



Код безопасности

Средство защиты информации

SECRET NET 7



Руководство администратора

Настройка механизмов защиты



Код безопасности

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

Все авторские права на эксплуатационную документацию защищены.

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

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

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

Оглавление

Список сокращений	7
Введение	8
Общие принципы управления	9
Функции администратора безопасности	9
Организация управления системой защиты	9
Централизованное и локальное управление	9
Использование групповых политик	11
Делегирование административных полномочий	12
Параметры механизмов защиты и средства управления	13
Параметры объектов групповой политики	13
Параметры пользователей	15
Атрибуты ресурсов	20
Параметры механизмов КЦ и ЗПС	20
Защита входа в систему	21
Управление персональными идентификаторами	21
Просмотр сведений об идентификаторах пользователя	22
Предъявление идентификатора	22
Инициализация идентификатора	23
Присвоение идентификатора	24
Настройка режимов использования идентификаторов	26
Удаление идентификатора	28
Проверка принадлежности	29
Смена пароля	29
Управление режимами механизма защиты входа в систему	29
Управление ключами для усиленной аутентификации	31
Генерация и выдача ключей	31
Копирование ключей	33
Настройка параметров смены ключей	33
Использование ПАК "Соболь" в режиме интеграции с Secret Net	34
Интеграция комплексов "Соболь" с системой Secret Net	35
Управление ключами централизованного управления ПАК "Соболь"	37
Копирование идентификатора администратора ПАК "Соболь"	41
Предоставление доступа к компьютерам с ПАК "Соболь"	42
Взаимодействие с СЗИ TrustAccess	44
Управление режимом интеграции Secret Net с СЗИ TrustAccess	44
Управление режимом синхронизации учетных данных с БД TrustAccess	45
Разрешение разового входа при усиленной аутентификации по паролю	47
Вход в систему в административном режиме	48
Настройка использования устройств и принтеров	50
Принципы управления устройствами и принтерами	50
Список устройств	50
Список принтеров	51
Настройки по умолчанию	51
Способы управления в автономном режиме функционирования	53
Способы управления в сетевом режиме функционирования	53
Правила наследования параметров списка устройств	54
Особенности применения групповых политик со списками устройств	55
Задание групповой политики и просмотр списка устройств	56
Задание групповой политики использования принтеров	57
Добавление устройств в список групповой политики	57
Добавление принтеров в список групповой политики	59
Контроль подключения и изменения устройств	59
Задание и настройка политики контроля устройств	60
Разрешение и запрет использования устройств на терминальных клиентах	62
Изменение перечня регистрируемых событий	63
Утверждение конфигурации	63

Избирательное разграничение доступа к устройствам и принтерам	63
Настройка прав доступа к устройствам	63
Настройка прав пользователей для печати на принтерах	65
Настройка регистрации событий и аудита операций с устройствами	66
Настройка механизмов КЦ и ЗПС	68
Модель данных	68
Способы и средства настройки	69
Управление работой механизмов	69
Принципы настройки в сетевом режиме функционирования	69
Запуск программы управления КЦ-ЗПС	71
Порядок настройки	72
Задачи, возникающие в процессе эксплуатации	72
Этап 1. Подготовка к построению модели данных	73
Этап 2. Построение фрагмента модели данных по умолчанию	73
Этап 3. Добавление задач в модель данных	74
Этап 4. Добавление заданий и включение в них задач	76
Этап 5. Подготовка ЗПС к использованию	80
Этап 6. Расчет эталонов	82
Этап 7. Включение ЗПС в "жестком" режиме	84
Этап 8. Включение механизма КЦ	85
Этап 9. Проверка заданий	85
Сохранение и загрузка модели данных	86
Сохранение	86
Оповещение об изменениях	86
Настройка автоматического запуска синхронизации	87
Принудительный запуск полной синхронизации	89
Загрузка и восстановление модели данных	89
Экспорт	89
Импорт	91
Внесение изменений в модель данных	93
Изменение параметров объектов	94
Добавление объектов	97
Удаление объектов	106
Связи между объектами	106
Формирование заданий ЗПС по журналу Secret Net	107
Подготовка ресурсов для замкнутой программной среды	109
Новый расчет и замена эталонов	110
Запрет использования локальных заданий	111
Поиск зависимых модулей	111
Замена переменных окружения	112
Настройка задания для ПАК "Соболь"	112
Полномочное управление доступом и контроль печати	114
Общие сведения	114
Категории конфиденциальности ресурсов	114
Уровни допуска и привилегии пользователей	115
Режим контроля потоков механизма полномочного управления доступом	116
Настройка механизма	117
Общий порядок настройки	117
Настройка категорий конфиденциальности	118
Назначение уровней допуска и привилегий пользователям	119
Присвоение категорий конфиденциальности ресурсам	120
Настройка регистрации событий	121
Управление режимом контроля потоков	121
Настройка маркировки распечатываемых документов	123
Настройка использования принтеров для печати документов	128
Дополнительная настройка функционирования механизма	129
Автоматическая настройка	130
Настройка вручную	131
Правила работы с конфиденциальными ресурсами	141
Настройка механизмов защиты информации на дисках	145

Дискреционное управление доступом к каталогам и файлам	145
Предоставление привилегии для изменения прав доступа к ресурсам	145
Назначение администраторов ресурсов	145
Настройка регистрации событий и аудита операций с ресурсами	146
Затирание файлов	146
Защита локальных дисков	147
Включение механизма защиты дисков	147
Включение и отключение защиты логических разделов	149
Отключение механизма защиты дисков	150
Настройка системы для задач аудита	151
Настройка регистрации событий на компьютерах	151
Изменение параметров журнала Secret Net	151
Выбор событий, регистрируемых в журнале	151
Настройка теневого копирования выводимых данных	152
Общее управление функцией теневого копирования	152
Выбор устройств и принтеров для теневого копирования	152
Изменение параметров хранилища теневого копирования	154
Настройка контроля запускаемых приложений	155
Предоставление прав доступа к журналам	156
Привилегии для работы с локальными журналами	156
Привилегии для работы с централизованными журналами	156
Вспомогательные средства администрирования	157
Формирование отчетов	157
Отчет "Паспорт ПО"	157
Отчет "Ресурсы рабочей станции"	158
Отчет "Допуск пользователей к ПАК "Соболь""	160
Отчет "Электронные идентификаторы"	160
Отчет "Журнал событий"	160
Средства экспорта и импорта параметров	161
Экспорт/импорт параметров политик	161
Экспорт/импорт параметров пользователей	161
Экспорт/импорт параметров механизмов КЦ и ЗПС	163
Редактирование учетной информации компьютера	163
Локальное оповещение о событиях НСД	163
Локальная регистрация серийных номеров	164
Временное отключение защитных механизмов	165
Приложение	167
Общие сведения о программе "Контроль программ и данных"	167
Интерфейс программы	167
Настройка элементов интерфейса	168
Параметры работы программы	169
Средства для работы со списками объектов	172
Общие сведения о программе редактирования маркеров	175
Интерфейс программы	175
Порядок действий при редактировании маркеров	176
Ресурсы, устанавливаемые на контроль целостности	179
Резервное копирование БД КЦ-ЗПС с использованием командной строки	180
Список групп и классов для контроля устройств	181
Примеры настройки использования подключаемых съемных дисков	182
Локальное присвоение пользователям определенных съемных дисков	182
Централизованное формирование списка используемых съемных дисков	183
События, регистрируемые в журнале Secret Net	184
Использование TCP-портов для сетевых соединений	209
Рекомендации по настройке Secret Net на кластере	210
Применение параметров групповой политики при обновлении	211
Аварийное снятие защиты локальных дисков	212
Работа с мастером аварийного восстановления	212
Использование загрузочного диска аварийного восстановления	213

Восстановление системы после сбоев питания компьютера	213
Восстановление базы данных КЦ-ЗПС	213
Восстановление локальной базы данных	214
Сведения о настройке защищенного соединения со службами каталогов	215
Защита взаимодействия с Active Directory	215
Защита взаимодействия с AD LDS/ADAM	216
Терминологический справочник	218
Документация	221

Список сокращений

AD	Active Directory
FAT	File Allocation Table
IEEE	Institute of Electrical and Electronics Engineers
LFN	Long File Name
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 7" RU.88338853.501410.015 (далее — система Secret Net, система защиты). В руководстве содержатся сведения, необходимые администраторам для настройки и управления основными механизмами защиты.

Перед изучением данного руководства необходимо ознакомиться с общими сведениями о системе Secret Net, изложенными в документе [1].

Условные обозначения

В руководстве для выделения некоторых элементов текста используется ряд условных обозначений.

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

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



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

Исключения.

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

Другие источники информации

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

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

Глава 1

Общие принципы управления

В системе Secret Net 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 приведено в документе [1].

Функции администратора безопасности

Функциональные возможности Secret Net 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 управления доступом и замкнутой программной среды;
- контролировать и предотвращать несанкционированное изменение целостности ресурсов;
- контролировать вывод документов на печать;
- контролировать аппаратную конфигурацию защищаемых компьютеров и предотвращать попытки ее несанкционированного изменения;
- загружать системные журналы для просмотра сведений о событиях, 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 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 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

Локальное управление — это управление работой механизмов защиты отдельного компьютера, которое осуществляется администратором безопасности непосредственно на компьютере. Локальное управление используется в тех случаях, когда возможности централизованного управления для отдельного компьютера недоступны или нецелесообразны. Например, локальное управление применяется, если требуется обеспечить безопасную работу локальных пользователей компьютера. Программные средства для локального управления

установлены по умолчанию и могут использоваться пользователями, входящими в локальную группу администраторов компьютера.

Централизованное управление параметрами Secret Net осуществляется администратором безопасности со своего рабочего места. Для этих целей может использоваться любой компьютер сети с установленными средствами централизованного управления.



Внимание!

В соответствии с концепцией Secret Net управление безопасностью в защищаемом домене рекомендуется осуществлять централизованно. Централизованное управление имеет приоритет перед локальным управлением. Например, если в групповой политике некоторые параметры заданы централизованно, то локально на компьютере их изменить нельзя.

В качестве средств централизованного управления параметрами групповых политик и параметрами доменных пользователей могут использоваться:

- стандартные средства централизованного управления ОС Windows;
- средства, входящие в состав ПО системы Secret Net: программа оперативного управления и программа управления пользователями.

Средства управления параметрами групповых политик и параметрами доменных пользователей можно использовать по отдельности (только стандартные средства Windows или только средства системы Secret Net) или комбинированно.

Для централизованного управления параметрами механизмов контроля целостности и замкнутой программной среды используется программа "Контроль программ и данных" в централизованном режиме работы. Программа входит в состав ПО системы Secret Net.

Ниже представлены общие сведения о развертывании средств централизованного управления на рабочем месте администратора безопасности.

Средства централизованного управления системы Secret Net

Для использования средств централизованного управления, входящих в состав ПО системы Secret Net, на компьютере администратора должны быть установлены следующие компоненты:

- компонент "Secret Net 7" в сетевом режиме функционирования (при установке необходимо включить параметр "установить средства централизованной настройки");
- компонент "Secret Net 7 — Программа управления".

Средства централизованного управления ОС Windows

Для использования средств централизованного управления ОС Windows на компьютере администратора безопасности должны быть установлены стандартные компоненты ОС. В зависимости от версии операционной системы установка компонентов выполняется со следующими особенностями:

- На компьютере под управлением ОС Windows 8 необходимо установить пакет "Средства удаленного администрирования сервера для Windows 8". После установки в списке компонентов Windows раскрыть раздел "Средства удаленного администрирования сервера" и включить функции "Средства администрирования возможностей | Средства управления групповыми политиками" и "Средства администрирования ролей | Средства служб AD DS и AD LDS | Средства служб AD DS | Центр администрирования Active Directory".
- На компьютере под управлением ОС Windows 7 необходимо установить пакет "Средства удаленного администрирования сервера для Windows 7". После установки в списке компонентов Windows раскрыть раздел "Средства удаленного администрирования сервера" и 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".

- На компьютере под управлением ОС Windows Vista необходимо установить пакет "Средства администрирования удаленного сервера для Windows Vista". После установки в списке компонентов Windows раскрыть раздел "Средства удаленного администрирования сервера" и включить функции "Средства администрирования возможностей | Средства управления групповыми политиками" и "Средства администрирования ролей | Средства доменных служб Active Directory | Средства контроллеров доменов Active Directory".
- На компьютере под управлением ОС Windows Server 2012 с помощью мастера добавления ролей и компонентов необходимо добавить компоненты "Управление групповой политикой" и "Средства удаленного администрирования сервера | Средства администрирования ролей | Средства AD DS и AD LDS | Средства AD DS | Оснастки и программы командной строки AD DS".
- На компьютере под управлением ОС Windows Server 2008 с помощью мастера добавления компонентов необходимо добавить компоненты "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").
- На компьютере под управлением ОС Windows XP или Windows Server 2003 необходимо установить компонент "Microsoft Administration Tools Pack" из состава дистрибутива ОС Windows Server 2003.

Использование групповых политик

В сетевом режиме функционирования системы Secret Net для централизованной настройки и применения параметров безопасности на защищаемых компьютерах могут использоваться групповые политики. Заданные параметры объектов групповых политик хранятся в Active Directory и применяются без учета значений, указанных для тех же параметров в локальной политике безопасности компьютера.

Параметры системы Secret Net могут быть заданы в групповых политиках домена, организационного подразделения и сервера безопасности. Соответственно эти параметры будут применяться на компьютерах, входящих в домен, включенных в организационное подразделение или подчиненных серверу безопасности. При этом действуют приоритеты применения групповых политик. Наименьший приоритет имеют параметры политики безопасности домена, заданные в стандартных оснастках ОС Windows. Эти параметры применяются на компьютерах домена, если отсутствуют другие значения в групповых политиках более высокого уровня.

В системе Secret Net могут использоваться следующие групповые политики в порядке возрастания приоритета применения параметров:

- политика безопасности домена, заданная в стандартных оснастках ОС Windows;
- политика организационного подразделения, заданная в стандартных оснастках ОС Windows, — для всех компьютеров, входящих в это организационное подразделение;
- политика домена, заданная в программе оперативного управления системой Secret Net;
- политика организационного подразделения, заданная в программе оперативного управления системой Secret Net, — для всех компьютеров, входящих в это организационное подразделение;
- политика, заданная для сервера безопасности в программе оперативного управления системой Secret Net, — применяется на всех компьютерах, подчиненных этому серверу безопасности.

Примечание.

Описания процедур настройки параметров политик в стандартных оснастках ОС Windows приводятся в данном документе. Сведения о работе с программой оперативного управления см. в документе [4].

За счет использования разных групповых политик можно реализовать централизованное управление параметрами с учетом особенностей информационной системы. Например, можно настроить общие параметры для всех компьютеров в политике домена и дополнительно указать значения отдельных параметров в политиках организационных подразделений. Это позволит применять на компьютерах различных организационных подразделений единые общие параметры и при этом задать специфические значения для компьютеров отдельных подразделений.

Обновление групповых политик

Параметры групповых политик на защищаемых компьютерах обновляются автоматически, в соответствии с действием механизма применения политик ОС Windows. При необходимости администратор может использовать средства принудительного обновления политик, чтобы ускорить процесс применения централизованно заданных параметров на компьютерах.

Принудительное обновление групповых политик можно осуществлять с помощью следующих средств:

- команда применения групповых политик в программе оперативного управления;
- стандартные инструменты командной строки gpupdate и secedit.

После обновления политик может потребоваться перезапуск компьютера или завершение текущего сеанса работы пользователя — чтобы применить параметры, которые действуют только при загрузке ОС или при входе пользователя в систему. Для этого предусмотрены специальные возможности как в программе оперативного управления (команды для перезагрузки или выключения компьютеров), так и в указанных инструментах командной строки.

Делегирование административных полномочий

В сетевом режиме функционирования системы Secret Net можно делегировать полномочия для администратора безопасности. Делегирование подразумевает возложение некоторых функций по настройке и управлению работой механизмов защиты на пользователей, не являющихся членами доменной группы администраторов. При этом настройка и управление будут осуществляться только в рамках определенных организационных подразделений, созданных внутри домена.

Ниже приводится порядок действий для делегирования административных полномочий. Процедуру делегирования следует выполнять в случае, если хранилище объектов централизованного управления Secret Net размещается в базе данных доменных служб Active Directory. Если хранилище объектов размещается вне AD — достаточно включить администратора безопасности в доменную группу Group Policy Creator Owners.

Порядок действий для делегирования полномочий:

1. Используя стандартные средства ОС, создайте в Active Directory структуру организационных подразделений.
2. Пользователям, уполномоченным настраивать механизмы защиты в рамках организационного подразделения, предоставьте 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;

- в стандартных оснастках ОС Windows создавать, редактировать и удалять групповые политики, назначенные для данного подразделения (обязательным условием является включение пользователя в группу Group Policy Creator Owners).
3. Включите пользователя, которому делегированы права на управление объектами организационного подразделения, в группу SecretNetAdmins.

Примечание.

Эта группа создается в домене автоматически при установке Secret Net.

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

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

Параметры механизмов защиты и средства управления

Параметры механизмов защиты Secret Net 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).

Ниже представлены разделы с общими сведениями о работе с перечисленными параметрами в соответствующих программных средствах.

Параметры объектов групповой политики

К общим параметрам безопасности ОС Windows добавляются параметры Secret Net. 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 политиками более высокого уровня (в сетевом режиме функционирования).

В системе Secret Net предусмотрены возможности настройки параметров групповых политик в стандартных оснастках ОС Windows и в программе оперативного управления.

Примечание.

Описания процедур настройки параметров политик в стандартных оснастках ОС Windows приводятся в данном документе. Сведения о работе с программой оперативного управления см. в документе [4].

В стандартных оснастках ОС Windows параметры Secret Net представлены в узле "Параметры безопасности" иерархии узлов групповой политики.

Для просмотра и изменения параметров в стандартных оснастках ОС Windows:

1. Вызовите нужную оснастку:

Политика безопасности домена или организационного подразделения	<p>Для открытия оснастки выполните соответствующее действие в зависимости от версии установленной операционной системы:</p> <ul style="list-style-type: none"> • на компьютере под управлением ОС Windows 8/7/Vista или Windows Server 2012/2008 — запустите оснастку "Управление групповой политикой", выберите политику домена или нужного организационного подразделения и в контекстном меню политики выберите команду "Изменить"; • на компьютере под управлением ОС Windows XP или Windows Server 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. <p>Для централизованного управления параметрами на рабочем месте администратора безопасности должны быть установлены средства централизованного управления ОС Windows (см. стр.9)</p>
Локальная политика безопасности	<p>Для открытия оснастки выполните соответствующее действие в зависимости от версии установленной операционной системы:</p> <ul style="list-style-type: none"> • на компьютере под управлением ОС Windows 8 или Windows Server 2012 — загрузите начальный экран "Пуск" и выберите элемент "Локальная политика безопасности" (относится к группе "Код безопасности"); • на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код безопасности Secret Net Локальная политика безопасности"

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
Настройки подсистем	<p>Управление режимами работы механизма защиты входа в систему (см. стр.29).</p> <p>Управление режимами работы механизмов полномочного управления доступом и контроля печати (см. стр.117).</p> <p>Настройка параметров хранения локального журнала Secret Net (см. стр.151).</p> <p>Управление механизмом затирания удаляемой информации (см. стр.146).</p> <p>Управление механизмом теневого копирования (см. стр.152).</p> <p>Управление режимом локального оповещения о событиях НСД (см. стр.163)</p>
Ключи пользователя	<p>Настройка параметров ключей для усиленной аутентификации пользователей (см. стр.33)</p>

Группа	Назначение
Привилегии	Назначение пользователям привилегий системы Secret Net: <ul style="list-style-type: none"> • для работы с локальным журналом Secret Net (см. стр. 156); • для работы в условиях замкнутой программной среды (см. стр. 80); • для изменения прав доступа к каталогам и файлам в механизме дискреционного управления доступом (см. стр. 145)
Регистрация событий	Настройка перечня событий, регистрируемых системой Secret Net (см. стр. 151)
Устройства	Управление параметрами контроля подключения и изменения устройств и правами доступа к устройствам (см. стр. 50)
Принтеры	Управление параметрами использования принтеров

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 управления доступом. Параметры применяются при входе пользователя в систему после выполнения процедуры идентификации и аутентификации.

В сетевом режиме функционирования системы Secret Net параметры доменных и локальных пользователей хранятся в хранилище объектов централизованного управления и в локальных базах данных защищаемых компьютеров соответственно. В автономном режиме функционирования параметры доменных и локальных пользователей хранятся в локальной базе данных компьютера.



Внимание!

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

Настройка параметров локальных пользователей осуществляется в стандартной оснастке ОС Windows "Управление компьютером". Также эта оснастка используется для настройки параметров доменных пользователей в автономном режиме функционирования системы Secret Net.

В сетевом режиме функционирования для настройки параметров доменных пользователей могут использоваться следующие средства:

- стандартная оснастка ОС Windows "Active Directory — пользователи и компьютеры";
- программа управления пользователями, входящая в состав клиентского ПО системы Secret Net.

Для работы с оснасткой "Active Directory — пользователи и компьютеры" на рабочем месте администратора безопасности должны быть установлены стандартные средства централизованного управления ОС Windows (см. стр. **9**). Параметры системы Secret Net для доменных пользователей представлены в оснастке при следующих условиях:

- установка системы Secret Net выполнена с модификацией схемы Active Directory или зарегистрированы конфигурационные данные Secret Net в разделе конфигурации каталога AD (при установке сервера безопасности или с использованием специального командного файла);
- на рабочем месте администратора безопасности установлены средства централизованной настройки системы Secret Net (при установке клиента в сетевом режиме функционирования).

Чтобы использовать программу управления пользователями, на рабочем месте администратора безопасности достаточно наличия установленных средств централизованной настройки системы Secret Net.

Сведения о порядке установки компонентов системы Secret Net для сетевого режима функционирования см. в документе [2].

Для просмотра и изменения параметров в стандартных оснастках ОС Windows:

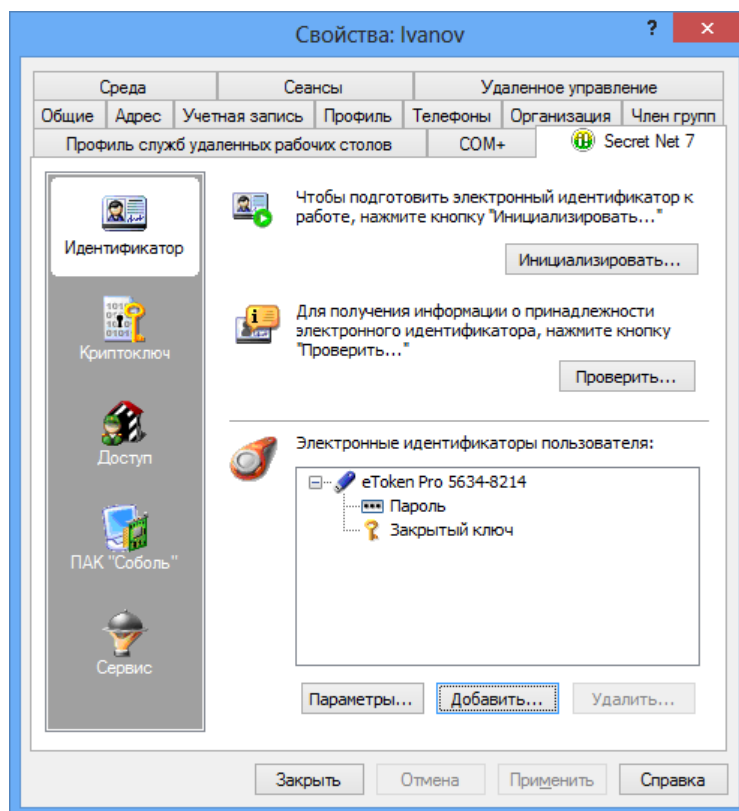
1. Вызовите нужную оснастку:

Active Directory — пользователи и компьютеры	<p>Для открытия оснастки выполните соответствующее действие в зависимости от версии установленной операционной системы:</p> <ul style="list-style-type: none"> • на компьютере под управлением ОС Windows 8 или Windows Server 2012 — загрузите начальный экран "Пуск", выберите элемент "Администрирование" и в открывшемся окне выберите ярлык "Пользователи и компьютеры Active Directory"; • на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Администрирование Active Directory — пользователи и компьютеры"
Управление компьютером	<p>Для открытия оснастки выполните соответствующее действие в зависимости от версии установленной операционной системы:</p> <ul style="list-style-type: none"> • на компьютере под управлением ОС Windows 8 или Windows Server 2012 — загрузите начальный экран "Пуск" и выберите элемент "Управление компьютером" (относится к группе "Код безопасности"); • на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код безопасности Secret Net Управление компьютером"

2. Выберите раздел или организационное подразделение, в котором находится нужный пользователь. В автономном режиме функционирования доменные пользователи представлены в разделе "Доменные пользователи", а локальные пользователи компьютера — в разделе "Локальные пользователи и группы | Пользователи").

В правой части окна появится список пользователей.

3. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 7".



В левой части диалога расположена панель выбора групп параметров. Средства для настройки представлены в правой части диалога. Для перехода к нужной группе параметров выберите на панели соответствующую пиктограмму:

- "Идентификатор" — содержит средства управления персональными идентификаторами пользователя;
- "Криптоключ" — содержит средства управления ключами для усиленной аутентификации пользователя;
- "Доступ" — содержит средства управления параметрами полномочного доступа и входа в систему;
- "ПАК "Соболь"" — содержит средства управления доступом пользователя к компьютерам с установленными комплексами "Соболь". Группа присутствует только для доменных пользователей в сетевом режиме функционирования;
- "Сервис" — содержит средства управления ключами централизованного управления ПАК "Соболь" и интеграцией системы Secret Net с программным средством TrustAccess.

Сведения о работе с параметрами представлены далее в соответствующих разделах.

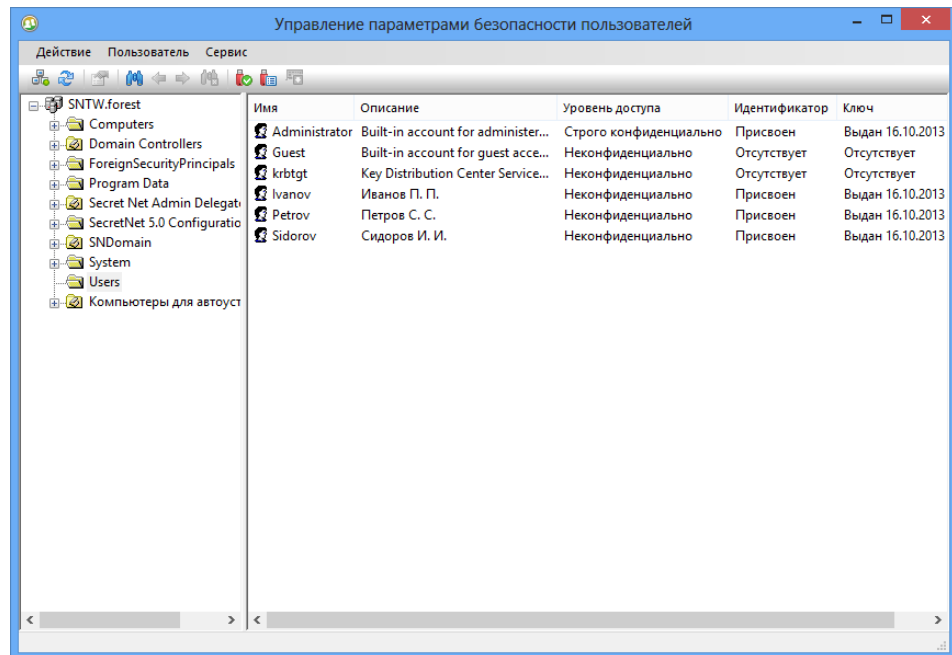
Примечание.

Если хранилище объектов централизованного управления Secret Net размещается вне Active Directory, по умолчанию возможность изменения параметров доступна только для пользователей текущего домена безопасности. При необходимости работы с параметрами других пользователей включите специальный расширенный режим редактирования параметров. Для этого вызовите контекстное меню любого пользователя и выберите команду "Включить расширенный режим". При работе в расширенном режиме следует иметь в виду, что изменения параметров пользователей других доменов безопасности не будут учтены в параметрах этих пользователей в их доменах безопасности.

Для просмотра и изменения параметров в программе управления пользователями:

1. Выполните соответствующее действие в зависимости от версии установленной операционной системы:
 - на компьютере под управлением ОС Windows 8 или Windows Server 2012 загрузите начальный экран "Пуск" и выберите элемент "Управление пользователями" (относится к группе "Код безопасности");
 - на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код безопасности | Secret Net | Управление пользователями".

На экране появится окно программы управления пользователями:



Интерфейс программы реализован аналогично стандартной оснастке ОС Windows "Active Directory — пользователи и компьютеры". В левой части окна отображается структура разделов и организационных подразделений домена, а в правой — список пользователей в выбранном контейнере. Список пользователей представлен в виде таблицы со сведениями о уровнях допуска пользователей, наличии идентификаторов и ключей для усиленной аутентификации.

2. По умолчанию в программу загружается структура текущего домена. При необходимости можно загрузить структуры других доменов Active Directory, если есть возможность подключения к этим доменам. Для этого используйте команду "Подключиться к домену Active Directory" в меню "Действие".
3. Выберите нужный раздел или организационное подразделение. В правой части окна появится список пользователей.

Совет.

При работе с большим количеством объектов удобно использовать функции сортировки и поиска пользователей. Сортировка выполняется стандартными способами по содержимому колонок таблицы в списке пользователей. Поиск можно выполнять по различным критериям. Для настройки параметров поиска выберите команду "Поиск" в меню "Пользователь" и укажите нужные критерии в диалоге настройки. Результаты поиска выводятся в самом диалоге настройки, а также выделяются в списках пользователей после закрытия диалога. Для переходов между найденными объектами используйте команды "Следующий" и "Предыдущий" в меню "Пользователь".

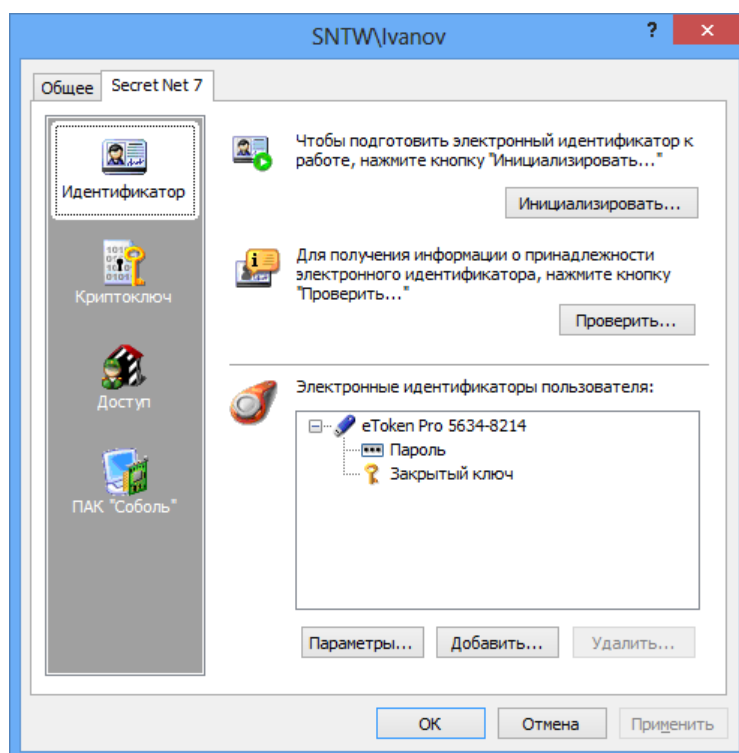
4. При необходимости используйте общие сервисные функции программы, которые могут потребоваться для настройки параметров пользователей и

функционирования системы. Команды запуска сервисных функций представлены в меню "Сервис". Описания процедур использования функций см. далее в соответствующих разделах документа.

5. Для просмотра и настройки параметров пользователя выберите его в списке и в меню "Пользователь" выберите команду "Свойства".

На экране появится диалоговое окно настройки свойств пользователя.

6. В диалоге "Общие" ознакомьтесь с общими параметрами пользователя и перейдите к диалогу "Secret Net 7".



Интерфейс диалога реализован аналогично, как в одноименном диалоге окна настройки свойств пользователя в стандартных оснастках ОС Windows (см. выше). Отличие состоит в том, что в диалоге программы управления пользователями отсутствует группа параметров "Сервис" — функции данной группы выведены в соответствующих командах меню "Сервис" основного окна программы.

Внимание!

Программа предоставляет возможность комплексно привести все значения параметров безопасности Secret Net для выбранного пользователя в состояние "не задано". Процедура выполняется с помощью команды "Удалить параметры безопасности" в меню "Пользователь" основного окна программы. После этой процедуры будут удалены параметры полномочного управления доступом, сведения о присвоенных идентификаторах, ключах, а также учетные данные пользователя в БД TrustAccess. Необходимо учитывать, что в результате удаления параметров для пользователя могут быть заблокированы определенные возможности, права и привилегии для работы в системе Secret Net.

Список доменных пользователей в автономном режиме функционирования

В автономном режиме функционирования параметры системы Secret Net для доменных пользователей настраиваются в стандартной оснастке ОС Windows "Управление компьютером". Список доменных пользователей представлен в разделе "Доменные пользователи". Если доменный пользователь не включен в раздел "Доменные пользователи", становится невозможным настроить параметры этого пользователя для работы в системе Secret Net.

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.



Внимание!

Если во время работы с оснасткой "Управление компьютером" зарегистрированный доменный пользователь был удален средствами администрирования домена, этот пользователь будет отображаться в разделе "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. Откройте оснастку "Управление компьютером". Для этого выполните соответствующее действие в зависимости от версии установленной операционной системы:
 - на компьютере под управлением ОС Windows 8 или Windows Server 2012 — загрузите начальный экран "Пуск" и выберите элемент "Управление компьютером" (относится к группе "Код безопасности");
 - на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код безопасности | Secret Net | Управление компьютером".
2. Выберите раздел "Доменные пользователи".
В правой части появится список пользователей.
3. В правой части окна вызовите контекстное меню и выберите команду "Добавить...".
На экране появится стандартный диалог ОС Windows для выбора объектов.
4. Выберите нужного пользователя и нажмите кнопку "ОК".
Имя выбранного пользователя появится в разделе "Доменные пользователи".

Атрибуты ресурсов

Параметры, относящиеся к атрибутам ресурсов файловой системы (файлов и каталогов), используются в механизмах полномочного и дискреционного управления доступом. Управление параметрами осуществляется с помощью расширения программы "Проводник". Описание процедур изменения параметров см. в документе [6].

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. 68).

Глава 2

Защита входа в систему

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 могут использоваться персональные идентификаторы eToken, iKey, Rutoken, JaCarta или идентификаторы iButton.

Пояснение.

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

Персональный идентификатор выдается пользователю администратором. Один и тот же персональный идентификатор не может быть присвоен нескольким пользователям одновременно. При этом одному пользователю можно присвоить несколько идентификаторов. Если используется ПАК "Соболь" в режиме интеграции с Secret Net, максимально возможное количество присвоенных идентификаторов для одного пользователя — 32.

Администратор безопасности может выполнять следующие операции с персональными идентификаторами:

Инициализация идентификатора
Форматирование, обеспечивающее возможность использования идентификатора в системе Secret Net. 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 сведений о том, что пользователю принадлежит персональный идентификатор данного типа с уникальным серийным номером
Отмена присвоения идентификатора
Удаление из базы данных Secret Net 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 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
Запись и удаление ключей для усиленной аутентификации
Используется для хранения в идентификаторе (или на сменном носителе) ключей для усиленной аутентификации пользователя

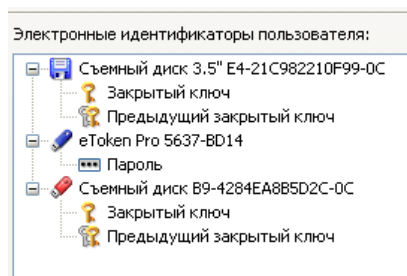
Проверка принадлежности

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 диалоге "Secret Net 7" окна свойств пользователя (при выборе группы параметров "Идентификатор"). Описания процедур вызова диалогового окна для настройки параметров пользователя см. на стр. 15.

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 или смарт-карты:

- Если точно известно, какой идентификатор нужно предъявить, вставьте его в разъем USB-порта компьютера или приложите к считывающему устройству.
- Если необходимо выбрать идентификатор из нескольких имеющихся, 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".

Примечание.

Если предъявлен идентификатор, 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, 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 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

Для инициализации идентификатора:

1. Загрузите нужную оснастку ОС Windows или запустите программу управления пользователями (см. стр. 15).
2. Вызовите окно настройки свойств любого пользователя, перейдите к диалогу "Secret Net 7" и нажмите кнопку "Инициализировать".

Совет.

В программе управления пользователями это же действие можно выполнить без вызова окна настройки свойств пользователя — для этого в меню "Сервис" выберите команду "Инициализация идентификатора".

На экране появится диалог "Предъявите идентификатор".

3. Предъявите идентификатор (см. выше).

Примечание.

Для USB-ключа предусмотрена возможность удаления данных, записанных в него вне системы Secret Net. 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.

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.

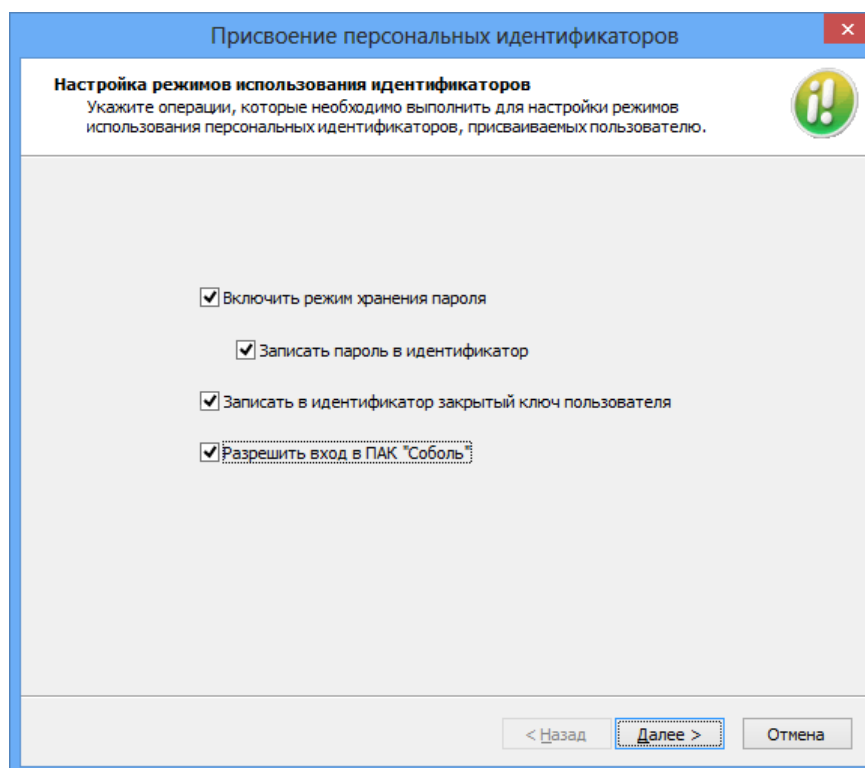
Примечания:

- 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. 34).

Для присвоения идентификатора пользователю:

1. Загрузите нужную оснастку ОС Windows или запустите программу управления пользователями (см. стр. 15).
2. Вызовите окно настройки свойств пользователя, перейдите к диалогу "Secret Net 7" и нажмите кнопку "Добавить".

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.

