вызовите оснастку для управления параметрами объектов групповой политики (политика безопасности домена или организационного подразделения) и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
2. Выберите папку "Устройства".
В правой части окна появится сообщение, что политика не определена.
3. Вызовите контекстное меню папки "Устройства" и активируйте в нем команду "Политика | Создать".
4. Нажмите на панели инструментов кнопку переключения режимов просмотра (см. выноску к рисунку).

Совет. Для переключения режимов просмотра можно использовать команду меню "Вид | Показывать все группы устройств".

В правой части консоли появится общий список групп и классов устройств, составляющих аппаратную конфигурацию.



5. Для сохранения параметров политики нажмите кнопку на панели инструментов (см. выноску к рисунку).

Описание списка устройств

Список устройств используется как при централизованном управлении, так и при локальном управлении. Порядок работы со списком при этом одинаков. Различие заключается только в том, что изначально после задания групповой политики список содержит только группы и классы устройств, а в локальной политике в него включены все обнаруженные устройства. Если устройство в данный момент отключено, его наименование будет зачеркнуто.

Предусмотрены 2 режима отображения списка устройств:

- просмотр **полного списка** элементов — показаны все возможные группы, классы и устройства (в централизованном управлении — только группы и классы) независимо от наличия включенных в них устройств;
- просмотр **актуального списка** элементов — показаны только те группы и классы, в состав которых входят используемые устройства.

При открытии папки "Устройства" действует режим просмотра актуального списка элементов. Если список не содержит отдельных устройств, то он будет пуст. В этом случае для просмотра списка классов и групп нажмите кнопку переключения режимов просмотра.

При формировании списка по умолчанию устанавливается контроль всех устройств группы "Локальные устройства", остальные устройства не контролируются. При этом параметры контроля для групп и устройств заданы явно, а для классов — наследуются от вышестоящих объектов (групп). В списке объекты, для которых параметры контроля заданы явно, помечаются отметкой **зеленого цвета**.

Одновременно с параметрами контроля устройств при формировании списка автоматически устанавливаются права доступа 3 групп пользователей (SYSTEM, Администраторы, Все) к группам устройств. По умолчанию для всех групп устройств устанавливаются разрешения на все операции (полный доступ), запреты не определены. Права доступа для групп устройств заданы явно. В списке это отображается отметкой **красного цвета**, стоящей перед наименованием группы. Для всех классов устройств по умолчанию включен признак наследования разрешений. Поэтому пользователям, входящим в 3 указанные группы, по умолчанию разрешен полный доступ ко всем классам устройств. Если изменить права доступа для класса, это будет означать, что параметры заданы явно. В этом случае перед его наименованием в списке появится отметка красного цвета.

Экспорт параметров устройств

Параметры устройств можно экспортировать. Сведения сохраняются в файлах специального формата описания устройств системы Secret Net 6 (*.sndeV). Содержимое файлов в дальнейшем можно импортировать с помощью мастера импорта (см. стр. 41).

Примечание. Экспорт в файл формата *.sndeV поддерживается только для устройств. Для сохранения сведений о классах и группах необходимо использовать процедуру экспорта параметров политики (см. стр. 86).

Для экспорта элемента списка устройств:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
2. Выберите папку "Устройства".
В правой части окна появится иерархический список устройств.
3. Вызовите контекстное меню нужного устройства и активируйте команду "Экспорт".
На экране появится стандартный диалог сохранения файла ОС Windows.
4. Укажите имя файла для сохранения сведений.

Контроль аппаратной конфигурации компьютера

Изменения аппаратной конфигурации могут быть вызваны выходом из строя, добавлением или заменой отдельных устройств. В процессе эксплуатации администратор безопасности в случае необходимости может вносить изменения в настройки механизма контроля аппаратной конфигурации. Например, он может редактировать список контролируемых устройств, изменять режим работы механизма и перечень регистрируемых событий.



Список устройств, входящих в состав компьютера (аппаратная конфигурация), формируется при установке клиентского ПО Secret Net 6 и автоматически утверждается при первой загрузке после установки или обновления. Поэтому, чтобы исключить несанкционированное подключение устройств, первый после установки (обновления) вход в систему должен быть выполнен под контролем администратора безопасности. Рекомендуется перезагрузить компьютер сразу после появления сообщения об успешном завершении установки Secret Net 6.

Для настройки механизма контроля аппаратной конфигурации необходимо:

1. Задать и настроить политику контроля.
2. При необходимости изменить перечень регистрируемых событий.
3. Включить требуемый режим работы механизма.

Задание и настройка политики контроля

Настройка политики контроля устройств заключается в формировании списка контролируемых устройств. Для этого необходимо выбрать устройство из общего списка аппаратной конфигурации и отменить или установить параметр "Не контролировать параметры устройства".

Настройку политики контроля можно выполнить:

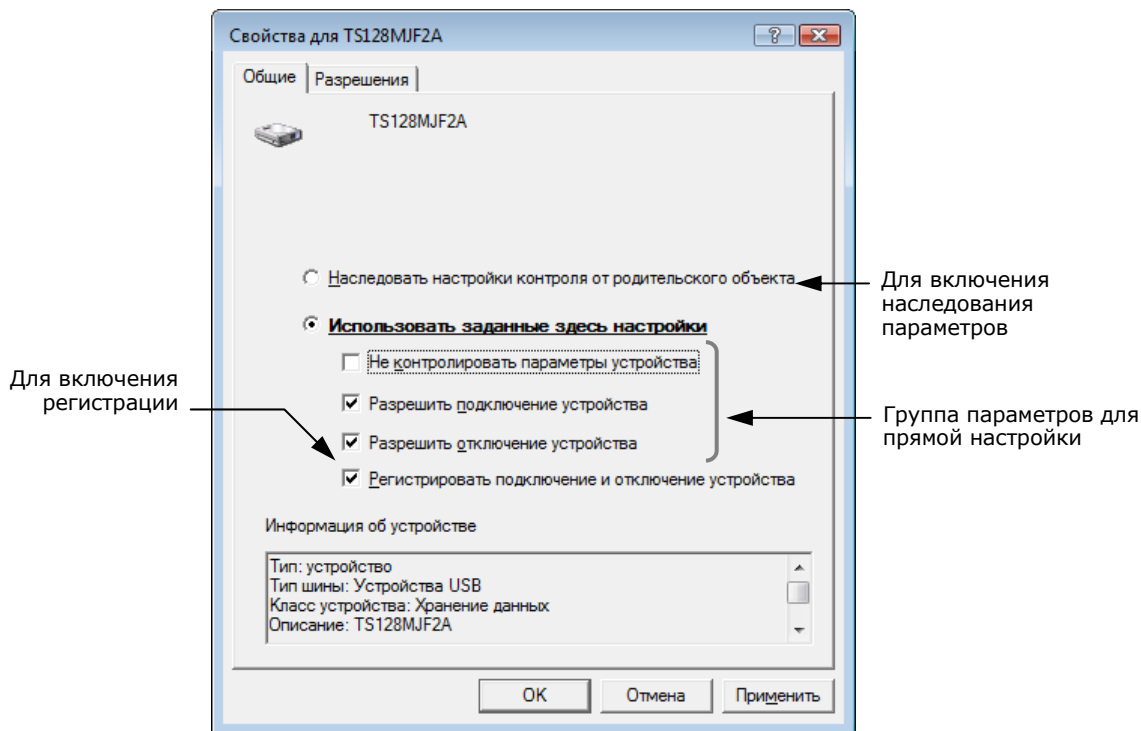
- индивидуально для каждого устройства;
- для класса или группы устройств с использованием принципа наследования параметров (рекомендуется).

В сетевом режиме функционирования системы Secret Net 6 можно задать политику контроля устройств в групповых политиках (см. стр. 37). Если политика не задана, на компьютерах действует локальная политика, включающая в себя настройки контроля аппаратной конфигурации по умолчанию (см. стр. 33). Если политика задана, работа механизма определяется действующей групповой политикой.

Для настройки политики контроля устройств:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
2. Выберите папку "Устройства".
В правой части окна появится общий список устройств аппаратной конфигурации.
3. Выберите в списке устройство (объект), для которого необходимо изменить параметр контроля, и вызовите окно настройки его свойств.

Появится окно свойств устройства:



Для объектов с явно заданными параметрами контроля поле "Использовать заданные здесь настройки" содержит отметку. Если отметка отсутствует, это означает, что параметр контроля для данного объекта наследуется от вышестоящего объекта (для устройства вышестоящим является класс, а для класса — группа). При этом настройки будут недоступны для изменения, но они будут отображать настройки родительского объекта.

4. Если данное устройство должно наследовать политику от вышестоящего элемента иерархии (группы или класса), установите отметку в поле "Наследовать настройки контроля от родительского объекта".

Если для данного устройства требуется задать явно политику контроля, установите отметку в поле "Использовать заданные здесь настройки" и измените нужным образом состояние выключателя "Не контролировать параметры устройства":

- удалите отметку — чтобы включить контроль устройства;
- установите отметку — если нужно снять устройство с контроля.

5. Нажмите кнопку "ОК".
6. Повторите действия 3–5 для настройки контроля другого устройства (класса, группы).

Изменение перечня регистрируемых событий

Для отслеживания произошедших событий, связанных с работой механизма контроля аппаратной конфигурации, необходимо выполнить настройку регистрации событий. Для этого следует указать, какие события категории "Контроль конфигурации" должны регистрироваться в журнале Secret Net. Полный перечень событий этой категории и процедура настройки регистрации событий приведены в документе [5].

Изменение режима работы механизма

Для изменения режима работы:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
2. Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.
3. Вызовите контекстное меню для параметра "Контроль устройств: Режим работы" и активируйте в нем команду "Свойства".
На экране появится диалог настройки параметра.
4. Настройте действие параметра и нажмите кнопку "ОК".

Утверждение конфигурации

В "мягком" и "жестком" режимах работы механизма при обнаружении системой изменений в аппаратной конфигурации на экран выводится сообщение об этом, а пиктограмма Secret Net 6 в Панели задач Windows меняет свой цвет на красный.

В "жестком" режиме работы механизма выполняется блокировка компьютера. Снять блокировку компьютера и утвердить изменения в аппаратной конфигурации может только администратор. В сетевом режиме функционирования утверждение конфигурации можно выполнить:

- централизованно в программе "Монитор" (см. документ [6]);
- локально на компьютере (см. ниже).

Пояснение. Утверждение аппаратной конфигурации не требуется при прозрачном режиме работы и в случае, когда устройство не входит в перечень контролируемых устройств. В этих случаях изменения сразу автоматически попадают в базу данных.

Для локального утверждения конфигурации:

1. Вызовите контекстное меню для пиктограммы Secret Net 6 в Панели задач и активируйте команду "Утвердить аппаратную конфигурацию" ("Утвердить изменения в конфигурации").
На экране появится диалог со списком изменений аппаратной конфигурации.
2. Нажмите кнопку "Утвердить" для утверждения изменений.
В результате подключенное или отключенное устройство (устройства) будет учтено в составе эталонной аппаратной конфигурации. При этом пиктограмма Secret Net 6 в Панели задач примет обычный вид.

Добавление устройств в аппаратную конфигурацию

После изменения аппаратной конфигурации компьютера и ее утверждения подключенное устройство добавляется в общий список устройств. При этом параметры контроля устройства устанавливаются в соответствии с настройками, заданными для объекта вышестоящего уровня (класса).

Если предполагается использовать в составе компьютера новое устройство, не входящее в аппаратную конфигурацию, его необходимо добавить в общий список устройств.

Предусмотрены следующие варианты добавления устройств:

- **Импорт параметров устройства из файла.** Добавляется устройство, параметры которого были предварительно сохранены на любом из компьютеров средствами экспорта (см. стр. 39).
- **Добавление из списка стандартных устройств.** Этот вариант используется, когда необходимо добавить одно или несколько стандартных устройств, таких как порты и диски.

Для добавления используется мастер импорта параметров устройств.

Для запуска мастера:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
2. Выберите папку "Устройства".
В правой части окна появится список устройств.
3. В меню оснастки активируйте команду "Действие | Политика | Добавить устройство".
На экране появится стартовый диалог мастера импорта параметров устройств.
4. Выберите вариант добавления устройства, нажмите кнопку "Далее >" и следуйте инструкциям мастера.

Избирательное разграничение доступа к устройствам

Для настройки этого механизма необходимо:

1. Задать политику контроля устройств и настроить права доступа пользователей к устройствам.
2. Настроить регистрацию событий и аудит операций с устройствами.
3. Включить нужный режим работы механизма.

После настройки администратор безопасности осуществляет поддержку функционирования механизма, выполняя следующие функции:

- корректировка прав доступа к устройствам;
- настройка регистрации событий и анализ нарушений;
- управление режимом работы механизма.

Задание политики и настройка прав доступа к устройствам

Права доступа к объектам могут устанавливаться как для отдельных устройств, так и для групп (классов). Для настройки необходимо выбрать в списке устройств объект (группу, класс и т. д.), составить список пользователей (групп пользователей), для которых назначаются права доступа к данному объекту, и затем установить разрешения и запреты на выполнение отдельных операций.

В централизованном управлении, если не выполнялась настройка механизма контроля аппаратной конфигурации, политика разграничения доступа не определена. Для централизованного управления механизмом ее необходимо задать (см. стр. 37). После задания в групповой политике устанавливаются права доступа к группам и классам по умолчанию (см. стр. 33).

Для настройки прав доступа к устройствам:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
2. Выберите папку "Устройства".
В правой части окна оснастки появится список устройств.
3. Выберите в списке объект (группу, класс или устройство), вызовите контекстное меню и активируйте команду "Свойства".

На экране появится диалоговое окно настройки свойств объекта.

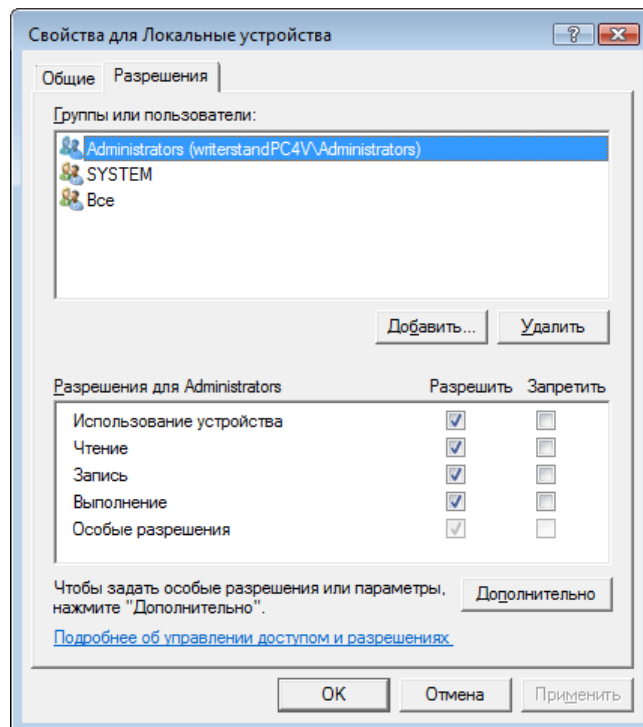
4. Если требуется отключить наследование параметров, установите отметку в поле "Использовать заданные здесь настройки".

После этого станут доступны параметры подключения и отключения устройства.

5. Удалите или установите отметки в параметрах подключения и отключения и перейдите к диалогу "Разрешения".



Следует иметь в виду, что диалог "Разрешения" присутствует для тех устройств, для которых возможна настройка разрешений и запретов: порты, диски, носители данных (для системного диска управление разрешениями запрещено).



В верхней части диалога "Разрешения" расположен список учетных записей, для которых выполняется настройка прав доступа к данной группе устройств. В нижней части диалога приведены параметры доступа (разрешения и запреты на выполнение операций) для выбранной учетной записи.

Если для класса установлен признак наследования от группы, изменить можно только ненаследуемые права, а также добавить в список других пользователей или группы.

Можно изменить права доступа для родительского объекта (группы) и затем, используя принцип наследования, применить их к классу.

6. При необходимости отредактируйте список учетных записей:
 - чтобы добавить в список учетную запись, нажмите кнопку "Добавить" и выберите нужный объект в стандартном диалоге выбора объектов ОС Windows;
 - чтобы удалить учетную запись из списка, выберите ее в списке и нажмите кнопку "Удалить".
7. Для изменения параметров доступа выберите в списке нужную учетную запись и затем расставьте разрешения и запреты на выполнение операций. При этом учитывайте принцип наследования параметров от родительских объектов дочерними: явно заданные параметры перекрывают унаследованные от родительских объектов.



Для отключения или включения режима переноса наследуемых разрешений нажмите кнопку "Дополнительно" и в открывшемся диалоговом окне удалите или установите отметку в поле "Наследовать от родительского объекта..." ("Добавить разрешения, наследуемые от родительских объектов").

8. В диалоге настройки свойств объекта нажмите кнопку "OK".

9. Для сохранения изменений нажмите на панели инструментов кнопку "Сохранить настройки политики контроля устройств".

Настройка регистрации событий и аудита операций

Изменение перечня регистрируемых событий

Для отслеживания произошедших событий, связанных с работой механизма разграничения доступа к устройствам, необходимо выполнить настройку регистрации событий. Для этого следует указать, какие события категории "Разграничение доступа к устройствам" должны регистрироваться в журнале Secret Net. Полный перечень событий этой категории и процедура настройки регистрации событий приведены в документе [5].

Настройка аудита успехов и отказов

Настройка аудита выполнения операций с устройствами может выполняться для групп, классов и конкретных устройств.

Для настройки аудита:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
2. Выберите папку "Устройства".
В правой части окна оснастки появится список устройств.
3. Выберите в списке устройство, вызовите контекстное меню и активируйте команду "Свойства".
На экране появится диалоговое окно настройки свойств устройства.
4. Перейдите к диалогу "Разрешения" и нажмите кнопку "Дополнительно".
На экране появится диалоговое окно настройки дополнительных параметров.
5. Перейдите к диалогу "Аудит" и настройте параметры аудита ОС Windows.

Изменение режима работы механизма

Для изменения режима работы:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
2. Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.
3. Вызовите контекстное меню для параметра "Разграничение доступа к устройствам: Режим работы" и активируйте в нем команду "Свойства".
На экране появится диалог настройки параметра.
4. Настройте действие параметра и нажмите кнопку "ОК".

Глава 4

Контроль целостности и замкнутая программная среда

Механизм контроля целостности (КЦ) предназначен для слежения за неизменностью содержимого ресурсов компьютера. Действие этого механизма основано на сравнении текущих значений контролируемых параметров проверяемых ресурсов и значений, принятых за эталон. Эталонные значения контролируемых параметров определяются или рассчитываются при настройке механизма. В процессе контроля при обнаружении несоответствия текущих и эталонных значений система оповещает администратора о нарушении целостности ресурсов и выполняет заданное при настройке действие, например, блокирует компьютер, на котором нарушение обнаружено.

Механизм замкнутой программной среды (ЗПС) предназначен для ограничения использования ПО на компьютере. Доступ разрешается только к тем программам, которые необходимы пользователям для работы. Для каждого пользователя определяется перечень ресурсов, в который входят разрешенные для запуска программы, библиотеки и сценарии. Попытки запуска других ресурсов блокируются, и в журнале безопасности регистрируются события несанкционированного доступа (НСД).

Модель данных

Состав

Параметры, определяющие работу механизмов контроля целостности и замкнутой программной среды, объединены в рамках единой модели данных. **Модель данных (МД)** представляет собой иерархию объектов и описание связей между ними. В модели используются 5 категорий объектов:

| Объект | Пояснение |
|---------------------------|---|
| Ресурс | Описание файла или каталога, переменной реестра или ключа реестра Windows. Однозначно определяет местонахождение контролируемого ресурса и его тип |
| Группа ресурсов | Объединяет несколько описаний ресурсов одного типа (файлы и каталоги или объекты системного реестра). Например, исполняемые файлы или ключи реестра, относящиеся к конкретному приложению. Однозначно определяется типом ресурсов, входящих в группу |
| Задача | Задача — это набор групп ресурсов одного и того же или разных типов. Например, задача может одновременно включать группу системных файлов и группу объектов системного реестра Windows |
| Задание | Определяет параметры проведения контроля целостности. Например, методы контроля, алгоритмы расчета контрольных сумм, расписание проведения контроля, реакции системы на обнаруженные ошибки. Включает в себя набор задач и групп ресурсов, подлежащих контролю. Например, при использовании замкнутой программной среды может объединять описания исполняемых файлов, разрешенных для запуска определенной группе пользователей |
| Субъект управления | Субъектом управления может быть компьютер и группа, включающая пользователей и компьютеры (при локальном управлении — также и отдельные пользователи). Определяет компьютеры, на которых выполняется контроль целостности в соответствии с назначенными заданиями, и пользователей, которым разрешено запускать программы, заданные заданиями замкнутой программной среды |

Структура

Объекты одной категории являются подчиненными или вышестоящими по отношению к объектам другой категории. Так, ресурсы являются подчиненными по отношению к группам ресурсов, а группы — задачам. Включение ресурсов в группы, групп в задачи, а задач — в задания называется установлением связей между объектами. В конечном итоге задания назначаются субъектам. Модель, включающая в себя объекты всех категорий, между которыми установлены все нужные связи, — это подробная инструкция системе Secret Net 6, определяющая, что и как должно контролироваться.

Пояснение. Модель также может содержать объекты, не связанные с другими, или неполные цепочки объектов, но работать будут только те фрагменты, которые объединяют все уровни модели.

Модель данных состоит из двух частей. Одна часть относится к замкнутой программной среде, другая — к контролю целостности. Набор заданий для каждой из этих частей модели свой. Задачи, группы ресурсов и ресурсы могут входить как в одну, так и в другую часть модели.

Хранение

Локальная база данных (ЛБД) КЦ-ЗПС организована в виде набора файлов, хранящихся в подкаталоге каталога установки Secret Net 6. В ЛБД КЦ-ЗПС на каждом компьютере хранится модель данных, относящаяся к этому компьютеру.

В сетевом режиме функционирования системы Secret Net 6 в качестве централизованного хранилища используется Active Directory (AD). В AD формируется центральная база данных (ЦБД) КЦ-ЗПС. Для организации централизованного управления создаются две модели данных — для компьютеров под управлением 32-разрядных версий ОС Windows и для компьютеров с 64-разрядными версиями операционных систем. Каждая из централизованных моделей данных является общей для всех защищаемых компьютеров под управлением версий ОС Windows соответствующей разрядности.

Способы и средства настройки

Для настройки механизмов КЦ и ЗПС используется программа **"Контроль программ и данных"** (далее — **программа управления КЦ-ЗПС**), входящая в состав клиентского ПО системы Secret Net 6.

Программа управления КЦ-ЗПС располагает как автоматическими, так и ручными средствами формирования элементов модели данных. Ручные методы можно использовать на любом уровне модели для формирования и модификации объектов и связей. Автоматические методы предпочтительнее при работе с большим количеством объектов, однако они требуют более тщательного контроля результатов. Для создания небольших фрагментов модели могут быть использованы ручные методы, что делает процесс более контролируемым и позволяет избежать случайных ошибок. В общем случае наиболее типичный путь состоит в комбинации этих двух методов.

Управление работой механизмов

В Secret Net 6 предусмотрена возможность включения или отключения локальных заданий КЦ и ЗПС, а также включения или отключения механизма ЗПС. Эти средства можно использовать для управления режимами работы механизмов или изменения действующей модели данных.

Принципы настройки в сетевом режиме функционирования

В сетевом режиме функционирования системы Secret Net 6 программа управления КЦ-ЗПС может работать в централизованном и локальном режимах.

Формирование модели данных для ЗПС

Модель данных для механизма ЗПС можно сформировать на основе сведений из журнала безопасности Secret Net. Администратор безопасности (или аудитор) с помощью программы просмотра журналов создает файл в dvt-формате, содержащий выборку записей журнала за интересующий период. Затем этот файл с помощью программы управления КЦ-ЗПС импортируется в базу данных КЦ-ЗПС. Далее на основании этих данных формируются задания ЗПС для отдельных компьютеров или групп компьютеров.

Формирование модели данных для КЦ

В централизованном режиме программы управления КЦ-ЗПС модели данных для механизма КЦ могут быть созданы с использованием тиражируемых и нетиражируемых заданий. Эти два вида заданий отличаются способом формирования задач и местом расчета и хранения эталонов.

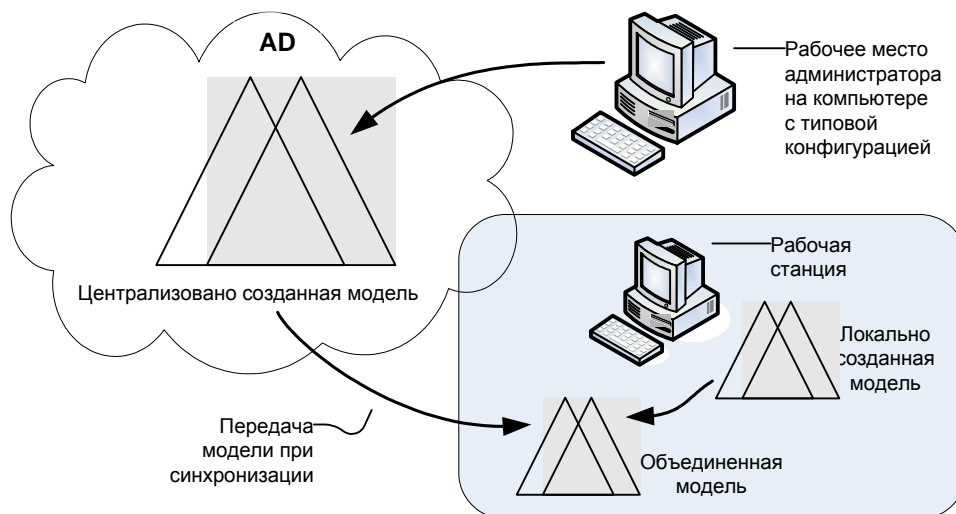
| Задания | Особенности |
|-----------------------|--|
| Тиражируемые | Эталонные значения для таких заданий рассчитываются централизованно и хранятся в ЦБД КЦ-ЗПС. При синхронизации вместе с задачами эталонные значения тиражируются на указанные рабочие станции и сохраняются в ЛБД КЦ-ЗПС. Таким образом, эталоны ресурсов тиражируемого задания одинаковы на всех компьютерах, с которыми связано данное задание |
| Нетиражируемые | Для нетиражируемых заданий эталонные значения не тиражируются, а вычисляются на рабочих станциях и хранятся только в ЛБД КЦ-ЗПС |

Синхронизация данных

При синхронизации происходит передача изменений, внесенных в ЦБД КЦ-ЗПС, на все те компьютеры, к которым эти изменения относятся, и сохранение изменений в ЛБД КЦ-ЗПС. Синхронизация выполняется системой в следующие моменты:

- при загрузке компьютера;
- при входе пользователя в систему;
- периодически через определенные интервалы времени;
- принудительно по команде администратора;
- непосредственно после внесения изменений в ЦБД КЦ-ЗПС (для этого на компьютере должна быть включена и настроена возможность рассылки оповещений). Если изменения модели относятся к этому компьютеру, будет выполнена синхронизация.