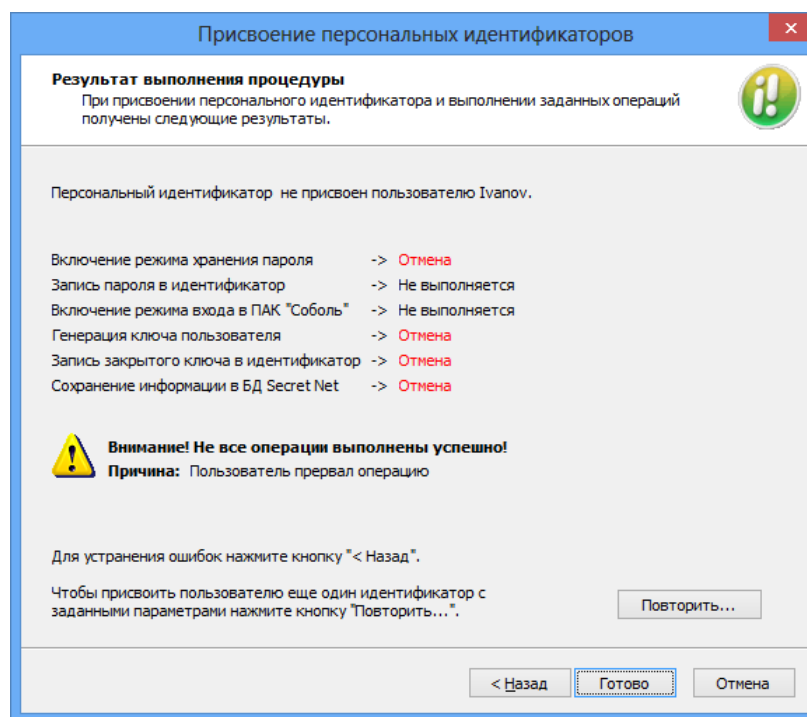
4. Если выбрана операция "Записать пароль в идентификатор", "Разрешить вход в ПАК "Соболь" или "Записать в идентификатор закрытый ключ пользователя", выполните действия по запросу программы:
 - При появлении диалога "Ввод пароля" введите пароль пользователя.
 - При появлении диалога "Предъявите идентификатор" предъявите идентификатор пользователя (см. стр. 22), содержащий его закрытый ключ.

Ошибки записи данных

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. 22) для присвоения пользователю и записи данных. Не нарушайте контакт идентификатора со считывателем до завершения всех операций.

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



Внимание!

Идентификатор не будет присвоен, если произошла ошибка при выполнении какой-либо операции или эта операция отменена из-за других ошибок. Для устранения ошибок нажмите кнопку "< Назад" и повторно предъявите идентификатор.

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

7. Чтобы присвоить пользователю еще один идентификатор с такими же параметрами, нажмите кнопку "Повторить...".
8. Для завершения работы нажмите кнопку "Готово".

Присвоение идентификатора другого пользователя

В процессе присвоения идентификатора выполняется проверка его принадлежности другому пользователю и наличия в идентификаторе ранее сохраненных структур Secret Net или ПАК "Соболь". Если идентификатор уже присвоен другому пользователю, о котором имеются сведения в данной системе, операция присвоения прерывается с выдачей соответствующего сообщения.

Если предъявленный идентификатор содержит данные Secret Net или ПАК "Соболь", но не принадлежит никому из пользователей данной системы (например, используется для входа локального пользователя на другом компьютере), выводится запрос на продолжение действий. В этом случае возможны следующие варианты:

- Идентификатор содержит закрытый ключ (или пару ключей — текущий и предыдущий), но пользователь, которому присваивается идентификатор,

уже имеет свой ключ — в этом варианте система предлагает заменить ключи в идентификаторе. При продолжении процедуры закрытый ключ из идентификатора будет удален. Запись текущего закрытого ключа пользователя в идентификатор осуществляется, если в мастере присвоения выбрана операция "Записать в идентификатор закрытый ключ пользователя" (см. выше).

- Идентификатор содержит закрытый ключ (или пару ключей — текущий и предыдущий), и пользователь, которому присваивается идентификатор, не имеет своего ключа — в этом варианте выводится запрос на использование ключей из идентификатора для пользователя. Чтобы оставить ключ в идентификаторе и использовать его для пользователя, которому этот идентификатор присваивается, нажмите кнопку "Да" в диалоге запроса. При нажатии кнопки "Нет" закрытый ключ из идентификатора будет удален. Генерация и запись нового закрытого ключа пользователя в идентификатор осуществляется, если в мастере присвоения выбрана операция "Записать в идентификатор закрытый ключ пользователя" (см. выше). Для отмены процедуры присвоения идентификатора нажмите кнопку "Отмена".

Примечание.

За счет использования ключа из идентификатора (ответ "Да" в диалоге запроса) можно реализовать, например, вход и усиленную аутентификацию с помощью этого идентификатора для различных локальных пользователей на нескольких компьютерах. В автономном режиме функционирования идентификатор можно будет использовать как для локальных, так и для доменных пользователей.

- Идентификатор содержит другие данные Secret Net или ПАК "Соболь" — выводится запрос для подтверждения операций удаления обнаруженных данных. Если вы уверены, что этим идентификатором никто больше не пользуется, нажмите кнопку "Да" и повторно предъявите данный идентификатор.

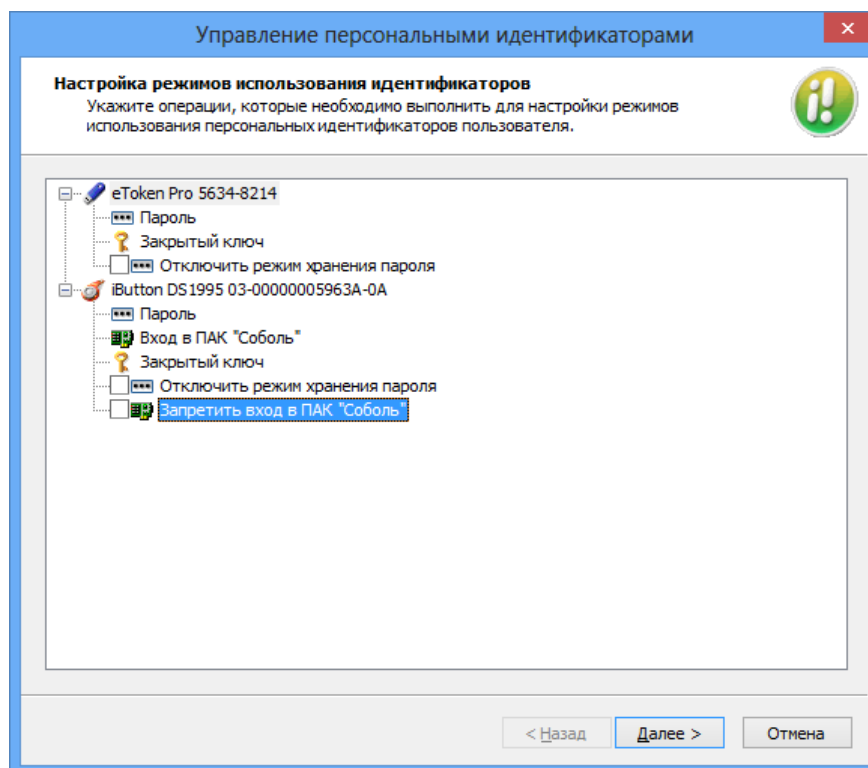
Настройка режимов использования идентификаторов

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:

1. Загрузите нужную оснастку ОС Windows или запустите программу управления пользователями (см. стр. 15).
2. Вызовите окно настройки свойств пользователя, перейдите к диалогу "Secret Net 7" и нажмите кнопку "Параметры".

На экране появится стартовый диалог мастера настройки режимов.



Диалог содержит список идентификаторов, присвоенных пользователю.

Примечание.

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 >".

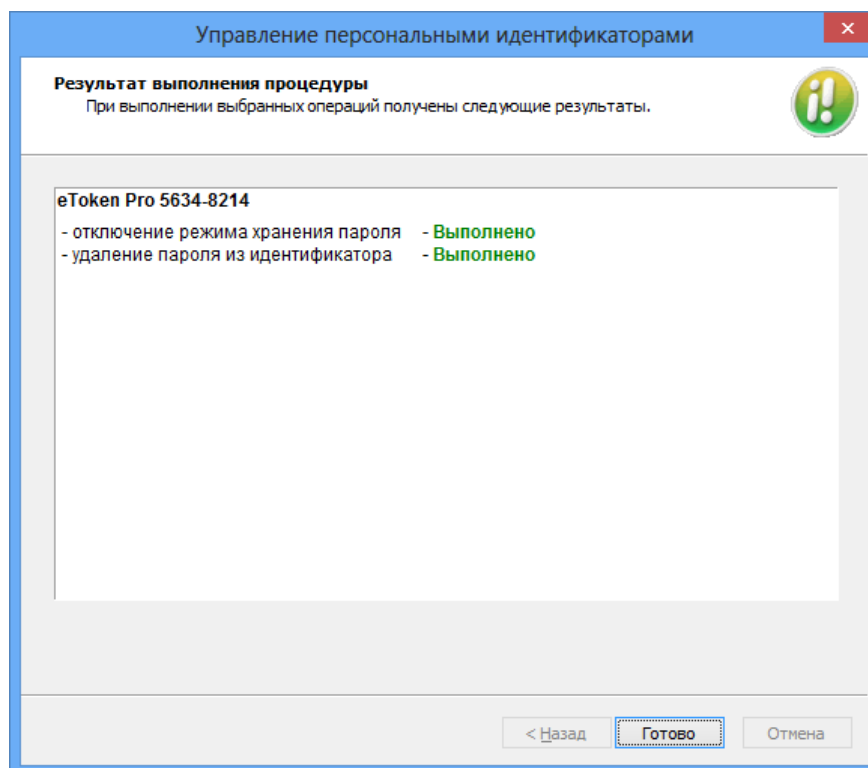
Если была выбрана любая операция, кроме операции "Включить режим хранения пароля", на экране появится диалог "Предъявите идентификатор". В диалоге отображаются наименования идентификаторов, для которых были выбраны операции, и статус их обработки: "Не обработан".

6. Предъявите все идентификаторы, указанные в списке (см. стр. 22).

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 нужную оснастку ОС Windows или запустите программу управления пользователями (см. стр. 15).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 7".
3. 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.
4. Нажмите кнопку "Да".
На экране появится запрос на очистку памяти идентификатора.
5. Нажмите кнопку "Да".
На экране появится диалог "Предъявите идентификатор".
6. Предъявите идентификатор (см. стр. 22).
Статус предъявленного идентификатора изменится на "Обработан".

Примечание.

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

7. Нажмите кнопку "Заккрыть".
Запись об удаленном идентификаторе исчезнет из списка идентификаторов.

Проверка принадлежности

Для проверки принадлежности идентификатора:

1. Загрузите нужную оснастку ОС Windows или запустите программу управления пользователями (см. стр. **15**).
2. Вызовите окно настройки свойств любого пользователя, перейдите к диалогу "Secret Net 7" и нажмите кнопку "Проверить".

Совет.

В программе управления пользователями это же действие можно выполнить без вызова окна настройки свойств пользователя — для этого в меню "Сервис" выберите команду "Проверка идентификатора".

На экране появится диалог "Предъявите идентификатор".

3. Предъявите проверяемый идентификатор (см. стр. **22**).
Если в базе данных Secret Net есть сведения о данном идентификаторе, они будут выведены на экран.

Смена пароля

Смена пароля пользователя может быть выполнена самим пользователем или администратором. Описание смены пароля пользователем см. в документе [6].



Внимание!

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 нужную оснастку ОС Windows или запустите программу управления пользователями (см. стр. **15**).
2. В списке пользователей вызовите контекстное меню нужного пользователя и выберите команду "Смена пароля" ("Задать пароль").
На экране появится диалог для ввода пароля.
3. 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.
4. Предъявите все указанные в списке идентификаторы (см. стр. **22**).
Новый пароль будет записан в идентификаторы и их статус изменится на "Обработан", а кнопка "Отмена" изменит название на "Закреть".

Примечание.

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

5. Нажмите кнопку "Закреть".

Управление режимами механизма защиты входа в систему

Для настройки режимов:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. **13**).
2. Выберите папку "Настройки подсистем".
3. Вызовите контекстное меню для нужного параметра (см. таблицу ниже) и выберите в нем команду "Свойства".
На экране появится диалог настройки параметра.

4. Настройте действие параметра и нажмите кнопку "ОК".

Вход в систему: Запрет вторичного входа в систему
<p>Если режим включен, блокируется возможность запуска команд и сетевых подключений с вводом учетных данных пользователя, не выполнившего интерактивный вход в систему.</p> <p>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)</p>
Вход в систему: Количество неудачных попыток аутентификации
<p>Устанавливает ограничение на количество неудачных попыток входа в систему при включенном режиме усиленной аутентификации по ключу или по паролю. При достижении ограничения компьютер блокируется и вход разрешается только для администратора.</p> <p>Если установлено значение "0" — ограничение не действует</p>
Вход в систему: Максимальный период неактивности до блокировки экрана
<p>Устанавливает максимально возможный период неактивности, после которого компьютер автоматически блокируется средствами системы Secret Net.</p> <p>В целях безопасности при продолжительном бездействии пользователя компьютер должен блокироваться. Блокировка по истечении заданного периода неактивности осуществляется средствами системы Secret Net. Пользователи с помощью стандартных средств операционной системы могут указать для компьютера другой период включения блокировки (заставки), но этот период не может быть больше значения данного параметра. В противном случае параметр ОС не будет действовать.</p> <p>Если установлено значение "0" — блокировка средствами системы Secret Net не осуществляется</p>
Вход в систему: Разрешить интерактивный вход только доменным пользователям
<p>Если режим включен, интерактивно в систему могут войти только пользователи, зарегистрированные в домене. Интерактивный вход в систему локальных пользователей (включая локальных администраторов) запрещен.</p> <p>Параметр отсутствует при функционировании системы Secret Net в автономном режиме</p>
Вход в систему: Реакция на изъятие идентификатора
<p>Нет реакции. При изъятии идентификатора из считывающего устройства блокировка компьютера не выполняется.</p> <p>Блокировать станцию при изъятии USB-идентификатора. Выполняется блокировка компьютера при изъятии из считывающего устройства идентификатора на базе USB-ключа или смарт-карты, использованного для идентификации пользователя в системе Secret Net (например, eToken).</p> <p>Блокировать станцию при изъятии любого идентификатора. Выполняется блокировка компьютера при изъятии из считывающего устройства идентификатора любого типа из числа поддерживаемых системой Secret Net для идентификации пользователей (iButton, eToken и др.).</p> <p>Функция блокировки при изъятии идентификатора действует в локальном сеансе работы пользователя, если идентификатор активирован средствами Secret Net и пользователь предъявил этот идентификатор для входа в систему</p>
Вход в систему: Режим аутентификации пользователя

Стандартная аутентификация. При входе пользователя выполняется только стандартная аутентификация ОС Windows.

Усиленная аутентификация по ключу. Дополнительно проверяется подлинность и актуальность (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 не подтверждается, вход запрещается и регистрируется значение ключа (если включен параметр "Регистрировать неверные аутентификационные данные"). Если срок действия ключа истек, пользователю предлагается выполнить смену ключей для усиленной аутентификации.

Усиленная аутентификация по паролю. При входе пользователя, кроме стандартной аутентификации ОС Windows, дополнительно выполняется аутентификация по паролю пользователя средствами системы Secret Net. В этом режиме пользователи, пароль которых не был сохранен в базе данных системы Secret Net, не смогут войти в систему (администратор может разрешить пользователю разовый вход для сохранения пароля, включив параметр "Доверять парольной аутентификации Windows" в диалоге настройки свойств пользователя).

При включенном режиме усиленной аутентификации по ключу вход в систему без предъявления ключа возможен только в административном режиме (см. стр. 48)

Вход в систему: Режим идентификации пользователя

По имени. 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, 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. Пользователи, не имеющие персональных идентификаторов, войти в систему не смогут. Администратор может войти в систему без предъявления идентификатора только в административном режиме (см. стр. 48).

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

При попытках входа пользователей в систему в журнале регистрируются соответствующие события. Состав регистрируемых событий можно изменять (см. стр. 151).

Управление ключами для усиленной аутентификации

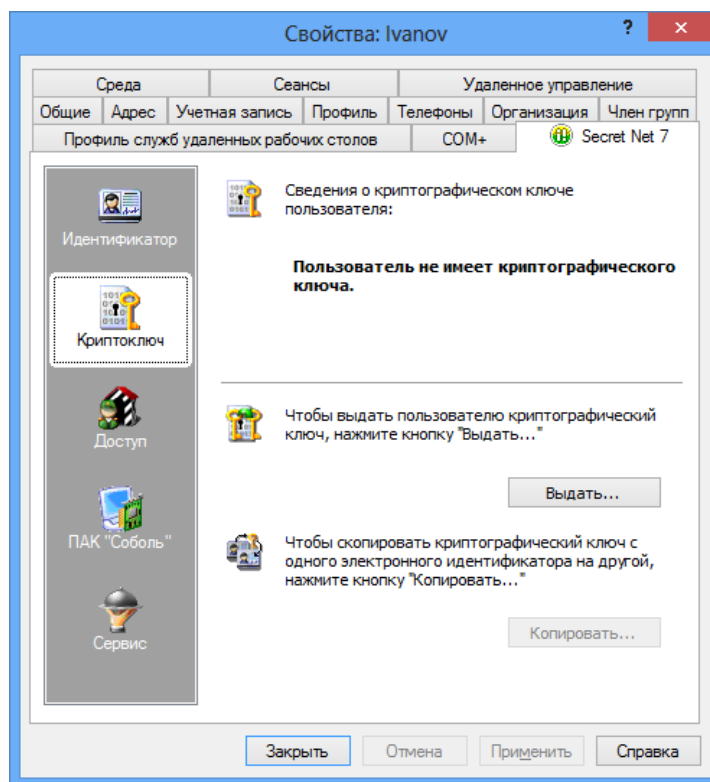
При включенном режиме усиленной аутентификации пользователь при входе в систему должен предъявить носитель, содержащий ключевую информацию. Ключевая информация пользователя может храниться в персональных идентификаторах или сменных носителях, присвоенных пользователю.

Генерация и выдача ключей

Генерация ключевой информации может выполняться средствами Secret Net либо при присвоении пользователю персонального идентификатора (см. стр. 24), либо, когда идентификатор уже присвоен пользователю, отдельной процедурой выдачи ключей.

Для выдачи ключей:

1. Загрузите нужную оснастку ОС Windows или запустите программу управления пользователями (см. стр. 15).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 7".
3. В панели выбора групп параметров выберите группу "Криптоключ".
В диалоге будут отображены сведения о ключах пользователя.



4. 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.

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



Внимание!

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".

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

6. Предъявите идентификатор (см. стр. 22), 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.

Примечание.

Продолжение процедуры без устранения ошибки невозможно.

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

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

8. 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 "Заккрыть".

9. Нажмите кнопку "Закрыть".

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

10. 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, можно скопировать с одного идентификатора пользователя на другой. Процедура копирования выполняется администратором безопасности.

Для копирования ключей:

1. Загрузите нужную оснастку ОС Windows или запустите программу управления пользователями (см. стр. **15**).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 7".
3. В панели выбора групп параметров выберите группу "Криптоключ".
4. Нажмите кнопку "Копировать".
На экране появится диалог "Предъявите идентификатор".
5. Предъявите идентификатор (см. стр. **22**), содержащий копируемые ключи пользователя.
Произойдет считывание ключей, и на экране появится диалог со списком идентификаторов пользователя.
6. Предъявите идентификатор, на который требуется записать ключи.
При успешной записи ключей в идентификатор его статус изменится на "Обработан".
7. Нажмите кнопку "Закрыть".

Настройка параметров смены ключей

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

- 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 (см. документ [6]). 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:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. **13**).
2. Выберите папку "Ключи пользователя".
В правой части окна появится список параметров смены ключей.

3. Вызовите контекстное меню нужного параметра и выберите в нем команду "Свойства".
На экране появится диалог настройки параметра.
4. 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

В Secret Net 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;
- формирование заданий на контроль целостности для ПАК "Соболь" средствами управления Secret Net (см. главу 4);
- автоматическая передача записей журнала регистрации событий ПАК "Соболь" в журнал Secret Net (см. таблицу ниже).

События комплекса "Соболь"	События системы Secret Net
Вход пользователя	Соболь: вход пользователя
Вход администратора	
Не рассчитаны контрольные суммы	Соболь: не рассчитаны контрольные суммы
Переход в автономный режим	Соболь: изменение режима работы
Переход в сетевой режим	
Удаление системного журнала	Соболь: очистка журнала
Ошибка КС внешнего запроса	Соболь: ошибка синхронизации параметров
Ошибка внешнего запроса	
Перерасчет контрольных сумм	Соболь: перерасчет контрольных сумм
Автоматический перерасчет КС	
Смена аутентификатора администратора	Соболь: смена аутентификатора
Смена аутентификатора пользователя	
Идентификатор не зарегистрирован	Соболь: запрет входа пользователя
Неправильный пароль	
Превышено число попыток входа	
Пользователь заблокирован	
Ошибка при контроле целостности	Соболь: нарушена целостность ресурса
Обработаны внешние запросы	Соболь: синхронизация параметров
Добавлен новый пользователь	
Пользователь удален	
Все пользователи удалены	
Добавление пользователя	
Удаление пользователя	

События комплекса "Соболь"	События системы Secret Net
Администратор сменил свой пароль	Соболь: смена пароля
Администратор сменил пароль пользователя	
Пользователь сменил свой пароль	
Ошибка КС в памяти идентификатора	Соболь: ошибка КС в памяти идентификатора
Изменены параметры загрузочного диска	Соболь: изменены параметры загрузочного диска

Следует обратить внимание на следующие особенности включения режима интеграции в сетевом режиме функционирования системы:

1. При инициализации всех ПАК "Соболь" необходимо использовать один общий идентификатор администратора ПАК "Соболь" или его копии.
2. 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.
3. После подключения ПАК "Соболь" к системе Secret Net администратор безопасности должен включить для своего персонального идентификатора режим разрешения входа в ПАК "Соболь". Включение режима осуществляется при настройке режимов использования идентификатора (см. стр. 26).

Интеграция комплексов "Соболь" с системой Secret Net

Включение и настройка режима интеграции комплексов "Соболь" и системы Secret Net осуществляется в следующем порядке:

1. Если используется сетевой режим функционирования системы Secret Net — на рабочем месте администратора безопасности выполните действия:
 - установите ПАК "Соболь". При установке выполните первичную регистрацию администратора и создайте необходимое количество резервных копий идентификатора администратора. После установки переведите комплекс из автономного режима в режим совместного использования. Сведения о установке и настройке ПАК "Соболь" см. в документации на изделие;
 - установите клиентское ПО системы Secret Net (см. документ [2]);
 - сгенерируйте ключи централизованного управления комплексами "Соболь" (см. ниже);
 - подключите ПАК "Соболь" к Secret Net (см. ниже);
 - настройте параметры пользователей для организации их доступа к компьютерам домена (назначение идентификаторов, паролей, формирование списка разрешенных компьютеров).
2. На каждом защищаемом компьютере выполните следующие действия:
 - установите ПАК "Соболь". При установке для сетевого режима функционирования системы Secret Net выполните повторную регистрацию администратора с использованием идентификатора, подготовленного при выполнении действия 1, и укажите ту же версию криптографической схемы, которая была задана на рабочем месте администратора безопасности. После установки переведите комплекс из автономного режима в режим совместного использования. Сведения о установке и настройке ПАК "Соболь" см. в документации на изделие;
 - установите ПО системы Secret Net (см. документ [2]);
 - подключите ПАК "Соболь" к Secret Net (см. ниже).

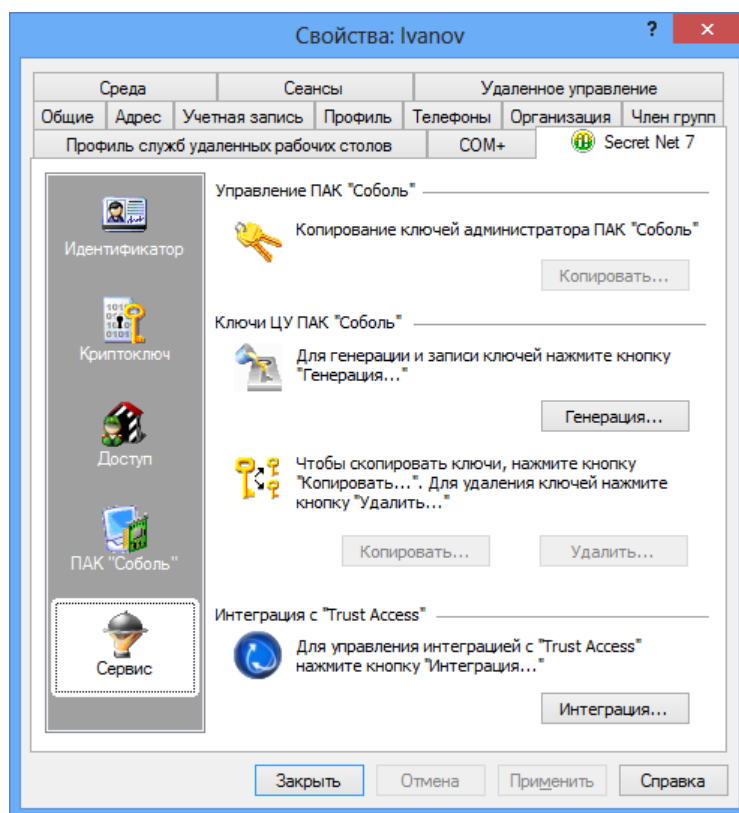
3. Если используется автономный режим функционирования системы Secret Net — настройте на защищаемых компьютерах параметры пользователей и персональных идентификаторов.

Генерация ключей централизованного управления

Процедуру генерации ключей централизованного управления ПАК "Соболь" можно выполнить в стандартной оснастке ОС Windows "Active Directory — пользователи и компьютеры" или в программе управления пользователями.

Для генерации ключей в оснастке "Active Directory — пользователи и компьютеры":

1. Загрузите оснастку "Active Directory — пользователи и компьютеры", вызовите окно настройки свойств любого пользователя и перейдите к диалогу "Secret Net 7" (см. стр. 15).
2. В панели выбора групп параметров выберите группу "Сервис".



Пояснение.

Кнопка "Копировать" в разделе "Управление ПАК "Соболь"" становится доступной после подключения комплекса "Соболь" и загрузки ключей в оснастке "Active Directory — пользователи и компьютеры". Кнопки "Копировать" и "Удалить" в разделе "Ключи ЦУ ПАК "Соболь"" становятся доступными после завершения генерации и записи ключей.

3. Нажмите кнопку "Генерация".
На экране появится диалог "Предъявите идентификатор".
4. Предъявите идентификатор (см. стр. 22), предназначенный для хранения ключей ЦУ комплексами "Соболь". По окончании процедуры генерации и записи ключей нажмите кнопку "ОК".

Для генерации ключей в программе управления пользователями:

1. Запустите программу управления пользователями (см. стр. 15).
2. В меню "Сервис" выберите команду "Создание ключей ЦУ ПАК "Соболь"". На экране появится диалог "Предъявите идентификатор".

3. Предъявите идентификатор (см. стр. 22), предназначенный для хранения ключей ЦУ комплексами "Соболь". По окончании процедуры генерации и записи ключей нажмите кнопку "ОК".



Предупреждение.

Не допустите потери ключей ЦУ. В случае их утраты необходимо заново создать структуру централизованного управления комплексами "Соболь".

Подключение комплекса "Соболь" к Secret Net

Для подключения комплекса:

1. В Панели управления Windows выберите ярлык "Управление Secret Net 7". На экране появится диалоговое окно "Управление Secret Net 7".
2. Перейдите к диалогу "Управление ПАК "Соболь"".
3. Выполните следующие действия:
 - для отображения в отчете "Ресурсы АРМ" заводского номера изделия введите этот номер в поле "Заводской номер ПАК "Соболь"" и нажмите кнопку "Применить". Заводской номер указан в паспорте изделия, а также на плате;
 - для подключения комплекса "Соболь" нажмите кнопку "Подключить".

Примечание.

После подключения комплекса "Соболь" в диалоге "Управление ПАК "Соболь"" появится поле "Разрешить автоматическую загрузку ОС". Установите в нем отметку, если необходимо организовать автоматический вход в ПАК "Соболь" без предъявления персонального идентификатора. Режим автоматического входа в комплекс "Соболь" начнет действовать после перезагрузки операционной системы компьютера.

4. В сетевом режиме функционирования системы Secret Net на экране появится диалог с предложением предъявить ключевой носитель (идентификатор) с ключами ЦУ комплексами "Соболь". В этом случае предъявите нужный идентификатор.
Система Secret Net перейдет в режим интеграции с комплексом "Соболь", и на экране появится сообщение об этом.
5. Нажмите кнопку "ОК" в диалоговом окне "Управление Secret Net 7".

Отключение режима интеграции Secret Net и "Соболь"

Для отключения режима интеграции:

1. В Панели управления Windows выберите ярлык "Управление Secret Net 7". На экране появится диалоговое окно "Управление Secret Net 7".
2. Перейдите к диалогу "Управление ПАК "Соболь"".
3. Нажмите кнопку "Отключить".
Режим интеграции с комплексом "Соболь" будет отключен, и на экране появится сообщение об этом.



Внимание!

Повторное включение в Secret Net режима интеграции с комплексом "Соболь" возможно только после перезагрузки компьютера.

4. Если не планируется дальнейшее использование режима интеграции, при следующей загрузке компьютера войдите с правами администратора в комплекс "Соболь" и переведите изделие в автономный режим работы (см. документацию на изделие).

Управление ключами централизованного управления ПАК "Соболь"

В сетевом режиме функционирования системы Secret Net при выполнении операций, связанных с организацией доступа пользователей к компьютерам, и

операций с ключами администратора ПАК "Соболь" необходимо загрузить ключи централизованного управления ПАК "Соболь".

В целях повышения надежности хранения ключей рекомендуется сохранять их копии на нескольких идентификаторах.

Операции с ключами централизованного управления ПАК "Соболь" осуществляются в стандартной оснастке ОС Windows "Active Directory — пользователи и компьютеры" или в программе управления пользователями.

Загрузка ключей

После загрузки ключи сохраняются в системе до закрытия оснастки "Active Directory — пользователи и компьютеры" или программы управления пользователями.

Для загрузки ключей в оснастке "Active Directory — пользователи и компьютеры":

1. Загрузите оснастку "Active Directory — пользователи и компьютеры" (см. стр. [15](#)), вызовите контекстное меню любого пользователя и выберите команду "Загрузить ключи ЦУ".

Примечание.

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

На экране появится диалог "Предъявите идентификатор".

2. Предъявите носитель (см. стр. [22](#)), на котором хранятся ключи централизованного управления ПАК "Соболь".

После успешной загрузки ключей на экране появится сообщение об этом.

Для загрузки ключей в программе управления пользователями:

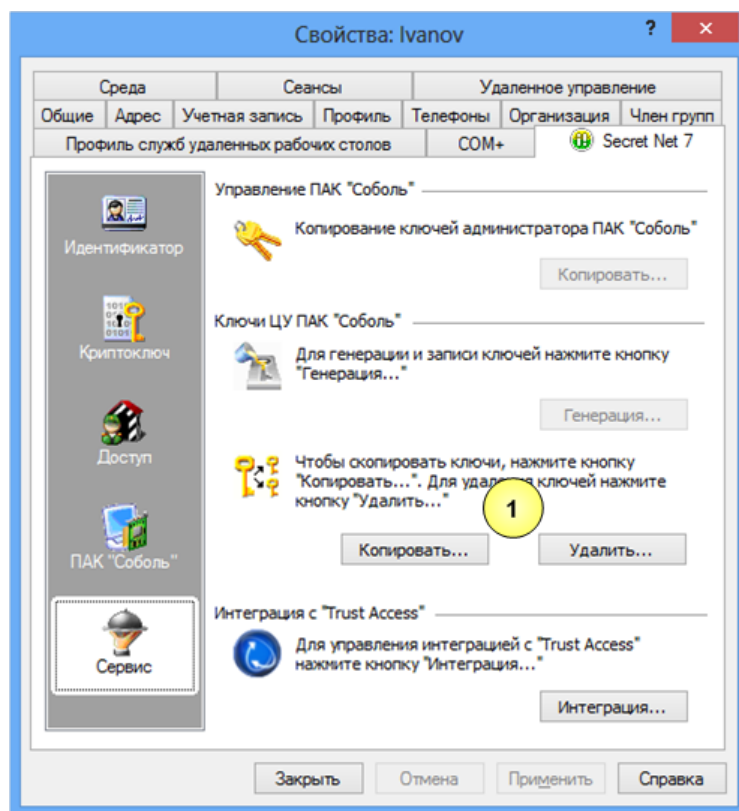
1. Запустите программу управления пользователями (см. стр. [15](#)).
 2. В меню "Сервис" выберите команду "Загрузка ключей ЦУ ПАК "Соболь"".
- На экране появится диалог "Предъявите идентификатор".
3. Предъявите носитель (см. стр. [22](#)), на котором хранятся ключи централизованного управления ПАК "Соболь".

После успешной загрузки ключей на экране появится сообщение об этом.

Копирование ключей

Для копирования ключей в оснастке "Active Directory — пользователи и компьютеры":

1. Загрузите оснастку "Active Directory — пользователи и компьютеры", вызовите окно настройки свойств любого пользователя и перейдите к диалогу "Secret Net 7" (см. стр. [15](#)).
2. В панели выбора групп параметров выберите группу "Сервис".

**Пояснение.**

На рисунке выносками обозначены элементы: 1 — кнопки для копирования и удаления ключей.

3. Нажмите кнопку "Копировать".

На экране появится диалог "Предъявите идентификатор".

4. Предъявите идентификатор (см. стр. 22), 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 "Закрыть".**Для копирования ключей в программе управления пользователями:****1. Запустите программу управления пользователями (см. стр. 15).****2. В меню "Сервис" выберите команду "Копирование ключей ЦУ ПАК "Соболь"".**
На экране появится диалог "Предъявите идентификатор".**3. Предъявите идентификатор (см. стр. 22), содержащий копируемые ключи централизованного управления ПАК "Соболь".**

Произойдет считывание ключей, после чего на экране появится следующий диалог для предъявления идентификатора.

4. Предъявите идентификатор, на который требуется записать ключи.

При успешной записи ключей в идентификатор его статус изменится на "Обработан".

5. Нажмите кнопку "Закрыть".



Удаление ключей

Предупреждение.

Удаление ключей централизованного управления ПАК "Соболь" осуществляется без возможности их восстановления в том же виде. Процедура приводит к необратимым последствиям очистки всех параметров текущей схемы централизованного управления ПАК "Соболь" в домене. Если возникнет необходимость вернуться к такой схеме, потребуется полная переинициализация централизованного управления ПАК "Соболь" во всем домене. Переинициализация выполняется в следующей последовательности:

- генерация новых ключей централизованного управления ПАК "Соболь";
- включение для электронных идентификаторов режима интеграции с ПАК "Соболь";
- настройка доступа пользователей к компьютерам;
- выполнение на каждом компьютере с ПАК "Соболь" процедур отключения режима интеграции с Secret Net и подключения комплекса "Соболь" к системе.

Для удаления ключей в оснастке "Active Directory — пользователи и компьютеры":

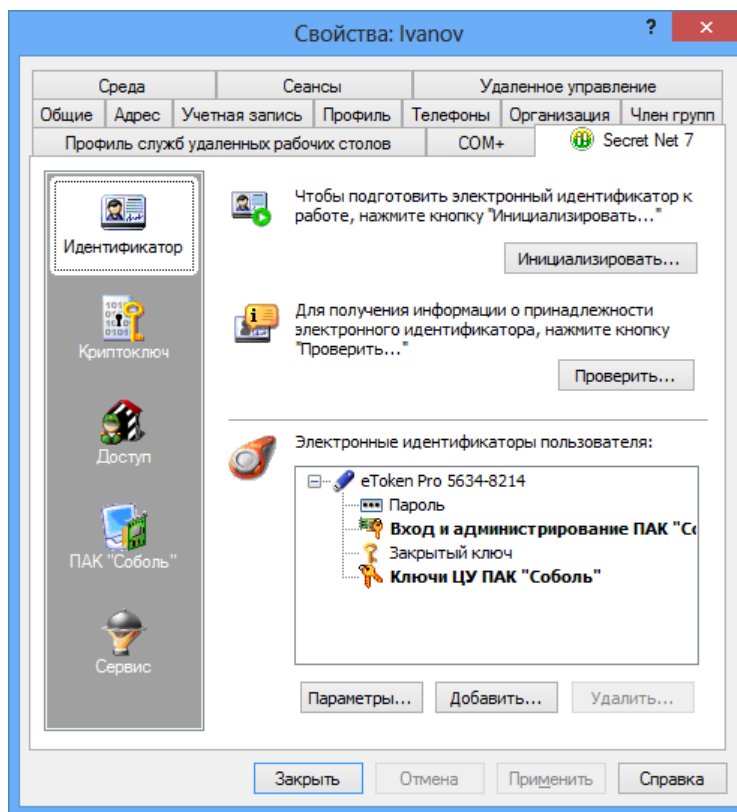
1. Загрузите оснастку "Active Directory — пользователи и компьютеры", вызовите окно настройки свойств любого пользователя и перейдите к диалогу "Secret Net 7" (см. стр.15).
2. В панели выбора групп параметров выберите группу "Сервис".
3. Нажмите кнопку "Удалить" (см. рисунок выше).
На экране появится сообщение о последствиях выполнения процедуры.
4. Нажмите кнопку "Да" в окне сообщения.
На экране появится запрос на продолжение операции.
5. Нажмите кнопку "Да" в диалоге запроса.
Произойдет удаление ключей из системы, после чего на экране появится запрос на удаление ключей из идентификаторов.
6. Выполните нужное действие:
 - Если удалять ключи из идентификаторов не требуется, нажмите кнопку "Нет" в диалоге запроса. На этом процедура удаления завершается.
 - Чтобы удалить ключи из идентификаторов, нажмите кнопку "Да" в диалоге запроса и затем после появления следующего диалога предъявите идентификатор, содержащий ключи для удаления.
7. После предъявления идентификатора для удаления ключей нажмите кнопку "ОК" в диалоге "Предъявите идентификатор".
На экране появится запрос на удаление ключей из этого идентификатора.
8. Нажмите кнопку "Да" в диалоге запроса.
На экране появится диалог со сведениями о выполнении операции. После завершения удаления статус идентификатора изменится на "Обработан".
9. Нажмите кнопку "Закрыть".
На экране появится запрос на удаление ключей из другого идентификатора.
10. Если требуется удалить ключи из другого идентификатора, нажмите кнопку "Да" и выполните действия в той же последовательности. Чтобы завершить процедуру, нажмите кнопку "Нет".

Для удаления ключей в программе управления пользователями:

1. Запустите программу управления пользователями (см. стр.15).
2. В меню "Сервис" выберите команду "Удаление ключей ЦУ ПАК "Соболь"".
На экране появится сообщение о последствиях выполнения процедуры.
3. Выполните действия в той же последовательности, как и в процедуре удаления ключей в оснастке "Active Directory — пользователи и компьютеры" (см. выше).