В результате синхронизации в ЛБД КЦ-ЗПС формируется объединенная актуальная модель данных, включающая локально и централизованно созданные задания, а также связанные с ними задачи, группы ресурсов и ресурсы.



Защита от дублирования ресурсов при синхронизации. Если в ЛБД поступает из ЦБД описание ресурса, которое уже имеется в локальной модели данных, то в ЛБД остается только одно описание ресурса, но все связи ресурса сохраняются (суммируются). Если же этот ресурс снимается с контроля в ЦБД, то связи этого ресурса, имевшиеся в ЛБД ранее, восстанавливаются.

Настройка механизма

В этом разделе рассматривается порядок настройки механизмов КЦ и ЗПС. В качестве основного метода настройки предлагается подход с максимальным использованием автоматических средств — мастера моделей данных и генератора задач.

| | |
|------------------------------|---|
| Этап 1 см. стр. 49 | Подготовка к построению модели данных Проводится анализ размещения ПО и данных на защищаемых компьютерах. Разрабатываются требования к настройке механизмов КЦ и ЗПС. Осуществляется подготовка рабочего места для проведения настройки |
| Этап 2 см. стр. 49 | Построение фрагмента модели данных по умолчанию Этот этап выполняется при формировании новой модели с нуля. В модель данных автоматически добавляются описания ресурсов для важных ресурсов ОС Windows, а также описания ресурсов некоторых прикладных программ |
| Этап 3 см. стр. 50 | Добавление задач в модель данных В модель данных добавляются описания задач (прикладное и системное ПО, наборы файлов данных и т. д.), контроль целостности и использование в ЗПС которых предусмотрены требованиями, разработанными на 1 этапе |
| Этап 4 см. стр. 52 | Добавление заданий и включение в них задач В модель данных добавляются все необходимые задания КЦ, ЗПС и ПАК "Соболь" и в них включаются задачи |
| Этап 5 см. стр. 55 | Подготовка ЗПС к использованию Субъектам назначаются задания ЗПС. Для того чтобы ресурсы контролировались механизмом ЗПС, они должны быть специально подготовлены — иметь признак "выполняемый". Для этого выполняется Подготовка ресурсов для ЗПС |
| Этап 6 см. стр. 57 | Расчет эталонов Для всех заданий рассчитываются эталоны ресурсов |
| Этап 7 см. стр. 58 | Включение ЗПС в "жестком" режиме Включается "жесткий" режим ЗПС. В "жестком" режиме разрешается запуск только разрешенных программ, библиотек и сценариев. Запуск других ресурсов блокируется, а в журнале Secret Net регистрируются события НСД |
| Этап 8 см. стр. 59 | Включение механизма КЦ Устанавливаются связи заданий контроля целостности с субъектами "компьютер" или "группа" (компьютеров). С этого момента механизм КЦ начинает действовать в штатном режиме |
| Этап 9 см. стр. 59 | Проверка заданий Перед началом эксплуатации механизма КЦ можно выполнить проверку корректности настроек заданий. Проверка заключается в немедленном выполнении задания независимо от расписания |

Задачи, возникающие в процессе эксплуатации

В процессе эксплуатации также могут возникнуть причины для корректировки или пересмотра модели данных. Необходимость изменения модели может быть вызвана:

- изменениями в программном обеспечении защищаемого компьютера (удаление, обновление, установка нового ПО);
- изменениями в политике безопасности, затрагивающими требования к настройке механизмов КЦ и ЗПС;
- сбоями в работе механизма.

Если предполагается кардинальная переработка модели, то лучше выполнить ее с нуля. Если переработке будет подвергнута небольшая часть модели, то в этом случае можно применить отдельные процедуры модификации модели (см. стр. 63).

Этап 1. Подготовка к построению модели данных

Проводится анализ размещения ПО и данных на защищаемых компьютерах. Разрабатываются требования к настройке КЦ и ЗПС, включающие в себя:

- сведения о защищаемых компьютерах (установленное ПО, пользователи и их функциональные обязанности, задачи, решаемые пользователями в рамках бизнес-процессов);
- перечень ресурсов, подлежащих контролю целостности;
- перечень программ, с которыми разрешено работать разным группам пользователей;
- задачи (список задач и их краткое описание).

В сетевом режиме функционирования системы Secret Net 6 из числа защищаемых компьютеров выделяются группы компьютеров с полным совпадением, частичным совпадением и с уникальной конфигурацией ПО и данных. Осуществляется подготовка рабочего места администратора для проведения настройки. На рабочем месте необходимо установить все программное обеспечение, описание ресурсов которого предполагается выполнять автоматическими средствами добавления задач в модель данных.

Примечание. Редактирование централизованных моделей данных осуществляется со следующими особенностями: для редактирования доступна та модель данных, которая соответствует разрядности ОС Windows на рабочем месте администратора. Модель данных другой разрядности доступна только для чтения (при этом можно экспортировать данные из этой модели в другую). Таким образом, если в системе имеются защищаемые компьютеры с версиями ОС различной разрядности, для централизованного управления моделями данных администратору следует организовать два рабочих места — на компьютере с 32-разрядной версией ОС Windows и на компьютере с 64-разрядной версией ОС.

Этап 2. Построение фрагмента модели данных по умолчанию

Данный этап выполняется только при формировании новой модели данных.

При первой настройке централизованными средствами выполнение этой команды не является необходимым, так как фрагмент модели, содержащий описания задач Windows и некоторых прикладных программ, создается автоматически при первом запуске программы управления КЦ-ЗПС в домене (или при пустой ЦБД).

Для построения фрагментов модели по умолчанию:

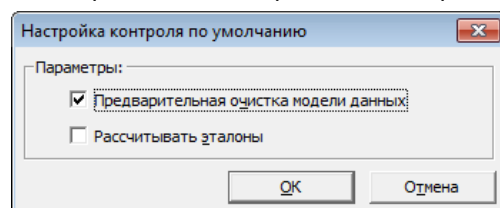
1. Нажмите кнопку "Пуск" ("Start") и выберите в главном меню Windows команду:
 - "Все Программы | Код безопасности | Secret Net | Контроль программ и данных (централизованный режим)" — для управления ЦБД КЦ;
 - "Все Программы | Код безопасности | Secret Net | Контроль программ и данных" — для управления ЛБД КЦ.

Описание основного окна и основных элементов интерфейса приведено на стр. 90.

В окне структуры отображены элементы модели данных, автоматически созданные при первом запуске программы управления КЦ-ЗПС в домене.

2. Активируйте команду "Файл | Новая модель данных".

В централизованном режиме на экране появится диалог:

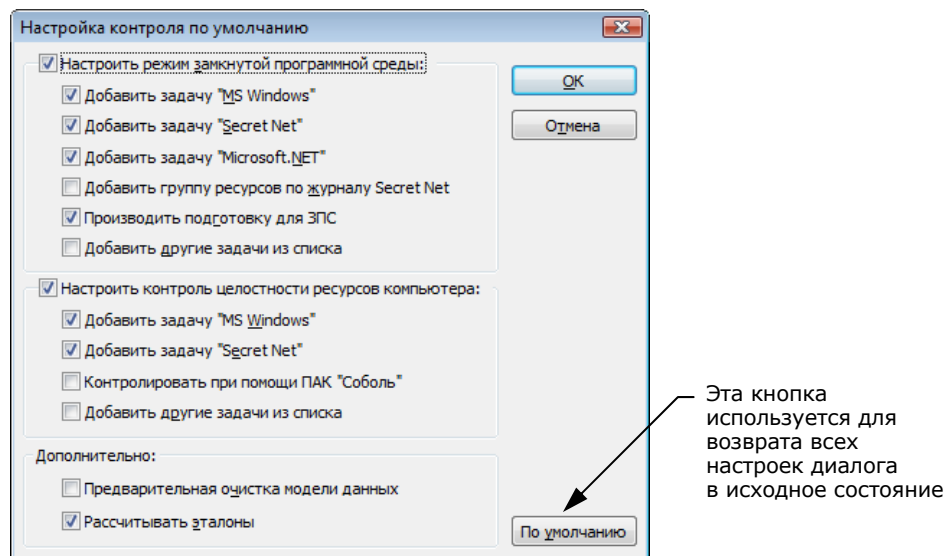


Согласитесь с предлагаемыми настройками и нажмите кнопку "OK".

Предыдущая модель данных соответствующей разрядности ОС будет удалена. Затем начнется автоматическое формирование модели данных, и после успешного завершения в основном окне программы управления КЦ-ЗПС появятся новые элементы модели данных. Новая модель будет содержать зада-

ние КЦ важных ресурсов системного реестра, связанное по умолчанию с доменной группой SecretNetICheckDefault (для 32-разрядных ОС) или группой SecretNetIcheckDefault64 (для 64-разрядных ОС). В группу автоматически включаются защищаемые компьютеры домена с версией ОС соответствующей разрядности. Кроме этого, ряд заданий и задач будут добавлены в модель, но не связаны с субъектами управления.

В локальном режиме на экране появится диалог:



Диалог предназначен для задания настроек, в соответствии с которыми автоматически будет создана модель данных. Отметки, установленные в диалоге по умолчанию, предлагают сформировать модель для ресурсов Windows и Secret Net.



Для настройки механизма ЗПС обязательно нужно выполнить операцию подготовки ресурсов, при которой ресурсы помечаются признаком "выполняемый" и для исполняемых файлов осуществляется поиск других связанных с ними модулей. Это основное назначение данной операции, без нее настройка ЗПС будет неполноценной.

В диалоге имеется возможность добавления в модель и других задач, относящихся к ресурсам других прикладных программ. Используйте для этого выключатели "Добавить другие задачи из списка".

Нажмите кнопку "ОК".

Начнется формирование модели данных, и после его успешного завершения в основном окне программы управления КЦ-ЗПС появится новая структура, включающая в себя субъект "Компьютер" с назначенными для него заданиями.

3. Активируйте в меню команду "Файл | Сохранить".

Этап 3. Добавление задач в модель данных

Целью данного этапа настройки является дополнение модели данных фрагментом, включающим список других необходимых задач (помимо ресурсов Windows и Secret Net 6). Для этого могут быть использованы как ручные методы, так и специальное средство — механизм генерации задач. Задачи создаются на основании сведений об установленных на компьютере программных продуктах. Для этого используются сведения MS Installer и ярлыки меню "Пуск" ОС Windows. Рекомендуется использовать механизм генерации при наполнении модели данных сложными задачами, включающими в себя большое количество ресурсов.

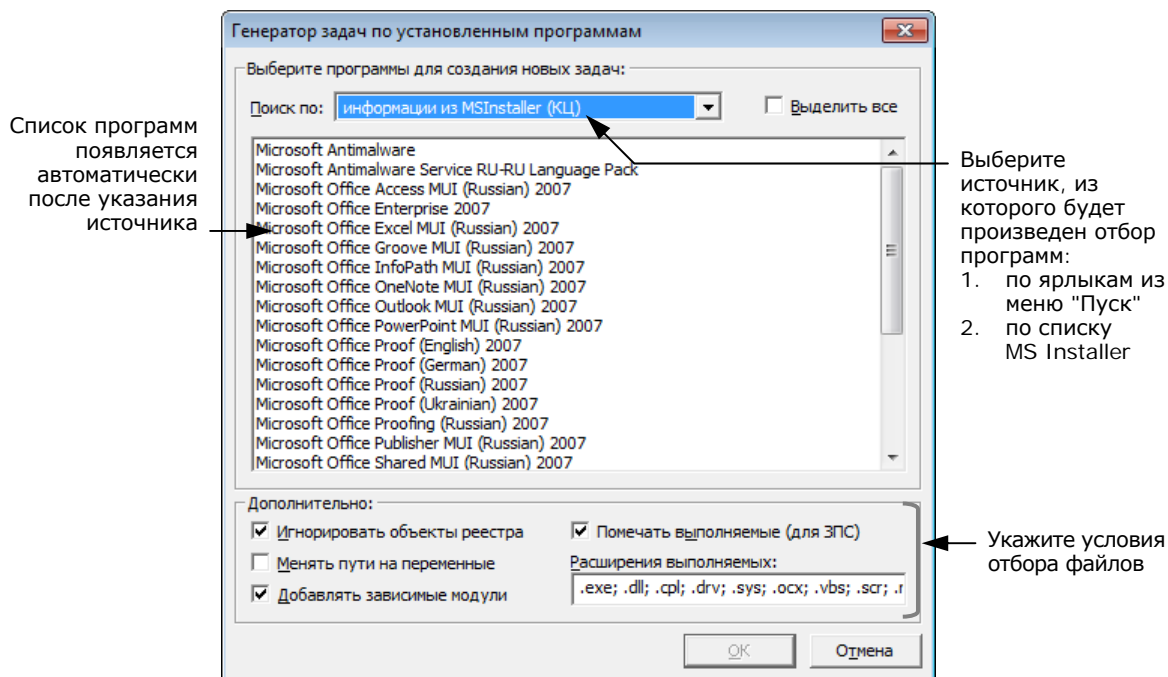
Перед началом генерации администратор безопасности может просмотреть список установленного ПО и наметить те компоненты (программы), для которых должны быть сгенерированы задачи. При этом в задачи будут автоматически включены ресурсы, связанные с исполняемыми модулями выбранного ПО. Можно также задать дополнительное условие фильтрации отбираемых ресурсов.

Кроме того, для ЗПС задачи можно добавить, используя способ формирования заданий ЗПС по журналу Secret Net (см. стр. 75).

Для добавления в модель задач с помощью механизма генерации:

1. Выберите в меню "Сервис" команду "Генератор задач".

На экране появится диалог:



Диалог предназначен для выбора программ, а также задания дополнительных условий отбора ресурсов.

2. Укажите в поле "Поиск по" — из какого списка должны выбираться программы.
3. Выберите в списке программы и укажите в нижней части диалога дополнительные условия отбора ресурсов.

Для выделения нескольких программ используйте клавишу <Ctrl>. Для выделения всего списка поставьте отметку в поле "Выделить все".


| Условие | Пояснение |
|-------------------------------------|--|
| Игнорировать объекты реестра | Ресурсы, являющиеся объектами реестра, в задачи не включаются |
| Менять пути на переменные | При записи в модель данных абсолютные пути к файлам и каталогам меняются на имена переменных окружения |
| Добавлять зависимые модули | Зависимые модули — это файлы, от которых зависит исполнение исходных файлов. Например, это могут быть драйверы и библиотеки, не входящие непосредственно в запускаемые пользователем приложения, но без которых работа этих приложений невозможна. Зависимые модули добавляются в ту же группу ресурсов, где находится исходный файл. Включение зависимых модулей в список осуществляется рекурсивно — файлы, от которых зависит исполнение самих зависимых модулей, также включаются в список |
| Помечать выполняемые | Выполняемые файлы при отображении в окне программы управления КЦ-ЗПС помечаются специальным значком. К выполняемым относятся файлы, имеющие расширения, указанные в строке "Расширения выполняемых". Перечень расширений можно изменить, вручную добавив или удалив из строки элементы |

При выборе из списка MS Installer можно задать каждое из приведенных выше дополнительных условий. При выборе по ярлыкам из меню "Пуск" можно задать только два условия: "менять пути на переменные" и "помечать выполняемые".

4. Нажмите кнопку "OK".

Начнется процесс генерации. Затем появится сообщение об успешном его завершении.

5. Нажмите кнопку "ОК" в окне сообщения.

В модель добавятся новые задачи, включающие в себя группы ресурсов, но не связанные с вышестоящими объектами (заданиями), на что указывает значок  (верхняя половина кружка окрашена красным цветом).

Этап 4. Добавление заданий и включение в них задач

Цель данного этапа — сформировать задания на основе задач, созданных на предыдущем этапе. Для заданий контроля целостности должна быть выполнена настройка, в которой указываются:

- методы и алгоритмы контроля защищаемых ресурсов;
- реакция системы в случаях нарушения целостности контролируемых ресурсов;
- перечень событий, регистрируемых в журнале;
- расписание, в соответствии с которым должна проводиться проверка.

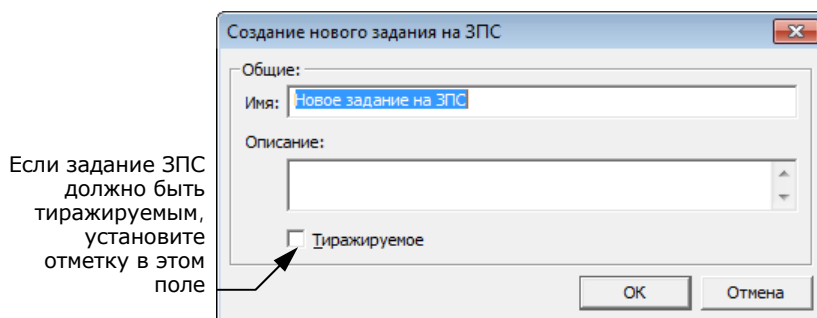
Для формирования задания:

1. Выберите категорию "Задания" и активируйте в меню "Задания | Создать задание".

На экране появится диалог выбора типа задания.

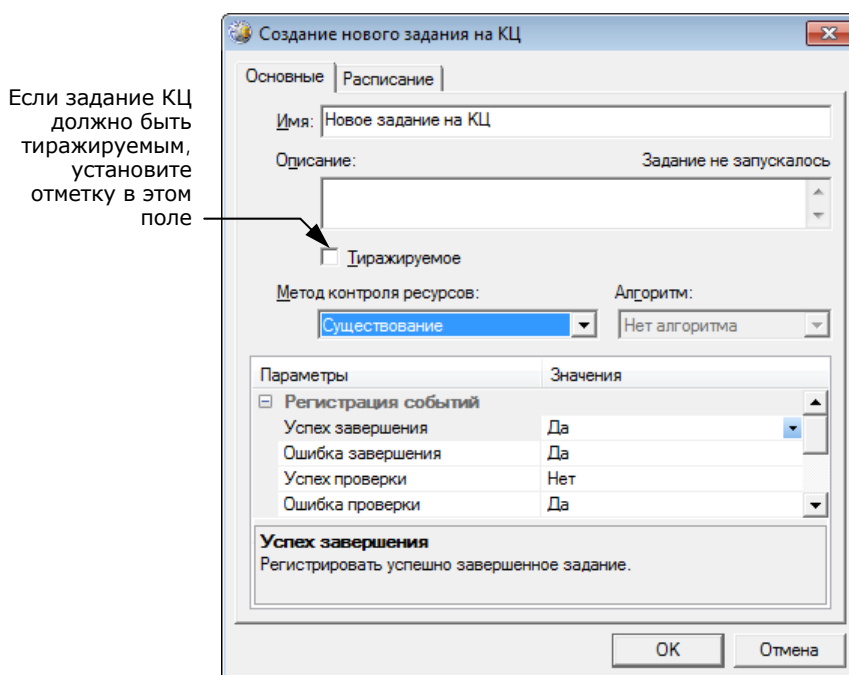
2. Выберите тип задания (КЦ, ЗПС, ПАК "Соболь") и нажмите кнопку "ОК".

Если выбрано задание ЗПС или ПАК "Соболь", на экране появится диалог:



Введите имя задания, его краткое описание и нажмите кнопку "ОК". Порядок настройки задания для ПАК "Соболь" описан на стр. 80.

Если выбрано задание КЦ, на экране появится диалог:



3. Введите имя и краткое описание задания КЦ.
4. Укажите метод контроля ресурсов, выбрав его из списка.

Предусмотрено 4 метода:

| Метод контроля | Что проверяется |
|----------------------|---|
| Содержимое | Целостность содержимого ресурсов |
| Атрибуты | Стандартные атрибуты, установленные для ресурсов |
| Права доступа | Категории конфиденциальности и атрибуты доступа Windows (дескриптор безопасности), установленные для ресурсов |
| Существование | Наличие ресурсов по заданному пути |



При выборе типа контролируемых данных необходимо иметь в виду, что проверка будет выполняться только для определенных типов ресурсов. Сведения о применимости методов контроля для каждого из типов ресурсов в зависимости от выбранного типа контролируемых данных приведены ниже. При выборе метода контроля может оказаться, что с заданием связаны ресурсы, несовместимые с используемым в задании алгоритмом. Это довольно типичная ситуация, когда на контроль ставится комплексная задача, состоящая из большого количества разнородных ресурсов. Такой ситуации не следует опасаться — несовместимые ресурсы подсистемой контроля игнорируются. При расчете эталонов желательно на несовместимые ресурсы использовать реакции: "игнорировать" или "выводить запрос". Таким образом, можно связывать с задачей сразу несколько разных заданий на контроль, не беспокоясь, что наличие несовместимых с заданиями ресурсов вызовет сбой или НСД.

Табл. 1. Соответствие типов ресурсов и методов контроля

| | Содержимое объекта | Атрибуты объекта | Права доступа | Существование объекта |
|-------------------------|--------------------|------------------|---------------|-----------------------|
| Файл | да | да | да | да |
| Каталог | нет | да | да | да |
| Ключ реестра | да | нет | да | да |
| Значение реестра | да | нет | нет | да |

5. Если указан метод контроля "Содержимое", укажите алгоритм, выбрав его из списка.

Предусмотрено 5 алгоритмов: "CRC7", "ЭЦП", "ХЭШ", "имитовставка", "полное совпадение".

Алгоритм "полное совпадение", в отличие от других, предусматривает возможность восстановления контролируемого объекта в случае нарушения его целостности. Однако при использовании данного алгоритма существенно увеличивается объем базы данных — поскольку эталонным значением для контроля является копия объекта.

6. Настройте регистрацию событий. Для этого в столбце "Параметры" выберите нужное событие. В соответствующей строке столбца "Значения" появится значок раскрывающегося списка. Выберите в списке значение "Да", чтобы данное событие регистрировалось, или "Нет", чтобы оно не регистрировалось.

Предусмотрена регистрация 4 событий:

| Событие | Описание события |
|--------------------------|--|
| Успех завершения | Обработка задания контроля завершена успешно |
| Ошибка завершения | Обнаружено нарушение целостности при обработке задания |
| Успех проверки | Проверка целостности ресурса завершена успешно |
| Ошибка проверки | Нарушение целостности ресурса |

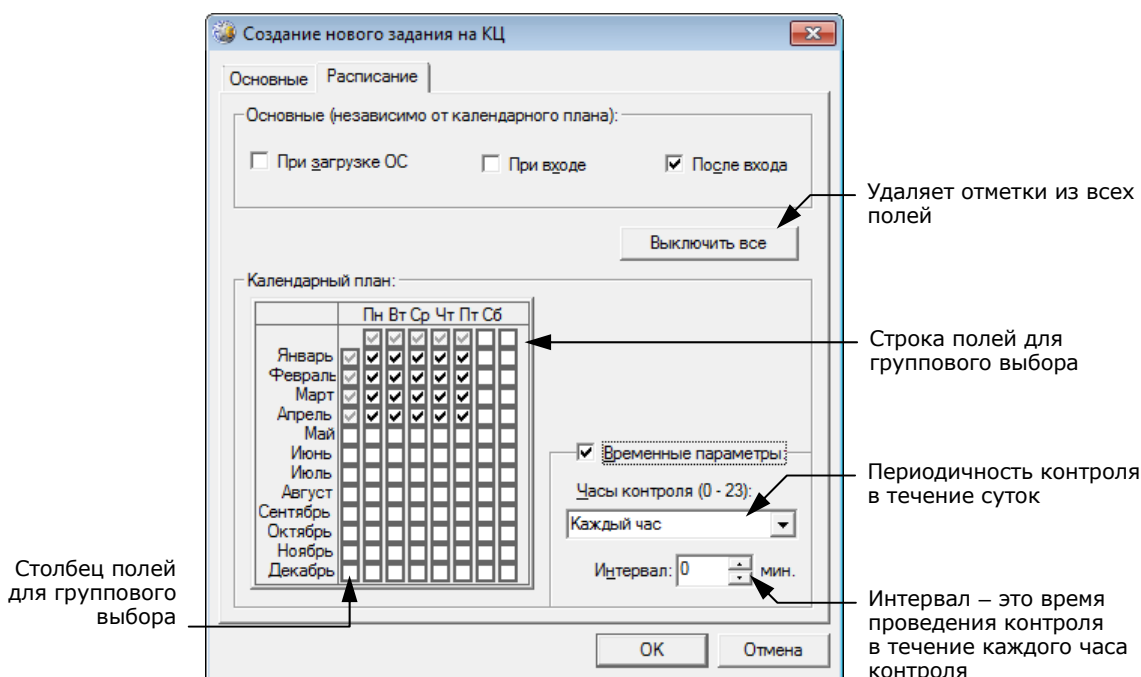
7. Настройте реакцию системы. Для этого выделите в столбце "Параметры" строку "Действие", а в столбце "Значения" выберите нужный вариант. Предусмотрены следующие варианты:

| Реакция | Пояснение |
|--------------------------------|---|
| Игнорировать | Реакция системы отсутствует |
| Заблокировать компьютер | Компьютер блокируется. Снять блокировку может только администратор безопасности |

| | |
|-----------------------------------|--|
| Восстановить из эталона | Текущее значение контролируемого параметра ресурса восстанавливается из эталона. Реакция доступна не для всех методов |
| Восстановить с блокировкой | Текущее значение контролируемого параметра ресурса восстанавливается из эталона. Компьютер блокируется. Снять блокировку может только администратор безопасности |
| Принять как эталон | Текущее значение контролируемого параметра ресурса принимается за эталон. Эта реакция недоступна для тиражируемых заданий |

Для файлов и значений реестра возможность восстановления имеет следующие особенности:

- восстановление не предусмотрено, если в качестве метода контроля для них применяется метод "Существование";
 - восстановление возможно, если в качестве метода контроля используется метод "Содержимое" и в нем применяется алгоритм "Полное совпадение";
 - могут быть восстановлены атрибуты файлов и каталогов (кроме меток конфиденциальности системы Secret Net).
8. Перейдите к диалогу "Расписание" и составьте расписание контроля в соответствии с требованиями к заданию.