Копирование идентификатора администратора ПАК "Соболь"

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

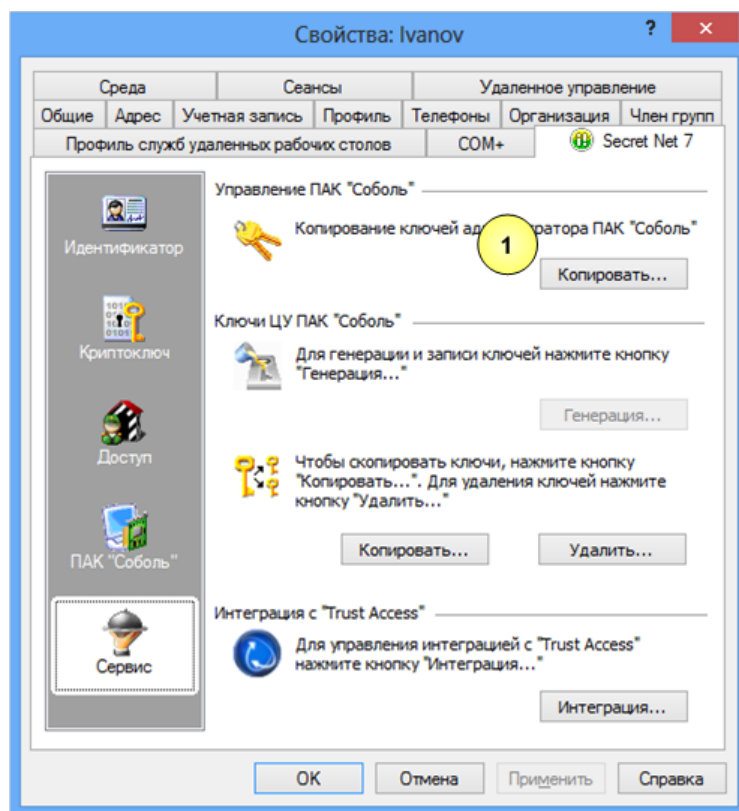


Если при инициализации ПАК "Соболь" не было создано достаточное количество резервных копий идентификаторов, можно скопировать содержимое идентификатора администратора ПАК "Соболь" на другой носитель. Новый идентификатор также можно будет использовать для администрирования комплексов "Соболь".

Чтобы копировать идентификатор администратора ПАК "Соболь" для доменного пользователя в сетевом режиме функционирования, предварительно загрузите ключи централизованного управления ПАК "Соболь" (см. стр. 37).

Для копирования идентификатора администратора ПАК "Соболь" в стандартной оснастке ОС Windows:

1. Загрузите нужную оснастку для управления параметрами пользователей, вызовите окно настройки свойств любого пользователя и перейдите к диалогу "Secret Net 7" (см. стр. 15).
2. В панели выбора групп параметров выберите группу "Сервис".



Пояснение.

На рисунке выносками обозначены элементы: 1 — кнопка для копирования идентификатора администратора ПАК "Соболь".

3. В разделе "Управление ПАК "Соболь"" нажмите кнопку "Копировать".
На экране появится диалог "Предъявите идентификатор".
4. Предъявите идентификатор (см. стр. 22) администратора ПАК "Соболь".
На экране появится диалог запроса пароля.
5. Введите пароль администратора ПАК "Соболь" и нажмите кнопку "ОК".
На экране появится следующий диалог для предъявления идентификатора.
6. Предъявите идентификатор, в который должны быть скопированы сведения из идентификатора администратора ПАК "Соболь".
После успешной записи сведений в идентификатор его статус примет значение "Обработан".
7. Нажмите кнопку "ОК".

Для копирования идентификатора администратора ПАК "Соболь" в программе управления пользователями:

1. Запустите программу управления пользователями (см. стр. 15).
2. В меню "Сервис" выберите команду "Копирование идентификатора администратора ПАК "Соболь"".
На экране появится диалог "Предъявите идентификатор".
3. Выполните действия в той же последовательности, как и в процедуре копирования идентификатора администратора ПАК "Соболь" в стандартной оснастке ОС Windows (см. выше).

Предоставление доступа к компьютерам с ПАК "Соболь"

В сетевом режиме функционирования системы Secret Net на компьютерах с ПАК "Соболь" при включенном режиме интеграции с Secret Net 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.

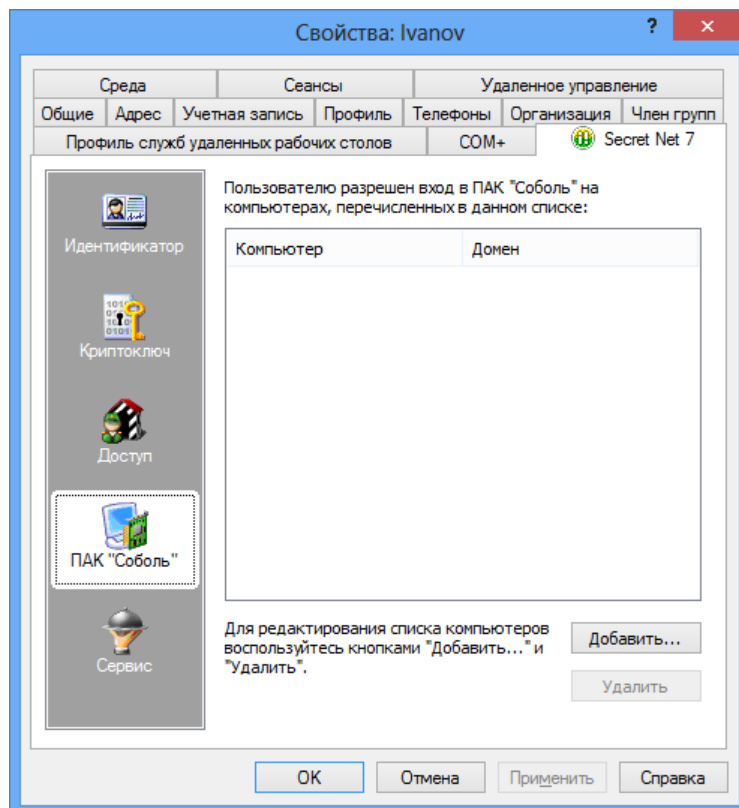
Чтобы предоставить такую возможность доменному пользователю, необходимо выполнить следующие действия:

- присвоить пользователю идентификатор с включенным режимом разрешения входа в ПАК "Соболь" (см. стр. 24). Для идентификаторов, присвоенных пользователю ранее, включить режим можно при настройке режимов использования идентификатора (см. стр. 26);
- сформировать список компьютеров, на которых пользователю разрешается выполнять вход в ПАК "Соболь" (см. процедуру ниже).

Перед формированием списка компьютеров предварительно загрузите ключи централизованного управления ПАК "Соболь" (см. стр. 37).

Для формирования списка компьютеров:

1. В оснастке "Active Directory — пользователи и компьютеры" или в программе управления пользователями вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 7" (см. стр. 15).
2. В панели выбора групп параметров выберите группу "ПАК "Соболь"".



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

Взаимодействие с СЗИ TrustAccess

Если в системе установлено ПО средства защиты информации TrustAccess, система Secret Net может взаимодействовать с этим средством. Для взаимодействия с СЗИ TrustAccess в системе Secret Net необходимо включить режим интеграции с TrustAccess и после этого включить режим синхронизации учетных данных для нужных пользователей. Управление режимами осуществляется на компьютере с установленным ПО "АРМ администратора TrustAccess".

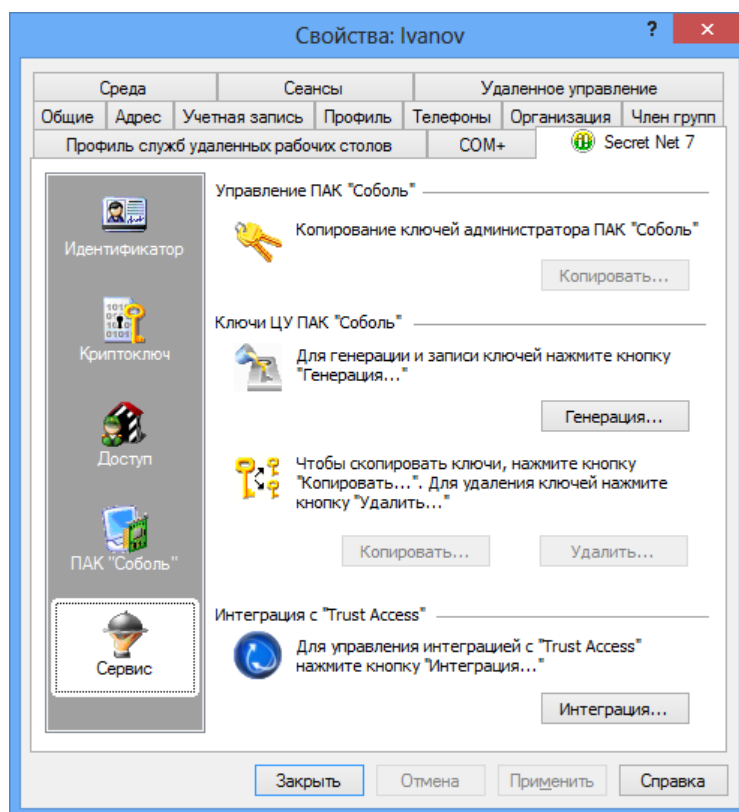
Управление режимом интеграции Secret Net с СЗИ TrustAccess

При совместном использовании системы Secret Net и средства защиты информации TrustAccess в системе Secret Net можно включить режим интеграции, позволяющий синхронизировать учетные данные доменных пользователей в базе данных TrustAccess. После включения режима интеграции необходимо включить режим синхронизации учетных данных для тех пользователей, которым требуется разрешить автоматическую авторизацию в домене TrustAccess при входе в систему.

Управление режимом интеграции доступно пользователям, входящим в группу администраторов домена безопасности. Процедуру можно выполнить в стандартной оснастке ОС Windows "Active Directory — пользователи и компьютеры" или в программе управления пользователями.

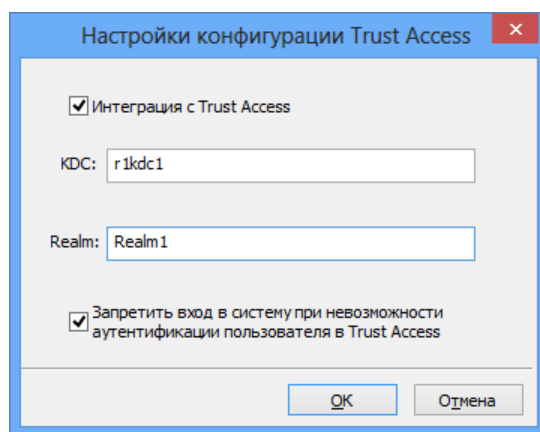
Для управления режимом интеграции с СЗИ TrustAccess в оснастке "Active Directory — пользователи и компьютеры":

1. Загрузите оснастку "Active Directory — пользователи и компьютеры", вызовите окно настройки свойств любого пользователя и перейдите к диалогу "Secret Net 7" (см. стр. 15).
2. В панели выбора групп параметров выберите группу "Сервис".



3. Нажмите кнопку "Интеграция..." (кнопка заблокирована, если на компьютере отсутствует ПО TrustAccess или если пользователь, открывший оснастку "Active Directory — пользователи и компьютеры", не входит в группу администраторов домена безопасности).

На экране появится диалог "Настройки конфигурации TrustAccess".



4. Для включения режима интеграции установите отметку в поле "Интеграция с TrustAccess" и введите имя компьютера, являющегося сервером управления СЗИ TrustAccess (в поле "KDC"), и имя домена TrustAccess (в поле "Realm"). Если требуется отключить режим интеграции, удалите отметку из поля "Интеграция с TrustAccess".
5. Дополнительно при включенном режиме интеграции можно отключить возможность входа в систему пользователей, не прошедших авторизацию в СЗИ TrustAccess. Для этого установите отметку в поле "Запретить вход в систему при невозможности аутентификации пользователя в TrustAccess". Параметр будет действовать для пользователей с включенным режимом синхронизации учетных данных.
6. Нажмите кнопку "ОК".

Для управления режимом интеграции с СЗИ TrustAccess в программе управления пользователями:

1. Запустите программу управления пользователями (см. стр.15).
2. В меню "Сервис" выберите команду "Интеграция с СЗИ TrustAccess" (команда неактивна, если отсутствует ПО TrustAccess или если пользователь, запустивший программу, не входит в группу администраторов домена безопасности).

На экране появится диалог "Настройки конфигурации TrustAccess".

3. Выполните действия в диалоге аналогично тому, как описано в процедуре управления режимом интеграции в оснастке "Active Directory — пользователи и компьютеры" (см. выше).

Управление режимом синхронизации учетных данных с БД TrustAccess

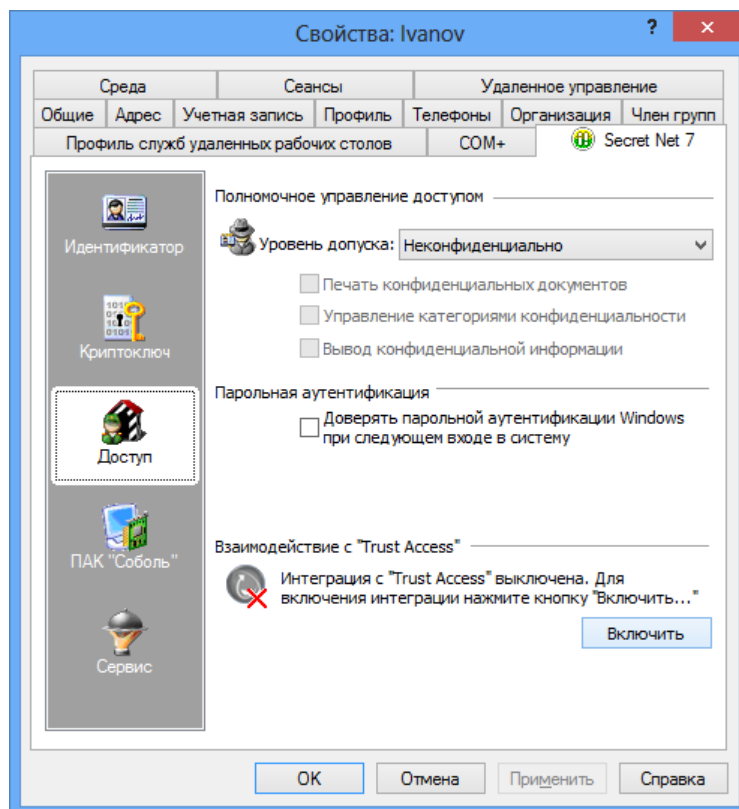
Если включен режим интеграции системы Secret Net и средства защиты информации TrustAccess, пользователи могут выполнять вход в систему с автоматической авторизацией в домене TrustAccess. Это дает возможность пользователям при входе в систему однократно указывать свои учетные данные обычным образом без необходимости последующего ввода учетных данных в окне агента СЗИ TrustAccess.

Чтобы разрешить пользователю автоматическую авторизацию в домене TrustAccess, нужно включить для этого пользователя режим синхронизации учетных данных с БД TrustAccess. После включения режима синхронизации в БД TrustAccess будет создана учетная запись, сопоставленная доменному пользователю, и учетные данные этой записи будут автоматически синхронизироваться с учетными данными доменного пользователя. При включении режима синхронизации учетных данных требуется указать пароль пользователя и учетные данные администратора СЗИ TrustAccess.

Возможности включения и отключения режима синхронизации учетных данных пользователей доступны при включенном режиме интеграции системы Secret Net и СЗИ TrustAccess.

Для включения режима синхронизации учетных данных пользователя:

1. Загрузите нужную оснастку ОС Windows или запустите программу управления пользователями (см. стр. 15).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 7".
3. В панели выбора групп параметров выберите группу "Доступ".



4. Нажмите кнопку "Включить". Кнопка присутствует при следующих условиях:
 - включен режим интеграции системы Secret Net и СЗИ TrustAccess;
 - на компьютере установлено ПО "АРМ администратора TrustAccess";
 - для данного пользователя отключен режим синхронизации учетных данных с БД TrustAccess.

На экране появится диалог для ввода пароля пользователя.

5. Введите пароль пользователя и нажмите кнопку "ОК".

На экране появится диалог для ввода учетных данных администратора СЗИ TrustAccess.

Примечание.

Диалог не появится, если учетные данные администратора СЗИ TrustAccess были введены ранее в текущем сеансе. В этом случае пропустите действие 6.

6. Введите имя и пароль администратора СЗИ TrustAccess и нажмите кнопку "ОК".
Будет выполнена регистрация учетных данных пользователя в БД TrustAccess, после чего название кнопки "Включить" в диалоге "Secret Net 7" изменится на "Выключить".

**Внимание!**

После включения режима синхронизации не рекомендуется переименовывать учетную запись пользователя, иначе будет нарушено сопоставление доменного пользователя и его учетной записи в СЗИ TrustAccess. Это приведет к невозможности автоматической авторизации переименованного пользователя в домене TrustAccess. Если требуется переименовать учетную запись доменного пользователя, отключите для него режим синхронизации учетных данных (см. ниже), выполните процедуру переименования и снова включите режим синхронизации.

Для отключения режима синхронизации учетных данных пользователя:

1. Выполните действия **1–3** вышеописанной процедуры.
2. Нажмите кнопку "Выключить". Кнопка присутствует при следующих условиях:
 - включен режим интеграции системы Secret Net и СЗИ TrustAccess;
 - на компьютере установлено ПО "АРМ администратора TrustAccess";
 - для данного пользователя включен режим синхронизации учетных данных с БД TrustAccess.

На экране появится диалог запроса на удаление из БД TrustAccess учетной записи, сопоставленной доменному пользователю.

3. В диалоге запроса нажмите соответствующую кнопку:
 - для удаления учетной записи нажмите кнопку "Да";
 - если учетную запись необходимо оставить в БД TrustAccess, нажмите кнопку "Нет".

Примечание.

Аналогично требуется выбрать вариант действий с учетной записью в БД TrustAccess при удалении доменного пользователя с включенным режимом синхронизации учетных данных.

4. Если при выполнении действия **3** был выбран вариант с удалением учетной записи из БД TrustAccess, на экране появится диалог для ввода учетных данных администратора СЗИ TrustAccess.

Примечание.

Диалог для ввода учетных данных администратора СЗИ TrustAccess не появится, если эти данные были введены ранее в текущем сеансе. В этом случае пропустите действие **5**.

5. Введите имя и пароль администратора СЗИ TrustAccess и нажмите кнопку "ОК".
Режим синхронизации учетных данных пользователя будет отключен, после чего название кнопки "Выключить" в диалоге "Secret Net 7" изменится на "Включить".

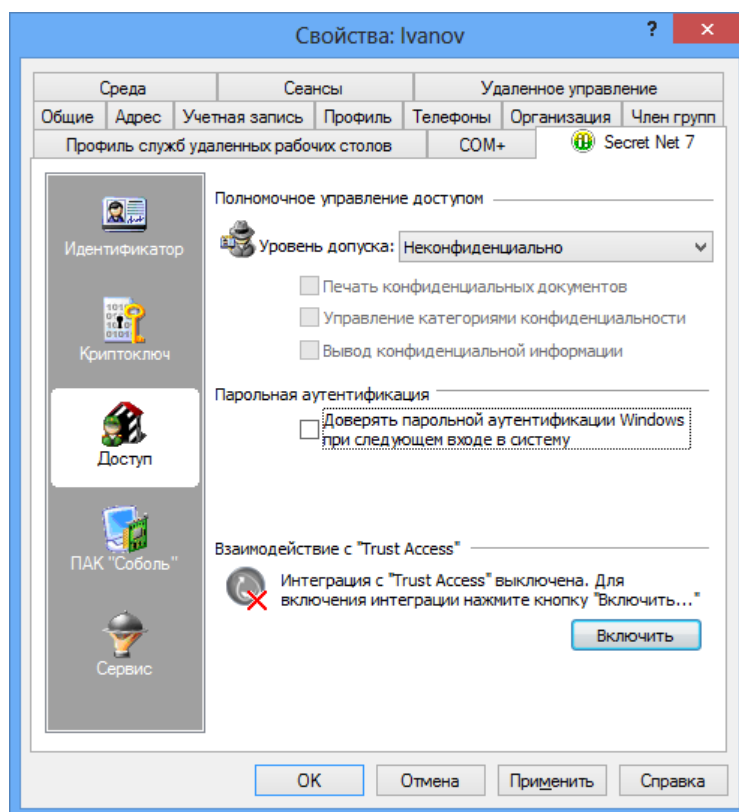
Разрешение разового входа при усиленной аутентификации по паролю

Если в системе включен режим усиленной аутентификации пользователей по паролю, при входе пользователя дополнительно выполняется аутентификация по его паролю средствами системы Secret Net. Для этого пароль пользователя должен быть сохранен в базе данных системы Secret Net. Сохранение выполняется при смене пароля пользователя администратором, а также при смене пароля самим пользователем, если режим был включен во время сеанса работы пользователя.

В случае если в базе данных системы Secret Net требуется сохранить текущий пароль пользователя, администратор может разрешить пользователю разовый вход в систему для ввода этого пароля с последующим сохранением. После того как пользователь выполнит вход в систему, разрешение автоматически отключается, и для пользователя в полном объеме будет действовать режим усиленной аутентификации по его паролю.

Для разрешения разового входа пользователя в систему:

1. Загрузите нужную оснастку ОС Windows или запустите программу управления пользователями (см. стр.15).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 7".
3. В панели выбора групп параметров выберите группу "Доступ".



4. Установите отметку в поле "Доверять парольной аутентификации Windows при следующем входе в систему".
5. Нажмите кнопку "OK".

Вход в систему в административном режиме

При штатном функционировании системы Secret Net вход любого пользователя компьютера, включая администратора, должен выполняться по одинаковым правилам, установленным соответствующими механизмами защиты. Во время загрузки компьютера перед входом пользователя система защиты проводит инициализацию компонентов и их функциональный контроль. После успешного проведения всех проверок вход в систему разрешается.

В тех случаях, когда необходимо получить доступ к компьютеру в обход действующих механизмов или прервать выполнение инициализации компонентов, администратор может активировать специальный административный режим входа.

Применение административного режима входа может потребоваться, в частности, в следующих ситуациях:

- при включенном режиме усиленной аутентификации, если администратор не имеет ключа;
- при включенном режиме входа в систему "Только по идентификатору", если администратор не имеет персонального идентификатора;
- при повторяющихся ошибках функционального контроля, приводящих к длительному ожиданию инициализации компонентов.

**Внимание!**

Административный режим входа следует использовать только в крайних случаях для восстановления нормального функционирования системы. Выполнив вход в административном режиме, устраните возникшую проблему и перезагрузите компьютер.

Для входа в систему в административном режиме:

1. Перезагрузите компьютер.
2. Во время загрузки компьютера при появлении сообщений о инициализации системных сервисов Secret Net нажмите клавишу <Esc>. Удерживайте клавишу или периодически нажимайте ее до появления экрана приветствия (приглашение на вход в систему).
3. Выполните стандартные действия процедуры входа в систему.

Глава 3

Настройка использования устройств и принтеров

Принципы управления устройствами и принтерами

Для защиты доступа к устройствам компьютера используются механизм контроля подключения и изменения устройств и механизм разграничения доступа к устройствам. Работа этих механизмов взаимосвязана. Механизм контроля подключения и изменения устройств предназначен для обнаружения и реагирования на изменения аппаратной конфигурации компьютера, а также для поддержания в актуальном состоянии списка устройств компьютера. По списку устройств с помощью второго механизма выполняется разграничение доступа пользователей к устройствам. Часть функций разграничения доступа к устройствам реализуется с использованием механизма полномочного управления доступом.

Защита доступа к принтерам реализуется механизмом контроля печати.

Список устройств

Для представления множества устройств, установленных или подключаемых к защищаемым компьютерам, используется иерархическая схема списка устройств. Устройства группируются в классы, а классы, в свою очередь, включены в состав групп. Группы являются элементами объединения верхнего уровня. Количество групп фиксировано. Предусмотрены следующие группы:

- "Локальные устройства" — объединяет фиксированные устройства компьютера, для которых не предполагается ограничивать подключение (например, последовательные и параллельные порты, процессоры, оперативная память);
- "Устройства USB" — объединяет устройства, подключаемые к шине USB;
- "Устройства PCMCIA" — объединяет устройства, подключаемые к шине PCMCIA;
- "Устройства IEEE1394" — объединяет устройства, подключаемые к шине IEEE1394;
- "Устройства Secure Digital" — объединяет устройства, подключаемые к шине Secure Digital;
- "Сеть" — объединяет устройства, являющиеся сетевыми интерфейсами (адаптеры). Если сетевым интерфейсом является нефиксированное подключаемое устройство, такое устройство может также присутствовать и в другой группе. Это дает возможность настроить реакцию системы на подключение устройства до его регистрации в качестве сетевого интерфейса.

Некоторые классы допускают дополнительное разбиение устройств по моделям. Модели объединяют устройства с одинаковыми идентификационными кодами, присвоенными производителем. В списке устройств присутствуют предопределенные модели — например, модели электронных идентификаторов. Также в список можно добавлять модели на основе имеющихся устройств, если в этих устройствах производителем были указаны идентификационные коды. В дальнейшем при обнаружении нового устройства с такими же идентификационными кодами это устройство автоматически будет добавлено в качестве экземпляра к той же модели. За счет этого можно управлять одинаковыми устройствами без необходимости настройки параметров каждого устройства по отдельности.

Для объектов каждого уровня (группа, класс, модель, устройство) определен набор параметров, с помощью которых настраиваются механизмы контроля подключения и изменения устройств, разграничения доступа к устройствам, теневого копирования и полномочного управления доступом. Иерархия списка устройств в большинстве случаев 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. **181**.

На компьютере список устройств создается сразу после установки клиентского ПО системы Secret Net 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.

В сетевом режиме функционирования системы защиты можно создать список устройств в групповой политике. После создания список устройств состоит из групп, классов и предопределенных моделей устройств. При необходимости в список можно добавить и конкретные устройства. Заданные параметры в этом списке устройств хранятся и распространяются в домене в составе доменных (групповых) политик.

Список принтеров

Настройка параметров использования принтеров осуществляется в отдельном списке "Принтеры". Параметры могут применяться по умолчанию при печати на любые принтеры или могут быть заданы для отдельных принтеров.

Печатающие устройства, представленные в списке принтеров, могут также присутствовать как устройства и в списке устройств. Это дает возможность настроить реакцию системы на подключение устройства до его регистрации в качестве принтера.

На компьютере список принтеров создается сразу после установки клиентского ПО системы Secret Net. Список принтеров изначально состоит из одного элемента "Настройки по умолчанию". Параметры использования принтеров, заданные для этого элемента, применяются ко всем принтерам, кроме тех, которые в явном виде присутствуют в списке принтеров. Добавление принтеров в список политики осуществляется с помощью специальной программы-мастера. Явно заданные параметры для конкретных принтеров имеют приоритет перед параметрами элемента "Настройки по умолчанию". Список принтеров локальной политики безопасности хранится в локальной базе данных системы Secret Net.

В сетевом режиме функционирования системы защиты можно задать параметры использования принтеров в групповой политике. Действия для формирования списка и настройки параметров выполняются так же, как и в локальной политике безопасности. Заданные параметры в этом списке принтеров хранятся и распространяются в домене в составе доменных (групповых) политик.

Настройки по умолчанию

По умолчанию после установки системы защиты в локальной политике безопасности заданы следующие правила использования устройств и принтеров, которые распространяются на всех пользователей компьютера:

- Для групп "Локальные устройства" и "Сеть" включен режим контроля "Устройство постоянно подключено к компьютеру". Для остальных групп включен режим "Подключение устройства разрешено".
- Для всех обнаруженных жестких дисков, а также сменных и оптических, включен режим контроля "Устройство постоянно подключено к компьютеру" с дополнительным параметром "Блокировать компьютер при изменении устройства". При этом для классов, к которым относятся такие устройства, включен режим "Подключение устройства разрешено".
- Для устройств с возможностью разграничения доступа предоставлен полный доступ трем стандартным группам пользователей: "Система", "Администраторы" и "Все".

- К принтерам предоставлен доступ стандартным группам пользователей: "Система", "Все" и "Все пакеты приложений".
- Теневое копирование отключено для всех устройств и принтеров.
- Для устройств с возможностью назначения категории конфиденциальности включен режим доступа "Устройство доступно без учета категории конфиденциальности".
- Для сетевых интерфейсов разрешено функционирование независимо от уровней конфиденциальности сессий в режиме контроля потоков механизма полномочного управления доступом.
- Для принтеров разрешена печать документов любой категории конфиденциальности.
- Регистрируются все события категорий "Контроль аппаратной конфигурации" и "Разграничение доступа к устройствам" (состав регистрируемых событий по категориям приводится в приложении на стр. 184).

Общие рекомендации по настройке устройств

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

1. После установки системы защиты администратор последовательно подключает к компьютеру все устройства, планируемые к использованию. На этом этапе устройства регистрируются в системе и для них или копируются разрешающие права доступа и параметры контроля от вышестоящих объектов (моделей, классов и групп), или настраиваются особые параметры (например, назначаются нужные категории конфиденциальности). После настройки наследование прав на эти устройства отключается.
2. По завершении регистрации устройств администратор отключает разрешающие права для соответствующих моделей, классов и групп (например, для группы "Устройства Secure Digital"). Это приведет к тому, что пользователь сможет подключать только устройства, зарегистрированные на шаге 1. Подключение других устройств будет запрещено.
3. В дальнейшем при необходимости разрешить подключение дополнительного устройства администратор может сам подключить устройство, скопировать его в нужную политику и выполнить настройку параметров или удаленно разрешить использование запрещенного устройства (только в сетевом режиме функционирования системы Secret Net).

Пояснение.

Метод удаленного разрешения устройств предполагает использование программы оперативного управления. Сведения о работе с программой см. в документе [4]. По запросу пользователя о необходимости разрешения использования имеющегося у него устройства (например, USB-флеш-накопителя) администратор безопасности предлагает подключить это устройство к компьютеру на рабочем месте пользователя. После подключения устройства, даже если оно будет запрещено к использованию, сведения о нем появятся в списке устройств локальной политики безопасности. Администратор на своем рабочем месте в программе оперативного управления загружает параметры локальной политики безопасности соответствующего агента и выполняет необходимые действия для разрешения использования устройства.

Общие рекомендации по настройке принтеров

Чтобы пользователь мог выполнять печать только на принтерах, разрешенных к использованию администратором безопасности, настройку системы рекомендуется выполнить следующим образом:

1. После установки системы защиты администратор последовательно выполняет процедуры установки (добавления) на компьютер всех принтеров, которые планируется использовать. При этом следует учесть, что подключение к одним и тем же принтерам может выполняться различными способами — например, если принтер (физическое устройство) установлен как локальный и как сетевой с IP-адресом. Для разграничения доступа к принтерам,

подключение к которым будет осуществляться различными способами, необходимо выполнить процедуру установки (добавления) принтера для каждого способа подключения. Этим будет обеспечена корректная идентификация таких принтеров системой защиты.

2. По завершении установки принтеров администратор в соответствующей политике формирует список принтеров. Список должен содержать элементы, соответствующие используемым принтерам, в том числе отдельные элементы для различных способов подключения. При этом для элемента "Настройки по умолчанию" нужно установить запрет печати для всех пользователей и включить ограничение печати документов всех категорий конфиденциальности. Для остальных элементов списка принтеров устанавливаются необходимые права пользователей и ограничения печати конфиденциальных документов. За счет этого пользователи не будут иметь возможность распечатывать документы в обход механизмов защиты на тех принтерах, которые они могут установить самостоятельно.
3. В дальнейшем при необходимости разрешить печать на новый принтер (или на тот же принтер, подключаемый другим способом) администратор может сам выполнить его установку, после чего добавить в список нужной политики и настроить параметры использования.

Способы управления в автономном режиме функционирования

Настраивать параметры контроля и права доступа можно непосредственно для каждого конкретного устройства. Если же для всех устройств данной модели, класса или группы должны действовать типовые параметры контроля и права доступа, рекомендуется выполнять настройку этих параметров соответственно для модели, класса или группы устройств. После настройки можно или применить заданные параметры ко всем дочерним объектам, или включить режим наследования параметров для конкретных устройств. Назначенные права доступа для группы, класса или модели автоматически распространяются на все включенные в них устройства. Причем это относится как к устройствам, присутствующим в системе (при условии, что права доступа для этих устройств наследуются), так и к вновь подключаемым устройствам.

Для принтеров также предусмотрена возможность настройки параметров использования отдельно для каждого печатающего устройства. Параметры, заданные для элемента "Настройки по умолчанию", применяются ко всем принтерам, кроме тех, которые присутствуют в списке принтеров политики. Явно заданные параметры для конкретных принтеров имеют приоритет перед параметрами элемента "Настройки по умолчанию".

Способы управления в сетевом режиме функционирования

В сетевом режиме функционирования системы Secret Net применение локальных и групповых политик обеспечивает гибкое управление механизмами контроля подключения и изменения устройств, разграничения доступа к устройствам и контроля печати.

Для управления устройствами можно использовать следующие методы:

- 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.

Управление принтерами можно осуществлять централизованно или локально.

Централизованное управление

Администратор безопасности использует редактор групповой политики для управления параметрами контроля и правами доступа доменных пользователей применительно к группам, классам или моделям устройств, а также принтеров. Выполненные настройки сохраняются в объектах групповых политик и вступают в силу после успешного их применения.

Этот вариант управления является предпочтительным, когда управление устройствами осуществляется на уровне групп или классов, а управление принтерами осуществляется на уровне общих параметров по умолчанию и при этом нет необходимости устанавливать особые настройки для отдельных устройств или принтеров.

Локальное управление на уровне конкретных устройств и принтеров

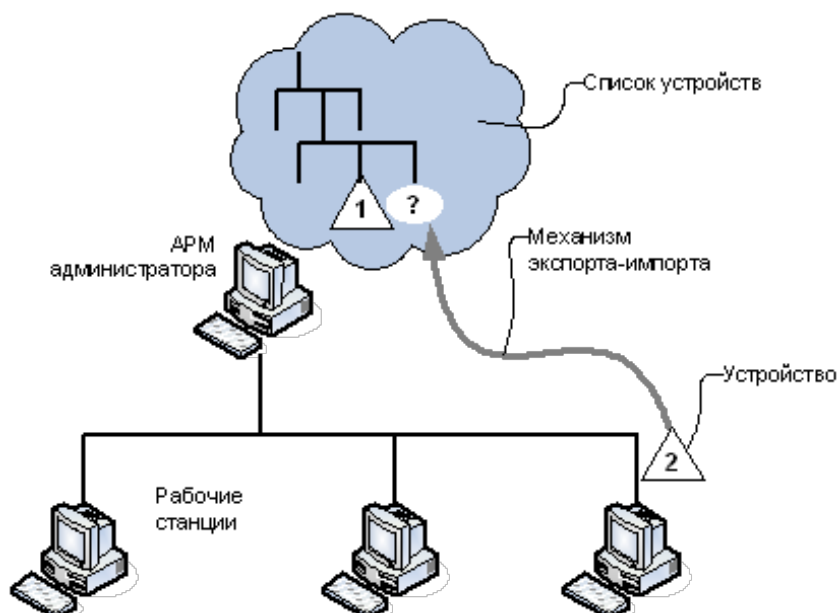
Если требуется установить особые параметры для конкретных устройств или принтеров, то можно выполнить настройку в локальной политике безопасности. С ее помощью администратор безопасности может настроить на компьютере параметры контроля и доступ пользователей и групп пользователей как к группам, классам или моделям устройств, так и к отдельным устройствам и принтерам (если настройки объектов не определены в групповой политике). Настройки локальной политики сохраняются в локальной базе данных. Редактировать параметры локальной политики можно локально в оснастке управления локальной политикой безопасности или на рабочем месте администратора безопасности в программе оперативного управления (см. документ [4]).

Централизованное управление на уровне конкретных устройств и принтеров

Если на компьютерах домена или организационного подразделения требуется использовать особые параметры для отдельных устройств и принтеров, можно управлять контролем и доступом к таким устройствам на рабочем месте администратора безопасности с помощью централизованных средств управления групповыми политиками. Для этого такие устройства и принтеры необходимо включить в список устройств групповой политики.

В список устройств можно добавить сведения об устройствах, подключенных к какому-либо компьютеру с установленным клиентским ПО системы Secret Net. В список принтеров можно добавить любой доступный принтер.

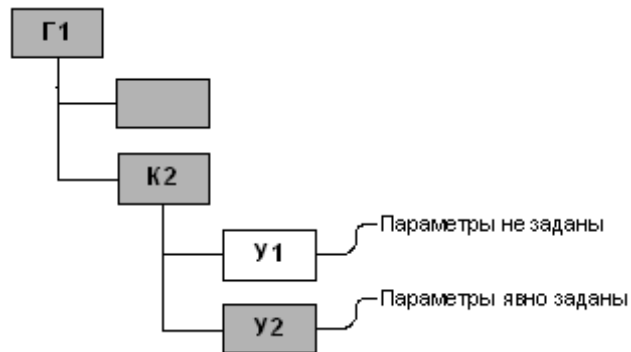
Описание предусмотренных возможностей для добавления устройств и принтеров см. на стр.57 и стр.59.



Правила наследования параметров списка устройств

В рамках групповой или локальной политики права доступа к каждому объекту, а также параметры контроля устройств определяются в соответствии с правилами наследования или явного задания параметров. Параметры могут быть заданы для групп, классов, моделей или конкретных устройств. При задании

параметров может использоваться принцип наследования параметров от вышестоящих элементов иерархии в списке. 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.

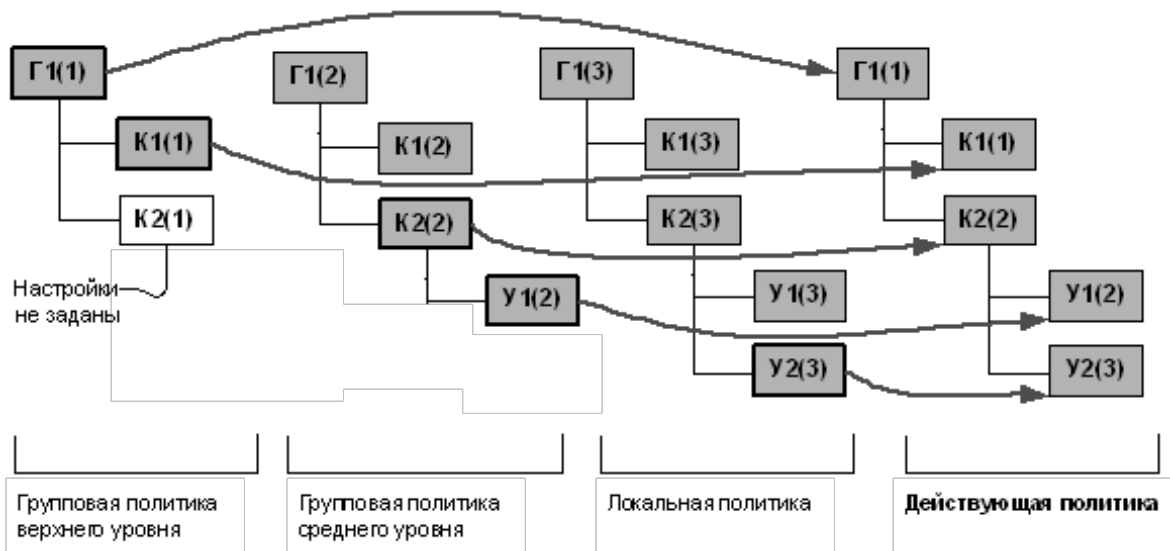


В приведенном на рисунке примере устройство "У1" наследует параметры, заданные для класса "К2". Для устройства "У2" действуют явно заданные параметры, которые могут отличаться от параметров, заданных для класса "К2".

Особенности применения групповых политик со списками устройств

В сетевом режиме функционирования системы Secret Net администратор безопасности имеет возможность создавать политики контроля устройств, которые могут применяться в домене в составе групповых политик. Политики контроля можно создавать как на уровне домена, так и на уровне организационных подразделений. При создании политики формируется список устройств и настраиваются права доступа и параметры контроля.

При входе пользователя в систему значения параметров контроля и доступа к устройствам устанавливаются в соответствии с действующей политикой. Действующая политика определяется по стандартному для Windows правилу применения на компьютере групповых политик (последовательность применения политик и их приоритет) с учетом параметров, 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 для групп (Г), классов (К) и отдельных устройств (У) показан на рисунке:



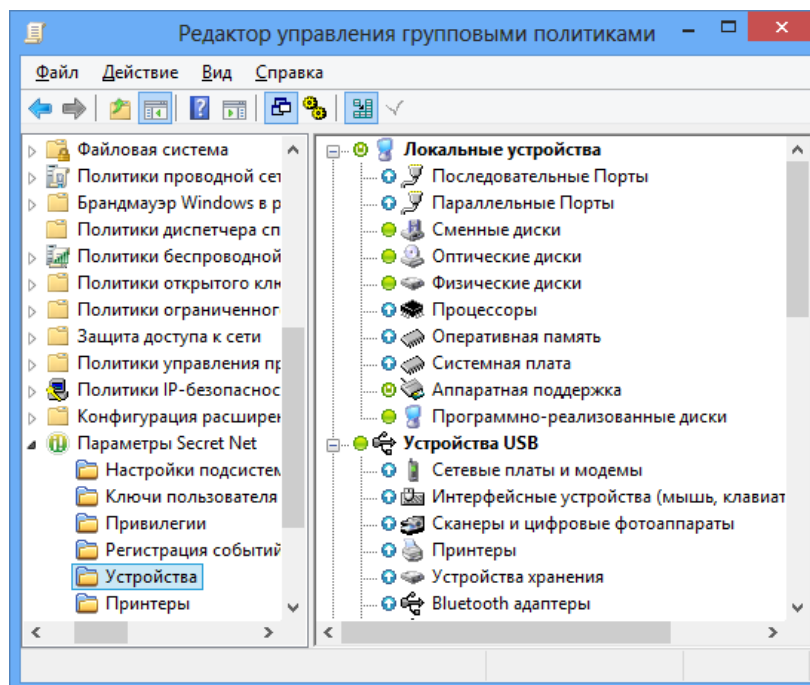
Задание групповой политики и просмотр списка устройств

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

После установки системы политика контроля устройств в групповых политиках отсутствует. Поэтому независимо от того, какой механизм настраивается, ее необходимо задать.

Для задания 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. 13).
2. Выберите папку "Устройства".
В правой части окна появится сообщение, что политика не определена.
3. Вызовите контекстное меню папки "Устройства" и выберите в нем команду "Политика | Создать".
В правой части окна появится общий список групп, классов и моделей устройств.



Удаление политики осуществляется с помощью команды "Политика | Удалить" в контекстном меню папки "Устройства".






Описание списка устройств

Управление устройствами осуществляется в списке устройств. Методы работы со списком устройств одинаковы для централизованного и локального управления. Различие заключается только в том, что после задания политики контроля устройств в групповой политике список содержит только группы, классы и предопределенные модели устройств. Добавление конкретных устройств в список осуществляется с помощью мастера импорта устройств (см. стр. 57).

В локальной политике безопасности в список устройств автоматически добавляются все обнаруженные устройства компьютера. Также в этот список помещаются сведения о устройствах, подключенных на терминальных клиентах данного компьютера во время терминальных сессий (при условии, что эти

устройства разрешены для использования — см. стр. 62). Подключенные в данный момент устройства отображаются в нормальном виде, отключенные — с зачеркнутыми именами.

Элементы списка устройств имеют определенную конфигурацию параметров, обеспечивающую функционирование всех нужных устройств с учетом логики управления в системе Secret Net. Конфигурация параметров не является одинаковой для различных элементов списка и зависит от принадлежности устройств группам, классам и от специфики использования устройств. Для удобного просмотра списка устройств и оперативного получения основных сведений о текущей конфигурации параметров предусмотрены специальные пиктограммы статуса, перечисленные в следующей таблице:

Пиктограмма	Описание
	Параметры контроля для устройства наследуются от вышестоящего элемента списка устройств
 (серый цвет)	Режим контроля для устройства отключен
	Для устройства включен режим контроля, при котором устройство должно быть постоянно подключено к компьютеру
 (зеленый цвет)	Для устройства включен режим контроля, при котором устройство разрешается подключать к компьютеру и отключать
 (красный цвет)	Для устройства включен режим контроля, при котором устройство запрещается подключать к компьютеру

Задание групповой политики использования принтеров

Для централизованного управления параметрами использования принтеров должна быть задана групповая политика, в которой определяются список принтеров и ограничения на их использование. После установки системы политика контроля принтеров в групповых политиках отсутствует.

Для задания политики контроля принтеров:

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. 13).
2. Выберите папку "Принтеры".
В правой части окна появится сообщение, что политика не определена.
3. Вызовите контекстное меню папки "Принтеры" и выберите в нем команду "Политика | Создать".
В правой части окна появится элемент списка принтеров "Настройки по умолчанию".

Удаление политики осуществляется с помощью команды "Политика | Удалить" в контекстном меню папки "Принтеры".

Добавление устройств в список групповой политики

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

Предусмотрены следующие способы добавления устройств:

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

**Внимание!**

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

Использование мастера импорта устройств

Мастер импорта предоставляет следующие возможности:

- добавление стандартного устройства из предопределенного списка (например, порт ввода/вывода);
- импорт устройства из файла, в котором сохранены (экспортированы) сведения об устройстве. Экспорт сведений об устройствах можно выполнить централизованно в программе оперативного управления (см. документ [4]), в программе просмотра локальных журналов (см. документ [5]) или в списке устройств групповой политики другого уровня (см. ниже);
- импорт устройств из записей журнала Secret Net со сведениями о подключенных к компьютеру устройствах. Мастер импорта обрабатывает записи, сохраненные в файлах форматов *.dvt и *.evt* (*.evt или *.evtx). Описание процедуры экспорта записей журнала в файл см. в документах [4] и [5].

Для импорта устройств в список групповой политики:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 13).
2. Выберите папку "Устройства".
В правой части окна появится список устройств.
3. В меню оснастки выберите команду "Действие | Политика | Добавить устройство".
На экране появится стартовый диалог мастера импорта устройств.
4. Выберите вариант добавления устройства, нажмите кнопку "Далее >" и следуйте инструкциям мастера.

Экспорт сведений об устройствах из списка устройств

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

Примечание.

Экспорт в файл формата *.sndev поддерживается только для устройств. Чтобы сохранить сведения о классах и группах, необходимо использовать процедуру экспорта параметров политики (см. стр. 161).

Для экспорта сведений об устройстве:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 13).
2. Выберите папку "Устройства".
В правой части окна появится иерархический список устройств.
3. Вызовите контекстное меню нужного устройства и выберите команду "Экспорт".
На экране появится стандартный диалог сохранения файла ОС Windows.
4. Укажите имя файла для сохранения сведений.

Использование буфера обмена для добавления устройств

Сведения об устройстве можно скопировать в буфер обмена из следующих

источников:

- список устройств групповой политики другого уровня;
- запись журнала Secret Net о событии подключения или запрета подключения устройства.

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

Копирование сведений об устройстве в буфер обмена из записи журнала Secret Net выполняется с помощью команды в контекстном меню записи журнала. Сведения о программных средствах для работы с журналами системы Secret Net см. в документах [4] и [5].

Добавление принтеров в список групповой политики

В список принтеров групповой политики можно добавлять элементы, соответствующие конкретным принтерам. Добавление осуществляется с помощью специальной программы-мастера. При необходимости принтер можно удалить из списка — для этого вызовите контекстное меню принтера и активируйте команду "Удалить".

Использование мастера добавления принтеров

Мастер добавления предоставляет следующие возможности:

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

Для добавления принтера в список групповой политики:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 13).
2. Выберите папку "Принтеры".
В правой части окна появится список принтеров.
3. В меню оснастки выберите команду "Действие | Добавить принтер".
На экране появится стартовый диалог мастера добавления принтеров.
4. Выберите вариант добавления принтера, нажмите кнопку "Далее >" и следуйте инструкциям мастера.

Контроль подключения и изменения устройств

Изменения аппаратной конфигурации могут быть вызваны выходом из строя, добавлением или заменой отдельных устройств. В процессе эксплуатации системы администратор безопасности в случае необходимости вносит изменения в настройки механизма контроля подключения и изменения устройств.



Список устройств, подключенных к компьютеру (аппаратная конфигурация), формируется при установке клиентского ПО Secret Net 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.

При настройке механизма контроля подключения и изменения устройств выполняются действия:

1. Настройка политики контроля устройств.
2. Разрешение и запрет использования определенных типов устройств при терминальных подключениях.
3. Изменение перечня регистрируемых событий.

Задание и настройка политики контроля устройств

Настройку политики контроля устройств можно выполнить:

- индивидуально для каждого устройства;
- для модели, класса или группы устройств с использованием принципа наследования параметров.

В сетевом режиме функционирования системы Secret Net можно задать политику контроля устройств в групповых политиках (см. стр. 56). Если политика не задана, на компьютерах действует локальная политика, включающая в себя настройки контроля подключения и изменения устройств по умолчанию (см. стр. 51). Если политика задана, работа механизма определяется действующей групповой политикой.

Для настройки политики контроля устройств:

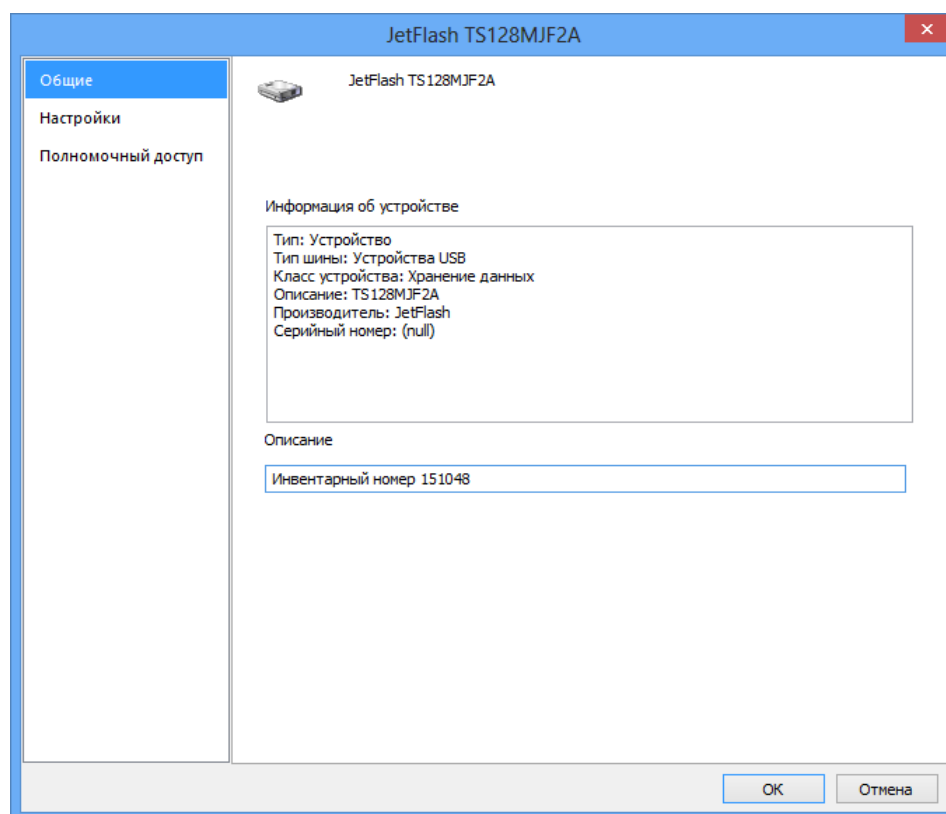
1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 13).

2. Выберите папку "Устройства".

В правой части окна появится общий список устройств аппаратной конфигурации.

3. Выберите в списке объект (группу, класс, модель или устройство), вызовите контекстное меню и выберите команду "Свойства".

На экране появится диалог для настройки параметров объекта. По умолчанию в диалоге отображаются параметры группы "Общие", представляющие основные сведения об объекте.

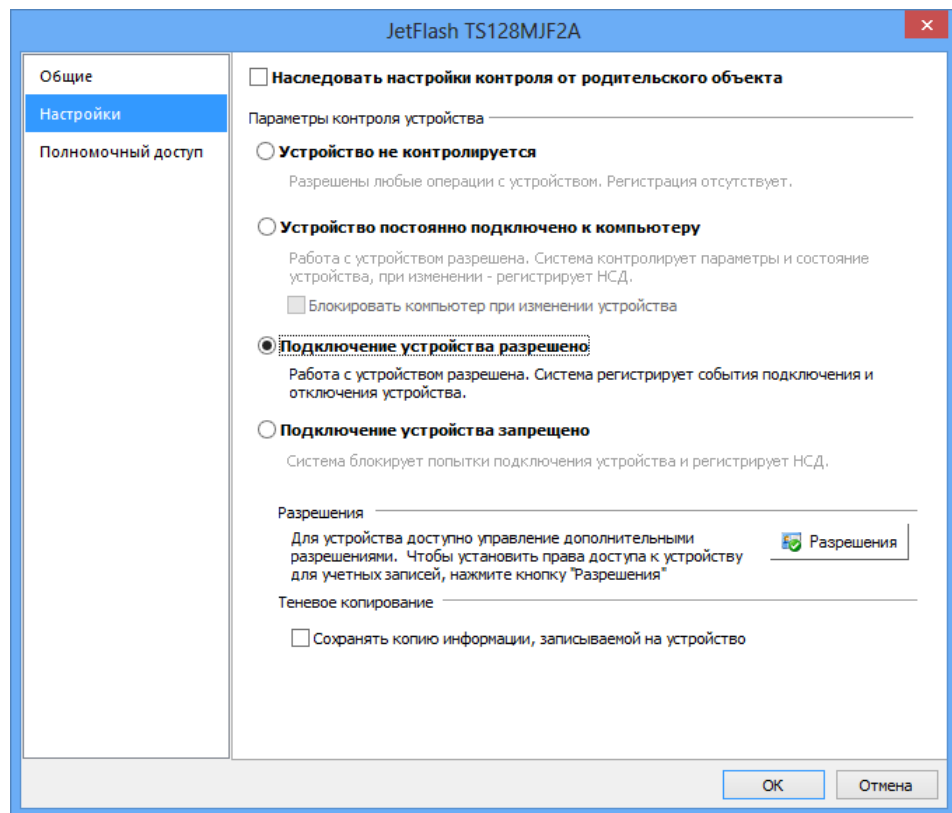


4. При необходимости введите дополнительные сведения об объекте в поле "Описание".

Примечание.

Дополнительные сведения, указанные для устройства, сохраняются в журнале при регистрации событий, связанных с этим устройством.

5. Перейдите к группе параметров "Настройки".



Для объекта с явно заданными параметрами контроля в поле "Наследовать настройки контроля от родительского объекта" отсутствует отметка. Если поле содержит отметку, это означает, что параметры контроля для данного объекта наследуются от вышестоящего объекта (для устройства вышестоящим является класс или модель, а для класса — группа). В этом случае параметры будут недоступны для изменения, но они будут отображать состояние параметров родительского объекта.

6. Если для данного объекта требуется задать явно политику контроля, удалите отметку из поля "Наследовать настройки контроля от родительского объекта" и настройте параметры контроля.

Поле "Устройство не контролируется"

Если в поле установлена отметка — для объекта отключен режим контроля

Поле "Устройство постоянно подключено к компьютеру"

Если в поле установлена отметка — для объекта включен режим контроля, при котором устройство должно быть постоянно подключено к компьютеру. В случае изменения состояния устройства в журнале регистрируются события несанкционированного доступа (НСД), и система ожидает утверждение изменений аппаратной конфигурации администратором безопасности.

Для усиления защиты можно дополнительно включить режим автоматического блокирования компьютера при изменении состояния устройства: для этого установите отметку в поле "Блокировать компьютер при изменении устройства". Возможность разблокировки компьютера будет иметь только администратор безопасности

Поле "Подключение устройства разрешено"

Если в поле установлена отметка — для объекта включен режим контроля, при котором устройство разрешается подключать к компьютеру и отключать. В случае изменения состояния устройства в журнале регистрируются соответствующие события. Утверждение изменений аппаратной конфигурации при этом не требуется. Параметр присутствует только для тех устройств, для которых отслеживается процесс подключения и можно запретить использование

Поле "Подключение устройства запрещено"

Если в поле установлена отметка — для объекта включен режим контроля, при котором устройство запрещается подключать к компьютеру. Попытки подключения устройства регистрируются в журнале как события НСД.
 Параметр присутствует только для тех устройств, для которых отслеживается процесс подключения и можно запретить использование

7. Если все вложенные элементы в списке устройств должны наследовать политику контроля от текущего элемента (группы, класса или модели), нажмите кнопку "Применить эти настройки ко всем дочерним объектам" — для всех подчиненных объектов будет включен режим "Наследовать настройки контроля от родительского объекта".

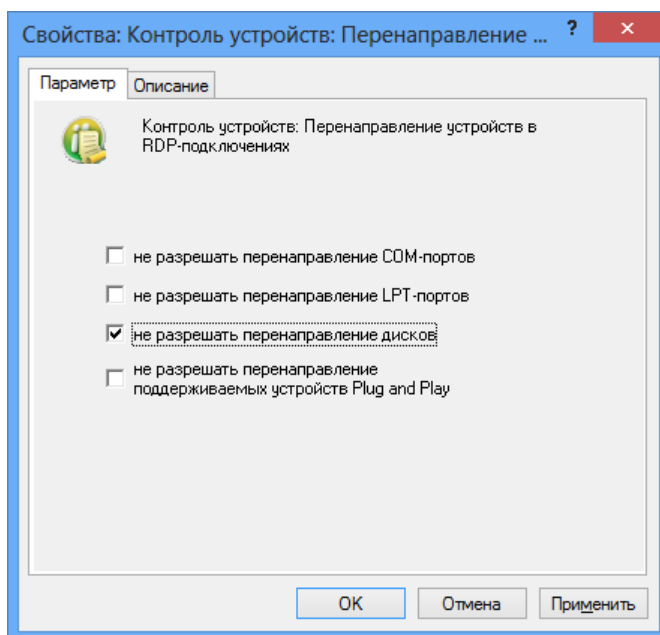
Разрешение и запрет использования устройств на терминальных клиентах

При функционировании компьютера в качестве сервера терминальных подключений по протоколу Remote Desktop Protocol (RDP) можно включить запрет использования определенных типов устройств на компьютерах терминальных клиентов. В этих условиях пользователи удаленных компьютеров не смогут использовать в терминальных сессиях соответствующие локальные устройства и ресурсы. Запрет действует и в случае, если в параметрах удаленного подключения такие устройства/ресурсы были отмечены для использования. Управление режимами разрешения и запрета предусмотрено для следующих типов устройств:

- устройства, подключенные к последовательным (COM) портам;
- устройства, подключенные к параллельным (LPT) портам;
- подключенные диски;
- устройства Plug and Play.

Для управления режимами разрешения и запрета использования устройств:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 13).
2. Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.
3. В списке параметров выберите элемент "Контроль устройств: Перенаправление устройств в RDP-подключениях" и вызовите диалог настройки параметра.



4. Чтобы запретить использование типов устройств, установите отметки в соответствующих полях. Для разрешения использования — удалите отметки.
5. Нажмите кнопку "ОК".

Изменение перечня регистрируемых событий

Для отслеживания произошедших событий, связанных с работой механизма контроля подключения и изменения устройств, необходимо выполнить настройку регистрации событий. Для этого следует указать, какие события категории "Контроль конфигурации" должны регистрироваться в журнале Secret Net. Описание процедуры настройки списка регистрируемых событий см. на стр. [151](#).

Утверждение конфигурации

Изменения аппаратной конфигурации отслеживаются системой защиты для устройств с включенным режимом контроля "Устройство постоянно подключено к компьютеру". При обнаружении изменений в журнале регистрируются события НСД. Если дополнительно включен режим "Блокировать компьютер при изменении устройства", выполняется блокировка компьютера. Снять блокировку компьютера и утвердить изменения в аппаратной конфигурации может только администратор.

Утверждение конфигурации можно выполнить локально или централизованно в программе оперативного управления (см. документ [4]).

Для локального утверждения конфигурации:

1. Вызовите оснастку "Локальная политика безопасности" и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. [13](#)).
2. Выберите папку "Устройства".
Если произошли изменения в аппаратной конфигурации компьютера, на экране появится запрос для вывода списка изменений и утверждения аппаратной конфигурации.
3. Нажмите кнопку "Да".
На экране появится диалог со списком изменений аппаратной конфигурации.
4. Нажмите кнопку "Утвердить" для утверждения изменений.



До утверждения конфигурации в панели инструментов оснастки отображается активная кнопка вызова диалога со списком изменений. Используйте кнопку, если по каким-либо причинам утверждение конфигурации не было выполнено.

Избирательное разграничение доступа к устройствам и принтерам

При настройке разграничения доступа пользователей к устройствам и принтерам выполняются действия:

1. Настройка прав доступа пользователей к устройствам и принтерам.
2. Настройка регистрации событий и аудита операций с устройствами.

Настройка прав доступа к устройствам

Права доступа пользователей могут устанавливаться для отдельных устройств или для классов.

Для настройки прав доступа к устройствам:

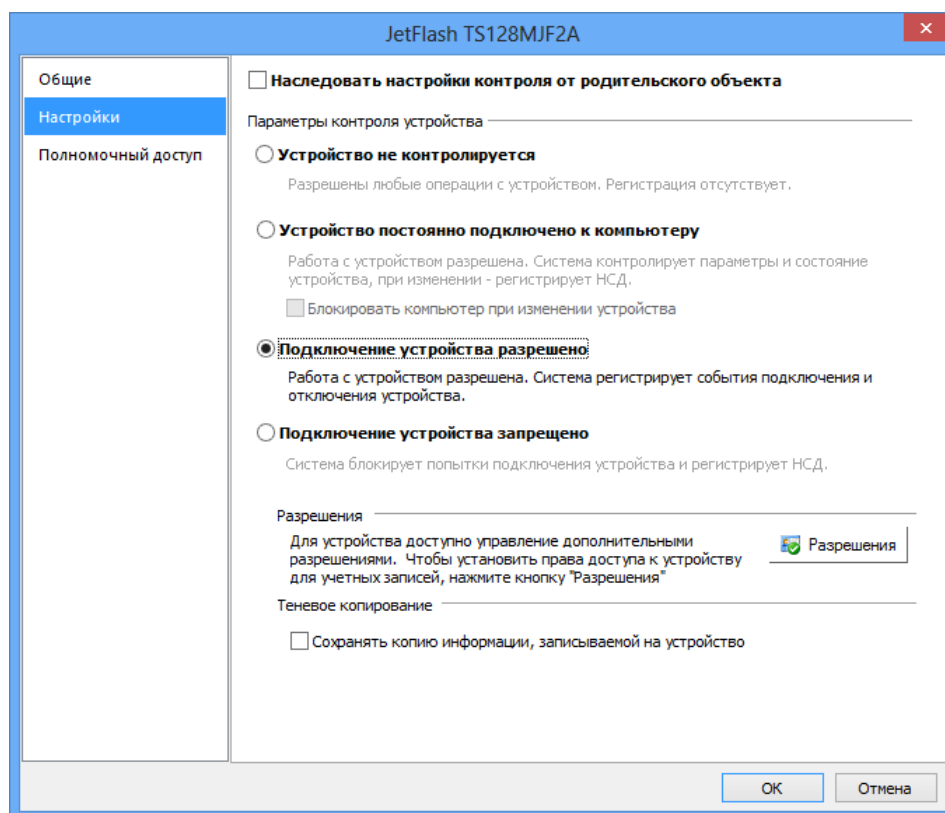
1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. [13](#)).
2. Выберите папку "Устройства".

В правой части окна оснастки появится список устройств.

3. Выберите в списке объект (класс или устройство), вызовите контекстное меню и выберите команду "Свойства".

На экране появится диалог для настройки параметров объекта.

4. Перейдите к группе параметров "Настройки".



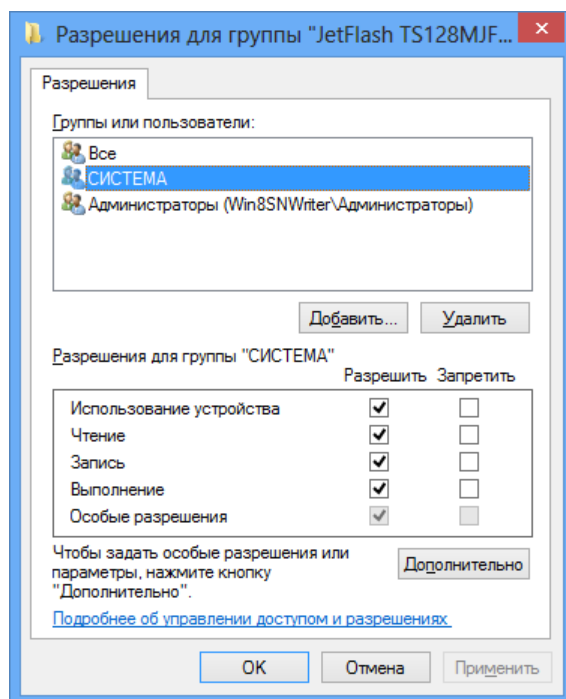
5. Удалите отметку из поля "Наследовать настройки контроля от родительского объекта".

После этого станут доступны параметры контроля устройства.

6. Отметьте режим контроля "Устройство постоянно подключено к компьютеру" или "Подключение устройства разрешено" и нажмите кнопку "Разрешения".

На экране появится диалог ОС Windows "Разрешения..."

Следует иметь в виду, что возможность вызова диалога "Разрешения..." предусмотрена только для тех устройств, для которых допускается настройка разрешений и запретов: порты, диски, носители данных (для системного диска управление разрешениями запрещено).



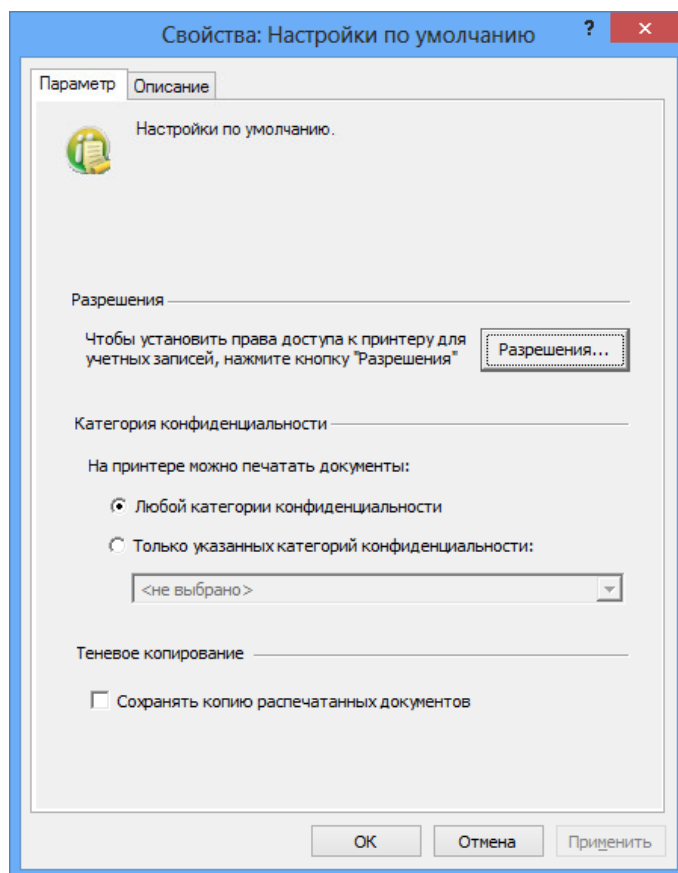
7. При необходимости отредактируйте список учетных записей в верхней части диалога.
8. Для изменения параметров доступа выберите в списке нужную учетную запись и затем расставьте разрешения и запреты на выполнение операций. При этом учитывайте принцип наследования параметров от родительских объектов дочерними: явно заданные параметры перекрывают унаследованные от родительских объектов.
Для настройки особых разрешений нажмите кнопку "Дополнительно" и настройте параметры в открывшемся диалоговом окне.

Настройка прав пользователей для печати на принтерах

Права пользователей для печати документов могут устанавливаться для конкретных принтеров или для элемента "Настройки по умолчанию".

Для настройки прав пользователей для печати:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 13).
2. Выберите папку "Принтеры".
В правой части окна оснастки появится список принтеров.
3. Выберите в списке нужный элемент, вызовите контекстное меню и выберите команду "Свойства".
На экране появится диалог для настройки параметров.



4. Нажмите кнопку "Разрешения".

На экране появится диалог ОС Windows "Разрешения...".

5. При необходимости отредактируйте список учетных записей в верхней части диалога.
6. Для изменения параметров доступа выберите в списке нужную учетную запись и затем отметьте разрешение или запрет на выполнение печати.

Настройка регистрации событий и аудита операций с устройствами

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. Описание процедуры настройки списка регистрируемых событий см. на стр. [151](#).

Настройка аудита успехов и отказов

Настройка аудита выполнения операций с устройствами может выполняться для 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. [13](#)).
2. Выберите папку "Устройства".
В правой части окна оснастки появится список устройств.

- 3.** Выберите в списке объект (класс или устройство), вызовите контекстное меню и выберите команду "Свойства".
На экране появится диалог для настройки параметров объекта.
- 4.** Перейдите к группе параметров "Настройки" и нажмите кнопку "Разрешения".
На экране появится диалог ОС Windows "Разрешения...".
- 5.** Нажмите кнопку "Дополнительно".
На экране появится диалоговое окно настройки дополнительных параметров.
- 6.** Перейдите к диалогу "Аудит" и настройте параметры аудита ОС Windows.

Глава 4

Настройка механизмов КЦ и ЗПС

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, 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. В ЛБД КЦ-ЗПС на каждом компьютере хранится модель данных, относящаяся к этому компьютеру.

В сетевом режиме функционирования системы Secret Net в централизованном хранилище 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. В данной главе рассматриваются методы работы с программой. Описание интерфейса программы приведено в приложении на стр. 167.

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 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 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 о запусках программ из журнала Secret Net. При централизованном управлении администратору безопасности (или аудитору) с помощью программы просмотра журналов необходимо создать файл журнала в dvt-формате, содержащий выборку записей за интересующий период. Затем этот файл с помощью программы управления КЦ-ЗПС в централизованном режиме импортируется в базу данных КЦ-ЗПС. При использовании программы управления КЦ-ЗПС в локальном режиме сведения о запусках программ можно загрузить

непосредственно из локального журнала. Далее на основании этих данных формируются задания ЗПС для субъектов.

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

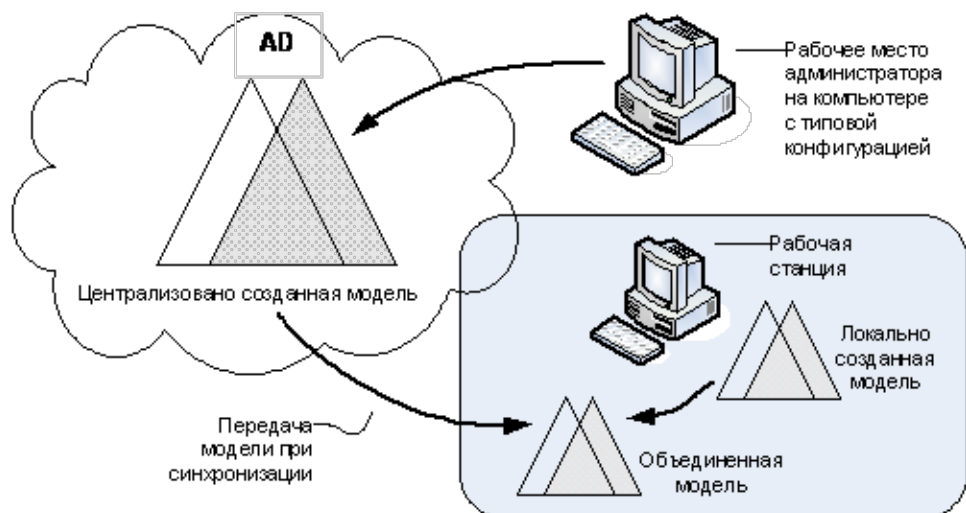
При синхронизации происходит передача изменений, внесенных в ЦБД КЦ-ЗПС, на все те компьютеры, к которым эти изменения относятся. Изменения сохраняются в ЛБД КЦ-ЗПС. Синхронизация может выполняться в следующие моменты:

- 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.

Примечание.

Чтобы синхронизация выполнялась незамедлительно при сохранении модели данных в ЦБД, необходимо разослать на компьютеры оповещения об изменениях. Запуск рассылки оповещений можно выполнять вручную или автоматически (см. стр. 86). Для оперативной синхронизации на компьютерах должны быть настроены определенные параметры ОС Windows (см. стр. 209).

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.

Запуск программы управления КЦ-ЗПС

Для работы с программой управления КЦ-ЗПС пользователь должен входить в локальную группу администраторов компьютера. Чтобы работать с программой в централизованном режиме, пользователь дополнительно должен входить и в группу администраторов домена безопасности. Если хранилище объектов централизованного управления Secret Net размещается в базе данных доменных служб Active Directory, необходимыми правами для запуска программы обладают как пользователи, входящие в доменную группу администраторов, так и пользователи доменной группы SecretNetAdmins (см. стр. [12](#)).

Описание интерфейса программы приведено в приложении на стр. [167](#).

Для запуска программы в локальном режиме:

- Выполните соответствующее действие в зависимости от версии установленной операционной системы:
 - на компьютере под управлением ОС Windows 8 или Windows Server 2012 загрузите начальный экран "Пуск" и выберите элемент "Контроль программ и данных" (относится к группе "Код безопасности");
 - на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код безопасности | Secret Net | Контроль программ и данных".

Для запуска программы в централизованном режиме:

1. Выполните соответствующее действие в зависимости от версии установленной операционной системы:
 - на компьютере под управлением ОС Windows 8 или Windows Server 2012 загрузите начальный экран "Пуск" и выберите элемент "Контроль программ и данных (централизованный режим)" (относится к группе "Код безопасности");
 - на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код безопасности | Secret Net | Контроль программ и данных (централизованный режим)".

При запуске программа проверяет возможность полного доступа к модели данных соответствующей разрядности в ЦБД КЦ-ЗПС. Полный доступ возможен только с одного компьютера системы.

2. Если возможность полного доступа к ЦБД отсутствует (на другом компьютере с ОС той же разрядности уже работает программа управления КЦ-ЗПС в централизованном режиме), на экране появится сообщение об этом с запросом на выполнение дальнейших действий. Предусмотрены следующие варианты:
 - отменить запуск программы (рекомендуется) — для этого нажмите кнопку "Отмена" в диалоге запроса;
 - запустить программу с доступом к ЦБД КЦ-ЗПС в режиме "только для чтения" — для этого нажмите кнопку "Нет" в диалоге запроса. В этом случае в программу будет загружена последняя сохраненная в ЦБД модель данных. Возможность редактирования модели будет отсутствовать;

- запустить программу и получить полный доступ к ЦБД — для этого нажмите кнопку "Да" в диалоге запроса. Это приведет к тому, что пользователь, работающий с программой управления КЦ-ЗПС на другом компьютере, потеряет возможность записи в ЦБД и сохранения сделанных изменений.

Порядок настройки

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. 73	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. 73	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. 74	Добавление задач в модель данных В модель данных добавляются описания задач (прикладное и системное ПО, наборы файлов данных и т. д.) для контроля целостности и использования в ЗПС в соответствии с требованиями, разработанными на 1-м этапе
Этап 4 см. стр. 76	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. 80	Подготовка ЗПС к использованию Субъектам назначаются задания ЗПС. Для того чтобы ресурсы контролировались механизмом ЗПС, они должны быть специально подготовлены — иметь признак "выполняемый"
Этап 6 см. стр. 82	Расчет эталонов Для всех заданий рассчитываются эталоны ресурсов
Этап 7 см. стр. 84	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. 85	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. 85	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

Во время установки клиентского ПО системы Secret Net проверяется наличие модели данных в БД КЦ-ЗПС. Если модель данных отсутствует, автоматически выполняется ее формирование и наполнение объектами по умолчанию: при установке клиента в автономном режиме функционирования формируется локальная модель данных, при установке в сетевом режиме — централизованная модель для ОС соответствующей разрядности.

При начальном формировании в модель добавляются следующие задания:

- "Задание для контроля ресурсов Secret Net";
- "Задание для контроля реестра Windows";
- "Задание для контроля файлов Windows".

Задания включают готовые задачи с ресурсами, сформированными по предопределенному списку. Для этих заданий устанавливаются связи со следующими субъектами:

- в локальной модели — с субъектом "Компьютер";
- в централизованной модели — с субъектом КЦ SecretNetIcheckDefault (для 32-разрядных ОС) или SecretNetIcheckDefault64 (для 64-разрядных ОС). Субъект содержит список компьютеров домена безопасности с версией ОС соответствующей разрядности и установленным клиентским ПО системы Secret Net.

Также в модель добавляются некоторые дополнительные задачи, не связанные с заданиями.

В процессе эксплуатации системы может возникнуть необходимость корректировки или пересмотра модели данных. 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. 93).

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);
- перечень ресурсов, подлежащих контролю целостности;
- перечень программ, с которыми разрешено работать разным группам пользователей.

В сетевом режиме функционирования системы Secret Net 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.

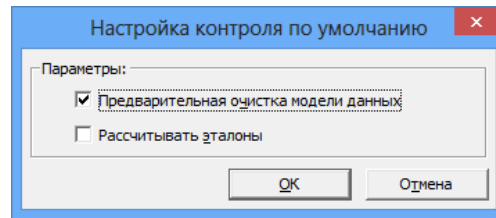
Редактирование централизованных моделей данных осуществляется со следующими особенностями: для редактирования доступна та модель данных, которая соответствует разрядности ОС Windows на рабочем месте администратора. Модель данных другой разрядности доступна только для чтения (при этом можно экспортировать 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

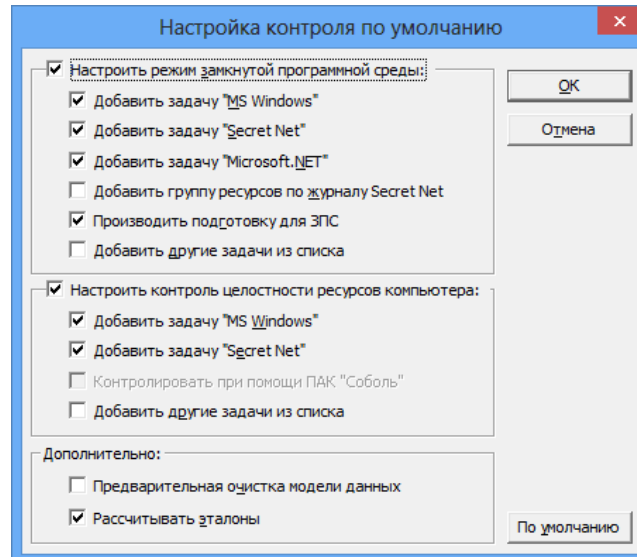
Данный этап выполняется только при формировании новой модели данных.

Для построения фрагментов модели по умолчанию:

1. В программе управления выберите команду "Файл | Новая модель данных".
 - В централизованном режиме на экране появится диалог:



- В локальном режиме на экране появится диалог:



2. Настройте параметры нужным образом и нажмите кнопку "ОК".

- В централизованном режиме рекомендуется оставить заданные параметры без изменения.

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.

- В локальном режиме предоставляется возможность детальной настройки параметров для формирования новой модели данных. Помимо стандартных задач в модель можно добавить задачи, сформированные на основе ресурсов приложений. Добавление таких задач осуществляется с помощью параметра "Добавить другие задачи из списка".

Примечание.

Для механизма ЗПС рекомендуется оставить включенным параметр "Производить подготовку для ЗПС" для выполнения операции подготовки ресурсов. Ресурсы будут помечены признаком "выполняемый", и для исполняемых файлов будет выполнен поиск других, связанных с ними модулей. Это основное назначение данной операции, без нее настройка ЗПС будет неполноценной.

После успешного формирования модели данных в основном окне программы управления КЦ-ЗПС появится новая структура объектов.