Диалог разделен на две части. В верхней части настраивается время проведения проверки независимо от календаря (при загрузке операционной системы, при входе пользователя в систему и после входа в систему). В нижней части расположены календарь и средства настройки расписания в течение суток.

| Поле | Использование |
|--|--|
| Основные (независимо от календарного плана) | С помощью полей этой группы можно указать, на каком этапе своей работы система защиты должна контролировать целостность ресурсов. Проверка может проводиться при загрузке операционной системы, при входе пользователя в систему и после входа в систему. В режиме "При входе" проверка начинается после ввода пользователем идентификационных признаков, и до завершения проверки процесс входа в систему приостанавливается. Если установлен режим "После входа" — проверка начнется после входа пользователя в систему и продолжится в фоновом режиме |
| Календарный план | Группа полей для включения контроля по месяцам, дням недели, часам и минутам |
| Календарь | С помощью календаря можно указать расписание контроля по месяцам и дням недели |

| | |
|----------------------------|---|
| Временные параметры | С помощью полей этой группы можно указать периодичность контроля в течение суток |
| Часы контроля | Введите или выберите из раскрывающегося списка значение периодичности контроля в течение суток. Можно выбрать период, а можно и непосредственно ввести конкретные значения. Следует иметь в виду, что отсчет начинается с нулевого часа. Поэтому если вы установите значение 4, что означает – "проводить контроль каждый четвертый час", контроль будет проводиться в 0, 3, 7, 11, и т. д. Часы контроля можно задать, не только указав периодичность, но и непосредственно введя конкретные значения. Например, если вы введете следующую строку: 2, 7–9, 16–18, 21, то контроль будет проведен в 2, 7, 8, 9, 16, 17, 18 и 21 час |
| Интервал | Укажите периодичность контроля в течение часа контроля. Если значение не указано, контроль выполняется в начале часа один раз. Так, например, если контроль должен проводиться в 7 часов, а в поле "Интервал" указано значение 10, то процесс контроля первый раз начнется в 7 часов 00 минут, а затем будет повторяться каждые 10 минут в течение этого часа |

9. Нажмите кнопку "ОК".

В дополнительном окне структуры появится новое задание контроля целостности , не связанное с субъектами. Тиражируемое задание обозначается пиктограммой .



Задания, созданные средствами централизованного управления, отображаются в программе, работающей в локальном режиме, жирным шрифтом. Такие задания нельзя удалить из модели данных. В них нельзя включать задачи.

Включение задач в задание

Для включения задач в задание:

1. Выберите категорию "Задание" на панели категорий.
2. В окне структуры вызовите контекстное меню для задания и активируйте команду "Добавить задачи/группы | Существующие".
Появится диалог со списком всех задач и групп ресурсов, еще не включенных в данное задание.
3. Выберите задачи, включаемые в задание, и нажмите кнопку "ОК".

Совет. Для выбора нескольких задач используйте клавишу <Ctrl> или поле "Выделить все".

Этап 5. Подготовка ЗПС к использованию

План действий на этом этапе

| | |
|----|--|
| 1. | Отключить контроль ЗПС у привилегированных пользователей (например, администратора) — это снимет ограничения в работе этих пользователей |
| 2. | Установка связей субъектов с заданиями ЗПС |
| 3. | Подготовка ресурсов для ЗПС |

Предоставление привилегии при работе в ЗПС

Для предоставления привилегии:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
2. Выберите папку "Привилегии".

В правой части окна появится список привилегий.

В Secret Net 6 используется одна привилегия, связанная с работой ЗПС:

| Привилегия | Пояснение |
|--------------|---|
| Не действует | На пользователя, имеющего данную привилегию, действие механизма замкнутой программной среды не распространяется. По умолчанию привилегия предоставлена группе "Администраторы" |

3. Вызовите контекстное меню для строки "Замкнутая программная среда: не действует" и активируйте в нем команду "Свойства".

Появится диалог для настройки параметра.

В списке диалога представлены пользователи и группы, которым предоставлена данная привилегия.

4. Для добавления в список нового пользователя или группы нажмите кнопку "Добавить пользователя или группу".

Для удаления пользователя или группы выделите имя в списке и нажмите кнопку "Удалить".

Появится стандартный диалог выбора пользователей.

5. Выберите пользователя или группу, нажмите кнопку "Добавить" и затем — кнопку "ОК".

Выбранные пользователи будут добавлены в список.

6. Нажмите кнопку "ОК".


В строке с названием привилегии появятся добавленные пользователи.

Установка связей субъектов с заданиями ЗПС

На данном этапе необходимо назначить субъектам сформированные задания замкнутой программной среды. Задания назначаются субъектам "компьютер" и "группа" (в локальном режиме — "компьютер", "пользователь" и "группа пользователей"). Для того чтобы назначить задания нужным субъектам, их необходимо добавить в модель данных. В модели должны присутствовать субъекты, соответствующие компьютерам с уникальным составом ПО, и группы, включающие компьютеры со сходным составом ПО.

Для добавления субъекта в модель данных:

1. Выберите категорию "Субъекты управления" на панели категорий.
2. В меню "Субъекты управления" выберите команду "Добавить в список".
Появится стандартный диалог выбора пользователей и групп.
3. Выполните стандартные действия для поиска и выбора нужных объектов.
4. Нажмите кнопку "ОК".

В окне программы управления КЦ-ЗПС появятся новые субъекты, отмеченные знаком  (т. е. не связанные с другими объектами).

Для установления связи субъекта с заданием:

1. Выберите категорию "Субъекты управления" на панели категорий.
2. Найдите в дополнительном окне структуры или в области списка субъекта, с которым требуется связать задание, вызовите контекстное меню и активируйте команду "Добавить задания | Существующие".

На экране появится диалог, содержащий список имеющихся заданий. Для каждого задания в списке указано количество субъектов, с которыми оно связано.

3. Выберите задания ЗПС, которые требуется назначить субъекту.

Совет. Для выделения нескольких заданий используйте клавишу <Ctrl> или поставьте отметку в поле "Выделить все".

4. Нажмите кнопку "ОК".

Выбранные задания будут назначены субъекту.

Подготовка ресурсов для ЗПС

Чтобы ресурсы контролировались механизмом замкнутой программной среды, они должны иметь признак "выполняемый" и входить в задание ЗПС. Также необходимо выполнить поиск зависимых модулей. В этом случае для каждого ресурса, которому будет установлен признак "выполняемый", будет выполняться поиск в ресурсах компьютера зависимых модулей. Найденные зависимые модули будут добавлены в модель данных в те же группы ресурсов, в которые входят исходные модули. Им также будет присвоен признак "выполняемый".

Выполнение этих операций называется подготовкой ресурсов для ЗПС. Процедура подготовки подробно описана на стр. 77.

Этап 6. Расчет эталонов

Расчет может быть выполнен сразу для всех или для отдельных имеющихся в модели заданий КЦ, а также для заданий ЗПС (если предусмотрен контроль целостности разрешенных для запуска программ).

Перед проведением расчета эталонов необходимо настроить реакцию системы на возможные ошибки, которые могут возникнуть в процессе расчета.

При перерасчете эталонов может возникнуть необходимость сохранения прежних ("старых") значений. Это связано с ситуацией, которая может возникнуть при автоматическом обновлении программного обеспечения на компьютере.

Рассмотрим подробно, как могут развиваться события во времени:

1. До появления в сети нового ПО текущий эталон соответствует прежнему ПО.
2. На сервере обновлений появляется новое ПО, выполняется расчет новых эталонов. Новое ПО готово к установке, но пользователь откладывает установку на более поздний срок.
3. Проверка эталонных значений может быть намечена на любой момент. И если проверка будет выполнена до установки нового ПО, обнаружится несоответствие прежнего ПО новым эталонным значениям. Для этого случая и сохраняются старые эталоны.
4. После обновления ПО на компьютере будут использоваться новые эталоны.

При централизованном управлении расчет эталонов выполняется для тиражируемых заданий КЦ и ЗПС (если используется контроль целостности запускаемых программ). Эталоны для ресурсов нетиражируемых заданий рассчитываются автоматически после передачи их в ЛБД после синхронизации. Также предусмотрена возможность выполнения отложенного расчета эталонов.

Для расчета эталонов тиражируемых заданий:

1. Активируйте в меню "Сервис" команду "Эталон | Расчет".
На экране появится диалог "Расчет эталонов".
2. Если требуется сохранить старые значения эталонов, установите отметку в поле "Режим".
3. Настройте реакцию системы защиты на возможные ошибки при расчете эталонов. Для этого в левой части таблицы выберите вид ошибки, а в правой выберите для него одно из 4 значений реакции системы.

Ошибки могут быть 3 видов:

- метод/алгоритм расчета для данного ресурса не поддерживается;
- к ресурсу нет доступа на чтение или он заблокирован;
- ресурс по указанному пути не найден.

Для каждого вида ошибки можно задать одну из 4 реакций:

| Реакция | Описание |
|----------------------------------|--|
| Игнорировать | Реакция системы на ошибку отсутствует |
| Выводить запрос | При возникновении ошибки система выводит соответствующее сообщение и запрос на выполнение последующих действий |
| Удалять ресурс | При возникновении ошибки ресурс удаляется из модели данных |
| Ресурс снимать с контроля | Ресурс снимается с контроля, но остается в модели данных. При этом нужно учитывать, что ресурс будет снят с контроля не только в том задании, где выявлена ошибка, но и во всех остальных заданиях, с которыми ресурс связан |

4. Нажмите кнопку "ОК".
Начнется расчет эталонов. Ход выполнения расчета отображается в специальном окне полосой прогресса.

Если в процессе расчета обнаруживается ошибка и в качестве реакции на нее установлено значение "Выводить запрос", процедура будет приостановлена и на экране появится запрос на продолжение процедуры.

Предусмотрено 4 варианта продолжения процедуры:

| Вариант | Описание |
|-------------------------|---|
| Игнорировать | Процедура расчета будет продолжена. Реакция системы на ошибку отсутствует. Ресурс, вызвавший ошибку, остается в составе задачи (или задач). Проверка целостности этого ресурса вызовет событие НСД с соответствующей реакцией |
| Снять с контроля | Процедура расчета будет продолжена. Ресурс, вызвавший ошибку, остается в составе задачи (или задач), снимается с контроля и не проверяется во всех заданиях, в которые входит |
| Удалить | Процедура расчета будет продолжена. Ресурс, вызвавший ошибку, автоматически удаляется из модели данных |
| Прервать | Процедура расчета будет прервана. Для расчета эталонов следует устранить причину, вызвавшую ошибку, и заново запустить процедуру расчета |

5. Для выбора варианта продолжения процедуры нажмите соответствующую кнопку в окне сообщения.

В зависимости от выбранного варианта процедура будет продолжена или прервана, в каждом из этих случаев на экране появится сообщение.

6. Примите к сведению содержание сообщения и нажмите кнопку "ОК".

Для расчета эталонов нетиражируемых заданий:

1. В основном окне выберите нужное нетиражируемое задание, вызовите контекстное меню и активируйте в нем команду "Расчет эталонов".

Появится диалог "Отложенный расчет эталонов".

2. Выберите в списке компьютеры, на которых требуется выполнить отложенный расчет эталонов для данного задания, и нажмите кнопку "ОК".

При следующей синхронизации ЦБД и ЛБД будет выполнен расчет эталонов ресурсов для выбранного задания на всех указанных компьютерах.

Этап 7. Включение ЗПС в "жестком" режиме

Для включения ЗПС в "жестком" режиме необходимо выключить "мягкий" режим в свойствах нужного субъекта.

Для включения механизма ЗПС в "жестком" режиме:

- Выберите категорию "Субъекты управления" на панели категорий.
- Выберите в дополнительном окне структуры или в области списка объектов компьютер или группу (компьютеров), вызовите контекстное меню и активируйте команду "Свойства". В появившемся окне "Свойства субъекта управления" перейдите к диалогу "Режимы".
- При работе в централизованном режиме установите отметку в поле "Режимы заданы централизованно".
- Установите отметку в поле "Режим ЗПС включен" и удалите отметку из поля "Мягкий режим" (если она там установлена).
- При необходимости установите дополнительные параметры контроля:

| Параметр | Пояснение |
|---|---|
| Проверять целостность модулей перед запуском | При запуске программ, входящих в список разрешенных, проверяется их целостность |
| Проверять заголовки модулей перед запуском | В процессе контроля включается дополнительный механизм, повышающий надежность разделения ресурсов на исполняемые и неисполняемые файлы, т. е. подлежащие и не подлежащие проверке |
| Контролировать исполняемые скрипты | Блокируется выполнение сценариев (скриптов), не входящих в перечень разрешенных для запуска и не зарегистрированных в базе данных системы Secret Net 6 |

6. Нажмите кнопку "ОК".

Для выбранного компьютера (или группы) начнет действовать механизм ЗПС в "жестком" режиме.

Этап 8. Включение механизма КЦ

Механизм контроля целостности будет включен, как только компьютеру будет назначено задание на контроль целостности с заданным расписанием (при управлении в централизованном режиме включение механизма на компьютере произойдет после синхронизации ЛБД данного компьютера с ЦБД).

Для включения механизма контроля целостности:

1. Выберите категорию "Субъекты управления" на панели категорий.
2. Выберите в дополнительном окне структуры или в области списка объектов компьютер или группу (компьютеров), вызовите контекстное меню и активируйте в нем команду "Добавить задания | Существующие".
Появится диалог, содержащий список заданий контроля целостности. Для каждого задания в списке указано количество субъектов управления, с которыми оно связано.
3. Выберите задания, назначаемые субъекту, и нажмите кнопку "ОК".

Для данного компьютера (или группы) начнет действовать механизм КЦ.

Этап 9. Проверка заданий

Перед началом эксплуатации механизма КЦ можно выполнить проверку корректности параметров заданий. Проверка заключается в немедленном выполнении задания независимо от расписания. Такая проверка позволяет предотвратить нарушения в работе пользователей, связанные с некорректной настройкой заданий, и своевременно исправить ошибки, допущенные в настройках.

Проверка выполняется отдельно для каждого задания. При этом для задания должны быть рассчитаны эталоны и оно должно быть связано с субъектом.

Для проверки задания предусмотрено 2 режима: облегченный и полная имитация задания. В облегченном режиме события в журнале не регистрируются и реакция на ошибки не отрабатывается. По завершении проверки выдается список обнаруженных ошибок. В режиме полной имитации события регистрируются и система отрабатывает реакцию на ошибки.

В централизованном режиме работы возможна проверка только тиражируемых заданий, в локальном режиме — любых заданий, включая задания, созданные централизованно.

Для запуска проверки:

1. Выберите в меню "Сервис | Запуск задания".
Появится диалог со списком всех заданий контроля целостности.
2. Выберите в списке задание, при необходимости укажите режим полной имитации и нажмите кнопку "ОК".

Начнется выполнение задания и по окончании будет выведено сообщение об успешном завершении или обнаруженных ошибках.

Хранение и перенос модели данных

Сохранение

Выполнив любые изменения в модели данных, ее текущее состояние можно сохранить в базе данных. Для сохранения модели активируйте в меню "Файл" команду "Сохранить".

Оповещение об изменениях

В сетевом режиме функционирования системы Secret Net 6 сведения об изменениях в модели данных, выполненных в централизованном режиме, распространяются на компьютеры домена в соответствии с настройкой параметра группы "Оповещения" (см. стр. 94).

Если параметр имеет значение "Да", оповещение об изменениях в модели данных рассылается при каждом сохранении модели.

Если параметр имеет значение "Нет", оповещение не рассылается. При таком значении параметра оповещение можно разослать принудительно. Для принудительной рассылки оповещения активируйте в меню "Сервис" команду "Оповестить об изменениях".

Загрузка и восстановление

Загрузка модели из базы данных осуществляется при каждом запуске программы или может быть выполнена по специальной команде в процессе работы.

Если вы вносите в модель изменения, в правильности которых вы не уверены, не сохраняйте их сразу в БД. В этом случае у вас будет возможность вернуться к варианту модели, сохраненной в БД. Для этого используется операция восстановления.

Для восстановления модели из базы данных:

1. В меню "Файл" активируйте команду "Восстановить из базы".
На экране появится предупреждение о потере последних изменений.
2. Нажмите кнопку "Да" в окне предупреждения.
Программа загрузит ранее сохраненную модель из базы данных.

Экспорт

Процедура экспортирования может осуществляться следующими способами:

- экспортирование всей модели данных;
- выборочное экспортирование объектов определенных категорий (не применяется к объектам категории "Субъекты доступа").

Для экспортирования текущей модели данных:

1. В меню "Файл" активируйте команду "Экспорт модели в XML".
На экране появится диалог настройки параметров экспортирования.
2. В поле "Путь к выходному файлу" введите полное имя файла. Для ввода используйте клавиатуру или нажмите кнопку "Выбрать...", чтобы указать файл в стандартном диалоге сохранения файла ОС Windows.
3. Если модель содержит ресурсы с рассчитанными эталонными значениями и требуется сохранить эти значения в файле, установите отметку в поле "Сохранять рассчитанные эталоны".

При включенном режиме экспортирования ресурсов вместе с эталонными значениями программе потребуется сохранить текущую модель в базе данных. Соответствующее сообщение появляется на экране после установки отметки в поле "Сохранять рассчитанные эталоны".

4. Нажмите кнопку "ОК" в диалоге настройки параметров экспортирования.

Для выборочного экспортирования объектов:

1. Выберите на панели категорий категорию, к которой относятся нужные объекты.
2. В окне структуры или в области списка объектов найдите экспортируемые объекты (кроме объектов категории "Субъекты доступа").

Предусмотрены следующие варианты выбора объектов:

- все объекты, относящиеся к текущей категории, — для этого в окне структуры выберите корневой элемент с названием категории;
 - группа объектов, выбранных произвольным образом, — для этого в области списка объектов выделите нужные объекты, удерживая нажатой клавишу <Ctrl> или <Shift>;
 - отдельный объект в окне структуры или в области списка объектов.
3. Вызовите контекстное меню объекта (объектов) и активируйте команду запуска процедуры экспортирования. В зависимости от того, какие объекты были выбраны, эта команда имеет название: "Экспорт всех", "Экспорт входящих в папку" или "Экспорт выбранных".

На экране появится диалог настройки параметров экспортирования.

4. В поле "Путь к выходному файлу" введите полное имя файла. Для ввода используйте клавиатуру или нажмите кнопку "Выбрать", чтобы указать файл в стандартном диалоге сохранения файла операционной системы Windows.
5. По умолчанию совместно с выбранными объектами экспортируются и те объекты, которые входят в цепочки связанных с ними объектов нижележащих уровней иерархии (например, задание — задача — группа ресурсов — ресурсы). Если требуется экспортировать только выбранные объекты, установите отметку в поле "Без подчиненных". (Данное поле отсутствует в диалоге, если экспортирование осуществляется для ресурсов.)
6. Если в числе экспортируемых объектов имеются ресурсы с рассчитанными эталонными значениями и требуется сохранить эти значения в файле, установите отметку в поле "Сохранять рассчитанные эталоны".

При включенном режиме экспортирования ресурсов вместе с эталонными значениями программе потребуется сохранить текущую модель в базе данных. Соответствующее сообщение появляется на экране после установки отметки в поле "Сохранять рассчитанные эталоны".

7. Нажмите кнопку "ОК" в диалоге настройки параметров экспортирования.

Импорт

Процедура импорта из файла может выполняться следующими способами:

- общее импортирование объектов в модель данных — позволяет импортировать все данные, хранящиеся в файле;
- импортирование объектов в текущую категорию (не применяется к категории "Субъекты доступа") — позволяет импортировать из файла объекты, относящиеся к той же категории.

Если централизованными средствами был создан файл, содержащий задачи со сценариями, то при импорте его в программу в локальном режиме будет запущено выполнение сценариев.

Для общего импортирования в модель данных:

1. В меню "Файл" активируйте команду "Импорт модели из XML".
2. Если с момента последнего сохранения модели в базе данных списки объектов были изменены, на экране появится сообщение, предупреждающее о потере изменений после загрузки модели. Нажмите кнопку "Да".

На экране появится диалог настройки параметров импортирования.

3. В поле "Путь к входному файлу" введите полное имя файла, в котором хранятся данные об объектах. Для ввода используйте клавиатуру или нажмите кнопку "Выбрать", чтобы указать файл в стандартном диалоге открытия файла ОС Windows.
4. В группе полей "Тип вносимых изменений" выберите режим импортирования. Для этого установите отметку в одном из следующих полей:

Предварительная очистка модели перед импортом

Перед импортом удаляются объекты текущей модели данных. После импорта модель будет состоять только из объектов, содержащихся в файле.

Добавление импортируемых объектов к существующим

После импорта модель будет содержать как импортированные объекты, так и объекты текущей модели данных.

При импорте возможна ситуация "дублирования" объектов. Это происходит, если отключен параметр "С учетом существующих групп, задач и заданий" или если в модели уже есть объекты этих категорий с такими же названиями.

Если объекты относятся к категориям "Задания", "Задачи" или "Группы ресурсов", то после импорта модель данных будет содержать пары дублирующихся объектов. Добавляемый объект каждой пары будет иметь имя: *имя_объекта<N>*, где "N" — порядковый номер дублируемого объекта. Для объектов категории "Ресурсы" дублирующиеся объекты не создаются.

При импорте ресурсов вместе с эталонными значениями (см. шаг 5 данной процедуры) можно выбрать режим сохранения эталонных значений дублирующихся ресурсов. Чтобы все эталонные значения были сохранены, установите отметку в поле "Оставлять старые эталоны у ресурсов (при импорте эталонов)". Иначе после импортирования будут оставлены только те эталонные значения дублирующихся ресурсов, которые хранятся в файле.

- В группе полей "Импортируемые объекты" выберите категории объектов, которые следует импортировать. Для этого установите отметки в полях с названиями соответствующих категорий (если в выбранном файле нет данных об объектах какой-либо категории, соответствующее ей поле заблокировано).



При выборе категорий следует учитывать возможные связи объектов различных категорий. Импортирование осуществляется только для объектов выбранных категорий, поэтому их связи с объектами других невыбранных категорий будут нарушены. Например, импортированные задания не будут включать в себя задачи и группы ресурсов, если не выбраны категории "Задачи" и "Группы ресурсов".

- Если выбрана категория "Ресурсы" и в файле хранятся сведения об эталонных значениях ресурсов, можно включить режим импортирования ресурсов вместе с эталонными значениями. Для этого установите отметку в поле "Эталоны".

При включенном режиме импортирования ресурсов вместе с эталонными значениями программе потребуется сохранить импортированную модель в базе данных. Соответствующее сообщение появляется на экране после установки отметки в поле "Эталоны".

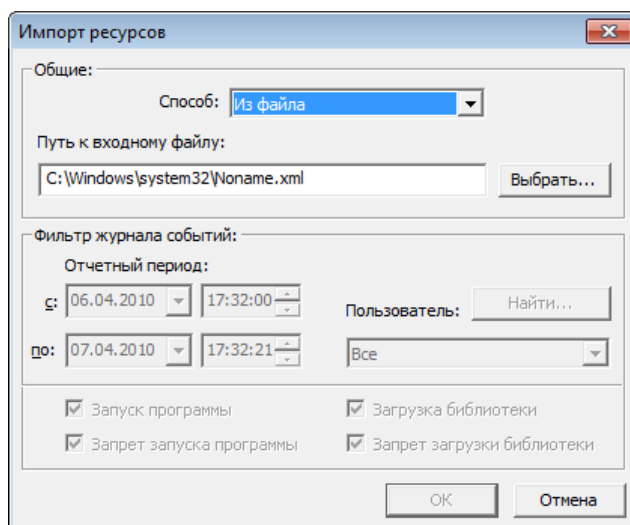
- Нажмите кнопку "ОК" в диалоге настройки параметров импортирования.

Для импортирования объектов текущей категории:

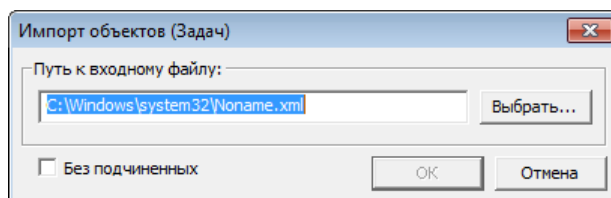
- Выберите на панели категорий категорию, к которой относятся нужные объекты.
- В окне структуры вызовите контекстное меню корневого элемента и активируйте команду "Импорт и добавление".

На экране появится диалог настройки параметров импортирования.

- Если выбрана категория "Ресурсы", диалог имеет вид:



- Если выбрана категория "Задания", "Задачи" или "Группы ресурсов", диалог имеет вид:



- В поле "Путь к входному файлу" введите полное имя файла, в котором хранятся данные об объектах. Для ввода используйте клавиатуру или нажмите кнопку "Выбрать", чтобы указать файл в стандартном диалоге открытия файла ОС Windows.
- По умолчанию совместно с объектами выбранной категории импортируются и связанные с ними цепочки объектов нижележащих уровней иерархии

(например, группа ресурсов – ресурсы). Если требуется импортировать только объекты выбранной категории без включенных в них объектов, установите отметку в поле "Без подчиненных". (Данное поле отсутствует в диалоге настройки параметров импортирования для категории "Ресурсы".)

5. Нажмите кнопку "ОК".