3. Выберите 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). 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

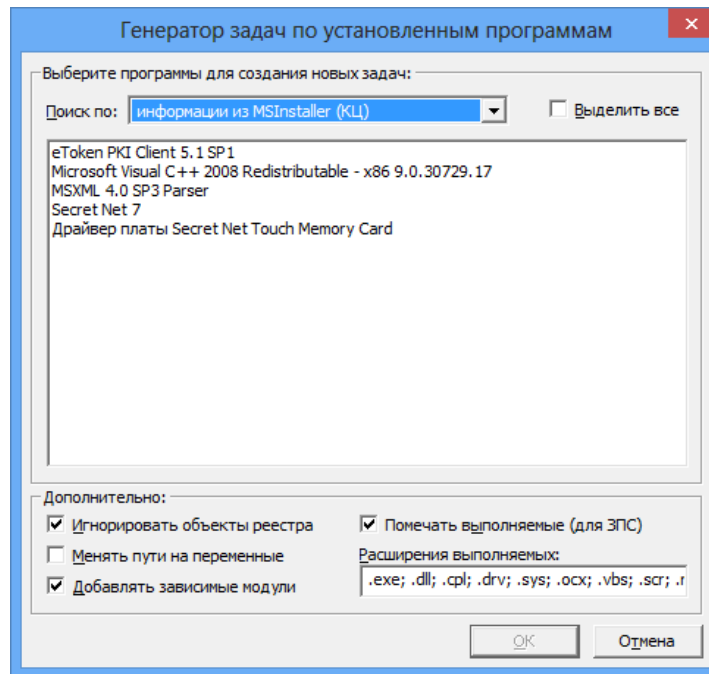
модели данных сложными задачами, включающими в себя большое количество ресурсов.

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. **107**).

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.

Совет.

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

Условие	Пояснение
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 (для ЗПС)	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

Примечание.

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 "ОК".

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 ресурсов;
- перечень событий, регистрируемых в журнале;
- расписание, в соответствии с которым должна проводиться проверка.

Для формирования задания:**1. Выберите категорию "Задания" и в меню "Задания" выберите команду "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. [112](#).

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.
Предусмотренные методы перечислены в следующей таблице.

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



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.

Соответствие типов ресурсов и методов контроля представлено в следующей таблице.

	Содержимое объекта	Атрибуты объекта	Права доступа	Существование объекта
Файл	Да	Да	Да	Да
Каталог	Да	Да	Да	Да

	Содержимое объекта	Атрибуты объекта	Права доступа	Существование объекта
Ключ реестра	Да	Нет	Да	Да
Значение реестра	Да	Нет	Нет	Да

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

Предусмотрены следующие алгоритмы: CRC7, ЭЦП, хэш, имитовставка, полное совпадение, встроенная ЭЦП.

Особенности некоторых алгоритмов:

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.

Алгоритм "встроенная ЭЦП" позволяет обеспечить выполнение контроля целостности файлов, обновленных при установке обновлений ПО приложений и операционной системы. Алгоритм отличается тем, что при контроле целостности осуществляется проверка встроенной цифровой подписи файлов (формат подписи Microsoft Authenticode). Необходимым условием для успешного завершения проверки является неизменность сертификата подписанного файла. Если при расчете эталонов для файла не обнаружена встроенная цифровая подпись, этот файл будет игнорироваться при контроле с использованием данного алгоритма.

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.

Предусмотренные события перечислены в следующей таблице.

Событие	Описание события
Успех завершения	Успешное завершение задания на контроль целостности
Ошибка завершения	Обнаружено нарушение целостности при обработке задания
Успех проверки	Успешная проверка целостности ресурса
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. Реакция доступна не для всех методов
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 продолжается 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

Поле	Использование
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 .



Внимание!

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 "Задания" на панели категорий.
2. В окне структуры вызовите контекстное меню для задания и выберите 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

В Secret Net используется одна привилегия, связанная с работой ЗПС. Эта привилегия по умолчанию предоставлена группе "Администраторы". На пользователей, которым предоставлена данная привилегия, действие механизма замкнутой программной среды не распространяется.

Для предоставления привилегии:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret

Net" (см. стр. **13**).

2. Выберите папку "Привилегии".
В правой части окна появится список привилегий.
3. Вызовите контекстное меню для строки "Замкнутая программная среда: не действует" и выберите 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 используйте 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".
На экране появится диалог для выбора объектов.
3. Найдите и выберите нужный объект. Если хранилище объектов ЦУ размещается вне Active Directory, предоставляется возможность создания и редактирования групп.
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 субъект, с которым требуется связать задание, вызовите контекстное меню и выберите 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. [109](#).

Этап 6. Расчет эталонов

Расчет эталонов необходим для контролируемых ресурсов, входящих в задания контроля целостности, а также и в задания ЗПС, если предусмотрен контроль целостности разрешенных для запуска программ. Процедура расчета выполняется автоматически, если модель данных создается с помощью мастера (см. стр. [73](#)). Если построение модели осуществляется с использованием генератора задач или вручную, расчет эталонов должен выполняться отдельно.

На этапе настройки механизмов КЦ и ЗПС целесообразно применять следующие способы расчета эталонов:

- расчет эталонов всех контролируемых ресурсов локальной модели данных (в централизованном режиме работы программы "Контроль программ и данных" в этом случае происходит расчет эталонов только тех ресурсов, которые относятся к тиражируемым заданиям);
- расчет эталонов контролируемых ресурсов, относящихся к определенному заданию.

В локальном режиме расчет эталонов может быть выполнен для всех ресурсов, имеющих в локальной модели данных. Исключение составляют те ресурсы, эталоны которых рассчитаны централизованно (ресурсы входят в тиражируемые задания).

В централизованном режиме используются различные методы расчета эталонов для тиражируемых и нетиражируемых заданий. Расчет эталонов тиражируемых заданий выполняется аналогично, как и в локальном режиме (эти эталоны будут затем переданы на компьютеры). Эталоны ресурсов для новых нетиражируемых заданий рассчитываются на компьютерах автоматически после передачи их в ЛБД при синхронизации. Если в нетиражируемое задание были внесены изменения, администратор может использовать команду для инициирования процесса расчета эталонов.

Для расчета эталонов в локальном режиме:

1. В зависимости от того, для каких ресурсов требуется рассчитать эталоны, выполните соответствующее действие:
 - чтобы выполнить расчет эталонов всех контролируемых ресурсов модели данных — выберите в меню "Сервис" команду "Эталон | Расчет";
 - чтобы выполнить расчет эталонов ресурсов отдельного задания — вызовите контекстное меню этого задания и выберите команду "Расчет эталонов".

На экране появится диалог "Расчет эталонов".

2. Если требуется сохранить предыдущие значения эталонов, установите отметку в поле "Оставлять старые".

Примечание.

Необходимость сохранения прежних ("старых") эталонных значений может возникнуть, например, при контроле содержимого файлов, изменяемых при автоматическом обновлении ПО. Дополнительные сведения об этом см. на стр. [110](#).

3. Настройте реакцию системы защиты на возможные ошибки при расчете эталонов. Для этого в левой части таблицы выберите вид ошибки, а в правой выберите нужную реакцию системы.

Ошибки могут быть следующих 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 реакций, перечисленных в следующей таблице.

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.

Предусмотренные варианты продолжения процедуры перечислены в следующей таблице.

Вариант	Описание
Игнорировать	Процедура расчета будет продолжена. Реакция системы на ошибку отсутствует. Ресурс, вызвавший ошибку, остается в составе задачи (или задач). При проверке целостности ресурса будет регистрироваться событие НСД с соответствующей реакцией (кроме варианта контроля по алгоритму "встроенная ЭЦП", если в файле отсутствует встроенная цифровая подпись на момент расчета эталона — в этом случае ресурс будет игнорироваться при контроле)
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 тиражируемых заданий (централизованный режим):

1. В зависимости от того, для каких ресурсов требуется рассчитать эталоны,

выполните соответствующее действие:

- чтобы выполнить расчет эталонов всех тиражируемых заданий — выберите в меню "Сервис" команду "Эталоны | Расчет";
- чтобы выполнить расчет эталонов ресурсов отдельного тиражируемого задания — вызовите контекстное меню этого задания и выберите команду "Локальный расчет эталонов".

На экране появится диалог "Расчет эталонов".

2. Выполните действия, описанные в процедуре расчета эталонов в локальном режиме, начиная с шага 2 (см. выше).

Для расчета эталонов нетиражируемого задания (централизованный режим):

1. Вызовите контекстное меню нетиражируемого задания и выберите нужную команду:
 - чтобы отложить расчет эталонов нетиражируемого задания до следующей синхронизации ЦБД и ЛБД на компьютерах — выберите команду "Отложенный расчет эталонов";
 - чтобы инициировать незамедлительный расчет эталонов — выберите команду "Удаленный расчет эталонов".

На экране появится диалог для выбора субъектов. Диалог содержит список субъектов, с которыми связано выбранное задание.

2. Выделите субъекты, на компьютерах которых требуется выполнить расчет эталонов для ресурсов данного задания. Нажмите кнопку "ОК".

Примечание.

Незамедлительный расчет эталонов (по команде "Удаленный расчет эталонов") следует выполнять только для компьютеров, включенных в данный момент. Если компьютер отключен, для расчета эталонов нетиражируемых заданий на этом компьютере можно использовать команду "Отложенный расчет эталонов" или выполнить на этом компьютере расчет эталонов в локальном режиме.

Этап 7. Включение ЗПС в "жестком" режиме

Для включения ЗПС в "жестком" режиме необходимо выключить "мягкий" режим в свойствах нужного субъекта. Одновременно с этим можно настроить дополнительные параметры контроля.

Параметры механизма ЗПС можно задать централизованно или локально. При этом в централизованном режиме доступна возможность задания параметров как для отдельных компьютеров, так и для групп компьютеров. Если заданы разные параметры механизма ЗПС для компьютера и для группы, в которую он входит, — на компьютере будут действовать все включенные параметры этих субъектов (параметры "суммируются"). Например, если для группы включен параметр "Мягкий режим", этот режим будет действовать на компьютере, даже если тот же параметр будет отключен для самого компьютера.

Для включения механизма ЗПС в "жестком" 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 выберите команду "Свойства". В появившемся окне "Свойства субъекта управления" перейдите к диалогу "Режимы".
3. При работе в централизованном режиме установите отметку в поле "Режимы заданы централизованно".
4. Установите отметку в поле "Режим ЗПС включен" и удалите отметку из поля "Мягкий режим" (если она там установлена).
5. 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. Нажмите кнопку "ОК".

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 выберите 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 своевременно исправить ошибки, связанные с некорректной настройкой заданий.

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

Для проверки задания предусмотрен облегченный режим и режим полной имитации. 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 локальном режиме работы программы проверку можно выполнить для любых заданий КЦ, связанных с компьютером (включая задания, созданные централизованно). В централизованном режиме возможна локальная проверка тиражируемых заданий, а также удаленная проверка любых централизованных заданий на включенных компьютерах выбранных субъектов.

Для запуска проверки в локальном режиме:

1. Выберите в меню "Сервис" команду "Запуск задания".
На экране появится диалог со списком всех заданий контроля целостности.
2. Выберите в списке нужное задание. При необходимости проверки в режиме полной имитации установите отметку в поле "Полная имитация".
3. Нажмите кнопку "ОК".

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

Для локальной проверки тиражируемых заданий (централизованный режим):

1. Выберите в меню "Сервис" команду "Запуск задания".
На экране появится диалог со списком тиражируемых заданий контроля целостности.
2. Выполните действия, описанные в процедуре запуска проверки в локальном режиме, начиная с шага 2 (см. выше).

Для удаленной проверки задания (централизованный режим):

1. Вызовите контекстное меню задания и выберите команду "Удаленный запуск заданий".
На экране появится диалог для выбора субъектов. Диалог содержит список субъектов, с которыми связано выбранное задание.
2. Выделите субъекты, на компьютерах которых требуется запустить проверку задания. Нажмите кнопку "ОК".

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

Примечание.

Удаленная проверка заданий может выполняться только для компьютеров, включенных в данный момент.

Сохранение и загрузка модели данных

Сохранение

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

В централизованном режиме работы программы сохранение модели данных в ЦБД возможно при условии полного доступа к базе данных. Если полный доступ заблокирован (например, по причине запуска программы управления КЦ-ЗПС в централизованном режиме на другом компьютере), при попытке сохранения модели на экране появится сообщение о невозможности внесения изменений в базу данных. Программа в этом случае перейдет в режим доступа к ЦБД "только для чтения", в результате чего станет невозможно сохранить сделанные изменения в текущем сеансе. Возможность записи в ЦБД будет доступна только в следующем сеансе работы с программой.

Чтобы загрузить в следующем сеансе текущую редакцию модели данных, можно выполнить процедуру экспорта модели в файл, перезапустить программу и затем импортировать модель из файла (см. стр.89, стр.91).

Оповещение об изменениях

В сетевом режиме функционирования системы Secret Net сведения об изменениях в модели данных, выполненных в централизованном режиме, распространяются на включенные компьютеры домена в соответствии с настройкой параметра группы "Оповещения" (см. стр.169).

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 выберите в меню "Сервис" команду "Оповестить об изменениях".

Настройка автоматического запуска синхронизации

При внесении изменений в ЦБД КЦ-ЗПС должна выполняться синхронизация этих изменений на компьютерах с последующим перерасчетом эталонных значений ресурсов (если это необходимо). Запуск синхронизации осуществляется локально на компьютерах в определенные моменты времени.

Настройка параметров запуска синхронизации осуществляется в централизованном режиме работы программы. Параметры могут быть заданы как для отдельных компьютеров, так и для групп. При этом действуют приоритеты применения параметров: наивысший приоритет имеют параметры компьютеров, затем параметры групп, кроме группы по умолчанию SecretNetICheckDefault, и, наконец, параметры самой группы по умолчанию. Например, если заданы разные параметры синхронизации для компьютера и для группы, в которую он входит, — на компьютере будут действовать только параметры компьютера.

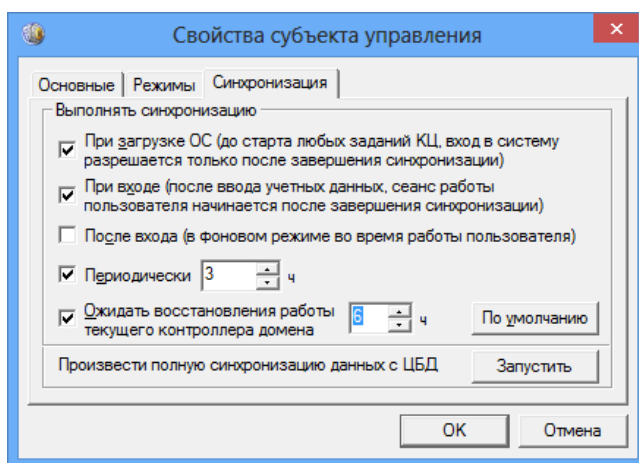
Пояснение.

Параметры групп, в которые включен компьютер, действуют в том случае, если в модели отсутствует субъект для этого компьютера со своими параметрами синхронизации. При этом между группами определен следующий порядок применения параметров: если компьютер включен в еще одну группу помимо группы по умолчанию SecretNetICheckDefault — на этом компьютере будут действовать параметры первой группы (не SecretNetICheckDefault). Если таких групп несколько и для них заданы разные параметры — применяются параметры группы по умолчанию.

Для своевременного выявления конфликтующих параметров синхронизации групп предусмотрена процедура проверки этих параметров. Проверку следует выполнять при наличии в модели нескольких групп, в которые могут быть включены одни и те же компьютеры.

Для настройки параметров запуска синхронизации:

1. В централизованном режиме программы управления КЦ-ЗПС 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 выберите команду "Свойства". В появившемся окне "Свойства субъекта управления" перейдите к диалогу "Синхронизация".



3. Настройте параметры запуска процесса синхронизации. Описание параметров представлено в следующей таблице.

Параметр	Пояснение
При загрузке ОС...	Если установлена отметка, запуск синхронизации происходит при загрузке операционной системы до момента старта выполнения заданий КЦ. Таким образом, до начала выполнения на компьютере любых заданий КЦ, они будут синхронизированы с ЦБД. При этом возможность входа пользователя в систему будет предоставлена только после завершения синхронизации. Действие данного параметра может приводить к задержкам входа при изменении в ЦБД объемных заданий и при низкой пропускной способности каналов связи
При входе...	Если установлена отметка, запуск синхронизации происходит после ввода пользователем своих учетных данных для входа в систему до момента старта выполнения заданий КЦ. Начало сеанса работы пользователя откладывается до завершения синхронизации. Действие данного параметра может приводить к задержкам входа при изменении в ЦБД объемных заданий и при низкой пропускной способности каналов связи
После входа...	Если установлена отметка, синхронизация выполняется в фоновом режиме после начала сеанса работы пользователя
Периодически	Если установлена отметка, запуск синхронизации происходит во время работы компьютера через указанный промежуток времени (в часах)

Примечание.

Если отключен автоматический запуск синхронизации (удалены отметки в полях "При загрузке ОС...", "При входе...", "После входа..." и "Периодически"), синхронизация на компьютере может выполняться только при поступлении оповещения об изменениях или по команде администратора. Для этого компьютер должен быть включен.

- В случае, если хранилище объектов централизованного управления Secret Net размещается в БД доменных служб Active Directory, можно включить режим ожидания восстановления связи с контроллером домена при его временной недоступности. Для этого установите отметку в поле "Ожидать восстановления работы текущего контроллера домена" и укажите период ожидания в часах. Это позволит откладывать запуск полной синхронизации ЦБД и ЛБД КЦ-ЗПС при проведении кратковременных регламентных работ на контроллере домена (перезагрузка и пр.) и снизить нагрузку на каналы связи при подключении резервного контроллера.

Пояснение.

Полная синхронизация подразумевает передачу из ЦБД сведений по всем ресурсам, а не только по измененным, как при очередной синхронизации. При включенном режиме ожидания, если произошла смена контроллера домена, полная синхронизация не выполняется до появления исходного контроллера (с которого выполнялась предыдущая успешная синхронизация). Запуск синхронизации происходит, но процесс прерывается с ошибкой "контроллер домена недоступен". Если по окончании указанного промежутка времени (начиная с момента первой неудачной синхронизации) исходный контроллер домена остался недоступен, выполняется полная синхронизация с имеющегося на данный момент контроллера домена.

При отключенном режиме ожидания, если произошла смена контроллера домена, незамедлительно выполняется полная синхронизация с имеющегося на данный момент контроллера.

В случае, если хранилище объектов централизованного управления размещается вне AD, данный параметр не действует, поскольку смена контроллера домена не вызывает необходимость полной синхронизации. В этих условиях контролируется доступность сервера служб каталогов AD LDS/ADAM. Если произошло переключение на другой сервер, при следующей синхронизации из ЦБД нового сервера будут загружены все сведения о ресурсах, то есть будет проведена полная синхронизация.

- Нажмите кнопку "ОК".

Для проверки параметров запуска синхронизации в группах:

- В централизованном режиме программы управления КЦ-ЗПС выберите в меню "Сервис" команду "Проверить синхронизацию групп".

Программа выполнит проверку вхождения компьютеров в группы с различными параметрами синхронизации. После проверки будут выведены сведения о результатах.

Принудительный запуск полной синхронизации

Запуск синхронизации изменений ЦБД КЦ-ЗПС на компьютерах может выполняться автоматически в соответствии с заданными параметрами (см. стр. [87](#)). При работе с программой в централизованном режиме администратор может запустить внеочередной процесс полной синхронизации изменений ЦБД КЦ-ЗПС на определенных компьютерах.

Запуск синхронизации можно выполнить как для отдельных компьютеров, так и для групп. Однако при этом следует учитывать текущую загрузку каналов передачи данных, локальных и сетевых ресурсов. Без необходимости не следует запускать синхронизацию для групп компьютеров. Если в ЦБД хранится значительный объем данных, для полной синхронизации может потребоваться длительное время. В течение этого времени будут ограничены возможности работы пользователей на тех компьютерах, где проходит синхронизация.

Для запуска полной синхронизации:

1. В централизованном режиме программы управления КЦ-ЗПС 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 выберите команду "Свойства". В появившемся окне "Свойства субъекта управления" перейдите к диалогу "Синхронизация".
3. Нажмите кнопку "Запустить".

Произойдет запуск процесса синхронизации.

Загрузка и восстановление модели данных

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 и не уверены в их правильности, не сохраняйте их сразу в БД. В этом случае будет возможность вернуться к варианту модели, сохраненной в БД. Для этого используется операция восстановления.

Для восстановления модели из базы данных:

1. В меню "Файл" выберите 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 управления").

Примечание.

Для автоматизации резервного копирования БД КЦ-ЗПС предусмотрена возможность экспорта и импорта модели данных путем запуска программы из командной строки. Описание параметров запуска приведено в приложении на стр. [180](#).

Для экспортирования текущей модели данных:

1. В меню "Файл" выберите 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".

Примечание.

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 управления").

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 выберите 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".

Примечание.

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 управления") — позволяет импортировать из файла объекты, относящиеся к той же категории.

Примечание.

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" выберите 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:

Поле	Пояснение
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 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

5. В группе полей "Импортируемые объекты" выберите категории объектов, которые следует импортировать. Для этого отметьте названия соответствующих категорий (если в выбранном файле нет данных об объектах какой-либо категории, соответствующее ей поле будет заблокировано).



Внимание!

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

6. 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".

Примечание.

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".

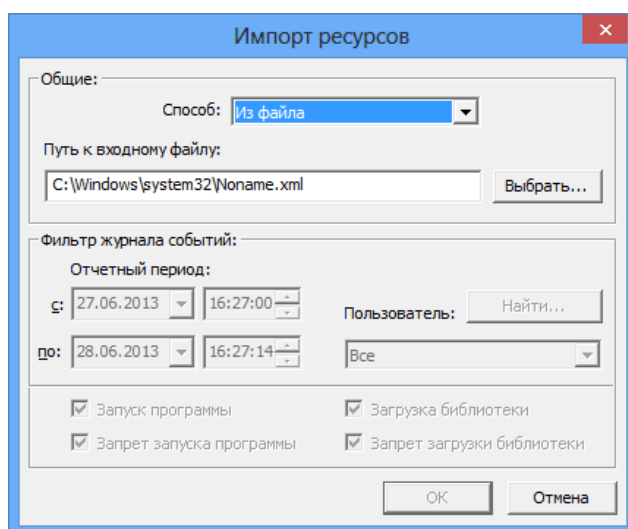
7. Нажмите кнопку "ОК" в диалоге настройки параметров импортирования.

Для импортирования объектов текущей категории:

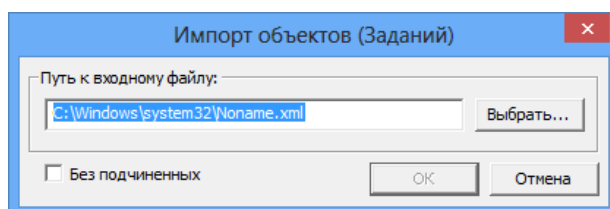
1. Выберите на панели категорий категорию, к которой относятся нужные объекты.
2. В окне структуры вызовите контекстное меню корневого элемента и выберите команду "Импорт и добавление".

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:



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. 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).

Внесение изменений в модель данных

На этапе создания модели данных, а также в процессе эксплуатации Secret Net 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. 94
Изменение параметров ресурса	стр. 94
Изменение параметров группы ресурсов	стр. 94
Изменение параметров задачи	стр. 94
Изменение параметров задания	стр. 94
Просмотр параметров субъекта управления	стр. 94
Добавление объектов	стр. 97
Добавление вручную одиночного ресурса	стр. 97
Добавление вручную нескольких ресурсов	стр. 97
Импорт списка ресурсов из журнала безопасности ОС Windows	стр. 97
Импорт списка ресурсов из журнала Secret Net	стр. 97
Добавление ресурса в группу	стр. 97
Добавление группы ресурсов вручную	стр. 97
Добавление группы ресурсов по каталогу	стр. 97
Добавление группы ресурсов по ключу реестра	стр. 97
Добавление группы ресурсов средствами импорта	стр. 97
Добавление задачи вручную	стр. 97
Добавление задачи с помощью генератора задач	стр. 74
Добавление задачи с помощью средств импорта	стр. 91
Добавление заданий	стр. 76
Добавление субъектов	стр. 85
Удаление объектов	стр. 106
Удаление объекта	стр. 106

Группа операций	Ссылка
Удаление всех объектов определенной категории	стр. 106
Связывание объектов	стр. 106
Связывание объектов	стр. 106
Удаление связи между объектами	стр. 106
Формирование задания ЗПС по журналу Secret Net	стр. 107
Подготовка ресурсов для ЗПС	стр. 109
Новый расчет и замена эталонов	стр. 110
Поиск зависимых модулей	стр. 111
Замена переменных окружения	стр. 112
Настройка задания для ПАК "Соболь"	стр. 112

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.

Ниже приведены параметры объектов каждой категории и даны пояснения по их применению.

Параметры ресурсов

Параметрами, определяющими свойства ресурса, являются:

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

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

Примечание.

Путь может быть задан явно (абсолютный путь) или с помощью переменных окружения (см. стр. [112](#)).

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.

Эталомом 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 ресурсов, являющихся файлами запуска программ (исполняемые файлы с расширением .exe), можно настраивать дополнительные параметры

исключений, которые будут применяться во время действия механизма ЗПС. Исключения позволяют разрешить выполнение процессом любых скриптов (например, запускаемых в программе Internet Explorer) или файлов из определенных каталогов, включая вложенные каталоги. С помощью этой функции реализуется возможность запуска в "жестком" режиме ЗПС таких программ, как, например, Photoshop CS2 и SolidWorks.

Для изменения параметров ресурса:

1. Выберите в области списка объектов ресурс, вызовите контекстное меню и выберите 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. Если для ресурса требуется указать исключения, применяемые во время действия механизма ЗПС (доступно только для исполняемых файлов с расширением .exe), нажмите кнопку "Дополнительно". В появившемся диалоге "Дополнительные свойства приложения" настройте параметры исключений и нажмите кнопку "ОК":
 - чтобы разрешить выполнение процессом любых скриптов, установите отметку в поле "Разрешено выполнять любые скрипты";
 - чтобы разрешить процессу запуск файлов из определенных каталогов, установите отметку в поле "Разрешено выполнять любые модули из указанных каталогов" и сформируйте список каталогов. Для добавления каталога в список введите путь к нему (путь можно ввести вручную или указать в стандартном диалоге, вызываемом с помощью кнопки справа от строки ввода) и нажмите кнопку добавления "+". Для удаления каталога из списка выберите этот каталог и нажмите кнопку удаления "-".
7. Нажмите кнопку "ОК".

Параметры группы ресурсов

Параметрами, определяющими свойства группы ресурсов, являются:

- имя группы;
- описание;
- тип ресурсов, входящих в данную группу.

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.

Для изменения параметров группы:

1. Выберите группу, вызовите контекстное меню и выберите 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

В свойствах задачи указываются имя, описание задачи и сценарий (при централизованном управлении). Задачи со сценарием обозначаются

пиктограммой .

Для изменения параметров задачи:

1. Выберите задачу, вызовите контекстное меню и выберите команду "Свойства".
Появится диалог для настройки параметров задачи.
2. Если требуется внести изменения в сценарий, нажмите кнопку "Сценарий" (составление сценария описано на стр. [97](#)).
3. Внесите изменения в поля "Имя" и "Описание" и нажмите кнопку "ОК".

Параметры задания

Свойства задания контроля целостности определяются группой общих параметров и расписанием. В общую группу параметров входят:

- имя и описание задания;
- вид задания — тиражируемое/нетиражируемое (только для централизованного управления);
- методы и алгоритмы контроля;
- реакция системы на результаты контроля.

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".

Свойства задания замкнутой программной среды определяют следующие параметры: имя задания, краткое описание и вид (тиражируемое/нетиражируемое).

Для изменения параметров задания:

1. Выберите задание, вызовите контекстное меню и выберите 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. [76](#)).

Параметры субъектов

Свойства субъектов управления определяют основные параметры и параметры работы защитных механизмов (в локальном управлении параметры работы механизмов доступны только для компьютеров). Основными параметрами являются:

- 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;
- параметры синхронизации ЦБД и ЛБД.

Кроме того, при размещении хранилища объектов ЦУ вне Active Directory для групп компьютеров предоставляется возможность редактировать состав группы путем добавления или удаления компьютеров.

Примечание.

Некоторые параметры (например, параметры синхронизации) настраиваются только в централизованном режиме работы программы. В локальном режиме такие параметры либо отсутствуют, либо отображаются без возможности редактирования.

Для изменения параметров субъекта:

1. Выберите субъект, вызовите контекстное меню и выберите команду "Свойства".

Появится диалог с основными параметрами выбранного субъекта.

2. Ознакомьтесь с основными параметрами и затем перейдите к другим диалогам (если они представлены в диалоговом окне).
3. Настройте доступные для изменения параметры 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/компьютеров.

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 выберите 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 вручную 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:

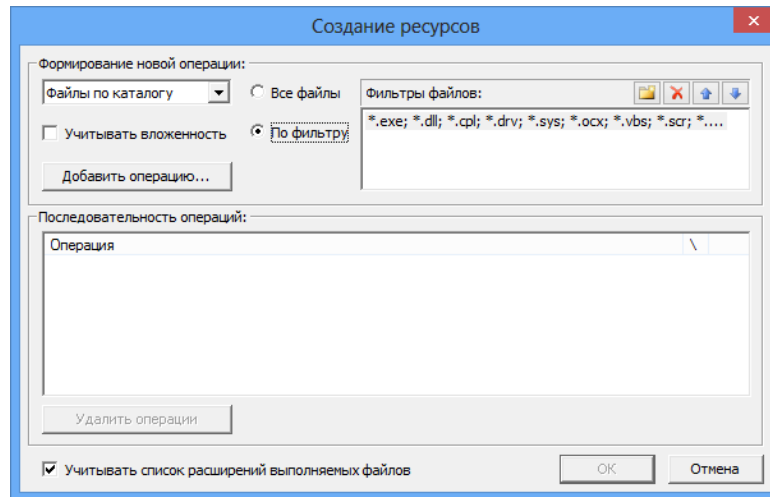
Параметр	Пояснение
Имя	Введите имя ресурса, уникальное для списка ресурсов. В качестве имени ресурса можно указать, например, имя файла, из которого загружен сценарий (скрипт)
Описание	Введите дополнительные сведения о ресурсе
Содержимое	Введите текст сценария (скрипта) — последовательность исполняемых 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 выберите в меню команду "Ресурсы | Создать ресурс(ы) | Несколько".

На экране появится диалог:



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	Предусмотрены следующие варианты: <ul style="list-style-type: none"> Выбранные файлы (стандартная процедура выбора файлов, дополнительные условия недоступны). Файлы по каталогу (добавляются файлы, входящие в указанный каталог, учитывается вложенность, можно использовать фильтр). Каталоги с файлами (учитывается вложенность, можно использовать фильтр). Каталоги по каталогу (учитывается вложенность). Переменные по ключу (выбираются переменные по ключу реестра, учитывается вложенность). 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 "Каталоги 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. 171). 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; *.ppf; *.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, выберите 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.

Примечание.

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.

Примечание.

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 закрывается и в нижней части диалога "Создание ресурсов" в список добавится описание выполненной операции.

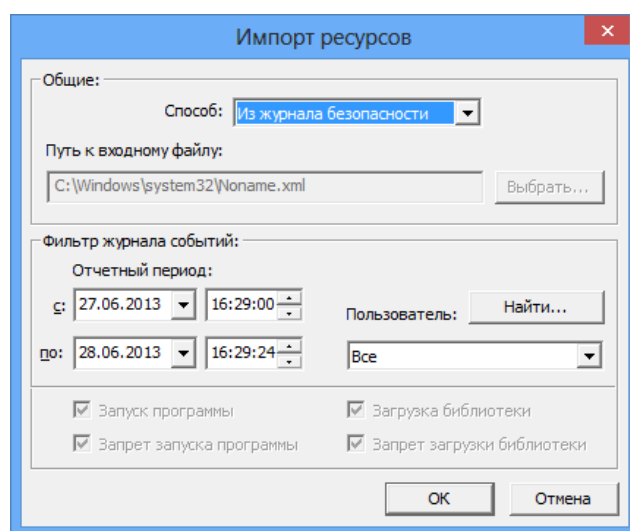
9. Проверьте список выполненных операций и, если он содержит все ресурсы, которые планировалось включить в модель данных, нажмите кнопку "ОК".

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 выберите 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 данном 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 "ОК".

Для импорта списка ресурсов из журнала Secret Net:

1. Выберите категорию "Ресурсы" и выберите 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.

Примечание.

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 "ОК".

Примечание.

По умолчанию импортируется информация о ресурсах, связанных со всеми предусмотренными 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 выберите команду "Добавить ресурсы", а затем команду:
 - "Существующие" — для выбора ресурсов из числа имеющихся в модели данных, но не входящих в данную группу.
 - "Новый одиночный" — для добавления одиночного ресурса (описание процедуры добавления вручную одиночного ресурса см. выше).
 - "Несколько новых" — для добавления нескольких ресурсов (описание процедуры добавления вручную нескольких ресурсов см. выше).
 - "Импортировать" — для импорта списка ресурсов из другого источника: из файла (описание процедуры импорта объектов см. на стр. 92), из журнала безопасности или журнала Secret Net (описание процедур импорта ресурсов из журналов см. выше).

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.

Примечание.

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".
На экране появится диалог для выбора типа ресурсов, которые будут определены по записям журнала — загружаемые модули приложений или исполняемые скрипты.
3. Выберите нужный тип ресурсов для получения из журнала:
 - "Загружаемые модули" — если группа должна содержать файлы, которые загружались при работе приложений;
 - "Исполняемые скрипты" — если группа должна содержать скрипты, о загрузке которых имеются сведения в журнале.
4. Нажмите кнопку "ОК".
На экране появится диалог настройки.
5. В централизованном режиме нажмите кнопку "Выбрать" и выберите файл формата dvt, в который предварительно были экспортированы сведения из журнала.
В локальном режиме выберите способ (журнал безопасности или журнал Secret Net).
В зависимости от режима и выбранного способа станут доступными настройки фильтра журнала событий.
6. 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. Выберите команду "Импорт и добавление" в меню "Группы ресурсов" или в контекстном меню, вызванном к папке "Группы ресурсов".
Появится диалог настройки параметров импортирования.
3. Выполните действия для импортирования объектов категории (описание процедуры импортирования см. на стр. 91).

Добавление задач

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

- вручную;
- вручную со сценарием;
- с помощью генератора задач (см. стр. 74);
- с помощью средств импорта (см. стр. 91).

Для добавления задачи вручную:

1. Выберите категорию "Задачи" и выберите 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:

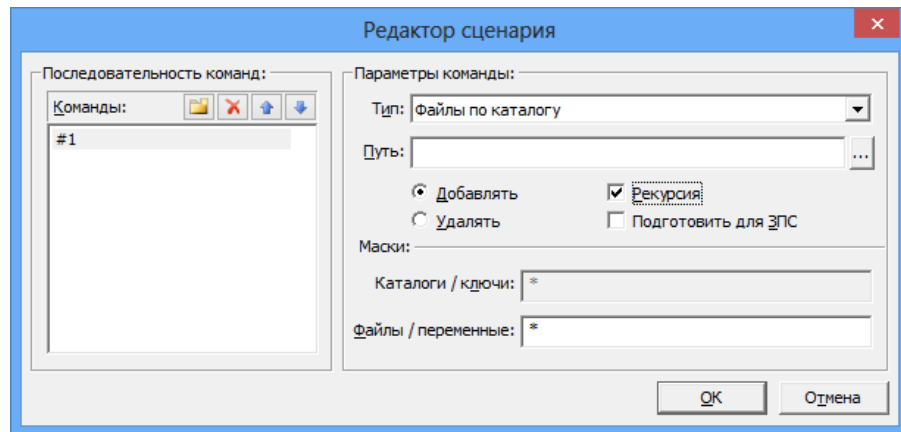
1. Выберите категорию "Задачи" и выберите в меню команду "Задачи | Создать задачу | Вручную".

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 задачу.

4. 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.

5. Выберите тип команды и укажите путь.

Предусмотренные типы команд перечислены в следующей таблице.

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"
Компоненты СЗИ Secret Net	Отбираются ресурсы из состава ПО клиента системы Secret Net

Тип команды	Пояснение
Файлы из переменных в указанном ключе реестра	Отбираются файлы, полученные из переменных реестра по заданному ключу реестра. Для задания базового ключа реестра указывается путь (например: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run). При отборе можно использовать маску, заданную в поле "Файлы/Переменные"
Загружаемые драйверы и сервисы Windows	Отбираются файлы драйверов и служб операционной системы

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".

6. 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.

7. Для применения команды ко всем вложенным ресурсам поставьте отметку в поле "Рекурсия".

8. Если выбраны команды "Файлы по каталогу" или "Каталоги с файлами", при необходимости используйте возможность добавления в список зависимых модулей (см. стр. 111). Для добавления зависимых модулей поставьте отметку в соответствующем поле.

9. 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.

Примечание.

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. 76.

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 диалог для 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.



Внимание!

После удаления ресурсов из задания следует выполнить перерасчет эталонов.



Предупреждение.

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.

В централизованном режиме при размещении хранилища объектов ЦУ вне Active Directory нельзя удалить группу по умолчанию SecretNet!CheckDefault или SecretNet!CheckDefault64 (в зависимости от разрядности ОС).

Для удаления объекта:

1. Найдите удаляемый объект, вызовите контекстное меню объекта и выберите 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 "Удалять 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 выберите 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.

**Внимание!**

В локальном режиме в объекты, созданные централизованными средствами, нельзя добавять: 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 выберите 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 выберите команду "Исключить из | <название объекта>".

Примечание.

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. 109)

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 выберите 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. Чтобы собрать нужные сведения, пользователям разрешается запускать любые приложения. Запуск приложений регистрируется в журнале Secret Net. На это отводится некоторый период времени. На время сбора сведений необходимо включить регистрацию всех событий категории "Замкнутая программная среда" на тех компьютерах, на которых замкнутая программная среда будет использоваться. Описание процедуры настройки списка регистрируемых событий см. на стр. **151**.

По окончании сбора сведений осуществляется формирование задач ЗПС в модели данных на основе сведений о запускаемых программах из журнала Secret Net. Экспорт сведений в модель данных может выполняться непосредственно из локального журнала Secret Net или из файла, в который предварительно были сохранены записи журнала. Описания процедур сохранения записей журнала в файл приводятся в документах [4] и [5].

Добавление задач ЗПС, созданных по журналу

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

Примечание.

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.

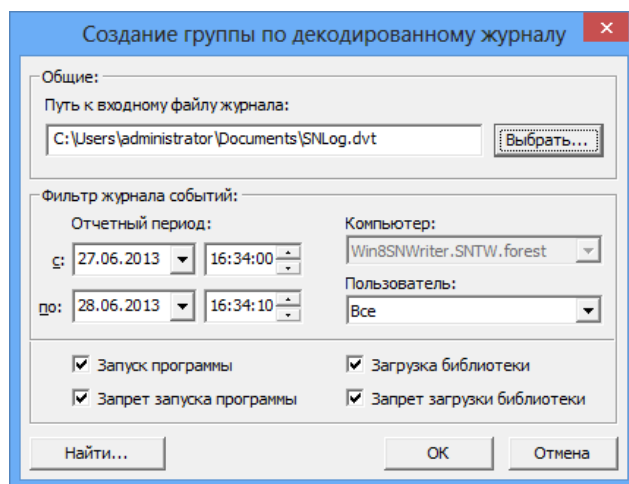
Для добавления задач ЗПС, созданных по журналу:

1. В основном окне программы управления КЦ-ЗПС выберите нужный субъект.
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 для выбора типа ресурсов, которые будут определены по записям журнала — загружаемые модули приложений или исполняемые скрипты.

4. Выберите нужный тип ресурсов для получения из журнала:
 - "Загружаемые модули" — если группа должна содержать файлы, которые загружались при работе приложений;
 - "Исполняемые скрипты" — если группа должна содержать скрипты, о загрузке которых имеются сведения в журнале.
5. Нажмите кнопку "ОК".

На экране появится диалог, подобный следующему:



6. 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 "ОК".

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 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.

Новый расчет и замена эталонов

При внесении изменений в модель данных новый расчет эталонов контролируемых ресурсов можно выполнить так же, как и при настройке модели данных (см. стр. 82). Кроме того, предусмотрены следующие способы:

- расчет эталонов отдельного ресурса;
- расчет эталонов нескольких произвольно выбранных ресурсов.

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.

При перерасчете эталонов может возникнуть необходимость сохранения прежних ("старых") значений. Например, при контроле содержимого файлов, изменяемых при автоматическом обновлении ПО.

Примечание.

Если для контроля содержимого используется алгоритм "встроенная ЭЦП", сохранение предыдущих эталонов для данного алгоритма в большинстве случаев не требуется. Обычно после обновления ПО сертификаты подписанных файлов остаются неизменными, благодаря чему эталоны для этих файлов будут действительны как до обновления ПО, так и после.

Предыдущие ("старые") эталоны удаляются из локальной базы данных автоматически при каждом успешном завершении задания контроля целостности. При необходимости можно использовать команду немедленного удаления старых эталонов.

Для пересчета эталона отдельного ресурса:

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

Появится диалог "Свойства ресурса" (см. стр. 94).

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".

Для расчета эталонов выбранных ресурсов:

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

2. Выделите в списке ресурс или несколько ресурсов, вызовите контекстное меню и выберите команду "Расчет эталонов".
На экране появится диалог "Расчет эталонов".
3. Выполните действия, описанные в процедуре расчета эталонов в локальном режиме, начиная с шага 2 (см. стр.82).

Для удаления старых эталонов:

- Выберите в меню команду "Сервис | Эталон | Удаление старых".
Старые эталоны будут удалены из модели данных.

Запрет использования локальных заданий

По умолчанию на компьютерах разрешается выполнение и локальных, и централизованных заданий. При необходимости можно отключить выполнение локальных заданий (созданных в ЛБД в локальном режиме работы программы), чтобы на компьютерах выполнялись только централизованные задания.

Отключение локальных заданий можно выполнить в свойствах нужного субъекта в централизованном режиме работы. Параметры могут быть заданы как для отдельных компьютеров, так и для групп компьютеров. При этом приоритет имеют отключенные параметры. Например, если для группы отключен параметр "Локальные задания ЗПС", такие задания будут запрещены на компьютере, даже если тот же параметр включен для самого компьютера.

Для отключения локальных заданий:

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 выберите команду "Свойства". В появившемся окне "Свойства субъекта управления" перейдите к диалогу "Режимы".
3. Удалите отметки в соответствующих полях:
 - чтобы отключить задания контроля целостности — удалите отметку из поля "Локальные задания КЦ";
 - чтобы отключить задания замкнутой программной среды — удалите отметку из поля "Локальные задания ЗПС".
4. Нажмите кнопку "ОК".

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 выберите 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 (для ЗПС)".
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 выберите 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. 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.

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" выберите категорию "Задания".
2. Добавьте в задание "Задание для ПАК "Соболь" все задачи контроля файлов средствами ПКЦ комплекса "Соболь".

Примечание.

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 выберите команду "Сохранить" в меню "Файл".
5. В меню "Сервис" выберите команду "Эталоны | Расчет".

После расчета эталонов на экране появится сообщение: "Завершение процедуры расчета эталонов будет произведено ПАК "Соболь" при перезагрузке".

6. Нажмите кнопку "ОК".



Внимание!

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

Полномочное управление доступом и контроль печати

Общие сведения

Механизм полномочного управления доступом обеспечивает разграничение доступа пользователей к конфиденциальным ресурсам. Ресурс считается конфиденциальным, если ему назначена категория конфиденциальности, отличная от категории для общедоступной информации (по умолчанию — "неконфиденциально"). Категорию можно назначить для следующих ресурсов:

- локальные физические диски (кроме диска с системным логическим разделом) и любые устройства, включаемые в группы устройств USB, PCMCIA, IEEE1394 или Secure Digital;
- каталоги и файлы на дисках с файловой системой NTFS.

Для сетевых интерфейсов можно указать уровни конфиденциальности сессий, в которых разрешается функционирование этих интерфейсов (используется в режиме контроля потоков).

Для принтеров можно указать категории конфиденциальности документов, разрешенных для печати.

Доступ пользователя к конфиденциальной информации осуществляется в соответствии с его уровнем допуска.

Категории конфиденциальности ресурсов

Категория конфиденциальности является атрибутом ресурса. По умолчанию в механизме полномочного управления доступом используются следующие категории конфиденциальности:

- "неконфиденциально";
- "конфиденциально";
- "строго конфиденциально".

При необходимости можно увеличить количество используемых категорий и задать для них названия в соответствии со стандартами, принятыми в вашей организации. Максимально возможное количество категорий — 16.

После установки клиентского ПО системы Secret Net всем каталогам и файлам на локальных дисках компьютера назначена категория "неконфиденциально" (если ресурсы не имеют ранее присвоенных категорий конфиденциальности). Повышение категорий конфиденциальности нужных файлов осуществляется пользователями в пределах своих уровней допуска. При этом понижать категории конфиденциальности ресурсов, а также повышать категории каталогов разрешено только пользователям, которым предоставлена привилегия на управление категориями конфиденциальности.

Для устройств, которым можно назначить категорию конфиденциальности или выбрать допустимые уровни конфиденциальности сессий, по умолчанию включен режим доступа "Устройство доступно без учета категории конфиденциальности" или "Адаптер доступен всегда". Для принтеров по умолчанию включен режим разрешения печати документов любой категории конфиденциальности. Данные режимы разрешают использование устройств и принтеров независимо от уровня допуска пользователя. Назначение устройствам и принтерам нужных категорий или уровней конфиденциальности осуществляется администратором.

Наследование категории конфиденциальности

В механизме полномочного управления доступом используется принцип наследования категорий конфиденциальности. Методы наследования различаются в зависимости от типов ресурсов.

Устройства наследуют категорию конфиденциальности от классов, к которым они относятся. При этом для класса разрешено указывать только категорию для общедоступной информации (по умолчанию — "неконфиденциально") или включить режим доступа "без учета категории конфиденциальности". За счет этого исключается возможность копирования конфиденциальной информации на неразрешенное подключенное устройство (при работе механизма в режиме контроля потоков и отсутствии у пользователя привилегии на вывод конфиденциальной информации).

В соответствии с правилами наследования при управлении устройствами (см. стр. 54) явно заданные параметры имеют приоритет перед наследуемыми параметрами старших элементов иерархии. Поэтому если для устройства явно назначена категория конфиденциальности, она действует независимо от того, какая категория указана для класса.

Назначение категорий конфиденциальности для устройств и классов выполняется администратором при работе со списком устройств групповой политики.

Категория конфиденциальности устройства имеет более высокий приоритет в сравнении с категориями файлов и каталогов, расположенных на этом устройстве. Если категория файла (каталога) ниже категории конфиденциальности устройства, система считает категорию файла (каталога) равной категории устройства. При обратной ситуации, когда категория файла (каталога) превышает категорию конфиденциальности устройства, такое состояние расценивается как некорректное, и доступ к файлу (каталогу) запрещается.

Между объектами файловой системы действует метод наследования внутри каталогов, имеющих категорию, отличную от категории для общедоступной информации (по умолчанию — "неконфиденциально"). Наследование категории конфиденциальности объектов внутри каталога осуществляется в соответствии с установленными признаками наследования в атрибутах этого каталога.

Присвоение новым подкаталогам и файлам категории конфиденциальности каталога может выполняться автоматически или по запросу. Включение и отключение режима автоматического присвоения категории осуществляется в диалоговом окне настройки свойств каталога (параметры "Автоматически присваивать новым каталогам" и "Автоматически присваивать новым файлам"). Установка признаков выполняется пользователем при условии наличия у него привилегии на управление категориями конфиденциальности.

Уровни допуска и привилегии пользователей

Уровни допуска

Доступ пользователя к конфиденциальной информации осуществляется при условии, если пользователю назначен соответствующий уровень допуска. Набор уровней допуска, применяемых в системе, совпадает с набором категорий конфиденциальности ресурсов (см. выше).

Пользователю разрешается доступ, если уровень допуска пользователя не ниже категории конфиденциальности ресурса. Например, пользователю с уровнем допуска "конфиденциально" разрешается выполнять чтение файлов с категориями "конфиденциально" и "неконфиденциально", но запрещено открывать файлы с категорией "строго конфиденциально". Наивысший уровень допуска предоставляет возможность открывать файлы с любой категорией конфиденциальности.

По умолчанию всем пользователям назначен уровень допуска "неконфиденциально". Описание процедуры назначения уровня допуска см. на стр. 119.

Привилегии пользователей

В механизме полномочного управления доступом могут действовать привилегии, перечисленные в следующей таблице:

Привилегия	Описание
Управление категориями конфиденциальности	Пользователь может: <ul style="list-style-type: none"> изменять категории конфиденциальности каталогов и файлов в рамках своего уровня допуска; управлять режимом наследования категорий конфиденциальности каталогов (см. стр. 120)
Печать конфиденциальных документов	Используется для разрешения пользователю выводить на принтер конфиденциальные документы. Привилегия применяется при включенном режиме контроля печати конфиденциальных документов
Вывод конфиденциальной информации	Пользователю разрешается выводить конфиденциальную информацию на внешние носители при включенном режиме контроля потоков. Устройство считается внешним носителем, если для него включен режим доступа "без учета категории конфиденциальности" и файловая система для хранения данных отличается от NTFS

Привилегии предоставляются администратором безопасности пользователям, уполномоченным управлять конфиденциальностью ресурсов, распечатывать и копировать конфиденциальную информацию (см. стр. **119**). По умолчанию пользователям привилегии не предоставлены.

Режим контроля потоков механизма полномочного управления доступом

Режим контроля потоков конфиденциальной информации обеспечивает строгое соблюдение принципов полномочного разграничения доступа и предотвращает несанкционированное копирование или перемещение конфиденциальной информации.

При включенном режиме контроля потоков возможность использования устройств и доступа к конфиденциальным файлам определяется уровнем конфиденциальности сессии, который устанавливается при входе пользователя в систему (см. ниже).

По умолчанию режим контроля потоков отключен. Для корректной работы системы перед включением режима следует выполнить дополнительную настройку параметров. Дополнительная настройка осуществляется локально с помощью программы настройки подсистемы полномочного управления доступом. Сведения о работе с программой см. на стр. **129**.

Уровень конфиденциальности сессии

Если включен режим контроля потоков, пользователи работают с ресурсами компьютера в рамках своих сессий, которым присваивается определенный уровень конфиденциальности. Сессия начинается и заканчивается вместе с сеансом работы пользователя на компьютере. Уровень конфиденциальности сессии устанавливается при входе пользователя в систему, и этот уровень нельзя изменить до окончания сессии.

Уровень сессии ограничивает категории конфиденциальности документов, с которыми пользователь работает в данном сеансе. При выполнении операций с ресурсами категории конфиденциальности ресурсов сравниваются с уровнем сессии. Доступ разрешается, если категория конфиденциальности ресурса ниже или совпадает с уровнем сессии. Запрещается доступ к ресурсам с более высокой категорией. Для всех создаваемых, скопированных или измененных документов присваивается категория конфиденциальности, равная уровню сессии.

В зависимости от заданных параметров присвоение уровня конфиденциальности сессии может выполняться по выбору пользователя или автоматически системой. При этом уровень сессии не может быть выше уровня допуска пользователя. Так, например, пользователь может выбрать уровень конфиденциальности сессии "конфиденциально" и тем самым запретить доступ к строго конфиденциальным ресурсам, даже если у него есть нужный уровень допуска. Однако следует иметь в виду, что неконфиденциальные документы, с которыми выполняются операции копирования и сохранения в конфиденциальной сессии, после выполнения операции станут конфиденциальными.

Автоматическое назначение уровня конфиденциальности для сессии пользователя выполняется в следующих случаях:

- если включен дополнительный параметр "строгий контроль терминальных подключений". Параметр определяет условие для уровня конфиденциальности терминальной сессии при терминальном входе — этот уровень должен быть равен уровню конфиденциальности локальной сессии на терминальном клиенте (соответственно, режим контроля потоков в этом случае также должен быть включен на клиенте);
- если включен дополнительный параметр "автоматический выбор максимального уровня сессии". Параметр задает принудительное назначение максимально возможного уровня конфиденциальности сессии пользователя в соответствии с уровнем допуска этого пользователя.

В режиме контроля потоков запрещается использование устройств, которым назначена категория конфиденциальности, отличающаяся от уровня сессии. Если на момент входа пользователя к компьютеру подключены устройства с различными категориями конфиденциальности, вход запрещается по причине конфликта подключенных устройств. Также запрещается вход в систему, если категория конфиденциальности подключенных устройств выше уровня допуска пользователя.

Режим контроля потоков позволяет установить ограничения на использование сетевых интерфейсов. Для каждого сетевого интерфейса можно указать уровни конфиденциальности сессий, в которых этот интерфейс будет доступен пользователю. Если открыта сессия с уровнем конфиденциальности, который не входит в список разрешенных уровней для сетевого интерфейса, его функционирование блокируется системой защиты.

Настройка механизма

Общий порядок настройки

Для использования на компьютерах механизма полномочного управления доступом выполните настройку в следующем порядке:

1. Задайте количество и названия категорий конфиденциальности (см. ниже).
2. Назначьте пользователям уровни допуска и привилегии (см. стр. [119](#)).
3. Присвойте ресурсам категории конфиденциальности (см. стр. [120](#)).
4. Настройте перечень регистрируемых событий (см. стр. [121](#)).
5. При необходимости включите режим контроля потоков (см. стр. [121](#)).
6. При необходимости настройте маркировку печати (см. стр. [123](#)).
7. При необходимости настройте использование принтеров (см. стр. [128](#)).

В документе с комментариями к выпущенной версии (Release Notes) приведены последние актуальные рекомендации разработчиков по настройке механизма для работы с приложениями.

Перед вводом механизма в использование разъясните пользователям правила работы с конфиденциальными ресурсами.

Настройка категорий конфиденциальности

Изменение количества используемых категорий конфиденциальности и их названий осуществляется в оснастке для управления параметрами объектов групповой политики.



Внимание!

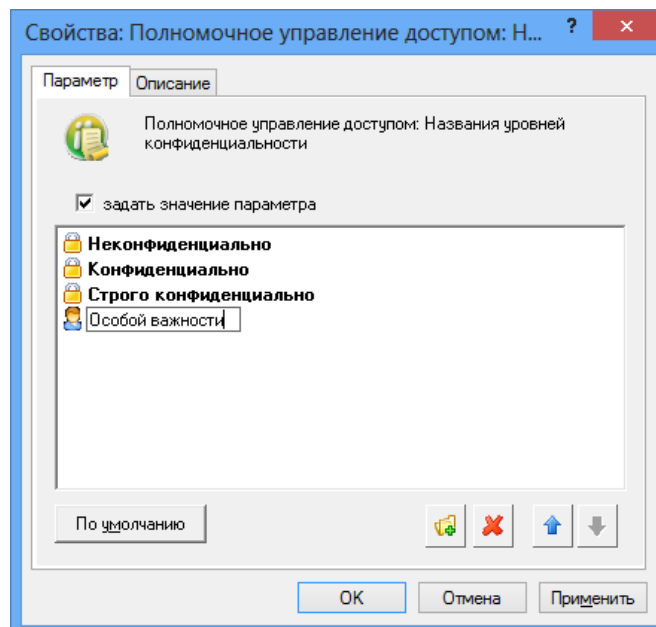
В сетевом режиме функционирования системы Secret Net, чтобы избежать конфликтов в названиях категорий конфиденциальности, количество и названия для категорий должны быть заданы в одной общей групповой политике, которая применяется на защищаемых компьютерах. В системе Secret Net могут использоваться следующие групповые политики в порядке возрастания приоритета применения параметров:

- политика безопасности домена, заданная в стандартных оснастках ОС Windows;
- политика организационного подразделения, заданная в стандартных оснастках ОС Windows, — для всех компьютеров, входящих в это организационное подразделение;
- политика домена, заданная в программе оперативного управления системы Secret Net;
- политика организационного подразделения, заданная в программе оперативного управления системы Secret Net, — для всех компьютеров, входящих в это организационное подразделение;
- политика, заданная для сервера безопасности в программе оперативного управления системы Secret Net, — применяется на всех компьютерах, подчиненных этому серверу безопасности.

Для настройки количества и названий категорий конфиденциальности:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 13).
2. Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.
3. Вызовите контекстное меню для параметра "Полномочное управление доступом: Названия уровней конфиденциальности" и выберите в нем команду "Свойства".

На экране появится диалог настройки параметра.



Диалог содержит список категорий конфиденциальности, используемых в системе. Список упорядочен по степени важности категорий с точки зрения конфиденциальности информации. Наименьший уровень (приоритет) имеет первый элемент списка, наибольший уровень — у последнего элемента.

4. Сформируйте список категорий конфиденциальности и нажмите кнопку "OK". Для добавления, удаления или перемещения элементов используйте соответствующие кнопки справа под списком или команды контекстного меню. Чтобы переименовать категорию, вызовите ее контекстное меню и выберите команду "Переименовать". При необходимости восстановить исходный набор категорий нажмите кнопку "По умолчанию".

Примечание.

Новые категории помещаются в конец списка, после чего их можно переместить на нужную позицию. Возможность удаления доступна для всех категорий, кроме первых трех элементов списка.

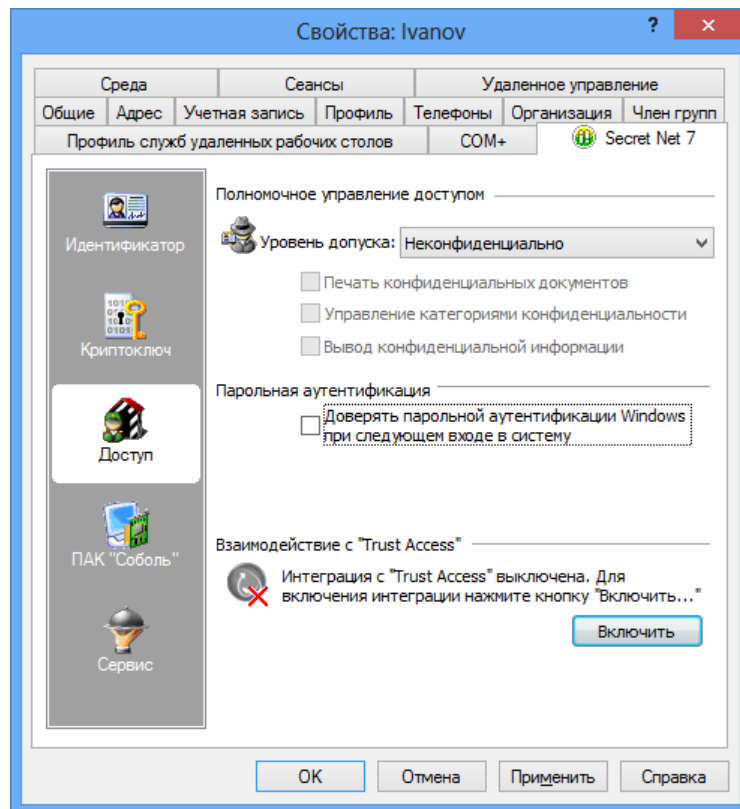
Назначение уровней допуска и привилегий пользователям

Уровень допуска и привилегии назначаются администратором безопасности каждому пользователю индивидуально.

Привилегия может быть назначена пользователю при условии, если ему назначен уровень допуска к конфиденциальной информации.

Для назначения уровня допуска и привилегий:

1. Загрузите нужную оснастку ОС Windows или запустите программу управления пользователями (см. стр. 15).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Secret Net 7".
3. В панели выбора групп параметров выберите группу "Доступ".



4. Установите уровень допуска пользователя в одноименном поле.
Для уровня допуска, отличного от категории для общедоступной информации (по умолчанию — "неконфиденциально"), становится доступным назначение привилегий.
5. Для предоставления или отмены привилегий пользователя установите или удалите отметки в соответствующих полях.
6. Нажмите кнопку "OK".

**Примечание.**

Параметры вступят в силу при следующем входе пользователя в систему.

Присвоение категорий конфиденциальности ресурсам

Категорию конфиденциальности можно назначить для следующих ресурсов:

- устройства, для которых поддерживается разграничение доступа с использованием механизма полномочного управления доступом;
- каталоги и файлы на дисках с файловой системой NTFS.

Присвоение категорий конфиденциальности устройствам

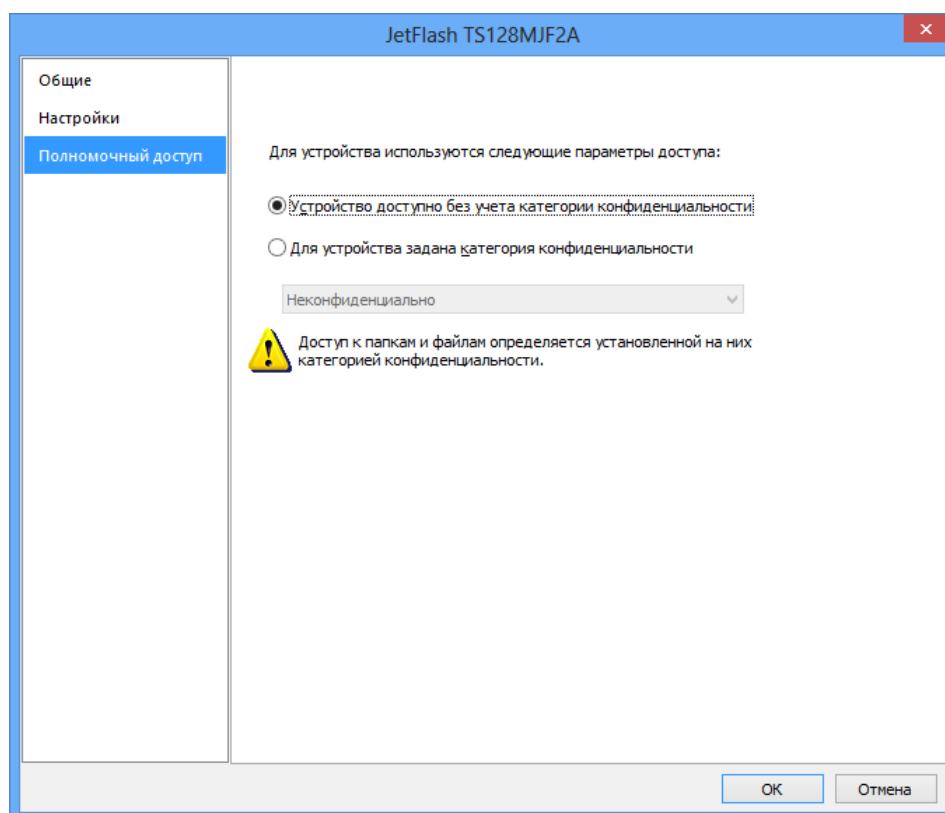
К устройствам, для которых можно назначить категорию конфиденциальности, относятся локальные физические диски (кроме диска с системным логическим разделом) и любые устройства, включаемые в группы устройств USB, PCMCIA, IEEE1394 или Secure Digital.

Категории конфиденциальности можно присвоить:

- индивидуально каждому устройству;
- группе, классу или модели в списке устройств для наследования категории новыми устройствами (только категорию для общедоступной информации — "неконфиденциально").

Для присвоения категорий конфиденциальности объектам в списке устройств:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. [13](#)).
2. Выберите папку "Устройства".
В правой части окна оснастки появится список устройств.
3. Выберите в списке объект (группу, класс, модель или устройство), вызовите контекстное меню и выберите команду "Свойства".
На экране появится диалог для настройки параметров объекта.
4. Перейдите к группе параметров "Полномочный доступ".



Для класса или модели параметры механизма полномочного управления доступом могут быть заданы явно или наследоваться от вышестоящего объекта. Для объекта с явно заданными параметрами в поле "Для новых устройств использовать настройки категории с родительского объекта" отсутствует отметка. Если поле содержит отметку, это означает, что заданные параметры для данного объекта наследуются от вышестоящего объекта и будут присвоены новым устройствам при их появлении в системе. В этом случае параметры будут недоступны для изменения, но они будут отображать состояние параметров родительского объекта.

5. Если для данного объекта требуется задать явно параметры механизма полномочного управления доступом, удалите отметку из поля "Для новых устройств использовать настройки категории с родительского объекта".
6. Для назначения категории при настройке параметров класса или модели установите отметку в поле "Неконфиденциально". Для назначения категории конфиденциальности конкретному устройству установите отметку в поле "Для устройства задана категория конфиденциальности" и выберите в раскрывающемся списке нужную категорию (полный список категорий представлен только для конкретного устройства). Если устройство должно функционировать независимо от уровня допуска пользователя, установите отметку в поле "Устройство доступно без учета категории конфиденциальности".

Присвоение категорий конфиденциальности каталогам и файлам

Присвоение ресурсам категорий конфиденциальности выполняется уполномоченными пользователями, имеющими привилегию "Управление категориями конфиденциальности". Категория конфиденциальности может быть присвоена только ресурсам, расположенным на дисках с файловой системой NTFS.

Описание процедур изменения категорий конфиденциальности каталогов и файлов см. в документе [6].



Внимание!

При присвоении ресурсам категорий конфиденциальности учитывайте следующие общие рекомендации:

- Не присваивайте категорию, отличную от категории для общедоступной информации (по умолчанию "неконфиденциально"), системным каталогам, каталогам, в которых размещается прикладное ПО, а также каталогу "Мои документы" и всем, подобным ему.
- Во избежание произвольного повышения категорий конфиденциальности файлов храните файлы в каталогах с категорией конфиденциальности, равной категории конфиденциальности файлов. При этом учитывайте категорию конфиденциальности устройства, на котором располагаются эти объекты, так как категория устройства имеет более высокий приоритет.

Настройка регистрации событий

Для отслеживания произошедших событий, связанных с работой механизма полномочного управления доступом, необходимо выполнить настройку регистрации событий. Для этого следует указать, какие события категорий "Полномочное управление доступом" и "Контроль печати" должны регистрироваться в журнале Secret Net.

Примечание.

По умолчанию после установки клиентского ПО системы защиты в локальной политике безопасности компьютера включена регистрация всех событий, связанных с работой механизма полномочного управления доступом и контролем печати.

Управление режимом контроля потоков

По умолчанию режим контроля потоков конфиденциальной информации отключен. Перед включением режима следует:

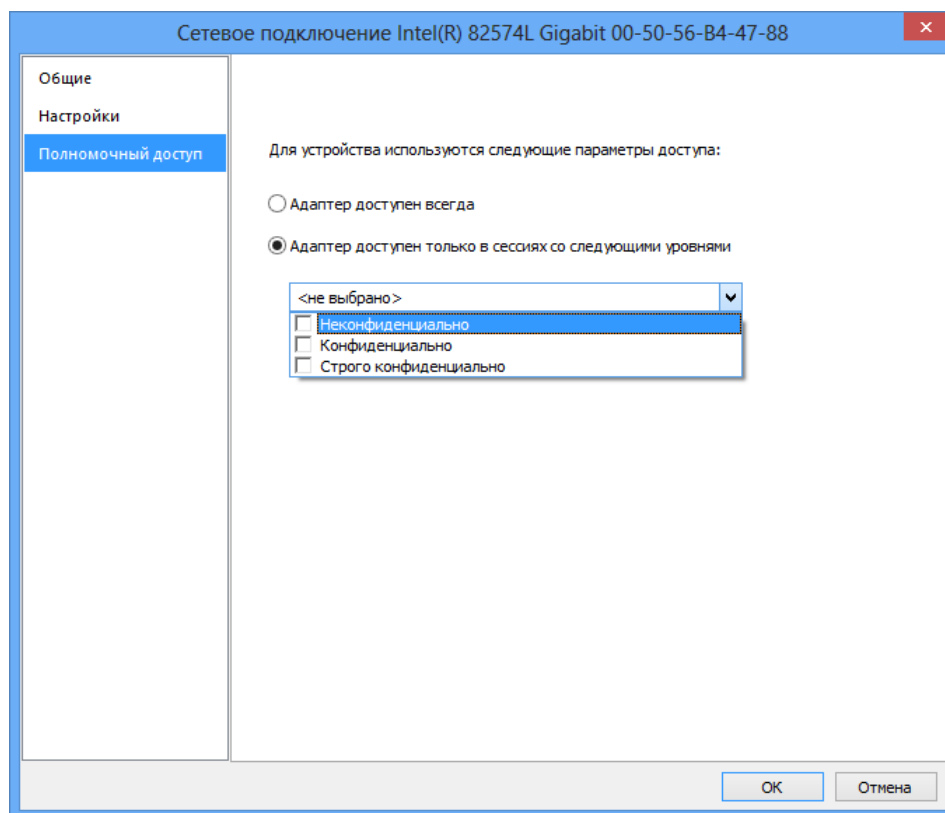
- провести дополнительную настройку параметров с помощью программы настройки подсистемы полномочного управления доступом (см. стр. [129](#));
- выбрать уровни конфиденциальности сессий, в которых будут доступны сетевые интерфейсы компьютера (см. ниже).

Выбор уровней конфиденциальности для сетевых интерфейсов

При настройке параметров сетевого интерфейса можно указать уровни конфиденциальности сессий, в которых этот интерфейс будет доступен пользователям в режиме контроля потоков.

Для настройки использования интерфейсов в режиме контроля потоков:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. [13](#)).
2. Выберите папку "Устройства".
В правой части окна оснастки появится список устройств.
3. В группе "Сеть" выберите нужный объект (группу, класс или сетевой интерфейс), вызовите контекстное меню и выберите команду "Свойства".
На экране появится диалог для настройки параметров объекта.
4. Перейдите к группе параметров "Полномочный доступ".



Для класса или модели параметры механизма полномочного управления доступом могут быть заданы явно или наследоваться от вышестоящего объекта. Для объекта с явно заданными параметрами в поле "Для новых устройств использовать настройки категории с родительского объекта" отсутствует отметка. Если поле содержит отметку, это означает, что заданные параметры для данного объекта наследуются от вышестоящего объекта и будут присвоены новым сетевым интерфейсам при их появлении в системе. В этом случае параметры будут недоступны для изменения, но они будут отображать состояние параметров родительского объекта.

5. Если для данного объекта требуется задать явно параметры механизма полномочного управления доступом, удалите отметку из поля "Для новых устройств использовать настройки категории с родительского объекта".
6. Для выбора уровней конфиденциальности сессий установите отметку в поле "Адаптер доступен только в сессиях со следующими уровнями" и отметьте в раскрывающемся списке нужные уровни. Если устройство должно функционировать независимо от уровня конфиденциальности сессии, установите отметку в поле "Адаптер доступен всегда" (установлена по умолчанию).

Включение и отключение режима контроля потоков

Процедуры включения или отключения режима контроля потоков выполняются в оснастке для управления параметрами объектов групповой политики. Сделанные изменения вступают в силу после применения групповой политики на соответствующих компьютерах и их перезагрузки.

Для включения режима контроля потоков:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. [13](#)).
2. Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.
3. Вызовите контекстное меню для параметра "Полномочное управление доступом: Режим работы" и выберите в нем команду "Свойства".
На экране появится диалог настройки параметра.
4. Установите отметку в поле "контроль потоков включен".
5. При необходимости настройте параметры автоматического назначения уровней конфиденциальности для сессий пользователей:
 - чтобы ограничить выбор уровней конфиденциальности для терминальных подключений — установите отметку в поле "строгий контроль терминальных подключений". В этом случае уровень конфиденциальности терминальной сессии будет устанавливаться равным уровню конфиденциальности локальной сессии на терминальном клиенте (соответственно, режим контроля потоков также должен быть включен на клиенте);
 - чтобы включить принудительное назначение максимально возможных уровней конфиденциальности для сессий пользователей — установите отметку в поле "автоматический выбор максимального уровня сессии". В этом случае сессии будет назначаться уровень конфиденциальности, равный уровню допуска пользователя, который выполняет вход в систему.
6. Нажмите кнопку "ОК".

Для отключения режима контроля потоков:

1. Выполните вход в систему в неконфиденциальной сессии.
2. Выполните действия **1–3** вышеописанной процедуры.
3. Установите отметку в поле "контроль потоков отключен".
4. Нажмите кнопку "ОК".

Настройка маркировки распечатываемых документов

При включенном режиме маркировки в распечатываемые документы автоматически добавляются специальные маркеры (грифы), содержащие учетные сведения для печати. Маркер представляет собой особую форму со сведениями и обычно располагается в колонтитулах или на полях страниц. Сведения содержат информацию о распечатанном документе (например, когда распечатан, кем, сколько страниц). В системе маркер представлен как набор шаблонов, являющихся макетами определенных страниц документа: первой, последней,

промежуточных и пр. В шаблонах заданы области расположения атрибутов со сведениями.

При печати документа происходит наложение макетов страниц из соответствующих шаблонов, и в результате на распечатанных листах вместе с содержимым документа выводятся сведения, относящиеся к маркеру. Печать этих сведений осуществляется независимо от расположения на листе текста самого документа.

Маркеры могут применяться для печати документов любых категорий конфиденциальности, в том числе неконфиденциальных документов. При этом для одной категории допускается использовать несколько маркеров, чтобы пользователь мог самостоятельно выбирать нужный маркер из числа предусмотренных.

По умолчанию в системе задан набор маркеров с predetermined шаблонами и атрибутами. При необходимости можно настроить маркировку в соответствии с действующими в организации требованиями оформления документов. Для настройки маркировки предоставляются возможности изменения параметров имеющихся объектов (маркеров, шаблонов, атрибутов) и добавления новых объектов.

Включение режима маркировки документов и настройка параметров использования маркеров осуществляются в оснастке для управления параметрами объектов групповой политики.



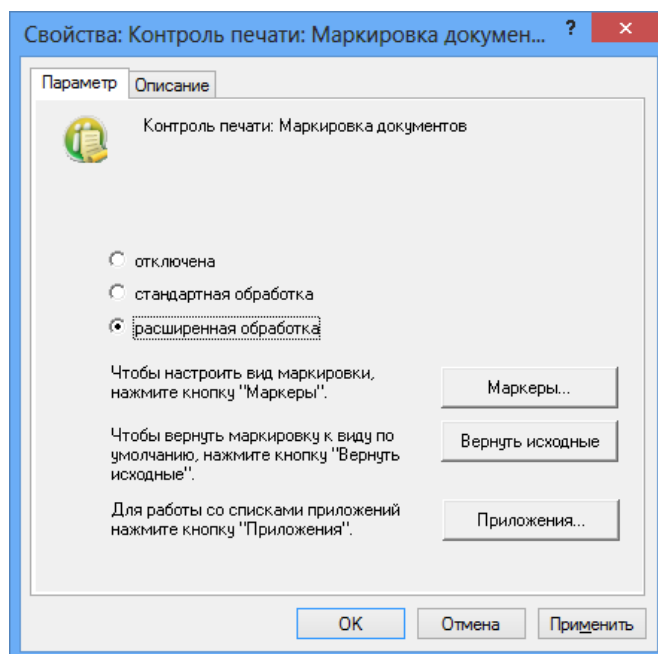
Внимание!

В сетевом режиме функционирования системы Secret Net параметры использования маркеров следует задать в одной общей групповой политике, которая применяется на всех компьютерах домена безопасности. Если хранилище объектов централизованного управления Secret Net размещается в БД доменных служб Active Directory, то задать эти параметры предпочтительнее в политике безопасности домена (Default Domain Policy). В случае размещения хранилища объектов централизованного управления вне AD для настройки следует использовать соответствующую групповую политику:

- политику безопасности домена — если домен безопасности Secret Net совпадает с доменом Active Directory;
- политику безопасности организационного подразделения — если домен безопасности сформирован на базе отдельного организационного подразделения.

Для включения и настройки режима маркировки:

- 1.** Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. [13](#)).
- 2.** Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.
- 3.** Вызовите контекстное меню для параметра "Контроль печати: Маркировка документов" и выберите в нем команду "Свойства".
На экране появится диалог настройки параметра.



4. Включите нужный режим маркировки, установив отметку в соответствующем поле:

- "стандартная обработка" — режим может использоваться во всех поддерживаемых приложениях. В этом режиме предпочтительнее осуществлять печать документов целиком. При печати фрагмента документа маркер будет содержать сведения только о распечатанных страницах без учета общего количества страниц документа (так как распечатанный фрагмент воспринимается как отдельный документ). В журнале Secret Net регистрируются события начала печати документа, окончания печати документа. При включенном теновом копировании в хранилище сохраняется копия распечатанного фрагмента, а не всего документа;
- "расширенная обработка" — режим может использоваться при печати из определенных приложений, с которыми реализована совместимость. При отправке на печать происходит обработка всего документа независимо от объема распечатанного фрагмента. Поэтому при печати части документа подсчет и нумерация страниц осуществляются с учетом общего количества страниц документа. При этом в журнале Secret Net регистрируются события начала печати документа, окончания печати документа, а также происходит регистрация начала и окончания печати каждой копии документа.

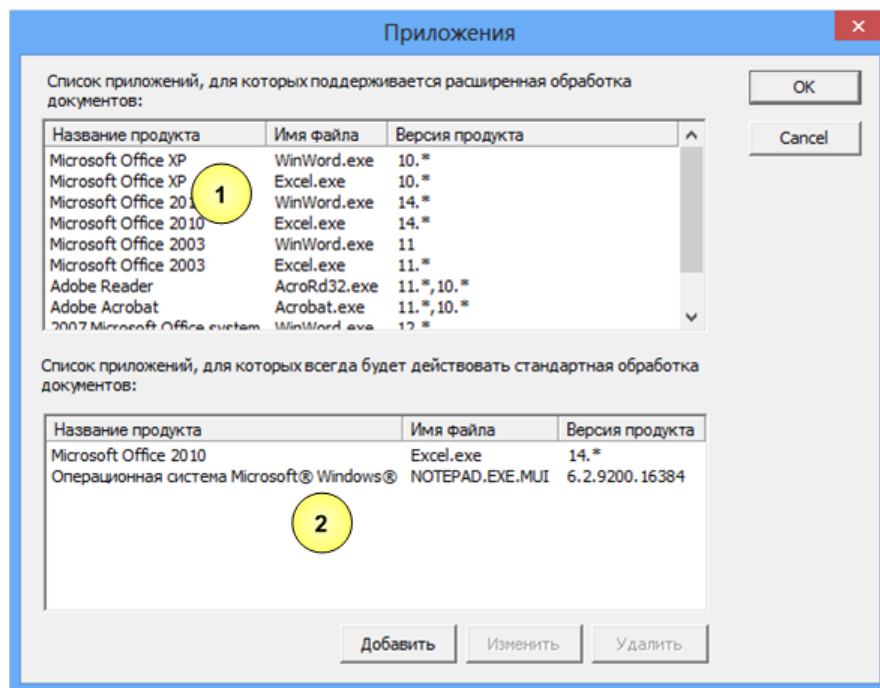
Примечание.

Если режим маркировки отключен, регистрация событий печати в журнале Secret Net осуществляется в зависимости от состояния параметра групповой политики, который определяет действие функции теневого копирования для всех принтеров (см. стр. 152). Если для параметра "Контроль печати: Теневое копирование" указано значение "Определяется настройками принтера", регистрируются события начала печати документа, окончания печати документа. При действующем значении "Отключено для всех принтеров" — в журнале регистрируются только события "Печать документа".

- 5. Настройте параметры использования маркеров.** Для этого нажмите кнопку "Маркеры" и выполните настройку в появившемся окне программы редактирования маркеров (описание интерфейса и общий порядок действий при работе с программой приведены в приложении на стр. 175). Если требуется вернуть параметры маркировки, заданные по умолчанию, — нажмите кнопку "Вернуть исходные".
- 6. Если включен режим "стандартная обработка"** — завершите процедуру, нажав кнопку "OK" в диалоге настройки параметра политики.