Объекты, хранящиеся в файле, будут добавлены в список объектов текущей категории. При импортировании возможны ситуации "дублирования" объектов, т. е. для импортируемых объектов имеются идентичные в текущей модели данных. Если такие объекты относятся к категориям "Задания", "Задачи" или "Группы ресурсов", после импортирования модель данных будет содержать пары дублирующихся объектов. При этом один из объектов каждой пары переименовывается следующим образом: имя_объекта<N>, где "N" — порядковый номер дублируемого объекта (например, "Группа ресурсов" и "Группа ресурсов1"). Для объектов категории "Ресурсы" дублирующиеся объекты не импортируются.

Примечание. Избирательное импортирование эталонных значений ресурсов не осуществляется. Если требуется импортировать эталонные значения, выполните процедуру общего импортирования модели данных (см. выше).

Модификация модели данных

На этапе создания модели данных, а также в процессе эксплуатации Secret Net 6 в модель можно вносить изменения. Необходимость изменений, как правило, обуславливается следующими факторами:

- появление новых задач по защите ресурсов;
- обновление программного обеспечения компьютера;
- изменения в задачах (расписание, методы контроля);
- полное или временное снятие задач с контроля.

Все операции, связанные с изменениями в модели данных, можно условно объединить в следующие группы:

| Группа операций | Ссылка |
|---|---------|
| Изменение параметров объектов | стр. 64 |
| Изменение параметров ресурса | стр. 64 |
| Изменение параметров группы ресурсов | стр. 65 |
| Изменение параметров задачи | стр. 65 |
| Изменение параметров задания | стр. 65 |
| Просмотр параметров субъекта управления | стр. 66 |
| Добавление объектов | стр. 66 |
| Добавление вручную одиночного ресурса | стр. 67 |
| Добавление вручную нескольких ресурсов | стр. 71 |
| Импорт списка ресурсов из журнала безопасности ОС Windows | стр. 70 |
| Импорт списка ресурсов из журнала Secret Net | стр. 70 |
| Добавление ресурса в группу | стр. 71 |
| Добавление группы ресурсов вручную | стр. 71 |
| Добавление группы ресурсов по каталогу | стр. 71 |
| Добавление группы ресурсов по ключу реестра | стр. 71 |
| Добавление группы ресурсов средствами импорта | стр. 72 |
| Добавление задачи вручную | стр. 72 |
| Добавление задачи с помощью генератора задач | стр. 50 |
| Добавление задачи с помощью средств импорта | стр. 62 |
| Добавление заданий | стр. 52 |
| Добавление субъектов | стр. 59 |
| Удаление объектов | стр. 74 |
| Удаление объекта | стр. 74 |
| Удаление всех объектов определенной категории | стр. 75 |
| Связывание объектов | стр. 75 |
| Связывание объектов | стр. 75 |
| Удаление связи между объектами | стр. 75 |

| Группа операций | Ссылка |
|--|---------|
| Формирование задания ЗПС по журналу Secret Net | стр. 75 |
| Подготовка ресурсов для ЗПС | стр. 77 |
| Расчет эталонов | стр. 78 |
| Поиск зависимых модулей | стр. 79 |
| Замена переменных окружения | стр. 80 |
| Настройка задания для ПАК "Соболь" | стр. 80 |

Далее в данном разделе рассматриваются вопросы, связанные с особенностями перечисленных операций, и приводятся процедуры их выполнения.

Изменение параметров объектов

Каждый объект имеет свой набор параметров. Следует иметь в виду, что изменение значений некоторых параметров объектов может быть недоступно.

Далее в этом разделе приведены параметры объектов каждой категории и даны пояснения по их применению.

Параметры ресурсов

Параметрами, определяющими свойства ресурса, являются:

- тип ресурса;
- имя;
- полный путь (кроме скриптов);
- признаки "контролировать" и "выполняемый";
- эталоны.

Значения параметров "тип ресурса" и "имя и полный путь" задаются при создании описания ресурса и изменению не подлежат.

Путь может быть задан явно (абсолютный путь) или с помощью переменных окружения (см. стр. 79).

Признак "контролировать" означает, что после включения механизма контроля целостности (т. е. после связывания задания с компьютером) данный ресурс будет подлежать контролю. Отсутствие признака означает, что ресурс, даже если включен в задание контроля целостности, контролироваться не будет. Таким образом, устанавливая или удаляя признак, можно включать или отключать контроль конкретного ресурса.


Признак "выполняемый" означает, что данный ресурс будет включен в список разрешенных для запуска программ при выполнении процедуры подготовки ресурсов для замкнутой программной среды. Аналогично предыдущему признаку его можно включать или отключать.

Следует иметь в виду, что признаки "контролировать" и "выполняемый" имеют ресурсы не всех типов.

Эталон называется вычисленное контрольное значение для ресурса. Ресурс может входить в несколько заданий, и в каждом из них может использоваться свой метод контроля. Кроме того, в зависимости от типа ресурса и метода контроля могут использоваться разные алгоритмы. Поэтому ресурс может иметь несколько значений эталонов.

Для изменения параметров ресурса:

1. Выберите в области списка объектов ресурс, вызовите контекстное меню и активируйте команду "Свойства".
Появится диалог настройки параметров ресурса.
2. Установите или удалите отметки в полях "Контролировать" и "Выполняемый".
3. Для пересчета эталона выберите его в списке и нажмите кнопку "Пересчитать".
Эталон будет пересчитан и в соответствующей ему строке в графе "Создан" появится новая запись о дате и времени пересчета.
4. Для расчета нового эталона и сохранения его предыдущего значения нажмите кнопку "Дубль-пересчет".
Новый эталон будет пересчитан и сохранен вместе с предыдущим значением.
5. Для удаления эталона выберите его в списке и нажмите кнопку "Удалить".
6. Нажмите кнопку "ОК".

| | |
|----------------------------------|---|
| Параметры группы ресурсов | <p>Параметрами, определяющими свойства группы ресурсов, являются:</p> <ul style="list-style-type: none"> • имя группы; • описание; • тип ресурсов, входящих в данную группу. <p>Имя группы и краткое описание можно изменить в любой момент. Тип ресурсов можно изменить только в том случае, если группа не содержит ни одного ресурса.</p> <p>Для изменения параметров группы:</p> <ol style="list-style-type: none"> 1. Выберите группу, вызовите контекстное меню и активируйте команду "Свойства". Появится диалог с параметрами группы. В полях "Имя" и "Описание" изменения вносятся вручную, а в поле "Тип" значение выбирается из списка. 2. Внесите необходимые изменения и нажмите кнопку "ОК". |
| Параметры задачи | <p>В свойствах задачи указываются имя, описание задачи и сценарий (при централизованном управлении). Задачи со сценарием обозначаются пиктограммой .</p> <p>Для изменения параметров задачи:</p> <ol style="list-style-type: none"> 1. Выберите задачу, вызовите контекстное меню и активируйте команду "Свойства". Появится диалог для настройки параметров задачи. 2. Если требуется внести изменения в сценарий, нажмите кнопку "Сценарий" (составление сценария описано на стр. 72). 3. Внесите изменения в поля "Имя" и "Описание" и нажмите кнопку "ОК". |
| Параметры задания | <p>Свойства задания контроля целостности определяются группой общих параметров и расписанием. В общую группу параметров входят:</p> <ul style="list-style-type: none"> • имя и описание задания; • вид задания — тиражируемое/нетиражируемое (только для централизованного управления); • методы и алгоритмы контроля; • реакция системы на результаты контроля. <p>Методы и алгоритмы контроля, реакция системы и расписание — параметры, определяющие порядок контроля целостности ресурсов в рамках данного задания. При изменении методов и алгоритмов контроля необходимо учитывать типы ресурсов, связанных с заданием, так как к каждому типу ресурсов может применяться только определенный метод (или набор методов) контроля целостности. Кроме того, следует учитывать, что после изменения метода контроля может потребоваться корректировка реакции системы на результат проверки. Например, метод восстановления содержимого может применяться только с алгоритмом "полное совпадение".</p> <p>Свойства задания замкнутой программной среды определяют 3 параметра — имя задания, краткое описание и вид (тиражируемое/нетиражируемое).</p> <p>Для изменения параметров задания:</p> <ol style="list-style-type: none"> 1. Выберите задание, вызовите контекстное меню и активируйте команду "Свойства". В зависимости от типа задания появится диалог для настройки заданий замкнутой программной среды, контроля целостности или ПАК "Соболь". 2. Внесите необходимые изменения, используя описание процедур формирования заданий (см. стр. 52). |
| Параметры субъектов | <p>Свойства субъектов управления определяют основные параметры и параметры работы защитных механизмов (в локальном управлении параметры работы механизмов доступны только у компьютеров). Основными параметрами являются:</p> <ul style="list-style-type: none"> • имя и описание; • тип; • SID. |

Основные параметры задаются автоматически при добавлении субъекта и доступны только для просмотра.

К параметрам работы защитных механизмов относятся:

- способ задания режима ЗПС (централизованно или локально);
- состояние механизма ЗПС (включен или отключен), а также:
 - режим работы ("жесткий" или "мягкий");
 - режимы дополнительной проверки целостности модулей и их заголовков перед запуском и контроля выполнения сценариев (скриптов);
- разрешение или запрет выполнения заданий КЦ и/или ЗПС, созданных в локальных моделях данных.

Для просмотра параметров субъекта:

1. Выберите субъекта, вызовите контекстное меню и активируйте команду "Свойства".
Появится диалог с основными параметрами выбранного субъекта.
2. После просмотра значений основных параметров перейдите к диалогу "Режимы".
3. Укажите необходимые значения параметров и нажмите кнопку "ОК".

Добавление объектов

Следует иметь в виду, что само по себе добавление объектов не влечет за собой изменений в работе защитных механизмов. Для того чтобы изменения вступили в силу, добавленные объекты должны быть связаны с уже существующими объектами. Так, например, новый ресурс, добавленный в модель, необходимо включить в задачу, а задачу, в свою очередь, необходимо включить в задание. И наконец, задание необходимо связать с одним из субъектов — компьютером, пользователем, группой пользователей.

Добавление ресурса

Добавить новые ресурсы в модель данных можно одним из следующих способов:

| Способ | Пояснение |
|---|--|
| Автоматически в процессе генерации задач | Генерация задачи сопровождается автоматическим включением в нее всех связанных с ней ресурсов. Перед началом генерации можно задать дополнительное условие: включать или не включать объекты реестра и добавлять или не добавлять зависимые модули. Добавленные ресурсы связаны с объектом "задача" |
| Вручную | Ресурсы выбираются из общего перечня ресурсов компьютера. Вручную можно добавить как одиночный ресурс (например, файл или ключ реестра), указав его явно, так и несколько ресурсов, удовлетворяющих задаваемому условию. Добавляемые ресурсы не связаны с другими объектами |
| Средствами импорта | Список ресурсов можно импортировать из следующих источников: <ul style="list-style-type: none"> • файл с сохраненной моделью данных; • журнал безопасности ОС Windows или журнал Secret Net; • dvt-файл с сохраненными записями журнала. Импорт из файла с сохраненной моделью данных добавляются списки ресурсов, экспортированные из другой модели данных. Данный способ используется при переносе настроек защитных механизмов с одного компьютера на другой. Компьютеры должны иметь сходные конфигурации и использовать одинаковое программное обеспечение |
| Добавлением ресурса в группу | Ресурс включается в одну из существующих групп. При этом ресурс может быть выбран как из списка уже включенных в модель, так и из общего списка всех ресурсов компьютера. Добавленный ресурс связан с объектом "группа ресурсов" |

Для добавления вручную одиночного ресурса:

1. Выберите категорию "Ресурсы" и активируйте в меню команду "Ресурсы | Создать ресурс(ы) | Одиночный".

На экране появится диалог для выбора назначения ресурса.

2. Выберите нужное назначение ресурса:
 - "Ресурс Windows" — если добавляется файл, каталог, переменная реестра или ключ реестра;
 - "Исполняемый ресурс" — для добавления исполняемого сценария (скрипта).
3. Нажмите кнопку "ОК".

Появится диалог для настройки параметров ресурса.

4. Укажите параметры добавляемого ресурса (см. таблицу ниже) и нажмите кнопку "ОК".

Для файла, каталога, переменной реестра или ключа реестра настраиваются следующие параметры:

| Параметр | Пояснение |
|-----------------------|---|
| Тип | Укажите тип добавляемого ресурса: файл, каталог, переменная реестра, ключ реестра |
| Имя и путь | Введите ручную имя и полный путь к добавляемому ресурсу или нажмите кнопку "Обзор" и воспользуйтесь стандартной процедурой ОС |
| Контролировать | Отметка, установленная в этом поле, означает, что после включения механизма контроля целостности данный ресурс будет контролироваться. Если по каким-либо причинам контроль данного ресурса требуется отложить на неопределенное время, удалите отметку. В этом случае описание ресурса сохранится в модели данных и его можно будет поставить на контроль позднее |
| Выполняемый | Параметр доступен, если тип добавляемого ресурса — файл. Используется для обозначения исполняемых файлов, которые формируют списки программ, разрешенных для запуска при включенной замкнутой программной среде |

Для исполняемого сценария (скрипта) настраиваются следующие параметры:

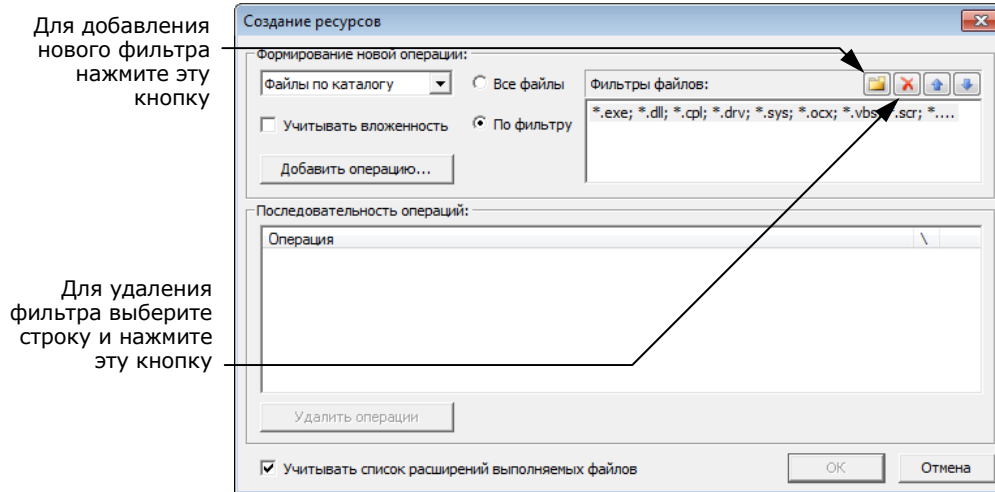
| Параметр | Пояснение |
|-------------------|---|
| Имя | Введите имя ресурса, уникальное для списка ресурсов. В качестве имени ресурса можно указать, например, имя файла, из которого загружен сценарий (скрипт) |
| Описание | Введите дополнительные сведения о ресурсе |
| Содержимое | Введите текст сценария (скрипта) — последовательность исполняемых команд и/или действий, обрабатываемых по технологии Active Scripts. Текст сценария можно ввести вручную или загрузить из файла с помощью кнопки "Загрузить...". Для загрузки текста могут использоваться файлы, содержащие сценарии с использованием технологии Active Scripts (например, vbs-файлы) |

Ресурс появится в списке основного окна программы. Далее с этим ресурсом можно выполнять все необходимые операции (добавить его в группу, включить в задачу и т. д.).

Для добавления вручную нескольких ресурсов:

1. Выберите категорию "Ресурсы" и активируйте в меню команду "Ресурсы | Создать ресурс(ы) | Несколько".

На экране появится диалог:



Для добавления нового фильтра нажмите эту кнопку

Для удаления фильтра выберите строку и нажмите эту кнопку

Диалог состоит из двух частей. Верхняя часть диалога предназначена для указания варианта отбора ресурсов и задания дополнительных условий. Дополнительные условия задаются в зависимости от выбранного варианта. Для одного и того же варианта может быть задано несколько условий. Добавление ресурсов по варианту и соответствующему ему дополнительному условию называется операцией. Таким образом, для одного и того же варианта может быть выполнено несколько операций.

Чтобы выполнить операцию, необходимо выбрать вариант, задать дополнительные условия и затем нажать кнопку "Добавить операцию".

Нижняя часть диалога предназначена для отображения последовательности выполненных операций.

Параметры, используемые при выполнении операции, описаны в приведенной ниже таблице.

| Параметр | Пояснение |
|---|--|
| Вариант отбора ресурсов | Имеется 6 вариантов: <ol style="list-style-type: none"> 1. Выбранные файлы (стандартная процедура выбора файлов, дополнительные условия недоступны). 2. Файлы по каталогу (добавляются файлы, входящие в указанный каталог, учитывается вложенность, можно использовать фильтр). 3. Каталоги с файлами (учитывается вложенность, можно использовать фильтр). 4. Каталоги по каталогу (учитывается вложенность). 5. Переменные по ключу (выбираются переменные по ключу реестра, учитывается вложенность). 6. Ключи с переменными (выбираются ключи с переменными, учитывается вложенность). |
| Учитывать вложенность | Учитывается вложенность ресурсов для всех вариантов отбора, кроме варианта "выбранные файлы" |
| Все файлы | Выбираются все ресурсы для вариантов "файлы по каталогу" и "каталог с файлами" |
| По фильтру | Включение фильтра для вариантов "файлы по каталогу" и "каталоги с файлами". Если в списке имеется несколько фильтров, то для отбора файлов будет использоваться тот, который выбран в списке |
| Учитывать список расширений выполняемых файлов | Устанавливать признак "выполняемый" для тех добавляемых в модель файлов, которые имеют расширения, заданные параметром "Расширения выполняемых" (см. стр. 93). Файлы с этим признаком при отображении в окне программы управления КЦ-ЗПС отмечаются специальным значком |

Настройка фильтров. При включении параметра "По фильтру" становится доступным список фильтров. Каждому фильтру соответствует одна строка, в которой указаны расширения файлов, добавляемых в модель данных. По умолчанию в списке содержится один фильтр, обеспечивающий отбор файлов с расширениями *.exe; *.dll; *.cpl; *.drv; *.sys; *.ocx; *.vbs; *.scr; *.rl; *.ime; *.bpl; *.ax; *.acm; *.com; *.ppl; *.cmd; *.bat. При необходимости его можно изменить или добавить в список новые фильтры. Расширения файлов в строке разделяются точкой с запятой, запятой или пробелом.

- Для изменения фильтра выберите строку, активируйте ее щелчком мыши и отредактируйте список расширений файлов.
- Для добавления нового фильтра нажмите кнопку "Новый" и в появившейся строке введите список расширений файлов.
- Для удаления фильтра из списка выберите его и нажмите кнопку "Удалить".
- Для перемещения строки в списке выберите ее и нажмите кнопку со стрелкой.

2. Настройте параметры отбора ресурсов.

Далее, в зависимости от выбранного варианта, перейдите к шагу процедуры, указанному в таблице:

| Если выбрано... | ...перейдите к шагу: |
|-----------------------------|----------------------|
| Выбранные файлы | 3 |
| Файлы по каталогу | 5 |
| Каталоги с файлами | 5 |
| Каталоги по каталогу | 5 |
| Переменные по ключу | 7 |
| Ключи с переменными | 7 |

3. Нажмите кнопку "Добавить операцию".

Появится стандартный диалог ОС Windows для выбора файлов.

4. Выберите нужные файлы.

В нижней части диалога появится список операций. Каждому выбранному файлу соответствует своя операция.

Если требуется удалить операции, выберите их в списке и нажмите кнопку "Удалить операции".

Далее:

- Если другие ресурсы добавлять не требуется, перейдите к действию **9**.
- Если требуется добавить другие ресурсы, вернитесь к выполнению действия **2** данной процедуры.

5. Настройте дополнительные параметры (при использовании фильтра выберите его в списке) и нажмите кнопку "Добавить операцию".

Появится стандартный диалог ОС Windows для выбора каталога.

6. Выберите каталог и нажмите кнопку "ОК".

Диалог выбора каталога закроется и в нижней части диалога "Создание ресурсов" в список добавится описание выполненной операции.

Если требуется удалить операции, выберите их в списке и нажмите кнопку "Удалить операции".

Далее:

- Если другие ресурсы добавлять не требуется, перейдите к шагу **9**.
- Если требуется добавить другие ресурсы, вернитесь к выполнению шага **2** данной процедуры.

7. Отметьте при необходимости поле "Учитывать вложенность" и нажмите кнопку "Добавить операцию".

Появится стандартный диалог ОС Windows для просмотра реестра.

8. Выберите ключ реестра и нажмите кнопку "ОК".

Диалог просмотра реестра закроется и в нижней части диалога "Создание ресурсов" в список добавится описание выполненной операции.

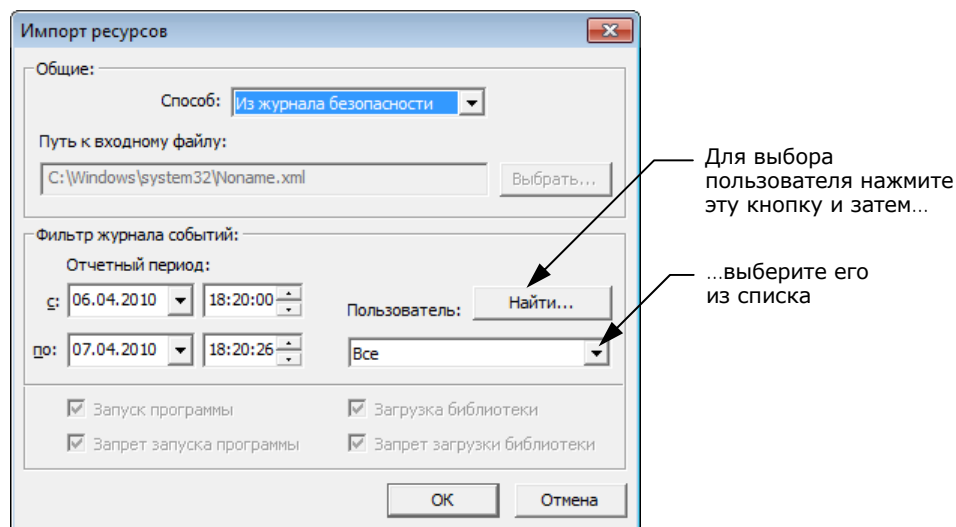
9. Проверьте список выполненных операций и, если он содержит все ресурсы, которые планировалось включить в модель данных, нажмите кнопку "ОК".

Диалог "Создание ресурсов" закрывается, а выбранные ресурсы будут добавлены в модель данных.

Для импорта списка ресурсов из журнала безопасности ОС Windows:

1. Выберите категорию "Ресурсы" и активируйте в меню команду "Ресурсы | Импорт и добавление".

На экране появится диалог:



2. Выберите в списке поля "Способ" значение "Из журнала безопасности".
Станут доступны настройки фильтра, по которым из журнала безопасности ОС Windows будут отбираться ресурсы. Настройки включают в себя отчетный период (дата и время) и имя пользователя.
3. Задайте отчетный период и укажите пользователя, по результатам работы которого будут отбираться ресурсы. При этом можно указать "Все", в этом случае будут отбираться ресурсы, к которым обращались все пользователи, или выбрать отдельного пользователя.

Для выбора пользователя выполните следующее:

- Нажмите кнопку "Найти".
Кнопка "Найти" исчезнет, начнется анализ журнала безопасности и, если в журнале были зарегистрированы обращения пользователей к ресурсам, эти пользователи будут внесены в раскрывающийся список.
 - Выберите нужного пользователя из раскрывающегося списка.
4. Нажмите кнопку "OK".

Для импорта списка ресурсов из журнала Secret Net:

1. Выберите категорию "Ресурсы" и активируйте в меню команду "Ресурсы | Импорт и добавление".

На экране появится диалог (см. предыдущую процедуру).

2. Выберите в списке поля "Способ" значение "Из журнала Secret Net".

Станут доступными настройки фильтра, по которым из журнала Secret Net будут отбираться ресурсы. Настройки включают в себя отчетный период (дата и время), имя пользователя и тип регистрируемого события.

Из журнала Secret Net импортируется информация о ресурсах, связанных событиями: запуск программы, запрет запуска программы, загрузка библиотеки и запрет загрузки библиотеки.

3. Настройте параметры фильтра и нажмите кнопку "OK".

По умолчанию импортируется информация о ресурсах, связанных со всеми 4 событиями. Чтобы не импортировать ресурсы, связанные с определенным событием, удалите соответствующую отметку. Для выполнения процедуры необходимо, чтобы была установлена хотя бы одна отметка.

Для добавления ресурса в группу:

1. Выберите категорию "Группы ресурсов".
2. Выберите в дополнительном окне структуры группу, в которую предполагается добавить новые ресурсы, вызовите контекстное меню и активируйте команду "Добавить ресурсы", а затем команду:
 - "Существующие" — на экране появится диалог со списком всех ресурсов, имеющихся в модели данных, но не входящих в данную группу. Выберите в списке те ресурсы, которые требуется включить в группу, и нажмите кнопку "ОК".
 - "Новый одиночный" — на экране появится диалог "Создание ресурса". Выполните, начиная с п. 2, действия процедуры, описанной на стр. 67.
 - "Несколько новых" — на экране появится диалог "Создание ресурсов". Выполните, начиная с п. 2, действия процедуры, описанной на стр. 68.
 - "Импортировать" — на экране появится диалог "Импорт ресурсов". В зависимости от необходимости выполните, начиная с п. 2, действия процедур, описанных на стр. 62, 70, 70.

Выбранные ресурсы будут добавлены в группу.

Добавление группы ресурсов

Новую группу ресурсов можно добавить в модель данных:

- вручную;
- по каталогу;
- по ключу реестра;
- по журналу;
- средствами импорта.

Следует иметь в виду, что вручную, по каталогу и по ключу реестра можно добавить группу ресурсов непосредственно в задачу. Добавленная таким способом группа ресурсов будет связана с вышестоящим объектом.

Источником при добавлении группы ресурсов по журналу в централизованном режиме является dvt-файл, в который предварительно были экспортированы сведения из журнала. В локальном режиме источником может быть журнал безопасности или журнал Secret Net.

Для добавления группы ресурсов вручную:

1. Выберите категорию "Группы ресурсов".
2. Выберите в меню команду "Группы ресурсов | Создать группу | Вручную". Появится диалог для настройки параметров группы ресурсов.
3. Заполните поля диалога и нажмите кнопку "ОК". Тип группы ресурсов (в поле "Тип") должен быть указан в соответствии с ее назначением. Новая группа будет добавлена в список групп ресурсов.

Для добавления группы ресурсов по каталогу:

1. Выберите категорию "Группы ресурсов".
2. Выберите в меню команду "Группы ресурсов | Создать группу | По каталогу". Появится стандартный диалог ОС Windows для выбора каталога.
3. Выберите каталог и нажмите кнопку "ОК". Новая группа будет добавлена в список групп ресурсов, а файлы каталога — в список ресурсов данной группы.

Для добавления группы ресурсов по ключу реестра:

1. Выберите категорию "Группы ресурсов".
2. Выберите в меню команду "Группы ресурсов | Создать группу | По ключу реестра". Появится стандартный диалог ОС Windows для просмотра реестра.
3. Выберите в соответствующем разделе нужный ключ реестра и нажмите кнопку "ОК". Ресурсы, соответствующие выбранному ключу реестра, будут добавлены в составе новой группы в модель данных.

Для добавления группы ресурсов по журналу:

1. Выберите категорию "Группы ресурсов".
2. Выберите в меню команду "Группы ресурсов | Создать группу | По журналу".
В централизованном режиме появится диалог настройки.
В локальном режиме вид диалога будет соответствовать рисунку, приведенному в процедуре импорта списка ресурсов (см. стр. 70).
3. В централизованном режиме нажмите кнопку "Выбрать" и выберите файл формата dvt, в который предварительно были экспортированы сведения из журнала (подробнее об экспорте сведений из журнала см. в [5]).
В локальном режиме выберите способ (журнал безопасности или журнал Secret Net).
В зависимости от режима и выбранного способа станут доступными настройки фильтра журнала событий.
4. Настройте параметры фильтра и нажмите кнопку "ОК".
Появится сообщение о добавлении в модель нового объекта.

Для добавления группы ресурсов средствами импорта:

1. Выберите категорию "Группы ресурсов".
2. Активируйте команду "Импорт и добавление" в меню "Группы ресурсов" или в контекстном меню, вызванном к папке "Группы ресурсов".
Появится диалог, приведенный в описании процедуры на стр. 62.
3. Выполните действия указанной процедуры, начиная с шага 3.

Добавление задач

Добавить новую задачу в модель данных можно одним из следующих способов:

- вручную;
- вручную со сценарием;
- с помощью генератора задач (см. стр. 51);
- с помощью средств импорта (см. стр. 62).

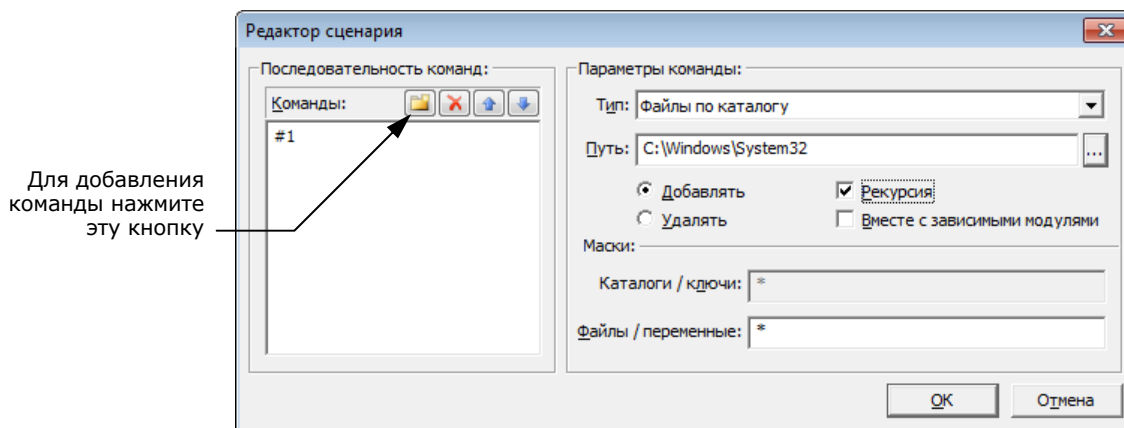
Для добавления задачи вручную:

1. Выберите категорию "Задачи" и активируйте в меню команду "Задачи | Создать задачу | Вручную".
Появится диалог для настройки параметров задачи.
2. Введите имя задачи, ее краткое описание и нажмите кнопку "ОК".
В модели данных появится новая задача, не связанная с другими объектами.

Для добавления задачи со сценарием вручную:

1. Выберите категорию "Задачи" и активируйте в меню команду "Задачи | Создать задачу | Вручную".
Появится диалог для настройки параметров задачи.
2. Введите имя задачи и ее краткое описание.
3. Нажмите кнопку "Сценарий".

Появится диалог:



Сценарий для задачи — это последовательность настраиваемых команд, определяющих правила отбора ресурсов в задаче.

- Для добавления команды нажмите кнопку в левой части диалога и введите имя команды, отображающее ее смысловое содержание.

В правой части диалога станут доступными поля для настройки параметров команды.

- Выберите тип команды и укажите путь.

Предусмотрено 5 типов команд:

| Тип команды | Пояснение |
|------------------------------------|---|
| Файлы по каталогу | Отбираются файлы из каталога, указанного в поле "Путь". Для отбора файлов можно использовать маску, заданную в поле "Файлы/Переменные" |
| Каталоги с файлами | Отбираются каталоги и файлы по указанному пути. При отборе можно использовать маски для каталогов и для файлов, заданные в полях группы "Маски" |
| Переменные по ключу | Отбираются только переменные реестра по заданному ключу реестра. Для задания базового ключа реестра указывается путь. При отборе можно использовать маску, заданную в поле "Файлы/Переменные" |
| Ключи с переменными | Отбираются переменные реестра по заданному ключу реестра и ключи. Для задания базового ключа реестра указывается путь. При отборе можно использовать маски, заданные в полях группы "Маски" |
| Установленные программы MSI | Отбираются ресурсы программы, выбранной в списке установленных программ (Microsoft Installer). Для отбора каталогов и файлов можно использовать маски, заданные в полях группы "Маски" |

В зависимости от выбранного типа команды некоторые поля для ввода параметров могут быть недоступны.

При выборе "Установленные программы MSI" поле "Путь" изменится на "Имя", а поле "Рекурсия" — на "Игнорировать объекты реестра".

- Укажите вид команды.

Команда "Добавить" используется для добавления отбираемых ресурсов в общий список ресурсов задачи. Команда "Удалить" используется для удаления ресурсов из общего списка, сформированного предыдущими командами.
- Для применения команды ко всем вложенным ресурсам поставьте отметку в поле "Рекурсия".
- Если выбраны команды "Файлы по каталогу" или "Каталоги с файлами", при необходимости используйте возможность добавления в список зависимых модулей (см. стр. 79). Для добавления зависимых модулей поставьте отметку в соответствующем поле.
- В зависимости от выбранного типа команды введите маску отбора ресурсов в поле "Каталоги/ключи" или "Файлы/переменные".

В поле можно ввести несколько масок, разделяя их символами "," (запятая), ";" (точка с запятой) или пробел. По умолчанию устанавливается маска вида "*". Это означает, что будут отобраны все ресурсы, удовлетворяющие параметрам команды. Если удалить маску "*" и оставить поле пустым, команда выполнена не будет.

Для команды типа "установленные программы MSI" маску можно задать непосредственно в поле "Имя". При этом можно использовать любой из следующих способов задания маски: <фрагмент текста>*, *<фрагмент текста> или *<фрагмент текста>*.

10. Для добавления и настройки следующей команды повторите действия **4–9**.

Для изменения последовательности выполнения команд используйте соответствующие кнопки в левой части диалога.

11. Нажмите кнопку "ОК". Затем нажмите кнопку "ОК" в диалоге свойств задачи.

В основном окне программы появится задача с пиктограммой .

Добавление заданий

Процедуры добавления задания подробно описаны на стр. [52](#).

Добавление субъектов

В централизованном режиме в модель данных можно добавлять компьютеры и группы, включающие в себя компьютеры.

Для добавления субъектов управления:


1. Выберите категорию "Субъекты управления" на панели категорий.
2. В меню "Субъекты управления" выберите команду "Добавить в список".

Появится стандартный диалог выбора компьютеров или групп.

3. Выберите нужный объект.

В нижней части диалога появится список выбранных объектов.

4. Нажмите кнопку "ОК".

В окне программы управления КЦ-ЗПС появятся новые субъекты, отмеченные знаком  (т. е. не связанные с другими объектами).

Удаление объектов

При удалении объекта из модели данных необходимо учитывать его связи с другими вышестоящими или подчиненными объектами. Так, перед удалением ресурса необходимо выяснить, в каких заданиях данный ресурс контролируется, и проанализировать возможные последствия его удаления.



После удаления ресурсов из задания следует выполнить перерасчет эталонов.



В локальном режиме из модели данных нельзя удалить субъект "Компьютер" и задания, задачи, группы ресурсов и ресурсы, добавленные в модель средствами централизованного управления. Также нельзя разорвать связи между такими объектами.

Для удаления объекта:

1. Найдите удаляемый объект, вызовите контекстное меню объекта и активируйте команду "Удалить".

Если в настройках программы отключено подтверждение удаления объектов, объект будет удален из модели данных. При этом будут удалены все подчиненные объекты, не имеющие связей с другими вышестоящими объектами, и на этом процедура удаления завершится.

2. Если в настройках программы включено подтверждение при удалении объектов, появится диалог, отображающий связи удаляемого объекта с вышестоящими и подчиненными объектами. При необходимости удалить из модели данных также подчиненные объекты поставьте отметку в поле "Удалить подчиненные". В этом случае будут удалены все подчиненные объекты, не имеющие связей с другими вышестоящими объектами.

3. Нажмите кнопку "Да".

Объект (объекты) будет удален из модели данных.

Для удаления всех объектов определенной категории:

1. Выберите нужную категорию, в окне структуры вызовите контекстное меню для корневой папки и активируйте команду "Удалить все".
Появится диалог, отображающий связи объектов.
2. Если требуется удалить все подчиненные объекты, поставьте отметку в поле "Удалять подчиненные". Нажмите кнопку "Да".
Все объекты, входящие в выбранную категорию, будут удалены из модели данных.

Связи между объектами

В зависимости от способа добавления новых объектов в модель соответствующие связи могут устанавливаться автоматически. Например, при добавлении в группу нового ресурса в модели устанавливается связь ресурс—группа. Связь может быть установлена также при импортировании объекта.

В других случаях в модель добавляются объекты, не связанные с другими объектами, например, при создании вручную новой задачи или задания. Поэтому после добавления недостающие связи должны быть установлены вручную связыванием вышестоящего и подчиненного объекта.



В локальном режиме в объекты, созданные централизованными средствами, нельзя добавить: в задание — задачу, в задачу — группу ресурсов, а в группу — ресурс.

Для связывания объектов:

1. Выберите категорию объекта, вызовите контекстное меню для нужного объекта и активируйте команду "Добавить <название объекта> | Существующие".
На экране появится диалог со списком объектов, которые еще не связаны с данным объектом.
2. Выберите в списке нужные объекты и нажмите кнопку "ОК".
В результате будет установлена связь между выбранными объектами и вышестоящим объектом.

Для удаления связи между объектами:

1. Выберите категорию объекта, у которого должна быть удалена связь с вышестоящим объектом, найдите объект, вызовите для него контекстное меню и активируйте команду "Исключить из | <название объекта>".

Следует иметь в виду, что объект можно исключить одновременно из всех объектов вышестоящей категории.

Появится предупреждение об удалении связей с вышестоящими объектами и предложение продолжить процедуру.

2. Нажмите кнопку "Да".

Формирование заданий ЗПС по журналу Secret Net

Эта процедура выполняется в следующем порядке:

| | |
|----|--|
| 1. | Включение ЗПС в "мягком" режиме |
| 2. | Сбор и подготовка сведений об используемых приложениях |
| 3. | Добавление задач ЗПС, созданных по журналу |
| 4. | Подготовка ресурсов для ЗПС (см. стр. 77) |

Включение ЗПС в "мягком" режиме

Для работы замкнутой программной среды предусмотрены два режима работы: "мягкий" и "жесткий". "Мягкий" режим нужен для настройки механизма, "жесткий" — это основной штатный режим работы. В "мягком" режиме пользователю разрешается запускать любые программы. Если при этом пользователь запускает программы, не входящие в перечень разрешенных, в журнале Secret Net регистрируются соответствующие события НСД. В "жестком" режиме разрешается запуск только тех программ, которые входят в список разрешенных. Запуск других программ блокируется, а в журнале Secret Net регистрируются события НСД.

"Мягкий" режим нужен для того, чтобы, не влияя на работу пользователей, накопить сведения в журнале о возможных ошибках, допущенных при настройке механизма ЗПС, и в последующем их устранить.

Для включения ЗПС в "мягком" режиме:

1. Выберите категорию "Субъекты управления" на панели категорий.
2. Выберите в дополнительном окне структуры или в области списка объектов компьютер или группу (компьютеров), вызовите контекстное меню и активируйте команду "Свойства". В появившемся окне "Свойства субъекта управления" перейдите к диалогу "Режимы".
3. Установите отметку в следующих полях:
 - "Режимы заданы централизованно" (в случае централизованного управления);
 - "Режим ЗПС включен";
 - "Мягкий режим" и нажмите кнопку "ОК".

Для выбранного компьютера (или группы) начнет действовать механизм ЗПС в "мягком" режиме.

Сбор сведений об используемых приложениях

Модель ЗПС может быть создана на основе данных журнала Secret Net. На этом этапе пользователям разрешается запускать любые приложения. Запуск приложений регистрируется в журнале Secret Net. Для того чтобы собрать достоверные сведения об используемых на защищаемых компьютерах приложениях, необходимо отвести для этого некоторый период времени. Кроме того, на время сбора сведений необходимо включить регистрацию всех событий категории "Замкнутая программная среда" на тех компьютерах, на которых замкнутая программная среда будет использоваться.

После окончания этого периода администратор безопасности (или аудитор) с помощью программы "Журналы" создает выборку записей за интересующий период из журнала Secret Net, а затем данные о запускаемых программах экспортируются в модель данных. Подробные сведения о работе с программой "Журналы" см. в документе [5].

Добавление задач ЗПС, созданных по журналу

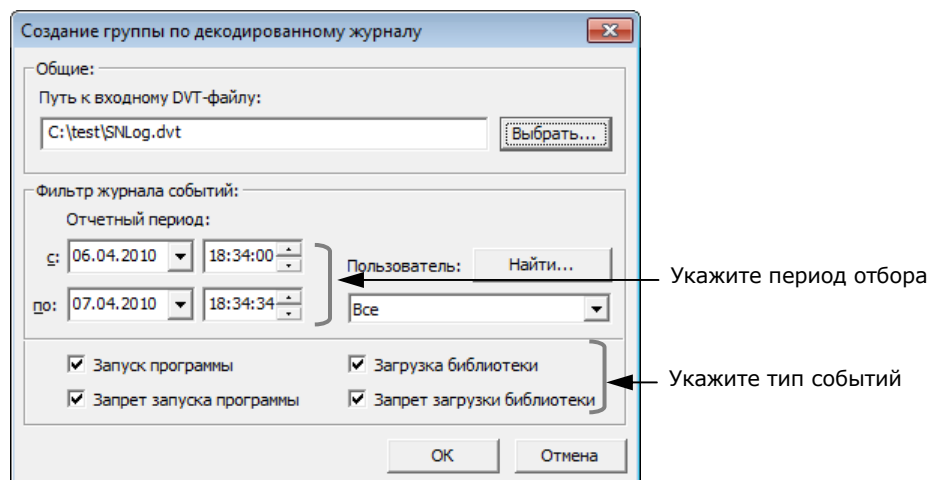
На этой стадии на основании данных из журнала Secret Net формируются задачи, добавляемые к заданиям ЗПС.

Источником при добавлении задач ЗПС по журналу в централизованном режиме является dvt-файл, в который предварительно были экспортированы сведения из журнала. В локальном режиме источником может быть журнал безопасности или журнал Secret Net.

Для добавления задач ЗПС, созданных по журналу:

1. В основном окне программы управления КЦ-ЗПС выберите нужного субъекта.
2. Выберите ранее созданное задание ЗПС, связанное с выбранным субъектом, или создайте новое задание ЗПС.
3. Вызовите контекстное меню и выберите в нем "Добавить задачи/группы | Новую группу по журналу".

На экране появится диалог, подобный следующему:



4. Укажите необходимые значения параметров (путь к dvt-файлу при работе в централизованном режиме или тип журнала при работе в локальном режиме, а также дополнительные условия отбора, если необходимо) и нажмите кнопку "OK".

К заданию будет добавлена группа ресурсов, сформированная на основании данных журнала.

Повторите эту процедуру и для других субъектов.

Подготовка ресурсов для замкнутой программной среды

Чтобы описания ресурсов использовались механизмом замкнутой программной среды, они должны иметь признак "выполняемый" и входить в задание ЗПС. Присвоение ресурсам признака "выполняемый" называется подготовкой ресурсов для ЗПС. Этот признак присваивается всем файлам, имеющим заданные расширения.

Таким образом, файлы, имеющие признак "выполняемый" и входящие в задание ЗПС, образуют список разрешенных для запуска программ. После связывания задания с пользователем и включения "мягкого" или "жесткого" режима система Secret Net 6 начнет контролировать запуск программ пользователем и регистрировать соответствующие события в журнале.

При построении модели данных с помощью автоматизированных средств (мастера и механизма генерации задач) подготовка ресурсов для ЗПС включена в соответствующие процедуры и выполняется по умолчанию. При построении модели вручную и ее модификации подготовка ресурсов для ЗПС выполняется как отдельная процедура.

В некоторых случаях (например, при ручном формировании заданий замкнутой программной среды или после добавления в модель новых ресурсов) может потребоваться заново построить список ресурсов, имеющих признак "выполняемый". Для этой цели в процедуре подготовки ресурсов предусмотрены две дополнительные возможности:

- Перед началом выполнения процедуры можно сбросить признак "выполняемый" у всех ресурсов в модели данных, у которых он имеется. В этом случае будут анализироваться все ресурсы, включенные в модель.
- Необходимо выполнить поиск зависимых модулей. В этом случае для каждого ресурса, которому будет установлен признак "выполняемый", будет проведен поиск в ресурсах компьютера зависимых модулей. Найденные зависимые модули будут добавлены в модель данных в те же группы ресурсов, в которые входят исходные модули.

Для подготовки ресурсов:

1. Выберите в меню "Сервис" команду "Ресурсы ЗПС".
На экране появится диалог для настройки параметров процедуры.
2. Если требуется, чтобы в ходе подготовки были проанализированы все имеющиеся в модели ресурсы (в том числе и те, у которых ранее был установлен признак "выполняемый"), оставьте отметку в поле "Предварительно

сбросить флаг "выполняемый" у всех ресурсов". В этом случае список ресурсов, имеющих признак "выполняемый", будет построен заново. При этом время выполнения процедуры будет зависеть от общего числа ресурсов в модели данных.

Если требуется, чтобы были проанализированы только ресурсы, не имеющие признака "выполняемый", удалите отметку.

3. Удалите из списка или добавьте в него расширения файлов, для которых должен быть установлен признак "выполняемый".
4. Для добавления в модель данных зависимых модулей оставьте отметку в поле "Добавлять зависимые модули".

Если добавление зависимых модулей не требуется, удалите отметку.

5. Нажмите кнопку "ОК".

Начнется процесс подготовки ресурсов к использованию в механизме замкнутой программной среды и появится информационное окно, отображающее ход выполнения процесса. После окончания появится сообщение об успешном завершении процесса.

Расчет эталонов

Если модель данных строится с помощью мастера (см. стр. 49), расчет эталонов выполняется автоматически. Если построение модели осуществляется с помощью генератора задач или вручную, расчет эталонов выполняется отдельной процедурой.



Расчет эталонов в централизованном режиме работы программы "Контроль программ и данных" выполняется только для ресурсов, входящих в тиражируемые задания.

В локальном режиме расчет эталонов нельзя выполнить для задач, входящих в задания, у которых эталоны рассчитаны централизованно (тиражируемые задания).

Предусмотрено 3 варианта расчета эталонов:

- для всех ресурсов модели данных;
- для выбранных ресурсов;
- для всех ресурсов, входящих в выбранное задание.

В двух первых вариантах расчет эталонов для ресурса выполняется по всем заданиям, в которые входит данный ресурс. Так как один и тот же ресурс может входить в разные задания и в каждом из заданий для него предусмотрен свой метод контроля, расчет эталонов выполняется для каждого метода.

Кроме перечисленных вариантов расчет эталонов может быть выполнен для отдельного ресурса, если ресурс входит в задание и заданы методы контроля. В отличие от указанных выше 3 вариантов расчет выполняется в диалоге "Свойства ресурса" (см. стр. 64) и используется в тех случаях, когда заведомо известно, что был изменен только данный ресурс и для него необходимо пересчитать эталон.

Для расчета эталонов всех ресурсов модели:

1. Выберите любую категорию и активируйте команду "Расчет" в меню "Сервис | Эталон".

Появится диалог расчета эталонов.

2. Выполните действия процедуры, описанной на стр. 57.

Для расчета эталонов выбранных ресурсов:

1. Выберите категорию "Ресурсы" или разверните структуру модели таким образом, чтобы в окне списка объектов оказались ресурсы.

2. Выделите в списке ресурс или несколько ресурсов, вызовите контекстное меню и активируйте команду "Расчет эталонов".

Появится диалог расчета эталонов.

3. Выполните расчет в соответствии с указанной процедурой.

Для расчета эталонов ресурсов задания:

1. Выберите категорию "Задания".
2. В дополнительном окне структуры вызовите контекстное меню к заданию, в котором должны быть рассчитаны эталоны, и активируйте команду "Расчет эталонов".

Команду "Расчет эталонов" можно активировать в меню с именем выбранного задания.

Появится диалог расчета эталонов.

3. Выполните расчет в соответствии с указанной процедурой.

Для пересчета эталона отдельного ресурса:

1. Выберите в области списка объектов ресурс, вызовите контекстное меню и активируйте команду "Свойства".

Появится диалог "Свойства ресурса" (см. стр. 64).

2. Выберите в списке эталон и нажмите кнопку "Пересчитать".

Эталон будет пересчитан и в его строке обновится дата расчета.

3. Выполните пересчет для остальных эталонов списка и нажмите кнопку "ОК".

Предусмотрено удаление старых эталонов, полученных в результате расчета, пересчета или выполнения команды "Дубль-пересчет" (см. стр. 64).

Удаление старых эталонов**Для удаления старых эталонов:**

- Выберите в меню команду "Сервис | Эталоны | Удаление старых".

Старые эталоны будут удалены.

Старые эталоны удаляются из локальной базы данных автоматически при каждом успешном завершении задания контроля целостности.

Поиск зависимых модулей

При работе пользователя с приложениями запуск исполняемых файлов может сопровождаться запуском модулей (драйверов и библиотек), не входящих непосредственно в приложения. Такие модули называются зависимыми.

При построении модели данных с помощью автоматизированных средств (мастера и механизма генерации задач) поиск зависимых модулей и добавление их в модель данных выполняются по умолчанию. При построении модели вручную и добавлении в нее новых ресурсов поиск зависимых модулей выполняется как отдельная процедура (см. ниже).

Для поиска и добавления зависимых модулей:

1. Выберите в области списка объектов ресурс или несколько ресурсов, вызовите контекстное меню и активируйте команду "Зависимости".

Появится диалог, содержащий список найденных зависимых модулей.

2. Если не требуется, чтобы зависимые модули были помечены в модели данных как выполняемые, удалите отметку из поля "Помечать как выполняемые".

3. Нажмите кнопку "Добавить".

Модули будут добавлены в модель данных, затем появится сообщение об успешном завершении процедуры.

Замена переменных окружения

Для корректной работы модели данных, перенесенной с одного компьютера на другой, а также при экспорте отдельных ресурсов, задач и заданий может потребоваться заменить абсолютные пути к ресурсам на переменные окружения.

Данная процедура выполняется на том компьютере, с которого будет осуществляться перенос модели или экспортирование ее отдельных элементов.

Замена переменных окружения на абсолютные пути — обратная операция, выполняемая в тех случаях, когда по каким-либо причинам необходимо восстановить абсолютные пути.

Для замены переменных окружения:

1. Выберите ресурс в модели данных и в контекстном меню активируйте команду "Переменные окружения".
Появится диалог, содержащий список имеющихся на компьютере переменных окружения.
2. Укажите направление замены:
 - Для замены абсолютных путей на переменные окружения оставьте установленную по умолчанию отметку в переключателе.
 - Для замены переменных окружения на абсолютные пути поставьте отметку в поле "Имена переменных окружения на значение путей в файлах и папках".
3. Выберите в списке те переменные, для которых будет выполнено действие.
4. Нажмите кнопку "ОК".

Настройка задания для ПАК "Соболь"

Задание для ПАК "Соболь" представляет собой перечень файлов жесткого диска, целостность которых должна контролироваться средствами ПАК "Соболь" до загрузки ОС.



Внимание! Комплекс "Соболь" обеспечивает контроль целостности файлов на жестком диске и физических секторов жесткого диска (см. документы [1] и [8]). Задание на контроль целостности физических секторов формируется средствами комплекса "Соболь". Задание на контроль целостности файлов формируется либо средствами комплекса "Соболь", либо средствами программы "Контроль программ и данных" из состава системы Secret Net 6.

Рекомендуется задание на контроль целостности файлов формировать средствами программы "Контроль программ и данных".

После формирования модели данных с помощью мастера в ней появляется задание на контроль целостности ПАК "Соболь" (при включенном режиме интеграции).