7. Если включен режим "расширенная обработка" — проверьте список совместимых приложений и при необходимости укажите программы, в которых должен действовать стандартный режим обработки. Для этого нажмите кнопку "Приложения".

На экране появится диалог со списками приложений.



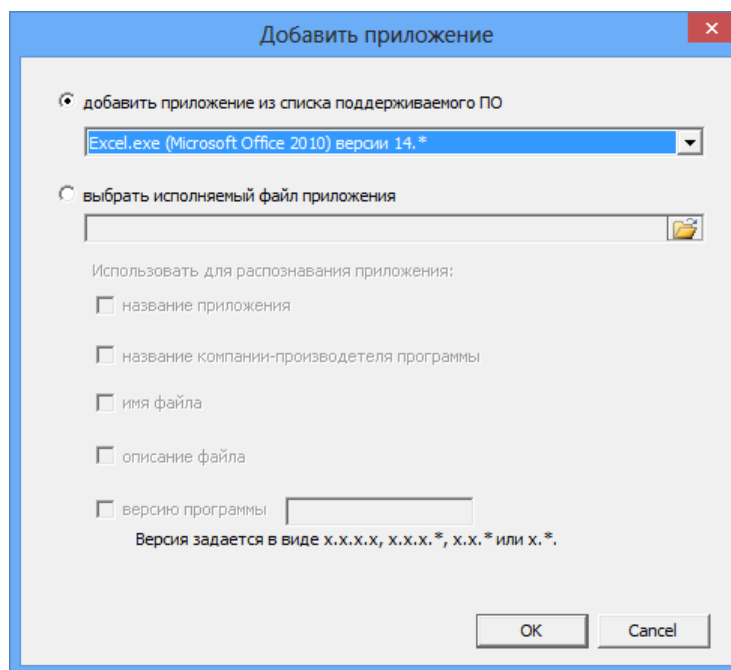
Пояснение.

На рисунке выносками обозначены элементы: 1 — список совместимых приложений; 2 — список приложений, для которых принудительно будет действовать режим стандартной обработки.

8. Ознакомьтесь со списком совместимых приложений. Список формируется автоматически, независимо от наличия приложений на компьютере, и состоит из программ, с которыми реализована совместимость на момент выпуска текущей версии системы Secret Net.
9. Отредактируйте, если требуется, список программ со стандартным режимом обработки и нажмите кнопку "ОК". Для редактирования списка используйте соответствующие кнопки под списком:

Кнопка	Описание
Добавить	Вызывает диалог добавления приложения (см. ниже)
Изменить	Вызывает диалог настройки параметров распознавания выбранного приложения (см. ниже)
Удалить	Удаляет выбранное приложение из списка

При добавлении приложения на экране появляется диалог для выбора и настройки параметров распознавания приложения.



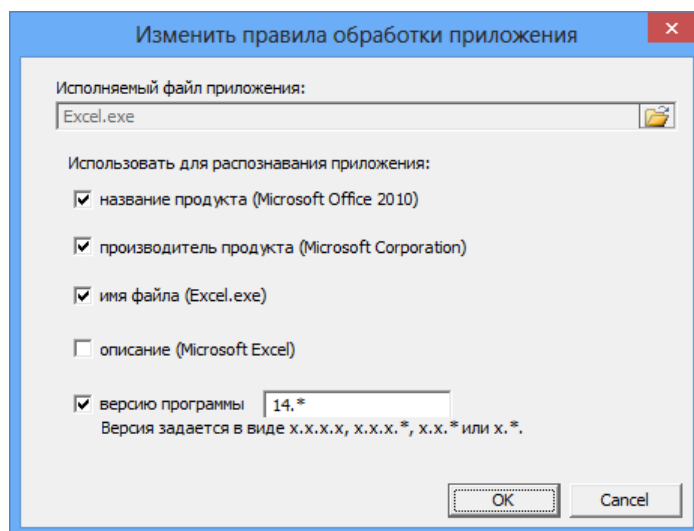
В диалоге выберите вариант добавления приложения, настройте доступные параметры и нажмите кнопку "OK". Предусмотрены следующие варианты выбора приложений:

- добавление из списка совместимых приложений — для этого установите отметку в поле "добавить приложение из списка поддерживаемого ПО" и выберите приложение из раскрывающегося списка (в этом случае параметры распознавания приложения системой будут заданы автоматически);
- добавление приложения по файлу его запуска — для этого установите отметку в поле "выбрать исполняемый файл приложения", нажмите кнопку справа и выберите файл в стандартном диалоге открытия файлов. При этом приложение должно быть установлено на данном компьютере, а исполняемый файл корректно указан. После выбора приложения настройте параметры его распознавания системой. Для этого отметьте подходящие методы, по которым система будет идентифицировать данное приложение (например, по производителю продукта, по имени файла и версии программы).

Примечание.

Необходимо учитывать, что идентификация приложения будет выполняться по значениям, полученным для выбранных методов из указанного файла. В частности, название производителя продукта должно в точности совпадать с названием в файле. Поэтому, например, локализованные названия одного производителя (Microsoft и Майкрософт) будут восприниматься как различные.

При изменении выбранного приложения на экране появляется диалог для настройки параметров распознавания.



В диалоге отметьте методы, по которым система будет идентифицировать данное приложение, и нажмите кнопку "OK".

10. По окончании работы со списком приложений нажмите кнопку "OK" в диалоге настройки параметра политики.

Для отключения режима маркировки:

1. Выполните действия **1–3** вышеописанной процедуры.
2. Установите отметку в поле "отключена".
3. Нажмите кнопку "OK".

Настройка использования принтеров для печати документов

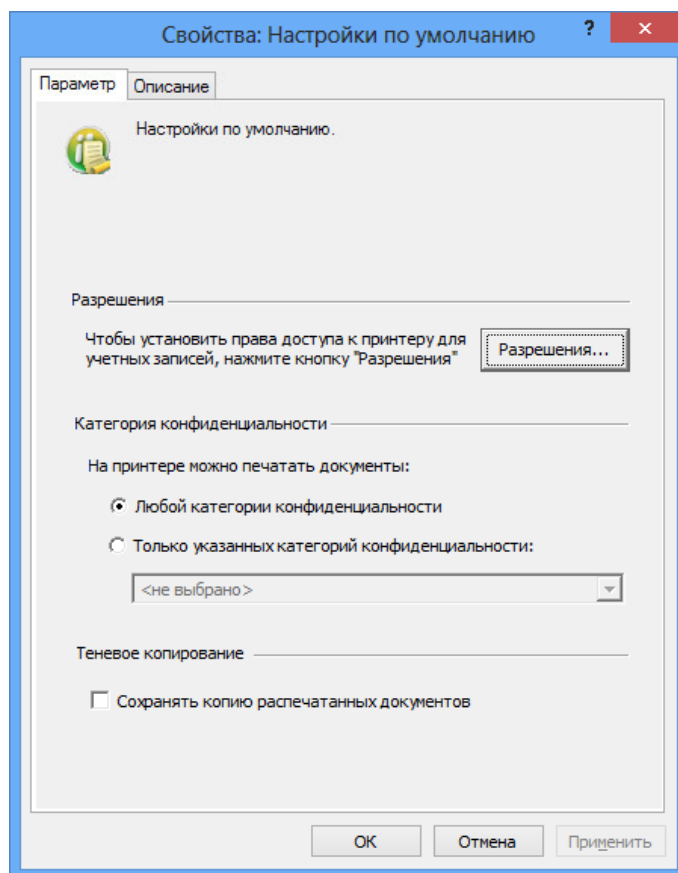
При необходимости можно ограничить использование принтеров для печати документов, которым присвоены определенные категории конфиденциальности. По умолчанию на всех принтерах разрешается печать документов с любой категорией конфиденциальности.

Категории конфиденциальности могут быть заданы для конкретных принтеров или для элемента "Настройки по умолчанию" в списке принтеров.

Также для принтеров предусмотрена возможность настройки прав пользователей для печати документов (см. стр. [65](#)).

Для настройки использования принтеров:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. [13](#)).
2. Выберите папку "Принтеры".
В правой части окна оснастки появится список принтеров.
3. Выберите в списке нужный элемент, вызовите контекстное меню и выберите команду "Свойства".
На экране появится диалог для настройки параметров.



4. Если требуется ограничить печать документов в зависимости от их категорий конфиденциальности, установите отметку в поле "Только указанных категорий конфиденциальности" и отметьте в раскрывающемся списке нужные категории. Для разрешения печати документов без учета категории конфиденциальности установите отметку в поле "Любой категории конфиденциальности".

Дополнительная настройка функционирования механизма

Для использования механизма полномочного управления доступом и контроля печати требуется определенная настройка операционной системы, системы защиты и самого механизма. Необходимый объем действий по настройке ОС и системы Secret Net выполняется автоматически при установке клиентского ПО системы защиты. Такая настройка достаточна для функционирования механизма при отключенном режиме контроля потоков.

Чтобы обеспечить функционирование механизма при включенном режиме контроля потоков, требуется дополнительная настройка параметров, которая осуществляется локально с помощью программы настройки подсистемы полномочного управления доступом (далее — программа настройки). Дополнительную настройку рекомендуется выполнить перед включением режима контроля потоков. Далее в процессе эксплуатации системы программу настройки следует использовать при добавлении новых пользователей, программ, принтеров, для оптимизации функционирования механизма и в других случаях.

Также с помощью программы настройки можно отключить вывод предупреждающих сообщений и регистрацию событий для случаев, когда такие оповещения не требуются. Это позволяет обеспечить удобную работу пользователей и администратора при функционировании механизма.

Для запуска программы выполните соответствующее действие в зависимости от версии установленной операционной системы:

- на компьютере под управлением ОС Windows 8 или Windows Server 2012 — загрузите начальный экран "Пуск" и выберите элемент "Настройка"

подсистемы полномочного управления доступом" (относится к группе "Код безопасности");

- на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код безопасности | Secret Net | Настройка подсистемы полномочного управления доступом".

Запуск программы невозможен в следующих случаях:

- если текущий пользователь не входит в локальную группу администраторов;
- если механизм полномочного управления доступом отключен.

Программа может функционировать в обычном режиме, который предоставляет все возможности для редактирования и настройки, или в режиме просмотра текущего состояния параметров (только чтение). Запуск программы в обычном режиме осуществляется при следующих условиях:

- пользователю назначен наивысший уровень допуска к конфиденциальной информации;
- пользователю предоставлена привилегия "Управление категориями конфиденциальности";
- режим контроля потоков отключен.

При невыполнении хотя бы одного из перечисленных условий запуск программы возможен только в режиме просмотра текущего состояния параметров.

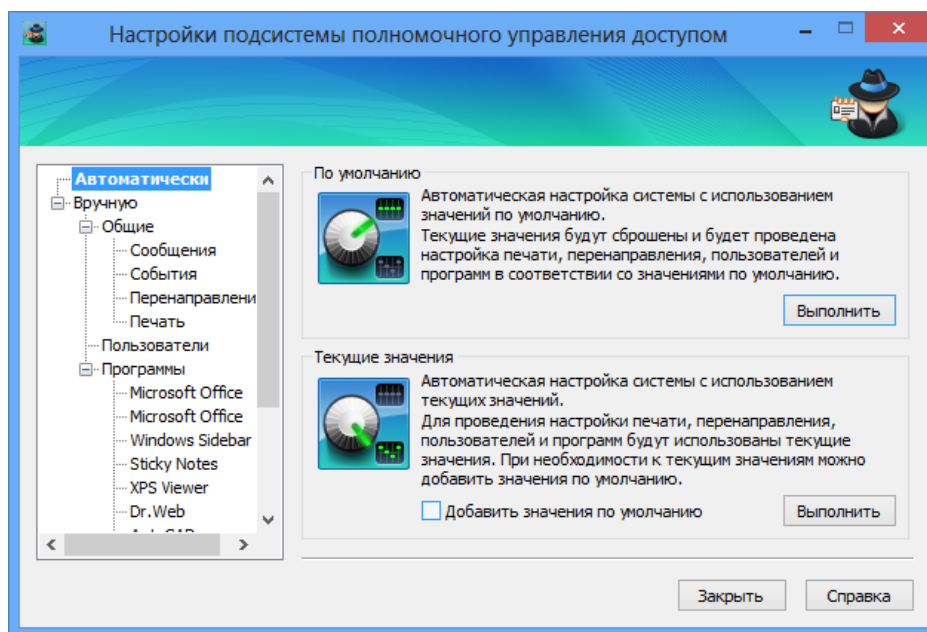
Автоматическая настройка

Настройка системы для функционирования механизма полномочного управления доступом и контроля печати может выполняться автоматически. Для автоматической настройки предусмотрены возможности использования значений параметров, задаваемых по умолчанию, или текущих заданных значений, сконфигурированных при настройке вручную.

Автоматическая настройка со значениями по умолчанию применяется в случае необходимости удалить текущую конфигурацию и вернуть исходные значения параметров. Это может потребоваться, если значения параметров некорректно заданы или удалены, а также при первичной настройке системы с минимально необходимой конфигурацией для функционирования механизма в режиме контроля потоков.

Настройка с текущими значениями предназначена для повторного применения в системе заданных значений параметров. Это позволяет восстановить настройку системы при сбоях функционирования механизма или при добавлении в систему новых пользователей, программ, принтеров и других объектов, задействованных в механизме полномочного управления доступом и контроля печати. При такой настройке дополнительно к текущим значениям параметров можно добавить исходные значения (значения по умолчанию). При этом текущие значения не удаляются.

Чтобы выполнить автоматическую настройку, в левой панели окна программы выберите режим "Автоматически".



Для удаления текущей конфигурации и настройки системы со значениями по умолчанию:

- В разделе "По умолчанию" нажмите кнопку "Выполнить".
Начнется процесс автоматической настройки системы. По окончании процесса на экране появится соответствующее сообщение.

Для настройки системы с текущими значениями параметров:

1. Если к текущим значениям параметров требуется добавить исходные значения, установите отметку в поле "Добавить значения по умолчанию".
2. В разделе "Текущие значения" нажмите кнопку "Выполнить".
Начнется процесс автоматической настройки системы. По окончании процесса на экране появится соответствующее сообщение.

Настройка вручную

Программа настройки предоставляет возможность вручную изменять параметры, относящиеся к работе механизма полномочного управления доступом и контроля печати. Это позволяет обеспечить функционирование механизма с учетом особенностей программной среды компьютера и предпочтений пользователя.

Средства для ручной настройки параметров представлены в следующих основных разделах:

- "Общие" — для настройки общих параметров работы пользователей и приложений;
- "Пользователи" — для настройки параметров, относящихся к профилям пользователей;
- "Программы" — для настройки параметров, относящихся к приложениям.

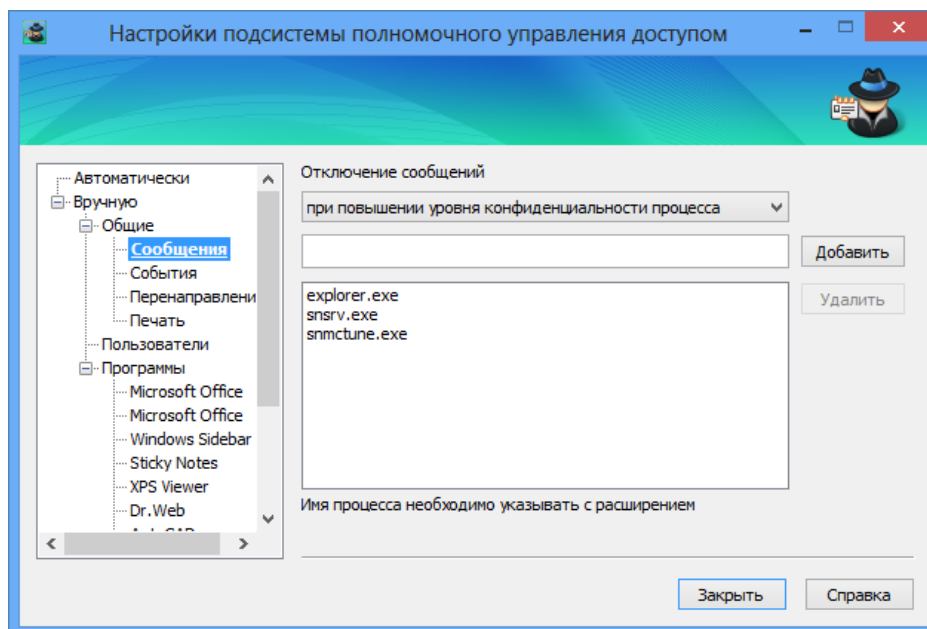
Отключение вывода предупреждающих сообщений системы

В определенных случаях система выводит пользователю предупреждающие сообщения об изменении категорий конфиденциальности файлов или процессов. Для удобной работы пользователя предусмотрены возможности отключения вывода сообщений в следующих случаях:

- при повышении уровня конфиденциальности процесса (например, explorer.exe) по причине доступа к файлу с более высокой категорией конфиденциальности (применимо при отключенном режиме контроля потоков);

- при повышении категории конфиденциальности файла, имеющего указанное расширение, или файла из указанного каталога. Данная возможность предназначена для обеспечения автоматического создания и редактирования служебных файлов, используемых некоторыми приложениями (например, редактором MS Word), в режиме контроля потоков при работе в конфиденциальных сессиях;
- при выводе конфиденциального файла, имеющего указанное расширение, на внешние носители, в результате чего происходит сброс категории конфиденциальности отчуждаемого файла (применимо в режиме контроля потоков при работе в конфиденциальных сессиях).

Чтобы настроить параметры отключения вывода сообщений, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Общие | Сообщения".



Для отключения сообщений при повышении уровня конфиденциальности процессов:

1. В поле "Отключение сообщений" укажите значение "при повышении уровня конфиденциальности процесса".

Ниже будет выведен список процессов (имена исполняемых файлов), для которых вывод сообщений данного типа отключен.

2. Отредактируйте список имен файлов:
 - чтобы добавить элемент в список, введите в строке имя исполняемого файла процесса (с указанием расширения) и нажмите кнопку "Добавить";
 - чтобы удалить элементы из списка, выделите их и нажмите кнопку "Удалить".

Для отключения сообщений при повышении категории конфиденциальности файлов с определенными расширениями:

1. В поле "Отключение сообщений" укажите значение "при повышении уровня файла (по расширению)".

Ниже будет выведен список расширений файлов, для которых вывод сообщений данного типа отключен.

2. Отредактируйте список расширений:
 - чтобы добавить элемент в список, введите в строке расширение имени файла в виде .<расширение> (например, .lnk) и нажмите кнопку "Добавить";
 - чтобы удалить элементы из списка, выделите их и нажмите кнопку

"Удалить";

- чтобы отключить вывод сообщений для файлов с любыми расширениями, добавьте в список элемент *.* или установите отметку в поле "Отключить вывод сообщений для всех типов файлов". При этом средства редактирования списка становятся неактивными. Чтобы снова активировать список расширений, удалите отметку из поля.

Для отключения сообщений при повышении категории конфиденциальности файлов из определенных каталогов:

1. В поле "Отключение сообщений" укажите значение "при повышении уровня файла (для директории)".

Ниже будет выведен список каталогов, для файлов которых вывод сообщений данного типа отключен (независимо от расширений файлов).

2. Отредактируйте список путей к каталогам:

- чтобы добавить элемент в список, введите в строке путь к каталогу и нажмите кнопку "Добавить";

Примечание.

Ввод пути к каталогу выполняется с учетом следующих особенностей:

- строка может содержать как полный путь, однозначно определяющий данный каталог, так и часть пути, позволяющую определить подмножество путей к каталогам. Если указывается подмножество путей, строка должна начинаться символом "\";
- путь к каталогу указывается БЕЗ символа "\" на конце;
- имена каталогов должны быть указаны в формате LFN (Long File Name).

- чтобы удалить элементы из списка, выделите их и нажмите кнопку "Удалить".

Для отключения сообщений при выводе конфиденциальной информации на внешние носители:

1. В поле "Отключение сообщений" укажите значение "при выводе конфиденциальной информации (по расширению)".

Ниже будет выведен список расширений файлов, для которых вывод сообщений данного типа отключен.

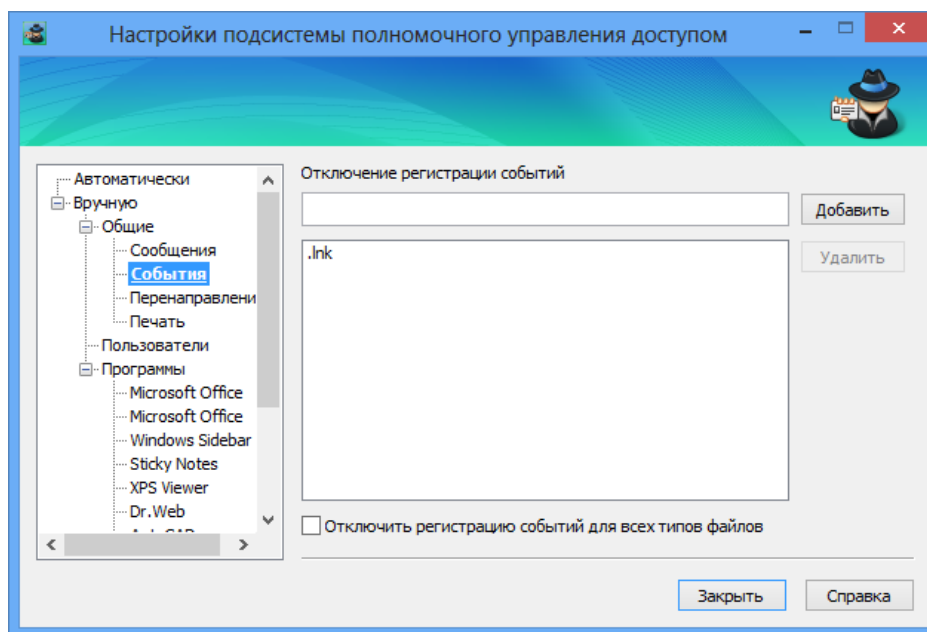
2. Отредактируйте список расширений:

- чтобы добавить элемент в список, введите в строке расширение имени файла в виде <расширение> (например, .lnk) и нажмите кнопку "Добавить";
- чтобы удалить элементы из списка, выделите их и нажмите кнопку "Удалить";
- чтобы отключить вывод сообщений для файлов с любыми расширениями, добавьте в список элемент *.* или установите отметку в поле "Отключить вывод сообщений для всех типов файлов". При этом средства редактирования списка становятся неактивными. Чтобы снова активировать список расширений, удалите отметку из поля.

Отключение регистрации событий обращения к файлам

В журнале Secret Net осуществляется регистрация событий внутрисистемных обращений к файлам при функционировании механизма полномочного управления доступом и контроля печати. При необходимости регистрацию таких событий можно отключить применительно к файлам, имеющим определенные расширения. Это позволяет сократить объем информации, сохраняемой в журнале.

Чтобы настроить параметры отключения регистрации событий, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Общие | События".



Для отключения регистрации событий обращения к файлам с определенными расширениями:

- Сформируйте список расширений файлов:
 - чтобы добавить элемент в список, введите в строке расширение имени файла в виде <расширение> (например, .lnk) и нажмите кнопку "Добавить";
 - чтобы удалить элементы из списка, выделите их и нажмите кнопку "Удалить";
 - чтобы отключить регистрацию событий для файлов с любыми расширениями, добавьте в список элемент .* или установите отметку в поле "Отключить регистрацию событий для всех типов файлов". При этом средства редактирования списка становятся неактивными. Чтобы снова активировать список расширений, удалите отметку из поля.

Перенаправление вывода общих служебных файлов

Механизм полномочного управления доступом и контроля печати выполняет проверку соответствия уровня допуска пользователя и категории конфиденциальности объекта доступа (каталог, файл). Однако в ряде приложений (например, MS Word) происходят обращения к служебным файлам, которые хранятся в специальных каталогах. При этом отсутствуют возможности изменять категории конфиденциальности этих файлов в зависимости от уровня допуска пользователя. При использовании механизма полномочного управления доступом в режиме контроля потоков такие особенности приводят к конфликтным ситуациям и невозможности корректной работы приложений.

Для устранения этой проблемы в системе реализована функция перенаправления вывода общих служебных файлов. Функция действует при работе в конфиденциальных сессиях. Чтобы обеспечить работу приложения в сессиях с различными уровнями конфиденциальности, создаются отдельные каталоги (по количеству категорий), в которые копируются общие служебные файлы, и этим копиям назначаются соответствующие категории конфиденциальности. Если приложение в конфиденциальной сессии осуществляет попытку обращения к общему файлу, система перенаправляет это обращение к копии общего файла, находящейся в отдельном каталоге, который был создан для сессий данного уровня конфиденциальности.

При настройке параметров перенаправления вывода файлов формируется список путей к каталогам с общими файлами, для которых должны быть созданы дополнительные каталоги различной категории конфиденциальности. В этих

каталогах будут храниться файлы, используемые в сессиях соответствующего уровня конфиденциальности. Например, для обслуживания обращений приложения MS Word русской версии в списке должна присутствовать запись \AppData\Roaming\Microsoft\Шаблоны (в ОС Windows Server 2003 и более ранних версиях: \Application Data\Microsoft\Шаблоны). В зависимости от уровня конфиденциальности сессии пользователя при обращении приложения к данным каталогам чтение/запись информации для общих файлов будет выполняться в одном из дополнительно созданных подкаталогов \Шаблоны(1), \Шаблоны(2) и т. д. в каталоге \AppData\Roaming\Microsoft. В ОС Windows Server 2003 и более ранних версиях подкаталоги создаются в каталоге \Application Data\Microsoft.

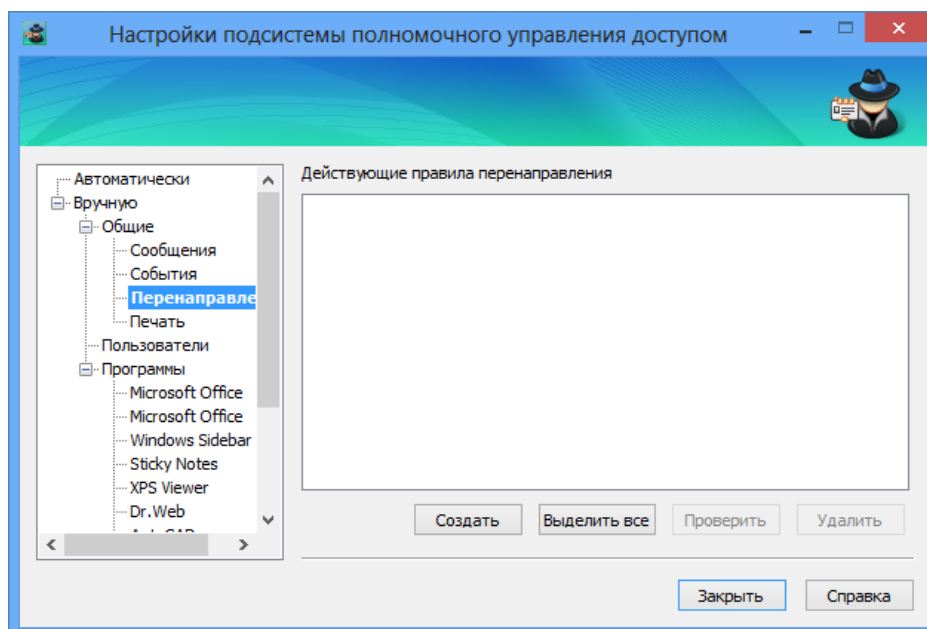


Примечание.

Следствием действия функции перенаправления вывода является независимость сделанных изменений в общих служебных файлах при работе с приложением в сессиях с различными уровнями конфиденциальности. Например, если общий файл был изменен в сессии с уровнем "строгое конфиденциально", эти изменения не будут учтены в сессиях с другими уровнями конфиденциальности, так как в этих сессиях обращение осуществляется к другим копиям общего файла.

При автоматической настройке системы (см. стр. 130) создание каталогов перенаправления выполняется только для системного диска. Если список путей формируется вручную, предоставляется возможность выбора дисков.

Чтобы сформировать список путей для перенаправления вывода файлов, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Общие | Перенаправление".



Для добавления путей в список:

1. Нажмите кнопку "Создать".

На экране появится диалог для добавления путей к каталогам.

2. Сформируйте в диалоге список добавляемых путей:

- чтобы добавить элемент в список, введите в строке путь к каталогу и нажмите кнопку "Добавить";

Примечание.

Ввод пути к каталогу выполняется с учетом следующих особенностей:

- строка может содержать как полный путь, однозначно определяющий данный каталог, так и часть пути, позволяющую определить подмножество путей к каталогам. Если указывается подмножество путей, строка должна начинаться символом "\";
- путь к каталогу указывается БЕЗ символа "\" на конце;
- имена каталогов должны быть указаны в формате LFN (Long File Name).

- чтобы удалить элементы из списка, выделите их и нажмите кнопку "Удалить".
3. Нажмите кнопку "Создать".
 4. Если на компьютере имеется несколько локальных дисков, на экране появится диалог для выбора дисков, в которых будет осуществляться поиск каталогов. В диалоге отметьте нужные диски и нажмите кнопку "ОК".
Начнется процесс поиска каталогов, удовлетворяющих добавляемым путям. Для найденных каталогов будут созданы каталоги *< имя_каталога > (1)*, *< имя_каталога > (2)* и т. д. с соответствующими категориями конфиденциальности (например, "конфиденциально" для первого каталога и "строго конфиденциально" для второго). В созданные каталоги будет скопировано содержимое соответствующего исходного каталога. По окончании процесса поиска пути к каталогам будут добавлены в список путей для перенаправления вывода файлов.

Примечание.

Возможность выбора дисков позволяет ускорить процесс поиска каталогов за счет пропуска содержимого неотмеченных дисков. Однако возможны ситуации, когда заданным путям будут удовлетворять каталоги на необработанных дисках. В таких случаях система будет выполнять попытки перенаправления вывода для этих каталогов, но из-за отсутствия на диске соответствующих структур будут возможны нарушения в работе ПО. Поэтому если поиск каталогов осуществляется не на всех дисках, рекомендуется указывать такие пути, для которых отсутствуют соответствующие каталоги на неотмеченных дисках.

Для проверки возможности перенаправления:

1. Выделите в списке пути, для которых требуется проверить действие функции перенаправления (для выделения всех элементов списка нажмите кнопку "Выделить все").
2. Нажмите кнопку "Проверить".
3. Если на компьютере имеется несколько локальных дисков, на экране появится диалог для выбора дисков, в которых будет осуществляться поиск каталогов. В диалоге отметьте нужные диски и нажмите кнопку "ОК".
Начнется процесс поиска каталогов, удовлетворяющих выбранным путям. Для найденных каталогов будет проверено наличие и корректность настройки каталогов *< имя_каталога > (1)*, *< имя_каталога > (2)* и т. д. с соответствующими категориями конфиденциальности. При необходимости каталоги будут созданы и заполнены заново. По окончании процесса поиска и проверки на экране появится соответствующее сообщение.

Для удаления путей из списка:

1. Выделите в списке пути, которые требуется удалить (для выделения всех элементов списка нажмите кнопку "Выделить все").
2. Нажмите кнопку "Удалить".
Выбранные пути будут незамедлительно удалены из списка. При этом сами каталоги перенаправления и содержащиеся в них файлы удалены не будут.

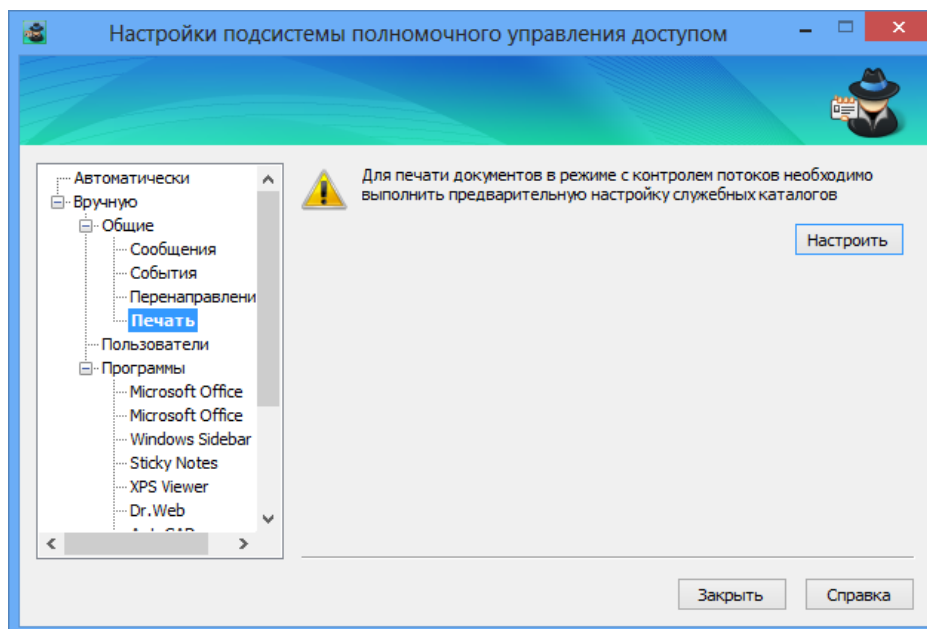
Настройка системы для печати на принтер

Для печати на принтер в режиме контроля потоков (при работе в конфиденциальных сессиях) должна быть выполнена настройка некоторых служебных каталогов ОС Windows.

Настройка параметров каталогов в необходимом объеме осуществляется при общей автоматической настройке (см. стр. **130**).

Программа настройки осуществляет проверку текущих заданных параметров в системе. Если обеспечивается возможность печати на принтер в режиме контроля потоков, средства для настройки печати неактивны. При выявлении необходимости проведения настройки программа предоставляет возможность запустить процесс вручную.

Чтобы настроить систему для печати на принтер, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Общие | Печать".



Для запуска процесса настройки печати:

- Нажмите кнопку "Настроить" (кнопка активна, если настройка не проведена в нужном объеме).

Начнется процесс настройки системы. По окончании процесса на экране появится соответствующее сообщение.

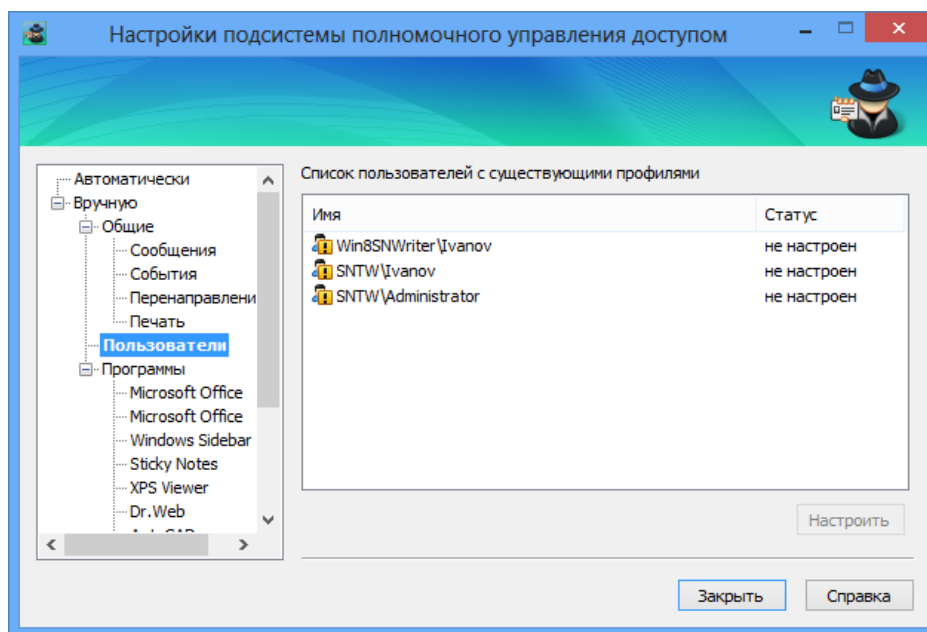
Настройка параметров, относящихся к профилям пользователей

Для работы пользователя в режиме контроля потоков (в конфиденциальных сессиях) должна быть выполнена настройка параметров, относящихся к профилю этого пользователя. Настройка заключается в создании структуры каталогов перенаправления вывода файлов для временных каталогов пользователя и установке соответствующих категорий конфиденциальности с определенной конфигурацией признаков наследования для этих каталогов. Настройка выполняется для тех пользователей, от имени которых хотя бы раз был выполнен вход в систему на данном компьютере.

Настройка всех профилей пользователей в необходимом объеме осуществляется при общей автоматической настройке (см. стр. 130). При добавлении в систему нового пользователя или при переименовании существующего необходимо выполнить настройку профиля этого пользователя для работы в режиме контроля потоков. Запуск процесса настройки профилей можно выполнить вручную.

Программа настройки осуществляет проверку текущих заданных параметров профилей пользователей. Если обеспечивается возможность работы пользователя в режиме контроля потоков, для этого пользователя отображается статус "настроен". При выявлении необходимости проведения настройки для пользователя отображается статус "не настроен".

Чтобы настроить профили пользователей, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Пользователи".



Для запуска процесса настройки профилей пользователей:

1. Выделите в списке пользователей, профили которых необходимо настроить (если для профиля пользователя настройка уже выполнена, он имеет статус "настроен").
2. Нажмите кнопку "Настроить".

Начнется процесс настройки системы. По окончании процесса на экране появится соответствующее сообщение.

Формирование списка приложений, подлежащих настройке

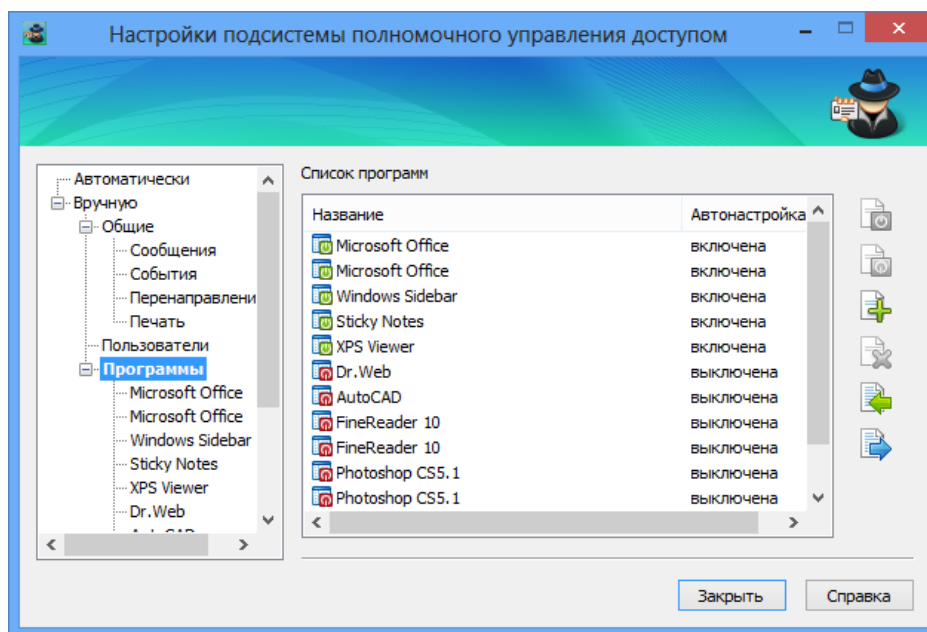
Некоторые приложения не полностью совместимы с механизмом полномочного управления доступом в режиме контроля потоков. Для корректного функционирования таких приложений требуется дополнительная настройка параметров, относящихся к приложению.

С помощью программы может осуществляться настройка параметров для приложений, представленных в списке. Список формируется независимо от наличия на компьютере установленных приложений. По умолчанию после установки клиентского ПО системы защиты список содержит названия программ, для которых выявлена несовместимость и определены необходимые действия по настройке на момент выпуска данной версии системы Secret Net.