Для настройки задания:

1. В главном окне программы "Контроль программ и данных" активируйте категорию "Задания".
2. Добавьте в задание "Задание для ПАК "Соболь" все задачи контроля файлов средствами ПКЦ комплекса "Соболь".

Для добавления задач используйте описанные выше процедуры модификации модели данных.

3. При централизованном управлении установите связь этого задания со всеми компьютерами или группами, к которым это задание относится.
4. Для сохранения модели данных в базе данных Secret Net 6 активируйте команду "Сохранить" в меню "Файл".
5. В меню "Сервис" активируйте команду "Эталоны | Расчет".
После расчета эталонов на экране появится сообщение: "Завершение процедуры расчета эталонов будет произведено ПАК "Соболь" при перезагрузке".
6. Нажмите кнопку "ОК".



Если до начала выполнения данной процедуры в ПАК "Соболь" хранились собственные шаблоны контроля целостности, они будут заменены новыми, сформированными в соответствии с настройкой задания в программе "Контроль программ и данных". При удалении всех задач из задания для ПАК "Соболь" или отключении режима интеграции собственные шаблоны ПАК "Соболь" будут восстановлены.

Глава 5

Дополнительные возможности

Затирание файлов

Механизм затирания файлов предназначен для предотвращения возможности восстановления удаленных файлов (безопасность повторного использования объектов). Стандартные средства операционной системы не обеспечивают физического удаления информации при выполнении операций удаления файлов на дисках. Поэтому информация, содержащаяся в удаленных файлах, может быть восстановлена с использованием специально предназначенных для этого средств. При действии механизма затирания записывается последовательность случайных чисел в область диска, где физически было расположено содержимое удаленного файла.

Для усиления степени защиты запись может быть осуществлена несколько раз подряд. В этом случае говорят о количестве проходов затирания. На практике заведомо достаточно двух проходов затирания данных.

Затирание данных выполняется автоматически при удалении файла с диска.



Затирание файла подкачки страниц выполняется стандартными средствами ОС Windows при выключении компьютера.

Не осуществляется затирание файлов, помещаемых в "Корзину", — так как во время нахождения в этой папке файлы не удаляются с диска. Затирание таких файлов происходит после очистки содержимого "Корзины".

Для настройки механизма:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
2. Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.
Для настройки механизма затирания данных используются 3 параметра:
 - количество циклов затирания на локальных дисках;
 - количество циклов затирания на сменных дисках;
 - количество циклов затирания конфиденциальной информации.
3. Вызовите контекстное меню для нужного параметра и активируйте в нем команду "Свойства".
На экране появится диалог настройки параметра.
4. Настройте действие параметра и нажмите кнопку "ОК".

Примечание. Если параметру присвоено значение "0", затирание не выполняется.

Запрет сетевых интерфейсов

С помощью механизма запрета сетевых интерфейсов администратор безопасности может отключить сетевые интерфейсы, устанавливаемые операционной системой при ее загрузке. В этом случае пользователи не смогут воспользоваться отключенными сетевыми интерфейсами.



Действие механизма распространяется только на те интерфейсы, для которых поддерживается запрет использования.

Настройка механизма заключается в составлении списка сетевых интерфейсов, которые требуется отключать при загрузке операционной системы.

Для настройки механизма:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
2. Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.
3. Вызовите контекстное меню для параметра "Запрет использования сетевых интерфейсов" и активируйте в нем команду "Свойства".
На экране появится диалог настройки параметра. Диалог содержит список доступных для запрета типов интерфейсов.
4. Настройте действие параметра и нажмите кнопку "ОК".

Контроль печати

Система Secret Net 6 контролирует вывод файлов на печать. При печати в журнале Secret Net регистрируются соответствующие события категории "Контроль печати". Состав регистрируемых событий можно изменять. Описание действий для настройки механизма регистрации событий см. в документе [5].

При включенном режиме контроля печати конфиденциальных документов в механизме полномочного управления доступом система Secret Net 6 дополнительно обеспечивает:

- предотвращение несанкционированного вывода на печать конфиденциальных документов;
- автоматическое добавление грифа конфиденциальности в распечатываемые конфиденциальные документы.

Подробные сведения о настройке механизма полномочного разграничения доступа и контроля печати см. в документе [4].

Формирование отчетов

В Secret Net 6 предусмотрено получение различных отчетов о состоянии системы. Отчеты могут содержать сведения:

- об установленном на компьютерах программном обеспечении;
- о настройках защитных механизмов и перечне защищаемых ресурсов;
- о пользователях системы и настройках их параметров;
- об установленных в системе комплексах "Соболь" и пользователях, имеющих к ним доступ;
- об идентификаторах пользователей и режимах их использования;
- о событиях, зафиксированных в журналах.

Администратор может запросить следующие отчеты:

Паспорт ПО (паспорт программного обеспечения АРМ). Отчет включает в себя учетную информацию о компьютере и перечень установленного на нем программного обеспечения.

Ресурсы АРМ. Отчет включает в себя учетную информацию о компьютере и подробные сведения о состоянии установленной на нем системы защиты.

Допуск пользователей к ПАК "Соболь". Отчет содержит сведения о ПАК "Соболь", установленном на компьютере, и список пользователей с указанием их идентификаторов и параметров (отчет недоступен в автономном режиме функционирования системы Secret Net 6).

Журнал событий. Отчет содержит настраиваемую выборку записей журнала и детализацию зарегистрированных в нем событий.

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



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

Отчет "Паспорт ПО"

В отчете содержатся следующие сведения о компьютере:

- учетная информация компьютера (имя компьютера, название подразделения, к которому относится компьютер, номер системного блока и др.);
- перечень установленного ПО. Для каждого программного пакета указываются компания-производитель, суммарный объем занимаемого пространства и др.;
- Ф.И.О. сотрудников, ответственных за эксплуатацию компьютера. Имена сотрудников указываются при формировании отчета.

Отчет можно сформировать локально на компьютере или централизованно на рабочем месте администратора. Процедура локального формирования отчета описана ниже. Централизованное формирование отчета осуществляется с помощью программы "Монитор", входящей в состав средств оперативного управления системы Secret Net 6. Описание процедуры централизованного формирования отчета см. в документе [6].

Для формирования отчета "Паспорт ПО":

1. Выберите в главном меню Windows "Пуск | Все программы | Код безопасности | Secret Net | Контроль программ и данных".
На экране появится основное окно программы "Контроль программ и данных" в локальном режиме работы.
2. Активируйте команду "Сервис | Отчеты | Паспорт ПО".
На экране появится стартовый диалог мастера формирования отчета.
3. В соответствующих полях введите Ф.И.О. сотрудников, ответственных за эксплуатацию данного компьютера. При необходимости настройте параметры нумерации страниц отчета (расположение номеров и отображение общего количества страниц). Для этого нажмите кнопку "Дополнительно...", в появившемся диалоге отметьте нужные параметры и нажмите кнопку "ОК".
4. Нажмите кнопку "Далее >".
На экране появится следующий диалог мастера.
5. Введите полное имя файла отчета. Для ввода используйте клавиатуру или нажмите кнопку справа от поля, чтобы указать файл в стандартном диалоге сохранения файла ОС Windows.
6. Нажмите кнопку "Построить".
Программа начнет процесс получения и обработки данных, и на экране появится соответствующее сообщение.

Отчет "Ресурсы рабочей станции"

В отчете содержатся следующие сведения о компьютере:

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

Отчет можно сформировать локально на компьютере или централизованно на рабочем месте администратора. Процедура локального формирования отчета описана ниже. Централизованное формирование отчета осуществляется с помощью программы "Монитор", входящей в состав средств оперативного управления системы Secret Net 6. Описание процедуры централизованного формирования отчета см. в документе [6].

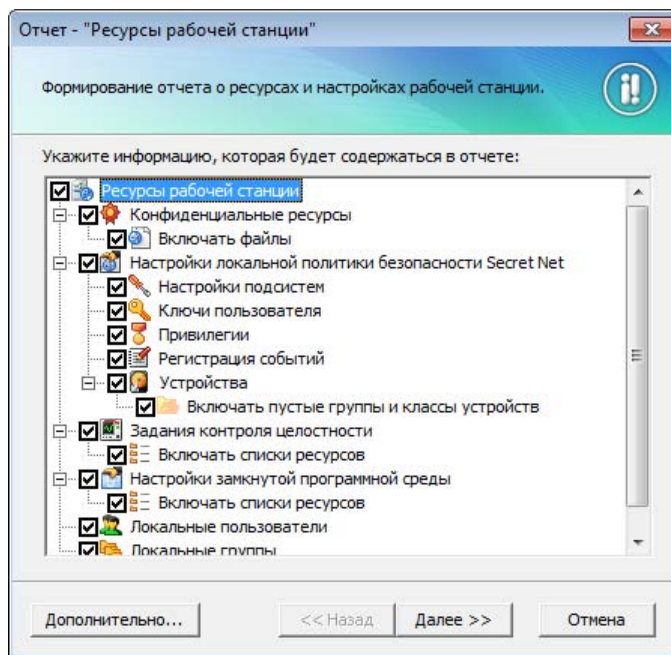
Для формирования отчета "Ресурсы рабочей станции":

1. Выберите в главном меню Windows "Пуск | Все программы | Код безопасности | Secret Net | Контроль программ и данных".

На экране появится основное окно программы "Контроль программ и данных" в локальном режиме работы.

2. Активируйте команду "Сервис | Отчеты | Ресурсы рабочей станции".

На экране появится стартовый диалог мастера формирования отчета:



3. Отметьте нужные элементы списка для сохранения соответствующих сведений в отчете. Можно сохранить следующие сведения:

- **Список конфиденциальных ресурсов.** Если установлена отметка у элемента "Конфиденциальные ресурсы" — в отчете будет сохранен список конфиденциальных каталогов компьютера. Если установлена отметка у подчиненного элемента "Включать файлы" — в отчет будет добавлен список конфиденциальных файлов.
- **Список результирующих значений параметров политики безопасности Secret Net 6, действующей на компьютере.** Чтобы сохранить список, отметьте элемент "Настройки локальной политики безопасности Secret Net". Для выборочного сохранения сведений отметьте подчиненные элементы с названиями нужных групп параметров. Если установлена отметка у элемента "Включать пустые группы и классы устройств", подчиненного элементу "Устройства", — в отчет будет добавлен список групп и классов, к которым не относится ни одно устройство.
- **Список заданий контроля целостности.** Чтобы сохранить список, отметьте элемент "Задания контроля целостности". Если установлена отметка у подчиненного элемента "Включать списки ресурсов" — для каждого задания в отчет будет добавлен список контролируемых ресурсов.
- **Параметры и список заданий замкнутой программной среды.** Чтобы сохранить сведения, отметьте элемент "Настройки замкнутой программной среды". Если установлена отметка у подчиненного элемента "Включать списки ресурсов" — для каждого задания в отчет будет добавлен список контролируемых ресурсов.

- **Список локальных пользователей.** Чтобы сохранить список, отметьте элемент "Локальные пользователи".
 - **Список локальных групп пользователей.** Чтобы сохранить список, отметьте элемент "Локальные группы".
 - **Список зарегистрированных доменных пользователей.** Чтобы сохранить список, отметьте элемент "Доменные пользователи" (данная возможность доступна только в автономном режиме функционирования системы Secret Net 6).
4. При необходимости настройте параметры нумерации страниц отчета (расположение номеров и отображение общего количества страниц). Для этого нажмите кнопку "Дополнительно...", в появившемся диалоге отметьте нужные параметры и нажмите кнопку "ОК".
 5. Нажмите кнопку "Далее >".
На экране появится следующий диалог мастера.
 6. Введите полное имя файла отчета. Для ввода используйте клавиатуру или нажмите кнопку справа от поля, чтобы указать файл в стандартном диалоге сохранения файла ОС Windows.
 7. Нажмите кнопку "Построить".
Программа начнет процесс получения и обработки данных, и на экране появится соответствующее сообщение.

Отчет "Допуск пользователей к ПАК "Соболь""

В отчете содержатся сведения о ПАК "Соболь", установленных на компьютерах системы (заводские номера, время последних синхронизаций, контрольные суммы), и список пользователей с указанием их идентификаторов и параметров.

Отчет формируется централизованно в программе "Контроль программ и данных" в централизованном режиме работы.

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

1. Выберите в главном меню Windows "Пуск | Все программы | Код безопасности | Secret Net | Контроль программ и данных (централизованный режим)".
На экране появится основное окно программы "Контроль программ и данных" в централизованном режиме работы.
2. Активируйте команду "Сервис | Отчеты | Пользователи ПАК "Соболь"".
На экране появится стартовый диалог мастера формирования отчета.
3. Если требуется, чтобы отчет содержал сведения только о компьютерах, на которых установлен ПАК "Соболь", удалите отметку в поле "Отображать все рабочие станции, входящие в домен". При необходимости настройте параметры нумерации страниц отчета (расположение номеров и отображение общего количества страниц). Для этого нажмите кнопку "Дополнительно...", в появившемся диалоге отметьте нужные параметры и нажмите кнопку "ОК".
4. Нажмите кнопку "Далее >".
На экране появится следующий диалог мастера.
5. Введите полное имя файла отчета. Для ввода используйте клавиатуру или нажмите кнопку справа от поля, чтобы указать файл в стандартном диалоге сохранения файла ОС Windows.
6. Нажмите кнопку "Построить".
Программа начнет процесс получения и обработки данных, и на экране появится соответствующее сообщение.

Отчет "Журнал событий"

В отчете содержатся следующие сведения о журнале компьютера:

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

Отчет можно сформировать в программе просмотра журналов локально на компьютере или централизованно на рабочем месте администратора. Описание процедуры формирования отчета см. в документе [5].

Средства экспорта и импорта параметров

Для того чтобы настроить систему защиты одинаковым образом на нескольких отдельных компьютерах или в нескольких организационных подразделениях, в Secret Net 6 реализована возможность экспорта и импорта параметров политик, параметров пользователей и параметров механизмов КЦ и ЗПС.

Экспорт/импорт параметров политик

Экспорт параметров системы Secret Net 6 в локальных и групповых политиках осуществляется в файлы, содержимое которых в дальнейшем можно импортировать в других политиках. Экспорт выполняется в файлы, формат которых соответствует формату файлов сведений ОС Windows (*.inf).

Для экспорта параметров:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
2. Вызовите контекстное меню раздела "Параметры Secret Net" и активируйте команду "Экспорт настроек политики в файл".
На экране появится стартовый диалог мастера экспорта.
3. Укажите имя файла для сохранения параметров.
4. Отметьте требуемый объем экспортирования (все или выборочные параметры) и нажмите кнопку "Далее >".
 - Если выбран экспорт всех доступных параметров, на экране появится диалог завершения подготовки к экспорту. Нажмите кнопку "Готово" для завершения работы мастера экспорта.
 - Если выбран экспорт выборочных параметров, появится диалог, содержащий список параметров. В этом случае перейдите к действию 5.
5. Отметьте в списке нужные параметры и нажмите кнопку "Далее >".
На экране появится диалог завершения подготовки к экспорту.
6. Нажмите кнопку "Готово".

Программа выполнит экспорт параметров в указанный файл. После успешного экспорта на экране появится сообщение об этом.

Для импорта параметров:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11).
2. Вызовите контекстное меню раздела "Параметры Secret Net" и активируйте команду "Импорт настроек политики из файла".
На экране появится стандартный диалог выбора файла.
3. Выберите нужный файл и нажмите кнопку "Открыть".

Программа выполнит импорт всех параметров из выбранного файла. После успешного импорта на экране появится сообщение об этом.

Экспорт/импорт параметров пользователей

Система Secret Net 6 предоставляет возможности экспорта и импорта параметров локальных пользователей (в автономном режиме функционирования — также и зарегистрированных доменных пользователей). Экспорт осуществляется в файлы, содержимое которых в дальнейшем можно импортировать на любом компьютере с установленным клиентом системы Secret Net 6. Экспорт выполняется в файлы формата XML (*.xml).



При экспорте и импорте параметров пользователя осуществляется и экспорт/импорт параметров электронных идентификаторов пользователя.

Если параметры локального пользователя были экспортированы на одном компьютере, то при импорте данные параметры будут применены к локальному пользователю с таким же именем.

Для экспорта параметров пользователей:

1. Активируйте команду "Пуск | Все Программы | Код безопасности | Secret Net | Управление компьютером".

На экране появится окно консоли с загруженной оснасткой для управления параметрами компьютера.

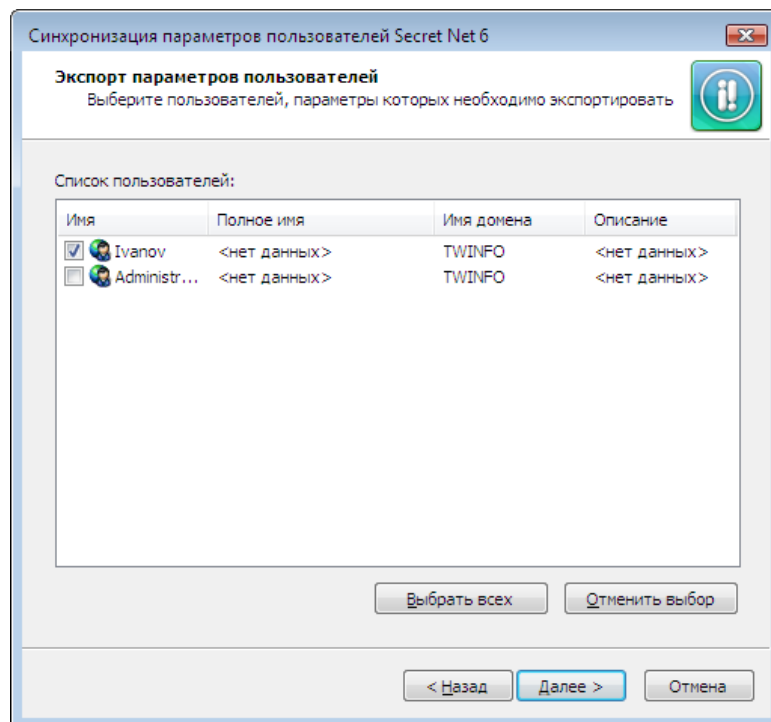
2. Перейдите к разделу "Управление компьютером (локальным) | Служебные программы".

3. В зависимости от того, параметры каких пользователей необходимо экспортировать (локальных пользователей или, в автономном режиме функционирования, зарегистрированных доменных пользователей), вызовите контекстное меню для папки "Локальные пользователи и группы | Пользователи" или, в автономном режиме функционирования, "Доменные пользователи" и активируйте соответствующую команду:
 - "Все задачи | Экспорт/Импорт параметров" — для папки "Пользователи";
 - "Экспорт/Импорт параметров" — для папки "Доменные пользователи" (в автономном режиме функционирования).

На экране появится стартовый диалог мастера экспорта.

4. Оставьте отмеченным поле "Экспорт параметров пользователей" и нажмите кнопку "Далее >".

На экране появится диалог со списком пользователей:



5. Отметьте имена тех пользователей, параметры которых требуется экспортировать, и нажмите кнопку "Далее >".

На экране появится диалог для выбора файла.

6. Введите полное имя файла. Для ввода используйте клавиатуру или нажмите кнопку справа от поля, чтобы указать файл в стандартном диалоге сохранения файла ОС Windows.
7. Нажмите кнопку "Далее >".

Программа выполнит экспорт параметров в выбранный файл и по окончании процесса на экране появится завершающий диалог мастера.

8. Для завершения работы мастера нажмите кнопку "Готово".

Совместно с результирующим файлом в том же каталоге создается специальный файл отчета о ходе процесса экспорта. От имени файла, выбранного для экспорта, файл отчета отличается расширением .log.

Для импорта параметров пользователей:

1. Выполните действия 1–3 предыдущей процедуры.
2. Установите отметку в поле "Импорт параметров пользователей" и нажмите кнопку "Далее >".

На экране появится диалог для выбора файла.

3. Введите или выберите имя файла и нажмите кнопку "Далее >".

На экране появится диалог со списком пользователей, параметры которых хранятся в файле.

4. Отметьте имена тех пользователей, параметры которых требуется импортировать, и нажмите кнопку "Далее >".

Программа выполнит импорт параметров из выбранного файла.

5. По окончании процесса нажмите кнопку "Готово".

Экспорт/импорт параметров механизмов КЦ и ЗПС

Описание процедур экспорта и импорта параметров модели данных КЦ-ЗПС см. на стр. 59.

Редактирование учетной информации компьютера

Учетная информация компьютера указывается при установке клиентского ПО системы Secret Net 6. Учетную информацию составляют следующие сведения:

- название подразделения, в котором используется компьютер;
- наименование автоматизированной системы предприятия;
- место расположения компьютера;
- номер системного блока.

Указанные сведения хранятся системой Secret Net 6 и используются в отчетах "Паспорт ПО" (см. стр. 83) и "Ресурсы рабочей станции" (см. стр. 83).

При необходимости учетную информацию можно изменить.

Для редактирования учетной информации:

1. В Панели управления Windows активируйте ярлык "Управление Secret Net 6".
На экране появится диалоговое окно "Управление Secret Net 6".
2. Перейдите к диалогу "Учетная информация".
3. Введите сведения о компьютере в соответствующих полях.
4. Нажмите кнопку "Применить" или "ОК".

Ввод серийного номера

В локальной базе данных системы Secret Net 6 хранится серийный номер клиента (СНК), содержащий лицензию на использование клиентского ПО системы защиты на компьютере. Наличие серийного номера обеспечивает работоспособность программного обеспечения определенной версии (версий).

При необходимости можно выполнить смену серийного номера клиента в локальной базе данных компьютера. Регистрация серийного номера необходима в следующих случаях:

- чтобы сменить демонстрационную лицензию на бессрочную;
- чтобы восстановить серийный номер в локальной базе данных при повреждении или удалении.

В сетевом режиме функционирования ввод нового серийного номера можно выполнить:

- централизованно в программе "Консоль управления" (см. документ [7]);
- локально на компьютере (см. ниже).

Для ввода нового серийного номера:

1. В Панели управления Windows активируйте ярлык "Управление Secret Net 6". На экране появится одноименное диалоговое окно.
2. Перейдите к диалогу "О системе" и нажмите кнопку "Сменить серийный номер". На экране появится запрос для ввода серийного номера.
3. Введите новый серийный номер и нажмите кнопку "ОК". При появлении на экране диалога запроса нажмите кнопку "Да" для продолжения процедуры.
4. При определенных условиях на экране может появиться сообщение о необходимости перезагрузки. В этом случае нажмите кнопку "ОК" в окне сообщения и перезагрузите компьютер после закрытия диалогового окна "Управление Secret Net 6".

Временное отключение защитных механизмов

При возникновении нестандартных ситуаций в процессе настройки или эксплуатации системы Secret Net 6 можно локально отключать отдельные механизмы защиты.

В перечень механизмов, для которых предусмотрено отключение, входят:

- полномочное управление доступом;
- затирание данных;
- замкнутая программная среда;
- контроль устройств.

В сетевом режиме функционирования системы Secret Net 6 дополнительно можно управлять режимом усиленной защиты трафика при обращениях к Active Directory. Режим усиленной защиты может использоваться, если в системе организована и настроена инфраструктура открытых ключей (Public Key Infrastructure — PKI).



Для внедрения PKI могут применяться стандартные средства ОС Windows или ПО сторонних производителей — например, ПО КриптоПро.

Для управления работой механизмов:

1. В Панели управления Windows активируйте ярлык "Управление Secret Net 6". На экране появится одноименное диалоговое окно.
2. Перейдите к диалогу "Защитные механизмы Secret Net".
3. Для отключения работы механизма удалите отметку слева от его названия. При появлении диалога запроса подтвердите решение для продолжения операции. Чтобы включить механизм — установите отметку.



Для включения режима усиленной защиты трафика при обращениях к AD установите отметку в поле "шифровать управляющий сетевой трафик". Перед сохранением изменений будет выполнена проверка возможности установки защищенного соединения с AD и, в случае неудачной попытки, на экране появится запрос о необходимости сохранения текущих заданных параметров. В этом случае рекомендуется отказаться от сохранения изменений, иначе доступ к AD будет невозможен для компонентов системы Secret Net 6. Включать режим усиленной защиты следует только после настройки инфраструктуры открытых ключей в системе.

4. Нажмите кнопку "ОК" и перезагрузите компьютер.

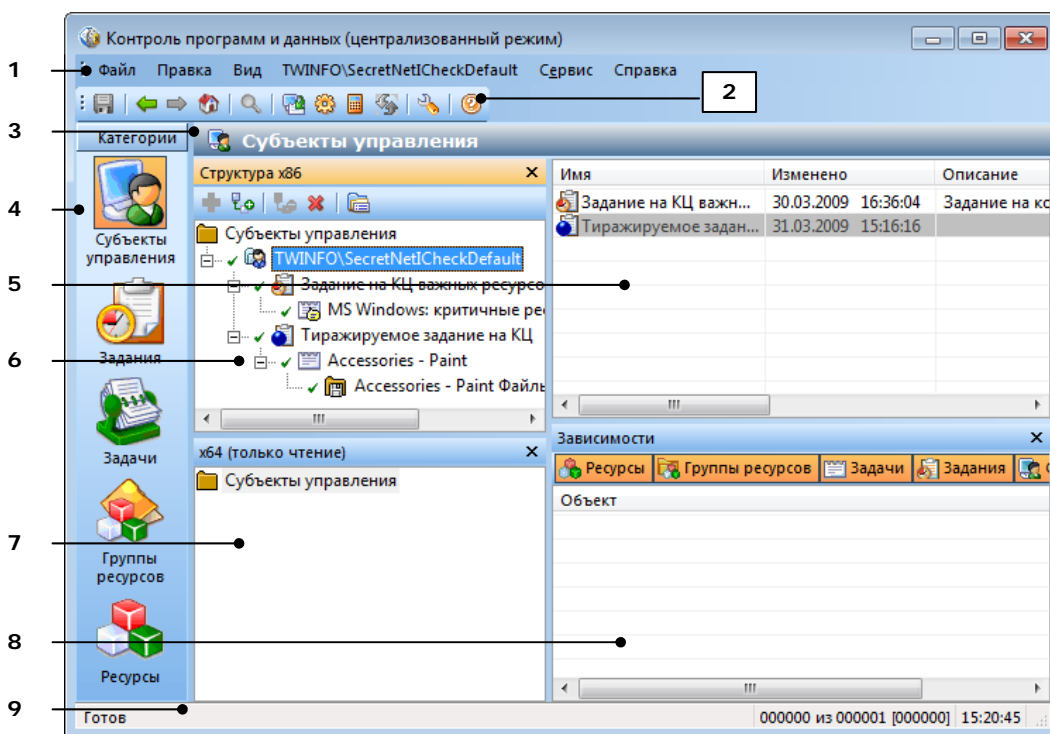
Приложение

Интерфейс программы "Контроль программ и данных"

Для того чтобы работать с программой в централизованном режиме, администратор безопасности должен входить в доменную группу администраторов или в доменную группу SecretNetAdmins (см. стр. 10). Чтобы работать с программой в локальном режиме, пользователь должен входить в локальную группу администраторов.

Интерфейс программы

При заданной по умолчанию настройке интерфейса основное окно программы управления выглядит следующим образом:











На рисунке представлен пример основного окна программы в централизованном режиме работы.

Основное окно программы может содержать следующие элементы интерфейса:





| |
|--|
| (1) Меню |
| Содержит команды управления программой |
| (2) Панель инструментов основного окна |
| Содержит кнопки быстрого вызова команд управления и программных средств |
| (3) Информационный заголовок |
| Содержит название выбранной для отображения категории объектов |
| (4) Панель категорий |
| Содержит ярлыки для выполнения одноименных команд меню "Вид". Чтобы отобразить в программе объекты, относящиеся к нужной категории, выберите на этой панели ее ярлык |
| (5) Область списка объектов |
| Содержит в виде таблицы список объектов, входящих в объект, выбранный в окне структуры. Строка таблицы выделяется соответствующим цветом, если объект находится в одном из следующих состояний: |
| <ul style="list-style-type: none"> • объект связан с вышестоящими и нижестоящими объектами — по умолчанию фон текста белый; • объект не связан с вышестоящими или нижестоящими объектами — по умолчанию фон розовый; • ресурс не поставлен на контроль — по умолчанию фон текста серый. |
| В локальном режиме объекты, созданные централизованно, отображаются жирным шрифтом. Параметры цветового оформления можно изменить (см. стр. 92) |

(6) Окно структуры

Содержит иерархический список объектов. Корневым элементом иерархии является выбранная категория объектов. Для обозначения объектов используются следующие пиктограммы:

 — субъект;  — задание ЗПС;  — тиражируемое задание ЗПС;  — задание КЦ;  — тиражируемое задание КЦ;  — задание ПАК "Соболь";  — задача;  — задача со сценарием.

Для отображения наличия связей между объектами используются следующие пиктограммы:

-  (нижняя половина кружка красная) — объект не включает в себя другие объекты;
-  (верхняя половина кружка красная) — объект не включен ни в один из других объектов;
-  — объект не имеет связей;
-  — для объекта установлены все предполагаемые связи с другими объектами.

Кнопки панели инструментов этого окна предназначены для управления списком объектов.

Окно структуры содержит список объектов той модели данных, которая соответствует разрядности ОС Windows на компьютере. Список объектов доступен для редактирования

(7) Окно структуры модели данных другой разрядности

Присутствует только в централизованном режиме работы программы. По своему назначению окно аналогично окну структуры (6), но содержит список объектов модели данных другой разрядности, чем ОС Windows на компьютере (например, модели для 64-разрядных версий ОС Windows, если на компьютере установлена 32-разрядная ОС).

Список объектов отображается в режиме "только для чтения". Можно копировать объекты в окно структуры (6) — для этого вызовите контекстное меню нужного объекта и активируйте команду "Добавить в рабочую модель..."

(8) Окно зависимостей

Содержит список объектов, связанных с объектом, который выбран в области списка объектов. В верхней части окна расположены кнопки, управляющие фильтрацией объектов списка

(9) Строка состояния

Содержит служебные сообщения программы. В правой части строки выделены зоны, в которых помещается следующая информация (по порядку слева направо):

- порядковый номер выбранного объекта, общее количество и количество выделенных объектов в области списка объектов или в дополнительном окне зависимостей;
- текущее время.

Настройка элементов интерфейса

Для удобства работы с программой пользователь может изменять состав отображаемых элементов интерфейса и управлять их размещением в основном окне программы. Внешний вид основного окна сохраняется в системном реестре и используется в следующих сеансах работы пользователя с программой.

Меню и панель инструментов можно перемещать в любое место экрана стандартными способами, принятыми в приложениях ОС Windows.

Панель категорий всегда располагается по левому краю основного окна программы. Положение дополнительных окон зафиксировано и не может быть изменено. Для изменения размеров панели и дополнительных окон используются их внутренние границы.

Управление элементами интерфейса осуществляется командами меню "Вид":

| Команда | Описание |
|---|--|
| Вид Строка состояния | Включает или отключает отображение строки состояния (9) |
| Вид Панели Кнопки | Включает или отключает отображение панели инструментов (2) |
| Вид Панели Заголовок | Включает или отключает отображение информационного заголовка (3) |
| Вид Панели Категории | Включает или отключает отображение панели категорий (4) |
| Вид Панели Структура | Включает или отключает отображение окна структуры (6) |
| Вид Панели Структура на чтение | Включает или отключает отображение окна структуры модели данных другой разрядности (7) |
| Вид Панели Зависимости | Включает или отключает отображение окна зависимостей (8) |

Параметры работы программы

Настройка параметров работы программы осуществляется в диалоге "Настройки приложения". Описание параметров приводится ниже.

Для настройки параметров:

1. Активируйте команду "Сервис | Настройки...".
На экране появится диалог "Настройки приложения".
2. Последовательно выбирая названия групп из списка в левой части диалога, укажите необходимые значения параметров (параметры представлены в правой части). В большинстве случаев для изменения значения параметра выберите нужное значение из раскрывающегося списка.

Группа параметров "Общие | Подтверждения"

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

Группа параметров "Общие | Цвета элементов списка"

Содержит параметры цветового оформления строк таблицы, расположенной в области списка объектов. Ячейка со значением каждого параметра содержит прямоугольник, окрашенный текущим выбранным цветом. Изменение значения параметра осуществляется с использованием стандартных средств выбора цвета, которые вызываются кнопкой в правой части ячейки.

| |
|---|
| Текст |
| Определяет цвет символов для отображения сведений об объектах, которые связаны и с вышестоящими, и с нижестоящими объектами иерархии |
| Фон |
| Определяет цвет фона строки для отображения сведений об объектах, которые связаны и с вышестоящими, и с нижестоящими объектами иерархии |
| Текст ошибки |
| Определяет цвет символов для отображения сведений об объектах, которые не связаны с вышестоящими или нижестоящими объектами |
| Фон ошибки |
| Определяет цвет фона строки для отображения сведений об объектах, которые не связаны с вышестоящими или нижестоящими объектами |
| Текст (неконтролируемые) |
| Определяет цвет символов для отображения: <ul style="list-style-type: none"> • сведений о ресурсах, для которых не включен признак контроля целостности; • заданий контроля целостности, у которых отсутствует расписание; • заданий ПАК "Соболь" при отсутствии самой платы на компьютере (в локальном режиме работы программы). |
| Фон (неконтролируемые) |
| Определяет цвет фона строки для отображения: <ul style="list-style-type: none"> • сведений о ресурсах, для которых не включен признак контроля целостности; • заданий контроля целостности, у которых отсутствует расписание; • заданий ПАК "Соболь" при отсутствии самой платы на компьютере (в локальном режиме работы программы). |
| Текст (нелокальные) |
| Определяет цвет символов для отображения сведений о ресурсах, которые находятся на других компьютерах и являются для данного компьютера сетевыми ресурсами. Используется только в локальном режиме работы программы |
| Фон (нелокальные) |
| Определяет цвет фона строки для отображения сведений о ресурсах, которые находятся на других компьютерах и являются для данного компьютера сетевыми ресурсами. Используется только в локальном режиме работы программы |

Группа параметров "Общие | Интерфейс"

Содержит отдельные параметры интерфейса, не относящиеся к вышеперечисленным группам.

Диалог при подготовке к ЗПС

Если установлено значение "Да", при запуске процедуры подготовки ресурсов для включения их в механизм замкнутой программной среды (например, по команде "Сервис | Ресурсы ЗПС") на экране появится диалог для настройки параметров поиска ресурсов. Если установлено значение "Нет", диалог не будет выводиться на экран и для подготовки ресурсов будут использованы параметры, заданные в группе параметров "Инструментарий | Подготовка для ЗПС" (см. ниже)

Диалог расчета эталонов

Если установлено значение "Да", то при запуске процедуры расчета эталонных значений для контроля целостности (например, по команде "Сервис | Эталоны | Расчет") на экране появится диалог настройки параметров расчета. Если установлено значение "Нет", диалог не выводится на экран, а для расчета эталонных значений используются параметры, заданные в группе параметров "Инструментарий | Расчет эталонов" (см. ниже)

Сетка в списке

Если установлено значение "Да", в области списка объектов и в дополнительном окне зависимостей отображаются линии, разделяющие ячейки таблиц

Группа параметров "Инструментарий | Подготовка для ЗПС"

Содержит параметры, задаваемые по умолчанию при подготовке списка ресурсов для включения их в механизм замкнутой программной среды.

Перевыбор выполняемых

Если установлено значение "Да", перед поиском выполняемых ресурсов (файлов) программа автоматически сбрасывает признак "выполняемый" со всех ресурсов, имеющихся в модели данных. Это позволяет установить признак "выполняемый" только для тех ресурсов, которые удовлетворяют заданным параметрам поиска. Если установлено значение "Нет", сброс признака не осуществляется

Расширения выполняемых

Содержит список расширений файлов, который используется при поиске выполняемых ресурсов или добавлении новых ресурсов в модель данных (кроме добавления единичных файлов). Признаки "выполняемый" будут установлены для тех файлов, расширения которых входят в этот список. Изменение значения параметра осуществляется редактированием текстового содержимого поля. Список расширений оформляется следующим образом: `.<расширение1>; <...>; .<расширениеN>`

Добавлять модули

Если установлено значение "Да", при поиске выполняемых ресурсов программа дополнительно включает в список ресурсов "зависимые модули" (файлы, от которых зависит выполнение исходных файлов, например, все библиотеки, необходимые для запуска winword.exe). При отсутствии в модели данных описания зависимого модуля оно будет автоматически создано и добавлено в группу ресурсов, содержащую описание исходного файла. Включение зависимых модулей в список осуществляется рекурсивно — файлы, от которых зависит выполнение самих зависимых модулей, также включаются в список.

Если установлено значение "Нет", поиск зависимых модулей не осуществляется

Группа параметров "Инструментарий | Расчет эталонов"

Содержит значения по умолчанию для параметров процедуры расчета эталонных значений.

Оставлять старые

Если установлено значение "Да", рассчитанные ранее эталонные значения будут сохранены в списке эталонных значений ресурса после очередной процедуры расчета. Если установлено значение "Нет", все рассчитанные ранее эталоны удаляются

Не поддерживается

Определяет реакцию программы в случае, если определенный в задании метод или алгоритм контроля целостности неприменим к ресурсу:

- "Игнорировать" — никакие действия не предпринимаются;
- "Выводить запрос" — на экран выводится диалог для выбора варианта продолжения процедуры;
- "Удалять ресурс" — ресурс удаляется из общего списка ресурсов (из модели данных);
- "Ресурс снимать с контроля" — для ресурса сбрасывается признак "контролировать".

Нет доступа

Определяет реакцию программы в случае, если при попытке расчета эталонного значения программа не получила доступ к ресурсу (например, отсутствует доступ на чтение файла или файл заблокирован другим процессом). Выбор вида реакции осуществляется так же, как для параметра "Не поддерживается"

Ресурс отсутствует

Определяет реакцию программы в случае, если при попытке расчета эталонного значения программа не обнаружила ресурс (например, файл был перемещен). Выбор вида реакции осуществляется так же, как для параметра "Не поддерживается"

Группа параметров "Инструментарий | Импорт и добавление"

Содержит значения по умолчанию для параметров процедур импорта объектов и добавления ресурсов в модель данных.

С учетом существующих

Если установлено значение "Да", то при импорте объектов, одноименных объектам текущей модели данных, они замещают объекты модели. Если установлено значение "Нет", то объекты модели остаются неизменными, а импортируемые объекты переименовываются следующим образом: *имя_объекта < N >*, где "N" — порядковый номер дублируемого объекта (например, "Группа ресурсов" и "Группа ресурсов1")

Помечать выполняемые

Если установлено значение "Да", то при добавлении новых файлов в модель данных (кроме добавления единичных файлов) автоматически выполняется проверка их расширений. Программа устанавливает признак "выполняемый" для тех файлов, расширения которых входят в список "Расширения выполняемых". Если установлено значение "Нет", такая проверка не выполняется

Группа параметров "Оповещения | Общие"

Содержит единственный параметр рассылки оповещений об изменениях в модели данных. Используется только в режиме централизованного управления.




Рассылка при сохранении

Если установлено значение "Да", при сохранении модели данных на все компьютеры домена, в отношении которых модель данных изменилась, будет отправлено оповещение об изменениях

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.

| 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 |

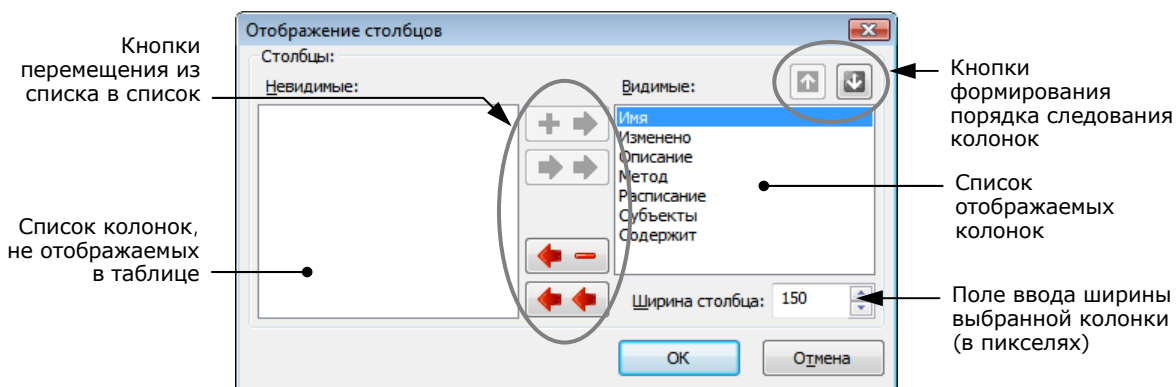
Настройка отображения колонок в таблицах

В области списка объектов и в окне зависимостей используется табличная форма представления списков объектов. Состав колонок таблицы зависит от того, объекты какой категории отображаются. Для оптимального отображения информации можно изменять ширину колонок, добавлять или удалять колонки либо перемещать колонки относительно других. Эти действия аналогичны стандартным операциям в ОС 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.

Сортировка списков объектов

Таблицы в области списка объектов и окна зависимостей сортируются по значениям, содержащимся в определенных колонках. Способы сортировки аналогичны стандартным способам управления таблицами, принятым в большинстве приложений Windows. В заголовке колонки, по которой отсортирована таблица, указывается соответствующее направление сортировки.

Поиск объектов в списках

Поиск осуществляется по значениям, содержащимся в отображаемых колонках таблицы из области списка объектов или дополнительного окна зависимостей.

Для поиска объекта:

1. Выберите в таблице объект, с которого начнется поиск.
2. Активируйте команду "Правка | Найти...".
На экране появится диалог настройки параметров поиска.
3. В поле "Что" введите строку поиска и при необходимости настройте параметры поиска. Нажмите кнопку "ОК".

| |
|--|
| Учитывать регистр |
| Если поле содержит отметку, будут найдены только те объекты, в сведениях о которых содержится заданная строка символов в том же регистре. При отсутствии отметки регистр символов не учитывается |
| Целиком значение |
| Если поле содержит отметку, будут найдены только те объекты, в сведениях о которых заданная строка символов содержится в виде отдельного слова (слов). При отсутствии отметки строка символов может являться частью других строк |
| Искать в поле |
| Если поле содержит отметку, поиск в таблице осуществляется только по значениям колонки, имя которой выбрано в поле справа. При отсутствии отметки поиск ведется во всех отображаемых в таблице колонках |

Программа выполнит поиск и выделит найденный объект в таблице. Если искомая строка не найдена, на экране появится соответствующее сообщение.

Чтобы найти другие объекты, удовлетворяющие заданным параметрам поиска, процедуру поиска можно продолжить, начиная с текущего выбранного объекта.

Переходы по связям объектов

При правильной организации модели данных каждый объект должен входить в одну или несколько цепочек связанных между собой ("зависимых") объектов. Если требуется определить, с какими объектами связан данный объект, используется окно зависимостей (см. стр. 91).

Для перехода к связанному объекту:

1. В области списка объектов выберите объект или группу объектов.
В окне зависимостей появится список объектов.
2. При необходимости настройте в окне зависимостей фильтрацию по категориям представления объектов. Для переключения режима фильтрации могут использоваться ярлыки в верхней части окна зависимостей.
3. В списке объектов окна зависимостей найдите объект, к которому требуется перейти в структуре объектов, вызовите контекстное меню объекта и активируйте команду "Перейти в дереве".

В окне структуры будет раскрыта соответствующая ветвь дерева и выделен искомый объект.

Настройка исключений для замкнутой программной среды

Администратор может создать список процессов, для которых исключается действие механизма ЗПС при запуске файлов из определенных каталогов, в том числе и из вложенных каталогов. Факты запуска таких файлов регистрируются в журнале в виде события "Использование исключения в механизме ЗПС". С помощью этой функции реализуется возможность запуска в "жестком" режиме ЗПС таких программ, как, например, Photoshop CS2 и SolidWorks.

Создание и редактирование списка процессов, для которых будет действовать исключение, осуществляется локально в системном реестре компьютера.

Для составления списка процессов:

1. В системном реестре создайте ключ HKLM\SYSTEM\CurrentControlSet\Services\SnExeQuota\Parameters\ и добавьте в него параметр PList типа REG_MULTI_SZ.
2. Отредактируйте значение созданного параметра. Необходимо указать пары вида <имя_процесса> <путь_к_каталогу>. Каждая пара вводится в две строки: в первой строке имя процесса, во второй — путь. Имя процесса нужно ввести так, как подсистема ЗПС регистрирует события запуска программ в данной операционной системе. Если компьютер работает под управлением ОС Windows 2000, указывается только имя процесса. Для других ОС — полный путь к исполняемому модулю процесса. В каждой паре указывается один путь. Если необходимо указать несколько путей для одного процесса, нужно создать отдельные пары для каждого пути.
3. Для ключа HKLM\SYSTEM\CurrentControlSet\Services\SnExeQuota\Parameters назначьте разрешения таким образом, чтобы доступ к этому ключу был предоставлен только администраторам и системе.
4. Завершив редактирование реестра, перезагрузите компьютер.

Ресурсы, устанавливаемые на контроль целостности

В данном разделе приведен перечень ресурсов, устанавливаемых на контроль целостности при первом запуске программы "Контроль программ и данных".

Для всех ресурсов используется метод контроля "проверка содержимого". В качестве реакции на нарушение целостности осуществляется регистрация события.

| Тип ресурса | Ресурс |
|---|--|
| Ключ реестра | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run |
| | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce |
| | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx |
| | HKLM\System\CurrentControlSet\Services |
| | HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components |
| | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler |
| | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad |
| | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks |
| | HKLM\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved |
| | HKLM\Software\Classes\Folder\ShellEx\ColumnHandlers |
| | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects |
| | HKLM\Software\Microsoft\Internet Explorer\Extensions |
| | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options |
| | HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls |
| | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify |
| | HKLM\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries |
| | HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors |
| HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers | |
| HKLM\SOFTWARE\Microsoft\Internet Explorer\Toolbar | |
| Параметр реестра | HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute |
| | HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms |
| | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDll |
| | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\UIhost |
| | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit |
| | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell |
| | HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations |
| | HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs |
| | HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages |
| | HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages |
| | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Startup |
| | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Startup |

Настройка системы для оперативной синхронизации заданий КЦ-ЗПС

На компьютерах под управлением ОС Windows XP и выше по умолчанию синхронизация централизованно заданных заданий КЦ-ЗПС осуществляется при перезагрузке компьютера или при входе пользователя в систему. Чтобы синхронизация выполнялась незамедлительно, следует выполнить настройку параметров ОС Windows в соответствии с описанной ниже процедурой.

Для настройки параметров:

1. Разрешите использование TCP-порта 21327 на всех компьютерах, работающих под управлением ОС Windows XP и выше. Кроме того, разрешите использование указанных портов на устройствах, контролирующих сетевой трафик между этими компьютерами.
2. На компьютерах разрешите RPC-вызовы от неаутентифицированных клиентов. Для этого средствами централизованного управления в групповой политике домена или нужного организационного подразделения установите для параметра "Конфигурация компьютера | Административные шаблоны | Система | Удаленный вызов процедур (RPC) | Ограничения для не прошедших проверку RPC-клиентов" значение "Включен", а дополнительному параметру присвойте значение "Отсутствует".

Англоязычное название параметра "Computer Configuration | Administrative Templates | System | Remote Procedure Call | Restrictions for Unauthenticated RPC clients".

3. На компьютерах разрешите анонимное соединение с именованным каналом. Для этого:
 - средствами централизованного управления в групповой политике домена или организационного подразделения добавьте значение "SnlcheckSrv" в список параметра "Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Параметры безопасности | Network access: Named Pipes that can be accessed anonymously";
 - или на каждом компьютере средствами управления локальной политикой добавьте значение "SnlcheckSrv" в список параметра "Локальные политики | Параметры безопасности | Network access: Named Pipes that can be accessed anonymously".

В ОС Windows 2000 добавьте значение "SnlcheckSrv" в список параметра реестра HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes.

Централизованное управление списком расширений исполняемых файлов

Для корректного применения централизованно заданных заданий ЗПС необходимо, чтобы на компьютерах системы использовались одинаковые списки расширений исполняемых файлов. Используемый по умолчанию список расширений можно изменить локально в программе управления КЦ-ЗПС при настройке параметров программы (см. стр. 92). Для большого количества компьютеров можно использовать возможность централизованного задания списка с помощью механизма групповых политик и специального файла административного шаблона.

Процедура настройки системы для централизованного задания списка расширений исполняемых файлов состоит из следующих этапов:

1. Создание организационного подразделения для группы компьютеров.
2. Создание групповой политики и добавление административного шаблона.
3. Включение и настройка административного шаблона.

Создание организационного подразделения

Чтобы выделить компьютеры домена, на которых будет централизованно задан список расширений исполняемых файлов, необходимо создать организационное подразделение (Organization Units) и включить в него нужные компьютеры. Также для этих целей можно использовать имеющиеся организационные подразделения.

Создание организационного подразделения и добавление объектов осуществляется стандартными способами.

Создание групповой политики и добавление шаблона

Для организационного подразделения необходимо создать групповую политику, с помощью которой будет осуществляться централизованное задание списка расширений.

Для создания групповой политики на контроллере домена под управлением ОС Windows 2008 (нерусифицированная версия):

1. Вызовите консоль "Group Policy Management".
2. Вызовите контекстное меню организационного подразделения и активируйте команду "Create a GPO in this domain, and Link it here".
3. В появившемся диалоге введите имя создаваемой политики и нажмите кнопку "OK".

Новая политика появится в иерархическом списке в качестве подчиненного объекта организационного подразделения.

4. Вызовите контекстное меню политики и активируйте команду "Edit".
На экране появится окно редактора групповых политик.
5. В дереве объектов политики вызовите контекстное меню раздела "Computer Configuration\Policies\Administrative templates..." и активируйте команду "Add/Remove Templates...".
На экране появится диалог "Add/Remove Templates".
6. В диалоге нажмите кнопку "Add ...".
На экране появится стандартный диалог выбора файла.
7. Выберите файл ExtExe.adm, расположенный на установочном компакт-диске системы Secret Net 6 в подкаталоге \Tools\Infosec\ExeExt\
8. Нажмите кнопку "Close" в диалоге "Add/Remove Templates".

В разделе "Computer Configuration\Policies\Administrative templates..." появится подраздел "Classic Administrative Templates (ADM)\Secret Net Integrity Check settings".

Для создания групповой политики на контроллере домена под управлением ОС Windows 2000/2003 (русифицированная версия):

1. Откройте оснастку "Active Directory — Пользователи и Компьютеры", выберите организационное подразделение и вызовите диалоговое окно настройки свойств организационного подразделения.
2. Перейдите на вкладку "Групповая политика" и нажмите кнопку "Создать".
3. Введите имя создаваемой политики и нажмите клавишу <Enter>.
4. Нажмите кнопку "Изменить".

На экране появится окно редактора групповых политик.

5. В дереве объектов политики вызовите контекстное меню раздела "Конфигурация компьютера\Административные шаблоны" и активируйте команду "Добавление и удаление шаблонов...".

На экране появится диалог "Добавление и удаление шаблонов".

6. В диалоге нажмите кнопку "Добавить...".

На экране появится стандартный диалог выбора файла.

7. Выберите файл ExtExe.adm, расположенный на установочном компакт-диске системы Secret Net 6 в подкаталоге \Tools\Infosec\ExeExt\

8. Нажмите кнопку "Закреть" в диалоге "Добавление и удаление шаблонов".

В разделе "Конфигурация компьютера\Административные шаблоны" появится подраздел "Secret Net Integrity Check settings".

Включение и настройка административного шаблона

После добавления административного шаблона в групповую политику осуществляется включение действия шаблона и редактируется список расширений выполняемых файлов.

Для включения действия шаблона на контроллере домена под управлением ОС Windows 2008 (нерусифицированная версия):

1. Вызовите консоль "Group Policy Management".
2. Вызовите контекстное меню политики, созданной для организационного подразделения, и активируйте команду "Edit".

На экране появится окно редактора групповых политик.

3. В дереве объектов политики перейдите к разделу "Computer Configuration\Policies\Administrative templates...\Classic Administrative Templates (ADM)\Secret Net Integrity Check settings" и вызовите диалоговое окно настройки свойств параметра "Extensions Executive".

4. Установите отметку в поле "Enabled" и затем отредактируйте нужным образом содержимое поля "Extensions Executive". Список расширений оформляется следующим образом: *.<расширение1> <...> .<расширениеN>*. По умолчанию представлены расширения: .dll .exe .cpl .drv.

5. Нажмите кнопку "ОК".

Для включения действия групповой политики на контроллере домена под управлением ОС Windows 2000/2003 (русифицированная версия):

1. Откройте оснастку "Active Directory — Пользователи и Компьютеры", выберите организационное подразделение и вызовите диалоговое окно настройки свойств организационного подразделения.

2. Перейдите на вкладку "Групповая политика", выберите созданную политику и нажмите кнопку "Изменить".

На экране появится окно редактора групповых политик.

3. В дереве объектов политики перейдите к разделу "Конфигурация компьютера\Административные шаблоны".

4. В меню "View" активируйте команду "Фильтрация..." ("Filtering").

5. В появившемся диалоге удалите отметку из поля "Показывать только управляемые параметры политики" ("Only show policy settings that can be fully managed") и нажмите кнопку "ОК".

6. В подразделе "Secret Net Integrity Check settings" вызовите диалоговое окно настройки свойств параметра "Extensions Executive".
7. Установите отметку в поле "Включен" и затем отредактируйте нужным образом содержимое поля "Extensions Executive". Список расширений оформляется следующим образом: *.<расширение1> <...> .<расширениеN>*. По умолчанию представлены расширения: *.dll .exe .cpl .drv*.
8. Нажмите кнопку "ОК".

Контролируемые устройства

Табл. 2. Группы и классы устройств

| Группа | Класс |
|----------------------------------|---------------------------------------|
| Локальные устройства | Последовательные порты |
| | Параллельные порты |
| | Сменные диски |
| | Оптические диски |
| | Логические диски |
| | Физические диски |
| | Процессоры |
| | Оперативная память |
| | Системная плата |
| | Сетевые платы |
| | Аппаратная поддержка |
| Устройства USB | Звук |
| | Соединения |
| | Устройства интерфейса с пользователем |
| | Мониторинг |
| | Аппаратный интерфейс |
| | Устройства захвата изображений |
| | Принтер |
| | Хранение данных |
| | Универсальный концентратор для USB |
| | Управление данными |
| | Микросхема (Смарт-карта) |
| | Устройства защиты данных |
| | Видео |
| | Диагностические устройства |
| | Контроллер беспроводного доступа |
| | Определяемые приложением |
| Прочие | |
| Устройства PCMCIA | Многофункциональное устройство |
| | Память |
| | Последовательные порты |
| | Параллельные порты |
| | Физические диски |
| | Видео |
| | Сетевые платы |
| | AIMS |
| | SCSI |
| | Устройства защиты данных |
| | Прочие |
| Устройства IEEE1394 | Сетевые устройства |
| | Системные устройства |
| | Устройства SBP-2 |
| | Мультимедиа устройства |
| | Прочие |
| Устройства Secure Digital | Карточки памяти |
| | Прочие |

Использование терминального доступа

В системе Secret Net 6 возможности механизма защиты входа в систему могут в полном объеме использоваться и при терминальном входе пользователя на удаленный компьютер. Для этого необходимо:

- установить клиентское ПО системы Secret Net 6 на всех компьютерах, с которых выполняется вход (далее — клиенты), а также на всех компьютерах, к которым выполняется подключение (далее — серверы). При использовании средств аппаратной поддержки (например, USB-ключей eToken) необходимо установить на клиентах и серверах программное обеспечение средств аппаратной поддержки;
- выполнить для всех клиентов и серверов, которые используются для организации терминального доступа, настройку параметров ОС Windows в соответствии с описанной ниже процедурой.

Для настройки параметров:

1. Разрешите использование TCP-портов 139, 445, 21326 на всех клиентах и серверах. Кроме того, разрешите использование указанных портов на всех устройствах, контролирующих сетевой трафик между этими компьютерами.
2. На всех клиентах и серверах, работающих под управлением ОС Windows, разрешите RPC-вызовы от неаутентифицированных клиентов. Для этого средствами централизованного управления в групповой политике домена или нужного организационного подразделения установите для параметра "Конфигурация компьютера | Административные шаблоны | Система | Удаленный вызов процедур (RPC) | Ограничения для не прошедших проверку RPC-клиентов" значение "Включен", а дополнительному параметру присвойте значение "Отсутствует".

Англоязычное название параметра "Computer Configuration | Administrative Templates | System | Remote Procedure Call | Restrictions for Unauthenticated RPC clients".

3. На всех клиентах и серверах разрешите анонимное соединение с именованным каналом. Для этого:
 - средствами централизованного управления в групповой политике домена или организационного подразделения добавьте значение "SnHwSrv" в список параметра "Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Параметры безопасности | Network access: Named Pipes that can be accessed anonymously";
 - или на каждом компьютере средствами управления локальной политикой добавьте значение "SnHwSrv" в список параметра "Локальные политики | Параметры безопасности | Network access: Named Pipes that can be accessed anonymously".

В ОС Windows 2000 добавьте значение "SnHwSrv" в список параметра реестра HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes.

После того как все указанные действия выполнены, идентификация и аутентификация пользователей при терминальном входе будут выполняться в соответствии с настройкой параметров механизма защиты входа в систему. После успешного терминального входа на компьютер действия пользователя будут контролироваться Secret Net 6 так же, как и при локальном входе пользователя.



Примечание. Пользователь, от имени которого осуществляется доступ на терминальный сервер, должен проходить аутентификацию по правилам Windows на терминальном клиенте. Например, это может быть доменный пользователь общего для терминального сервера и клиента домена. Терминальный вход от имени локального пользователя терминального сервера, который не имеет доступа (не может аутентифицироваться) на терминальном клиенте, может привести к невозможности работы с электронными идентификаторами во время сеанса терминального доступа.

Рекомендации по настройке Secret Net 6 на кластере

Кластерные технологии позволяют объединить группу компьютеров (узлов), независимо работающих под управлением своих ОС, в единый сервер. При настройке клиентов системы Secret Net 6, установленных на кластер, учитывайте следующие рекомендации:

- 1** Все службы клиентского ПО должны постоянно работать на всех узлах кластера, включая неактивные. Эти службы не следует кластеризовать, то есть включать в ресурс, которым управляет сервис кластеров. Иначе при переключении будет потеряна работоспособность системы защиты на неактивных узлах, а механизм функционального контроля заблокирует работу кластера, определив отсутствие базовых компонентов системы защиты.
 - 2** Общий ресурс (логический диск) не следует включать в перечень средств, которые контролируются механизмом контроля аппаратной конфигурации. Иначе при переключении узлов кластера этим механизмом будет зафиксировано нарушение аппаратной конфигурации компьютера.
 - 3** Общий ресурс (физический диск) также не следует включать в перечень средств, которые контролируются механизмом контроля аппаратной конфигурации. Такой ресурс при загрузке операционной системы может определяться ОС позже запуска данного механизма защиты, что приведет к фиксации нарушения аппаратной конфигурации компьютера.
- Примечание.** Аналогичная ситуация может возникать и на одиночном компьютере, на котором установлены несколько SCSI-дисков.
- 4** Не следует включать контроль целостности для файлов, размещенных на общем ресурсе. Это вызвано тем, что при переходе узла кластера в неактивное состояние он теряет доступ к общему ресурсу. В случае если для данного узла процедура контроля была предусмотрена, то в момент ее проведения будет зафиксировано нарушение целостности объектов, поставленных на контроль.
 - 5** При настройке замкнутой программной среды для пользователя не следует указывать локальный путь для исполняемых файлов, размещенных на общем ресурсе кластера. В этом случае необходимо использовать сетевые пути для разрешенных исполняемых модулей.
 - 6** Для автономного режима функционирования клиента Secret Net 6 необходимо установить на всех узлах кластера тождественные настройки доменных пользователей. В противном случае работа системы Secret Net 6 будет отличаться в зависимости от того, какой узел активен. Данная рекомендация наиболее актуальна для функционирования механизма полномочного управления доступом, поскольку этот механизм обрабатывает сетевые обращения к файлам и определяет возможность доступа к ним, используя настройки пользователей, размещенные в локальной базе данных на кластере.

Применение параметров групповой политики при обновлении

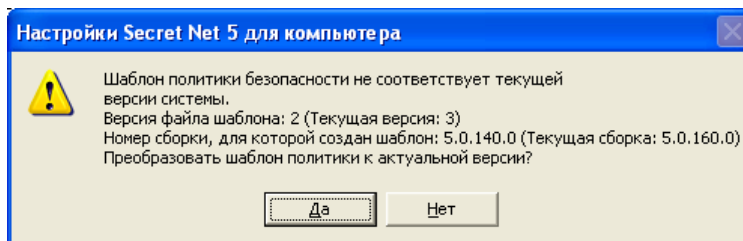
Параметры групповых политик Secret Net 6 и их значения хранятся в специальных файлах-шаблонах. При развертывании системы Secret Net 6 эти файлы-шаблоны помещаются в каталог \SYSVOL контроллера домена. Наряду с другими параметрами в файле-шаблоне хранится информация о версии Secret Net 6, поставляемая в составе дистрибутива системы.

Переход на новую версию Secret Net 6 выполняется обновлением компонентов системы. Обновление должно выполняться в определенном порядке, описанном в документе [2].

При обновлении Secret Net 6 информация о номере версии в файле-шаблоне не изменяется, поэтому для корректной работы системы шаблон необходимо преобразовать. В результате преобразования в файл шаблона записывается номер новой версии.

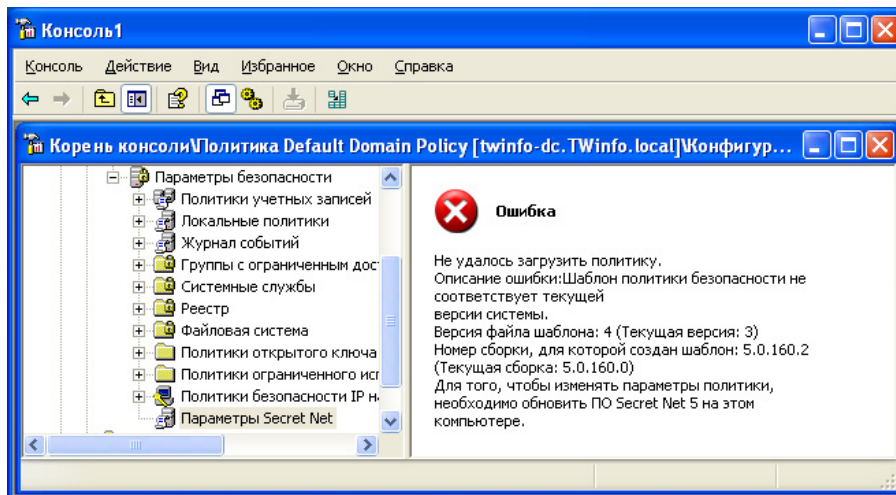
Если обновление Secret Net 6 было выполнено не в полном объеме или не было выполнено преобразование файла шаблона, это может привести к некорректной работе, вызванной несоответствием версий компонентов системы. Некорректная работа проявляется в 2 случаях:

1. Номер версии, хранящийся в файле шаблона, отличается от номера версии клиентского ПО Secret Net 6 компьютера, с которого осуществляется редактирование групповых политик. При этом возможны 2 варианта:
 - Номер версии файла шаблона старый, а номер версии клиентского ПО новый. В этом случае в групповой политике при обращении к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 11) на экране появится предупреждение о несоответствии версий:



Указываются номер версии, хранящийся в файле шаблона, и номер текущей (новой) версии, установленной на компьютере, с которого осуществляется редактирование групповых политик.

- Для преобразования файла шаблона нажмите кнопку "Да". Шаблон будет преобразован и приведен в соответствие текущей (новой) версии системы Secret Net 6.
- Для отказа от преобразования шаблона нажмите "Нет". В этом случае редактирование групповых политик с данного компьютера будет недоступно.
- Номер версии файла шаблона новый (полученный в результате преобразования шаблона), а номер версии клиентского ПО — старый. В этом случае при попытке доступа к параметрам Secret Net 6 в правой части оснастки появится сообщение об ошибке.



Редактирование групповой политики с данного компьютера возможно только после обновления на нем клиентского ПО Secret Net 6.

2. Номер версии, хранящийся в файле шаблона, отличается от номера версии клиентского ПО Secret Net 6 компьютера, к которому применяются групповые политики. При этом также возможны 2 варианта:
 - Номер версии файла шаблона старый, а номер версии клиентского ПО — новый. В этом случае в действующую политику будут занесены значения только тех параметров, которые входят и в состав файла шаблона, и в состав обновленного клиентского ПО. При этом в журнале безопасности регистрируется предупреждение о несовпадении версий файла шаблона и версии клиентского ПО. Файл шаблона остается без изменений.
 - Номер версии файла шаблона новый, а номер версии клиентского ПО — старый. В этом случае групповая политика файла шаблона не применяется. В журнале регистрируется предупреждение о попытке применения более новой версии шаблона политики.

Восстановление системы после сбоев питания компьютера

В большинстве случаев внезапное отключение питания компьютера не приводит к потере работоспособности системы Secret Net 6 при следующих запусках. Однако возможны ситуации (в особенности если компьютер работает под управлением ОС Windows 2000), когда после сбоя питания происходит блокировка компьютера или другие проявления нештатного поведения системы.

В таких случаях проблемы могут возникать из-за повреждения следующих функциональных компонентов системы защиты:

- база данных КЦ-ЗПС;
- локальная база данных системы Secret Net 6;
- программные модули системы Secret Net 6.

Ниже приводится порядок действий администратора для восстановления работоспособности БД КЦ-ЗПС и ЛБД системы защиты. В дальнейшем для решения проблемы рекомендуется добавить подкаталоги \Icheck и \GroupPolicy, находящиеся в каталоге установки Secret Net 6, в список исключений из проверки антивирусом. Если описанные действия не приводят к устранению проблем, переустановите на компьютере ПО системы Secret Net 6 (см. документ [2]). При дальнейших проявлениях нештатного поведения системы обратитесь за консультацией в Службу технической поддержки компании "Информзащита".

Восстановление базы данных КЦ-ЗПС

При повреждении БД КЦ-ЗПС система во время загрузки компьютера продолжительное время ожидает старта подсистемы контроля целостности. Время ожидания может длиться до одного часа. Также для этих случаев характерны ошибки функционального контроля, сообщающие об отсутствии подсистемы КЦ-ЗПС.

Для восстановления БД КЦ-ЗПС:

- Удалите каталог \Icheck, расположенный в каталоге установки компонента "Secret Net 6", и перезагрузите компьютер.

После восстановления БД КЦ-ЗПС локальные параметры механизмов КЦ и ЗПС будут приведены в состояние по умолчанию. При загрузке компьютера автоматически выполняется синхронизация, в результате которой на компьютер загружаются централизованно заданные параметры. Ранее заданные локальные параметры потребуются восстановить вручную.

Восстановление локальной базы данных

При повреждении локальной базы данных системы Secret Net 6 во время загрузки компьютера возникают ошибки функционального контроля, сообщающие об отсутствии или неработоспособности ядра системы защиты.

Для восстановления локальной БД:

1. Запустите консоль командной строки (cmd.exe).
2. Перейдите в каталог \GroupPolicy, расположенный в каталоге установки компонента "Secret Net 6".
3. Последовательно введите команды del *.chk, del *.log и del *.edb.
4. Введите команду esentutil /p snet.sdb (на запрос ответить "ОК").
5. Снова введите команды del *.chk, del *.log и del *.edb.
6. Перезагрузите компьютер.

После восстановления локальной БД параметры Secret Net 6 в локальной политике безопасности будут приведены в состояние по умолчанию. При загрузке компьютера автоматически применяются централизованно заданные параметры в соответствии с действием механизма групповых политик. Параметры политики безопасности, ранее заданные локально, потребуются восстановить вручную.

Совет. Сохраняйте резервные копии параметров системы, используя функции экспорта (см. стр. 86). Импорт параметров из файла резервной копии позволяет существенно упростить процесс восстановления.

Терминологический справочник

А

- Администратор безопасности** Лицо или группа лиц, ответственных за обеспечение безопасности системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты
- Алгоритм контроля** Один из пяти стандартных алгоритмов, применяемых в методе контроля целостности "Содержимое": CRC7, ЭЦП, ХЭШ, имитовставка, полное совпадение
- Аппаратная конфигурация** Список устройств, входящих в состав защищаемого компьютера
- Аппаратные средства** Дополнительные устройства, применяемые для повышения эффективности защиты входа в систему: средства идентификации и аутентификации, программно-аппаратные комплексы "Соболь", изделия Secret Net Card и Secret Net Touch Memory Card
- Аутентификация** Проверка регистрационной информации о пользователе

В

- Вход в систему по идентификатору** Режим входа в систему, в котором вход разрешен только с помощью персонального идентификатора пользователя

Г

- Группа устройств** Одна из групп, на которые разделены все устройства, входящие в состав компьютера и подключаемые к нему. Для группы можно установить права доступа пользователей и задать параметры контроля аппаратной конфигурации

Ж

- Жесткий режим** Режим работы механизма системы Secret Net 6, обеспечивающий максимальный уровень защиты
- Журнал регистрации событий** Хранилище с информацией о событиях, зарегистрированных в системе защиты, например, попытках входа в систему

З

- Зависимые модули** Драйверы и библиотеки, не входящие непосредственно в запускаемые пользователем приложения, но без которых работа этих приложений невозможна
- Замкнутая программная среда** Режим работы системы защиты, при котором для каждого пользователя определяется перечень доступных ему программ. Совокупность этих программ и образует замкнутую среду работы пользователя
- Затирание данных** Предотвращение возможности восстановления удаленных файлов путем записи последовательности случайных чисел в область диска, где физически было расположено содержимое этих файлов

И

- Избирательный доступ** Избирательный (дискреционный) принцип разграничения доступа основан на матрице доступа – когда либо объекту ставится в соответствие список субъектов, имеющих к нему доступ, либо – наоборот

| | |
|---|---|
| Инициализация идентификатора | Форматирование, обеспечивающее возможность применения идентификатора с конкретным аппаратным устройством в системе Secret Net 6 |
| Интервал неактивности | Время, в течение которого не используются устройства ввода (мышь, клавиатура и т. п.) |
| К | |
| Категория объекта модели данных | В модели данных используются 5 категорий объектов: ресурсы, группы ресурсов, задачи, задания, субъекты |
| Класс устройств | Объединение устройств внутри группы по определенному признаку. Примеры классов: последовательные порты, физические диски, процессоры и т. п. Для класса можно установить права доступа пользователей и задать параметры контроля аппаратной конфигурации |
| Контроль аппаратной конфигурации | Отслеживание изменений в аппаратной конфигурации защищаемого компьютера |
| Контроль заголовков | В замкнутой программной среде дополнительный механизм, повышающий надежность разделения ресурсов на исполняемые и неисполняемые файлы, т. е. подлежащие и не подлежащие проверке |
| Контроль целостности | Проверка наличия несанкционированной модификации файлов и секторов жесткого диска защищаемого компьютера |
| Контрольная сумма | Числовое значение, вычисляемое по специальному алгоритму и используемое для контроля неизменности данных |
| Копирование ключей | Копирование ключевой информации пользователя из одного персонального идентификатора в другой |
| Л | |
| Локальное управление | Управление работой механизмов защиты на отдельном компьютере средствами локального администрирования |
| М | |
| Метод контроля | Один из применяемых в Secret Net 6 методов контроля целостности ресурсов: содержимое, атрибуты, права доступа, существование |
| Механизм защиты | Совокупность настраиваемых программных и аппаратных средств, ограничивающих доступ к информационным ресурсам, а также осуществляющих контроль действий пользователей и регистрацию событий, связанных с безопасностью |
| Модель данных | В контроле целостности и замкнутой программной среде — список объектов и описание связей между ними. Модель данных — это подробная инструкция для системы Secret Net 6, указывающая на то, какие ресурсы и как должны контролироваться |
| Мягкий режим работы | Один из возможных режимов работы механизма защиты. В мягком режиме допускаются несанкционированные действия пользователей. Несанкционированные действия фиксируются, но не блокируются системой. Режим, как правило, используется на этапе настройки или проверки работы механизма защиты |
| П | |
| Пакет контроля целостности | Список, содержащий информацию о местоположении контролируемых файлов и секторов на жестком диске и их контрольные суммы |

| | |
|---|---|
| Персональный идентификатор | Устройство, предназначенное для идентификации пользователя. В Secret Net 6 в качестве персональных идентификаторов могут использоваться USB-ключи eToken, iKey, Rutoken и электронные идентификаторы iButton |
| Подготовка ресурсов для ЗПС | В замкнутой программной среде — присвоение ресурсам признака "выполняемый". Ресурсы с таким признаком, входящие в задание ЗПС, образуют список разрешенных для запуска программ |
| Предварительная очистка модели данных | В механизмах контроля целостности и замкнутой программной среды — удаление из базы Secret Net 6 модели данных перед началом построения новой модели |
| Признак хранения ключа | В списке присвоенных пользователю идентификаторов — отметка, свидетельствующая о том, что в идентификаторе хранится закрытый ключ пользователя |
| Признак хранения пароля | В списке присвоенных пользователю идентификаторов — отметка, свидетельствующая о том, что в идентификаторе может храниться пароль пользователя |
| Присвоение идентификатора | Добавление в базу данных Secret Net 6 сведений о том, что пользователю присвоен персональный идентификатор, включая информацию о самом идентификаторе (тип, уникальный серийный номер) |
| Р | |
| Разграничение доступа к устройствам | Избирательное предоставление пользователям прав и привилегий на доступ к устройствам, входящим в состав компьютера |
| Режим хранения пароля в идентификаторе | Режим использования пользователем персонального идентификатора. В этом режиме пользователю предоставляется возможность хранить в идентификаторе пароль |
| С | |
| Связи между объектами | Связь означает, что объект подчиненной категории включен в объект вышестоящей категории, например, ресурс включен в группу ресурсов или задача включена в задание. Для объектов категорий "задание" и "субъект" связь означает, что задание назначено субъекту |
| Смешанный режим входа в систему | Режим входа в систему, в котором пользователю разрешается для ввода своих учетных данных использовать стандартные средства ОС Windows или предъявлять персональный идентификатор |
| Стандартный режим входа в систему | Режим входа в систему, в котором пользователь должен ввести свои учетные данные, используя только стандартные средства ОС Windows |
| У | |
| Утверждение конфигурации | Утверждение изменений в аппаратной конфигурации компьютера. Т. е. принятие текущей аппаратной конфигурации компьютера в качестве эталонной |
| Ц | |
| Централизованное управление | Управление работой системы защиты, осуществляемое администратором безопасности со своего рабочего места. Рабочим местом администратора безопасности может быть контроллер домена или любой компьютер сети с установленными средствами централизованного управления ОС Windows |

Э

Эталон Значения параметров контролируемого ресурса, по неизменности которых определяется его целостность

Эталонный компьютер Компьютер, на котором выполняется настройка механизмов защиты. После проверки корректности работы системы защиты параметры настройки средствами экспорта и импорта распространяются на другие компьютеры, имеющие такую же конфигурацию и использующие такое же программное обеспечение. Это упрощает настройку системы защиты для группы компьютеров, так как отпадает необходимость выполнять настройку на каждом из них отдельно

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

| | | | |
|--|------------|-------------------------------------|------------|
| В | | О | |
| Включение и отключение механизмов..... | 89 | Отчеты..... | 82 |
| Г | | П | |
| Генератор задач..... | 50 | Параметры | |
| Групповые политики..... | 9, 11 | атрибутов ресурсов..... | 14 |
| З | | КЦ и ЗПС..... | 14 |
| Замкнутая программная среда | | объектов групповой политики..... | 11 |
| выполняемые файлы..... | 51, 68 | пользователей..... | 12 |
| зависимые модули..... | 51, 79 | смены ключей..... | 26 |
| режимы работы..... | 48, 58, 76 | Переменные окружения..... | 51, 79 |
| сценарии..... | 58, 67 | Пиктограммы объектов..... | 91 |
| Затирание файлов..... | 81 | Политика контроля устройств..... | 39 |
| И | | Права доступа к устройствам..... | 33 |
| Идентификатор | | Р | |
| инициализация..... | 17 | Режимы входа в систему..... | 24 |
| настройка режимов..... | 19 | Ресурсы | |
| присвоение..... | 17 | восстановление из эталона..... | 54 |
| проверка принадлежности..... | 22 | выполняемые..... | 64, 67 |
| удаление..... | 21 | контролируемые..... | 67 |
| хранение пароля..... | 15, 16 | подготовка для ЗПС..... | 50, 77 |
| Интеграция с ПАК "Соболь"..... | 27 | типы..... | 53 |
| Интервал неактивности..... | 23 | С | |
| К | | Серийный номер..... | 88 |
| Ключи централизованного управления ПАК "Соболь"..... | 27 | Синхронизация моделей данных..... | 47 |
| загрузка..... | 27 | Смена пароля..... | 22 |
| копирование..... | 28 | Средства экспорта и импорта..... | 86 |
| удаление..... | 28 | Сценарий для задачи..... | 65, 72 |
| Контроль целостности | | У | |
| алгоритмы..... | 53 | Усиленная аутентификация..... | 24 |
| включение механизма..... | 59 | Ф | |
| методы..... | 53 | Функции администратора..... | 8 |
| расписание..... | 52, 54 | Ц | |
| реакция на отказ..... | 53 | Центральная база данных КЦ-ЗПС..... | 46 |
| М | | Э | |
| Модель данных | | Эталоны..... | 57, 64 |
| импорт..... | 61 | восстановление из эталона..... | 54 |
| параметры объектов..... | 64–66 | пересчет..... | 78 |
| связи между объектами..... | 56, 75 | расчет..... | 48, 57, 78 |
| экспорт..... | 60 | | |