Настройка параметров, относящихся к приложениям, может осуществляться при общей автоматической настройке (см. стр. 130). Автоматическая настройка со значениями по умолчанию всегда применяется к тем приложениям, для которых установлен статус автоматической настройки "включена" в сформированном по умолчанию списке приложений (например, для приложения Microsoft Office). При этом наличие приложения в текущем списке и его статус автоматической настройки не учитываются. Если выполняется автоматическая настройка с текущими значениями, она применяется только к тем приложениям, которые имеют статус "включена" в текущем списке приложений.

Запуск процесса настройки параметров приложения можно также выполнить и вручную.

Чтобы сформировать список приложений, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Программы".



При формировании списка приложений можно выполнять следующие операции:

- импорт списка из xml-файла (с предварительным удалением всех элементов текущего списка);
- экспорт текущего списка в xml-файл;
- управление режимом автоматической настройки приложений;
- добавление списка из xml-файла (без удаления элементов текущего списка);
- удаление выбранных элементов списка.

Для импорта списка из xml-файла:

1. Нажмите кнопку "Импортировать список программ".
На экране появится стандартный диалог выбора файла.
2. Выберите нужный файл.
В программу будет загружен список приложений, хранящийся в указанном файле. При этом текущий список будет удален.

Для экспорта списка в xml-файл:

1. Нажмите кнопку "Экспортировать список программ".
На экране появится стандартный диалог сохранения файла.
2. Укажите имя и место расположения сохраняемого файла.

Для управления режимом автоматической настройки приложений:

1. Выделите в списке приложения, для которых требуется включить или отключить режим автоматической настройки.
2. Нажмите соответствующую кнопку:
 - чтобы включить режим, нажмите кнопку "Включить автоматическую настройку";
 - чтобы отключить режим, нажмите кнопку "Выключить автоматическую настройку".

Будет установлен соответствующий статус автоматической настройки выбранных приложений.

Для добавления списка из xml-файла:

1. Нажмите кнопку "Добавить программы".
На экране появится стандартный диалог выбора файла.
2. Выберите нужный файл.

В дополнение к текущему списку приложений в программу будет загружен список, хранящийся в указанном файле.

Для удаления приложений из списка:

1. Выделите в списке приложения, которые требуется удалить.
2. Нажмите кнопку "Удалить программы" и подтвердите решение в появившемся диалоге запроса.

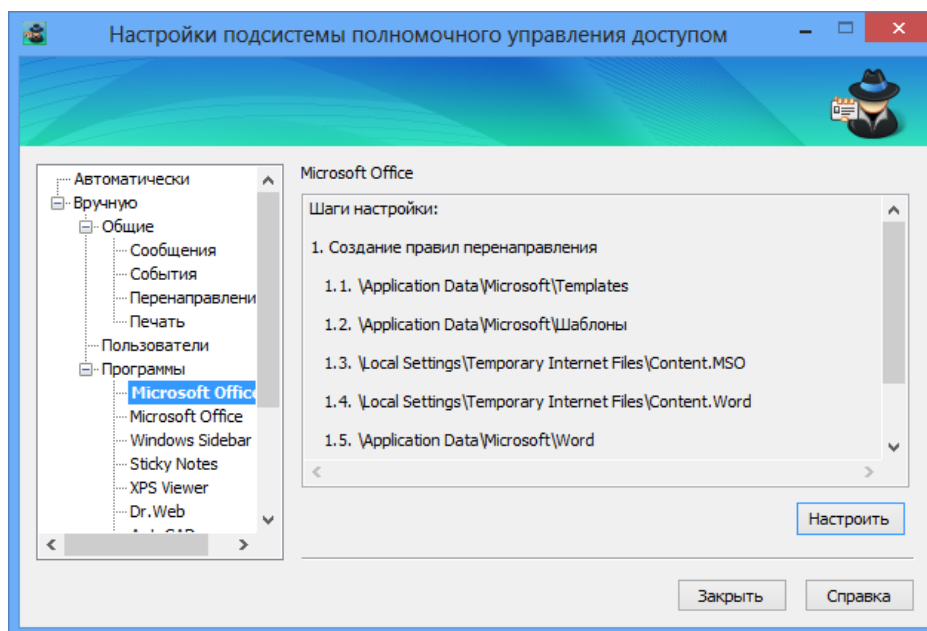
Выбранные приложения будут незамедлительно удалены из списка.

Настройка параметров приложения

Для корректного функционирования приложения в режиме контроля потоков (при работе в конфиденциальных сессиях) должна быть выполнена настройка параметров, относящихся к этому приложению. Сведения о том, какие действия выполняются программой при настройке, приведены в виде последовательности шагов.

Настройка параметров, относящихся к приложению, может осуществляться автоматически, если в списке приложений установлен статус автоматической настройки "включена". Также запуск процесса настройки для данного приложения можно выполнить вручную.

Чтобы настроить параметры, относящиеся к приложению, в левой панели окна программы выберите режим "Вручную" и в нем подраздел "Программы | <имя_приложения>".



Для запуска процесса настройки параметров приложения:

1. Нажмите кнопку "Настроить".
2. Если на компьютере имеется несколько локальных дисков, на экране появится диалог для выбора дисков, в которых будет осуществляться поиск каталогов для создания правил перенаправления. В диалоге отметьте нужные диски и нажмите кнопку "OK".

Начнется процесс настройки параметров. По окончании процесса на экране появится соответствующее сообщение.

Правила работы с конфиденциальными ресурсами

В данном разделе приведены обобщенные правила работы с конфиденциальными ресурсами в условиях работающего механизма полномочного управления доступом. Ниже в таблице приведены правила работы, действующие при отключенном и включенном режиме контроля потоков конфиденциальной информации.

Без контроля потоков	При контроле потоков
Доступ к устройствам	
Запрещен вход пользователя в систему, если подключены устройства с категорией конфиденциальности выше, чем уровень допуска пользователя	Запрещен вход пользователя в систему, если подключены устройства: <ul style="list-style-type: none"> с категорией конфиденциальности выше, чем уровень допуска пользователя; с различными категориями конфиденциальности; с категорией конфиденциальности выше, чем категория "неконфиденциально", при первом входе пользователя на данном компьютере (конфигурационный вход)
Запрещено подключение устройства, если его категория конфиденциальности выше, чем уровень допуска работающего пользователя	Запрещено подключение устройства, если его категория конфиденциальности отличается от уровня сессии работающего пользователя
Разрешено функционирование всех сетевых интерфейсов	Запрещено использование сетевых интерфейсов, для которых текущий уровень конфиденциальности сессии не указан в списке разрешенных уровней
Отсутствуют ограничения по доступу к устройствам, для которых включен режим доступа "без учета категории конфиденциальности"	
Доступ к файлам	
Если задана категория конфиденциальности для устройства, содержащего файл, при доступе к этому файлу система считает, что он имеет категорию конфиденциальности устройства (без учета типа файловой системы). Запрещено изменение категории конфиденциальности файла	
Запрещен доступ к файлу, если его категория конфиденциальности выше, чем заданная категория для устройства, содержащего файл	
Доступ пользователя к файлу разрешается, если уровень допуска пользователя не ниже категории конфиденциальности файла	Доступ пользователя к файлу разрешается, если уровень конфиденциальности пользовательской сессии не ниже категории конфиденциальности файла
Запрещено удаление конфиденциального файла с помещением в "Корзину"	Запрещено удаление любого файла с помещением в "Корзину"
Доступ к каталогам	
Если задана категория конфиденциальности для устройства, содержащего каталог, при доступе к этому каталогу система считает, что он имеет категорию конфиденциальности устройства (без учета типа файловой системы). Запрещено изменение категории конфиденциальности каталога	
Запрещен доступ к каталогу, если его категория конфиденциальности выше, чем заданная категория для устройства, содержащего каталог	
Конфиденциальные файлы размещаются в каталогах, имеющих категорию конфиденциальности не ниже категории конфиденциальности файла. Например, в каталоге с категорией "конфиденциально" могут размещаться как неконфиденциальные файлы, так и файлы с категорией "конфиденциально"	

Без контроля потоков	При контроле потоков
Пользователь, не имеющий доступ к файлу, может просмотреть содержимое конфиденциального каталога, в котором находится файл, но не может открыть файл. Поэтому названия конфиденциальных файлов не должны содержать конфиденциальную информацию	
Запрещено удаление конфиденциального каталога с помещением в "Корзину"	Запрещено удаление любого каталога с помещением в "Корзину"
Наследование категории конфиденциальности каталога	
Если включен режим автоматического присвоения категории конфиденциальности при создании, сохранении (перезаписи), копировании или перемещении подкаталога/файла в каталог, ему присваивается категория конфиденциальности каталога	Если включен режим автоматического присвоения категории конфиденциальности при создании, сохранении, копировании или перемещении подкаталога/файла в каталог, ему присваивается категория конфиденциальности каталога. Ограничение: устанавливаемая категория конфиденциальности должна быть равна текущему уровню конфиденциальности сессии
<p>Если отключен режим автоматического присвоения категории конфиденциальности:</p> <ul style="list-style-type: none"> • при создании, сохранении или копировании подкаталога/файлу присваивается категория "неконфиденциально"; • при перемещении подкаталога/файла внутри логического раздела он сохраняет свою категорию конфиденциальности (при этом перемещение файла разрешено, если его категория конфиденциальности не превышает категорию конфиденциальности вышестоящего каталога). Для перемещения подкаталогов требуется соответствующая привилегия пользователя 	<p>Если отключен режим автоматического присвоения категории конфиденциальности:</p> <ul style="list-style-type: none"> • при создании, сохранении или копировании подкаталога/файлу присваивается категория, соответствующая уровню конфиденциальности сессии, но не выше категории конфиденциальности каталога; • при перемещении подкаталога/файла внутри логического раздела он сохраняет свою категорию конфиденциальности (при этом перемещение подкаталога/файла разрешено, если его категория конфиденциальности не превышает категорию конфиденциальности каталога и уровень конфиденциальности сессии)
Каталоги с отключенным режимом автоматического присвоения категории конфиденциальности целесообразно использовать для хранения файлов с различными категориями конфиденциальности (меньшими или равными категории конфиденциальности каталога). Чтобы исключить неожиданное изменение категорий конфиденциальности файлов после выполнения операций с ними, рекомендуется использовать каталоги, для которых установлено одинаковое состояние режима автоматического присвоения категории	
Работа в приложениях	
Приложению присваивается уровень конфиденциальности, равный наивысшей категории конфиденциальности среди открытых в приложении файлов. Уровень конфиденциальности приложения не снижается после закрытия конфиденциального файла и сохраняется до закрытия приложения	Приложению присваивается уровень конфиденциальности, равный текущему уровню сессии пользователя. Разрешается открывать файлы не выше этого уровня. Категория файлов с более низким уровнем конфиденциальности повышается до уровня конфиденциальности сессии (повышение категории происходит при сохранении файла)

Без контроля потоков	При контроле потоков
Некоторые приложения при запуске автоматически обращаются к определенным файлам. Например, к ранее открывавшимся файлам в приложении. При этом не происходит непосредственное открытие файла (документа). В силу особенностей механизма полномочного управления доступом при таких обращениях к конфиденциальным файлам пользователю предлагается повысить уровень конфиденциальности приложения до категории файлов. В таких случаях, если не планируется работать с предложенным уровнем конфиденциальности, достаточно отказаться от повышения уровня конфиденциальности приложения	
Изменение категории конфиденциальности ресурса	
Пользователь, не обладающий привилегией "Управление категориями конфиденциальности", может только повысить категорию конфиденциальности файлов не выше своего уровня допуска (при этом повышение категории конфиденциальности файла возможно, если его категория ниже, чем категория конфиденциальности каталога)	Пользователь, не обладающий привилегией "Управление категориями конфиденциальности", может только повысить категорию конфиденциальности файлов не выше уровня конфиденциальности сессии (при этом повышение категории конфиденциальности файла возможно, если его категория ниже, чем категория конфиденциальности каталога)
Пользователь, обладающий привилегией "Управление категориями конфиденциальности", может: <ul style="list-style-type: none"> • повысить категорию конфиденциальности каталогов и файлов, но не выше уровня допуска пользователя; • понизить категорию конфиденциальности каталогов и файлов, текущая категория конфиденциальности которых не выше уровня допуска пользователя; • изменять состояние режима автоматического присвоения категории конфиденциальности каталога, если текущая категория конфиденциальности каталога не выше уровня допуска пользователя 	Пользователь, обладающий привилегией "Управление категориями конфиденциальности", может: <ul style="list-style-type: none"> • повысить категорию конфиденциальности каталогов и файлов, но не выше текущего уровня сессии; • понизить категорию конфиденциальности каталогов и файлов, текущая категория конфиденциальности которых не выше текущего уровня сессии; • изменять состояние режима автоматического присвоения категории конфиденциальности каталога, если текущая категория конфиденциальности каталога не выше текущего уровня сессии
Печать конфиденциальных документов	
Если включен режим контроля печати: <ul style="list-style-type: none"> • пользователь, не обладающий привилегией "Печать конфиденциальных документов", может распечатывать только неконфиденциальные документы; • пользователь, обладающий привилегией "Печать конфиденциальных документов", может распечатывать конфиденциальные документы с категорией конфиденциальности, не превышающей уровень допуска пользователя 	Если включен режим контроля печати: <ul style="list-style-type: none"> • пользователь, не обладающий привилегией "Печать конфиденциальных документов", может распечатывать только неконфиденциальные документы (если документ не редактировался); • пользователь, обладающий привилегией "Печать конфиденциальных документов", может распечатывать конфиденциальные документы с категорией конфиденциальности, не превышающей текущий уровень сессии
Если отключен режим контроля печати конфиденциальных документов, любому пользователю, имеющему доступ к конфиденциальным документам, разрешен вывод этих документов на печать независимо от наличия у него привилегии "Печать конфиденциальных документов". При этом документы распечатываются без грифа конфиденциальности	
При включенном режиме контроля печати конфиденциальные документы можно выводить на печать в любых приложениях, использующих стандартные методы настройки параметров печати (например, MS Word или MS Excel). При выводе на печать документы автоматически маркируются (добавляется гриф)	

Без контроля потоков	При контроле потоков
Вывод на внешние носители	
Пользователь, имеющий доступ к конфиденциальным документам, может копировать файлы или сохранять их содержимое на любые носители независимо от наличия привилегии "Вывод конфиденциальной информации"	Пользователь, не обладающий привилегией "Вывод конфиденциальной информации", не может копировать конфиденциальные файлы или сохранять их содержимое на внешние носители. Устройство считается внешним носителем, если для него включен режим доступа "без учета категории конфиденциальности" и файловая система для хранения данных отличается от NTFS

Глава 6

Настройка механизмов защиты информации на дисках

В данной главе приведены описания настройки следующих механизмов защиты:

- механизм дискреционного управления доступом;
- механизм затирания информации, удаляемой с дисков;
- механизм защиты информации на локальных дисках.

Дискреционное управление доступом к каталогам и файлам

При настройке дискреционного разграничения доступа пользователей к каталогам и файлам на локальных дисках выполняются действия:

1. Предоставление привилегии для изменения прав доступа на любых ресурсах.
2. Назначение администраторов ресурсов.
3. Настройка регистрации событий и аудита операций с ресурсами.

Предоставление привилегии для изменения прав доступа к ресурсам

В механизме дискреционного управления доступом предусмотрена возможность для привилегированных пользователей изменять права доступа на любых каталогах и файлах локальных дисков независимо от установленных прав доступа к самим ресурсам. Для этого пользователю должна быть предоставлена привилегия "Дискреционное управление доступом: Управление правами доступа". Привилегия в частности позволяет назначить администраторов ресурсов, которые в дальнейшем смогут настраивать права доступа к ресурсам для остальных пользователей.

По умолчанию привилегией на управление правами доступа обладают пользователи, входящие в локальную группу администраторов.

Для предоставления привилегии:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. [13](#)).
2. Выберите папку "Привилегии".
В правой части окна появится список привилегий.
3. Выберите элемент "Дискреционное управление доступом: Управление правами доступа" и вызовите диалог настройки параметра.
4. В диалоге отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия, и нажмите кнопку "ОК".

Назначение администраторов ресурсов

Администраторы ресурсов в механизме дискреционного управления доступом могут изменять права доступа других пользователей к определенным каталогам и файлам на локальных дисках. Администратором ресурса считается пользователь, для которого установлено разрешение на операцию "Изменение прав доступа" в параметрах доступа к ресурсу. Описание процедуры изменения прав доступа см. в документе [\[6\]](#).

Настройка регистрации событий и аудита операций с ресурсами

Изменение перечня регистрируемых событий

Для отслеживания произошедших событий, связанных с работой механизма дискреционного управления доступом к каталогам и файлам, необходимо выполнить настройку регистрации событий. Для этого следует указать, какие события категории "Дискреционный доступ" должны регистрироваться в журнале Secret Net. Описание процедуры настройки списка регистрируемых событий см. на стр. **151**.

Настройка аудита успехов и отказов

Настройка параметров аудита операций с ресурсом выполняется при изменении прав доступа к этому ресурсу. Описание процедуры изменения прав доступа см. в документе [6].

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, содержавшаяся 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.



Внимание!

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. **13**).
2. Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.
Для настройки механизма затирания данных используются следующие параметры:
 - 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 выберите 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.

Защита локальных дисков

Защита доступа к локальным дискам (логическим разделам) компьютера осуществляется с использованием механизма защиты дисков. Механизм блокирует доступ к дискам при несанкционированной загрузке компьютера. Загрузка считается санкционированной, если она выполнена средствами операционной системы с установленным клиентским ПО Secret Net. Все другие способы загрузки ОС считаются несанкционированными с точки зрения функционирования механизма (например, загрузка с внешнего носителя или загрузка другой ОС, установленной на компьютере).



Примечание.

Возможность использования механизма защиты дисков становится доступной после регистрации соответствующей лицензии. Ввод серийного номера для регистрации лицензии можно выполнить при установке клиентского ПО Secret Net или в процессе эксплуатации системы.

Процедура настройки механизма защиты дисков состоит из следующих этапов:

1. Включение механизма.
2. Включение/отключение режима защиты логических разделов.

Включение механизма защиты дисков

По умолчанию после установки клиентского ПО Secret Net и регистрации лицензии механизм защиты дисков отключен. Процедура включения выполняется администратором.

При включении механизма система модифицирует основную загрузочную запись Master Boot Record (MBR) на физическом диске, с которого выполнена загрузка ОС. Поэтому загрузочный диск компьютера должен быть с MBR. При модификации генерируется или загружается специальный ключ, на основе которого в дальнейшем будут модифицироваться загрузочные секторы (boot-секторы) логических разделов на жестких дисках компьютера. Генерация нового ключа выполняется в обязательном порядке при первом включении механизма на данном компьютере. В дальнейшем для повторного включения механизма допускается использовать тот же ключ.



Внимание!

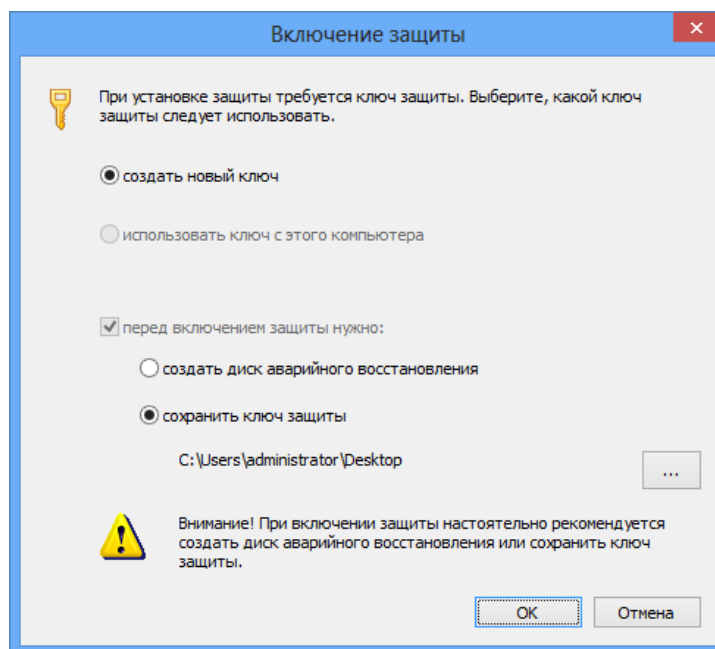
В настройках BIOS компьютера должна быть отключена функция проверки загрузочных вирусов. Если такая функция поддерживается BIOS, установите значение "Disabled" для параметра "Boot Virus Detection" (название параметра может отличаться в зависимости от модели компьютера и версии BIOS).

Чтобы иметь возможность аварийного снятия защиты дисков, необходимо сохранить копию ключа. Ключ можно сохранить следующими способами:

- создать загрузочный диск аварийного восстановления, на котором также будет сохранен и ключ;
- записать ключ в заданную пользователем папку.

Для включения механизма защиты дисков:

1. В Панели управления Windows выберите ярлык "Управление Secret Net 7". На экране появится одноименное диалоговое окно.
2. Перейдите к диалогу "Защита диска" и нажмите кнопку "Включить защиту". На экране появится диалог "Включение защиты".



3. Если на данном компьютере механизм защиты дисков ранее функционировал и был отключен, укажите, какой ключ следует использовать:
 - новый ключ (рекомендуется) — при включении механизма будет сгенерирован новый ключ, и предыдущий ключ станет непригодным. Для генерации нового ключа установите отметку в поле "создать новый ключ";
 - ключ, ранее использовавшийся на данном компьютере, — при включении механизма будет загружен предыдущий ключ (используйте этот вариант только в случае полной уверенности, что ключ не был скомпрометирован, или при необходимости снять защиту логических разделов, если она осталась после некорректного отключения механизма). Для загрузки предыдущего ключа установите отметку в поле "использовать ключ с этого компьютера".
4. Выберите вариант сохранения копии ключа. Для этого оставьте отмеченным поле "перед включением защиты нужно:" (поле заблокировано, если генерируется новый ключ) и укажите нужный вариант сохранения:
 - на загрузочном диске аварийного восстановления (рекомендуется) — будет создан загрузочный диск с копией ключа. Для создания диска установите отметку в поле "создать диск аварийного восстановления";
 - в произвольной папке — файл с ключом будет сохранен в указанной папке. Для сохранения ключа установите отметку в поле "сохранить ключ защиты". Текущий заданный путь к папке отображается ниже. Чтобы указать другое местоположение, нажмите кнопку справа и выберите нужную папку в стандартном диалоге.

Примечание.

Если выбран вариант использования предыдущего ключа и при этом копия этого ключа имеется в наличии, можно отказаться от сохранения новой копии. Для этого удалите отметку из поля "перед включением защиты нужно:".

5. Нажмите кнопку "OK".

Диалог "Включение защиты" закроется, и система приступит к включению механизма защиты дисков.

Если выбран один из вариантов сохранения копии ключа, включение механизма происходит после успешного сохранения. Для создания загрузочного диска аварийного восстановления автоматически запускается специальная программа-мастер (описание процедуры работы с мастером см. ниже). После сохранения ключа на экране появляется соответствующее сообщение.

6. После включения механизма перезагрузите компьютер.

Мастер создания диска аварийного восстановления

В состав программных средств, обеспечивающих функционирование механизма защиты дисков, входит специальная программа-мастер, с помощью которой выполняется создание загрузочного диска аварийного восстановления. В качестве носителей для создания загрузочных дисков поддерживаются компакт-диски и USB-флеш-накопители. Кроме того, можно записать файл образа диска и использовать его для записи диска в других программных средствах.

Запуск мастера происходит при выборе варианта создания диска аварийного восстановления во время включения механизма защиты дисков (см. выше) или при работе с программой-мастером аварийного восстановления (см. стр. 212).

Для создания загрузочного диска аварийного восстановления:

1. В стартовом диалоге мастера нажмите кнопку "Далее".
На экране появится диалог для выбора варианта загрузки ключа.
2. В зависимости от того, какой ключ требуется загрузить, выполните соответствующее действие:
 - чтобы загрузить ключ из специального хранилища на данном компьютере (последний сгенерированный ключ) — установите отметку в поле "использовать ключ с этого компьютера";
 - чтобы загрузить ключ из файла — удалите отметку из поля "использовать ключ с этого компьютера" (если она там установлена) и нажмите кнопку "Указать". В появившемся стандартном диалоге выберите файл с ключом. Имя файла должно содержать расширение .RK. Данный способ загрузки ключа используется, например, если нет возможности загрузить ключ из хранилища на компьютере, или при создании диска аварийного восстановления на другом компьютере.
3. После загрузки ключа нажмите кнопку "Далее".
На экране появится диалог для настройки параметров записи.
4. В поле "Вид носителя" выберите нужный носитель для создания загрузочного диска: компакт-диск или USB-флеш-накопитель.
5. Если для создания загрузочного диска выбран компакт-диск, доступна возможность записи файла образа диска в указанной папке. Для записи файла установите отметку в поле "сохранить образ диска в папке". Текущий заданный путь к папке отображается ниже. Чтобы указать другое местоположение, нажмите кнопку справа и выберите нужную папку в стандартном диалоге.
6. Для записи загрузочного диска установите отметку в поле "записать образ на носитель в устройстве" и укажите устройство в поле справа. Раскрывающийся список содержит имена устройств, совместимых с выбранным типом носителя.
7. Нажмите кнопку "Далее".
Начнется формирование диска. Ход процесса отображается в информационном окне в виде полосы прогресса.
8. По завершении создания диска нажмите кнопку "Готово" для прекращения работы мастера.

Включение и отключение защиты логических разделов

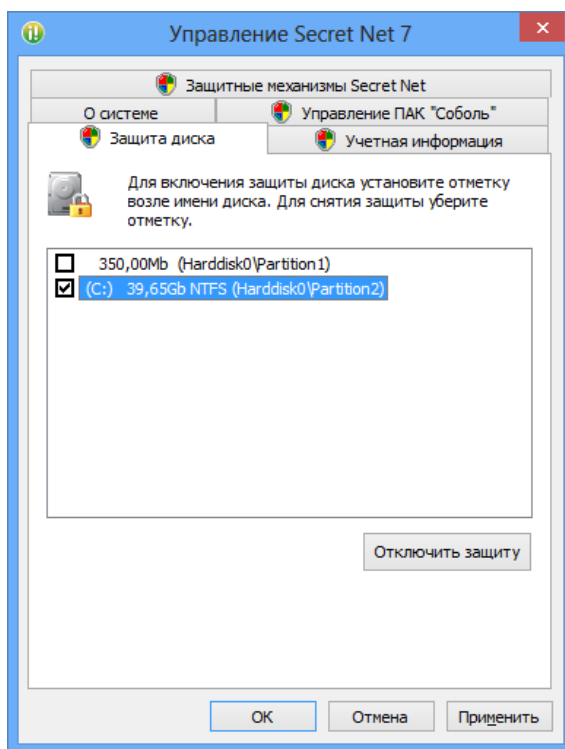
По умолчанию после включения механизма защиты дисков режим защиты отключен для всех логических разделов. Включение режима защиты нужных разделов осуществляется выборочно.

Механизм обеспечивает защиту до 128 логических разделов при общем количестве физических дисков до 32. Логические разделы, для которых устанавливается режим защиты, должны иметь файловую систему NTFS, FAT32 или FAT16. Поддерживаются физические диски с основной загрузочной записью

(MBR) или с таблицей разделов на идентификаторах GUID Partition Table (GPT). Диски с другими типами разбиения на логические разделы не поддерживаются (например, динамические диски).

Для включения/отключения режима защиты:

1. В Панели управления Windows выберите ярлык "Управление Secret Net 7".
На экране появится одноименное диалоговое окно.
2. Перейдите к диалогу "Защита диска".
В диалоге отображается список дисков, для которых можно включить режим защиты.



3. Отметьте логические разделы, для которых необходимо включить режим защиты. Если необходимо отключить защиту логического раздела, удалите отметку слева от его названия.
4. Нажмите кнопку "ОК" и перезагрузите компьютер.

Отключение механизма защиты дисков

При отключении механизма защиты дисков происходит снятие защиты со всех логических разделов и возвращение к первоначальному состоянию MBR на физическом диске, с которого выполняется загрузка ОС. При этом ключ не удаляется из системы и может использоваться повторно на данном компьютере.

Для отключения механизма защиты дисков:

1. В Панели управления Windows выберите ярлык "Управление Secret Net 7".
На экране появится одноименное диалоговое окно.
2. Перейдите к диалогу "Защита диска" и нажмите кнопку "Отключить защиту".
Произойдет отключение механизма, после чего название кнопки изменится на "Включить защиту".
3. После отключения механизма перезагрузите компьютер.

Глава 7

Настройка системы для задач аудита

Настройка регистрации событий на компьютерах

Изменение параметров журнала Secret Net

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

Для настройки параметров журнала:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. [13](#)).
2. Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.
3. Выберите элемент "Журнал: Максимальный размер журнала системы защиты" и вызовите диалог настройки параметра.
4. В диалоге установите значение максимально допустимого размера журнала в килобайтах. Диапазон значений — от 64 до 4 194 240 КБ (с шагом 64).
5. В списке параметров выберите элемент "Журнал: Политика перезаписи событий" и вызовите диалог настройки параметра.
6. В диалоге выберите способ очистки журнала при его переполнении (если размер журнала достигает максимального значения). Для этого установите отметку в одном из полей диалога. Затем нажмите кнопку "ОК".

Затирать события по мере необходимости

При переполнении журнала система защиты автоматически удаляет из журнала необходимое количество самых старых записей

Затирать события старше <...> дней

При переполнении журнала система защиты автоматически удаляет записи, время хранения которых превысило заданный период. Новые записи не будут добавляться, если журнал достиг максимального размера и не содержит записей старше заданного периода. Диапазон ввода значений — от 1 до 365 дней

Не затирать события

После достижения максимального размера записи хранятся в журнале. Новые события в журнале не регистрируются. Журнал можно очистить только вручную с помощью программы просмотра журналов. Очистка должна выполняться периодически по мере накопления записей, чтобы не допустить переполнение журнала, так как это может привести к нарушениям в работе системы и вызвать блокировку компьютера

Выбор событий, регистрируемых в журнале

По умолчанию в журнале Secret Net регистрируются все возможные события, кроме событий категории "Контроль приложений" и некоторых событий категорий "Контроль целостности" и "Дискреционный доступ". Подробное описание регистрируемых событий содержится на стр. [184](#).



Внимание!

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

Для настройки списка регистрируемых событий:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр.13).
2. Выберите папку "Регистрация событий".
В правой части окна появится список регистрируемых событий.
3. В списке событий выберите элемент с именем события, для которого необходимо изменить режим регистрации, и вызовите диалог настройки параметра.
4. Установите отметку в поле "отключена" (чтобы событие не регистрировалось в журнале) или "включена" (чтобы включить регистрацию) и нажмите кнопку "ОК".
5. При необходимости повторите действия 3–4 для других событий в списке.

Настройка теневого копирования выводимых данных**Общее управление функцией теневого копирования**

Функцию теневого копирования можно отключить для всех устройств следующих типов:

- устройства, подключаемые к системе в качестве дисков;
- принтеры.

Если функция теневого копирования включена, будут действовать параметры, заданные соответственно для устройств и/или принтеров.

Для общего управления функцией теневого копирования:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр.13).
2. Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.
3. Вызовите контекстное меню для нужного параметра (см. таблицу ниже) и выберите в нем команду "Свойства".
На экране появится диалог настройки параметра.
4. Настройте действие параметра и нажмите кнопку "ОК".

Контроль печати: Теневое копирование

Отключено для всех принтеров. Теневое копирование при выводе на печать не выполняется.

Определяется настройками принтера. Теневое копирование выполняется для принтеров с включенным режимом "Сохранять копию распечатанных документов" (настройка параметров использования принтеров осуществляется в папке "Принтеры")

Контроль устройств: Теневое копирование

Отключено для всех устройств. Теневое копирование при записи информации на устройства не выполняется.

Определяется настройками устройства. Теневое копирование выполняется для устройств с включенным режимом "Сохранять копию информации, записываемой на устройство" (настройка параметров использования устройств осуществляется в папке "Устройства")

Выбор устройств и принтеров для теневого копирования

Теневое копирование поддерживается для устройств следующих видов:

- подключаемые сменные диски;
- дисководы гибких дисков;

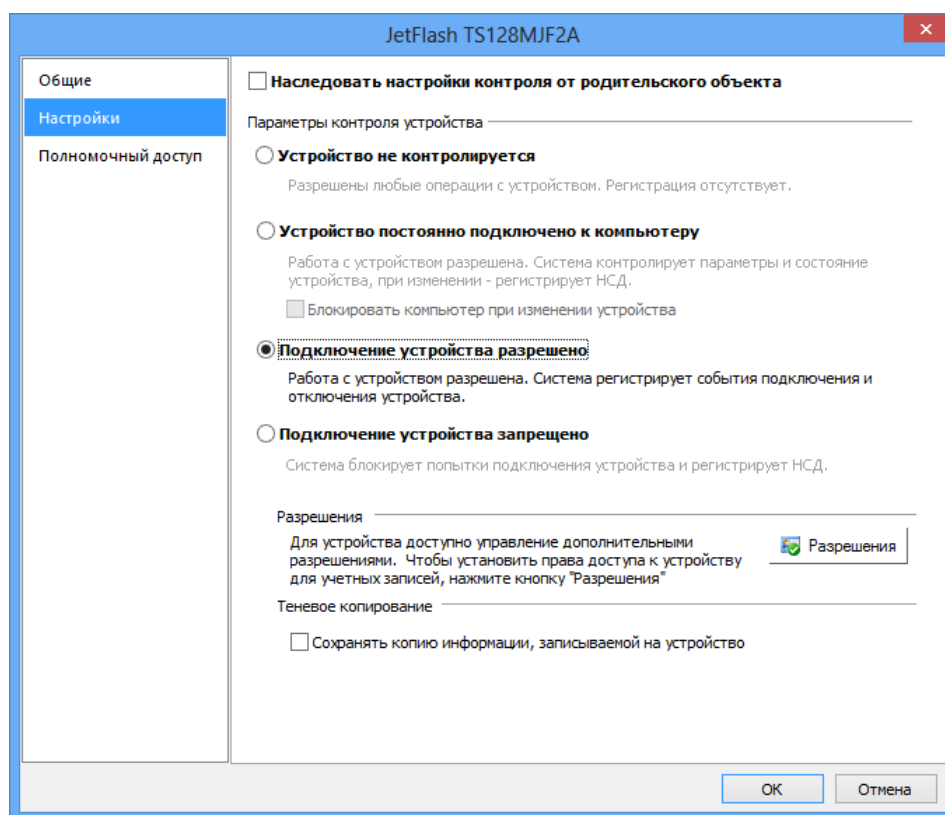
- дисководы оптических дисков с функцией записи.

Для перечисленных устройств и для классов, к которым относятся такие устройства, доступна возможность включения режима сохранения копий при записи информации.

Теневое копирование также может выполняться при печати документов. Управлять режимом сохранения копий можно для конкретных принтеров или для элемента "Настройки по умолчанию" в списке принтеров.

Для управления режимом сохранения копий в списке устройств:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 13).
2. Выберите папку "Устройства".
В правой части окна появится список устройств.
3. Выберите в списке объект (класс или устройство), вызовите контекстное меню и выберите команду "Свойства".
На экране появится диалог для настройки параметров объекта.
4. Перейдите к группе параметров "Настройки".



5. Удалите отметку из поля "Наследовать настройки контроля от родительского объекта".
После этого станут доступны параметры контроля устройства.
6. Отметьте режим контроля "Устройство постоянно подключено к компьютеру" или "Подключение устройства разрешено".
7. Измените нужным образом состояние выключателя "Сохранять копию информации, записываемой на устройство":
 - установите отметку — чтобы включить режим сохранения копий;
 - удалите отметку — если нужно отключить режим.

Для управления режимом сохранения копий в списке принтеров:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры

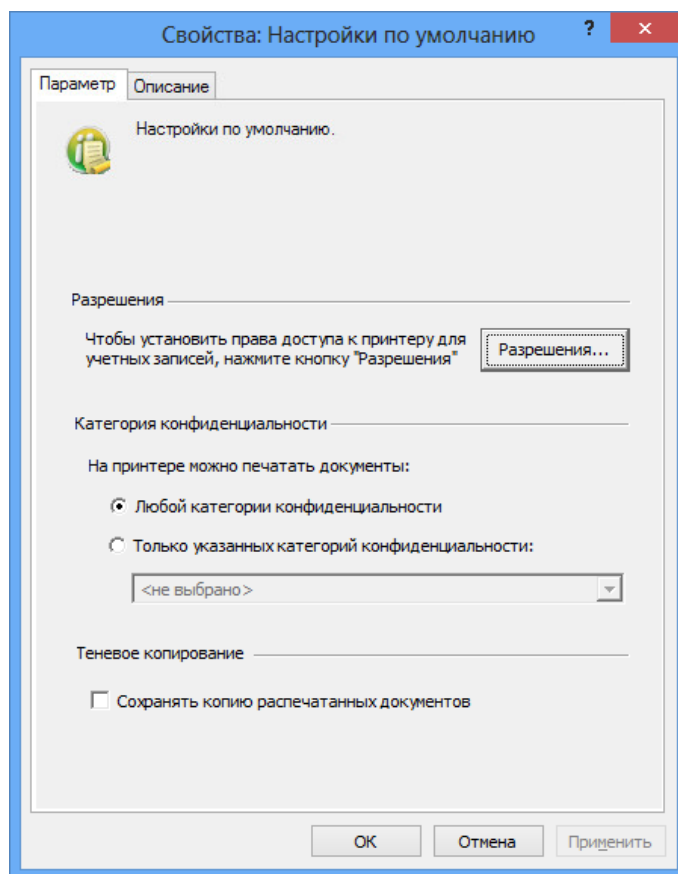
Secret Net" (см. стр. [13](#)).

2. Выберите папку "Принтеры".

В правой части окна оснастки появится список принтеров.

3. Выберите в списке нужный элемент, вызовите контекстное меню и выберите команду "Свойства".

На экране появится диалог для настройки параметров.



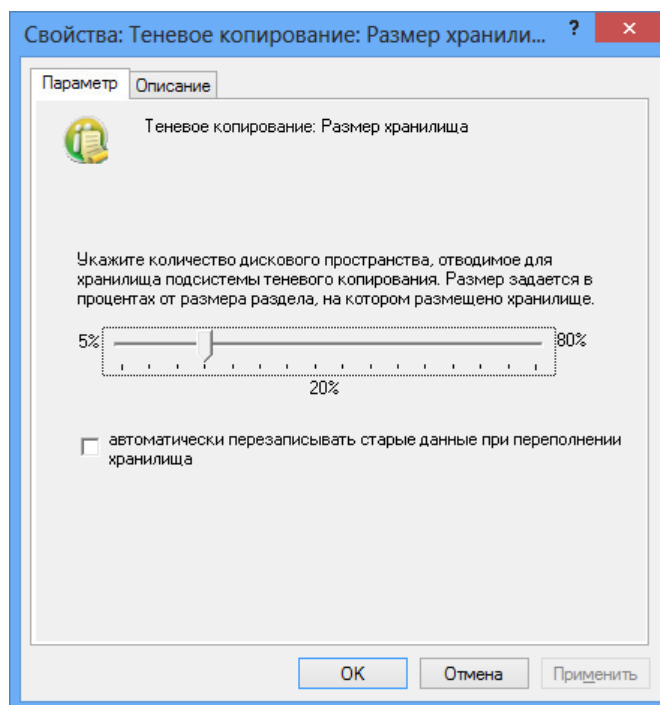
4. Чтобы включить режим сохранения копий — установите отметку в поле "Сохранять копию распечатанных документов". Если требуется отключить режим — удалите отметку.

Изменение параметров хранилища теневого копирования

При настройке параметров можно изменить ограничение максимального объема хранилища, а также включить или отключить возможность перезаписи.

Для настройки параметров хранилища:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. [13](#)).
2. Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.
3. В списке параметров выберите элемент "Теневое копирование: Размер хранилища" и вызовите диалог настройки параметра.



4. Укажите нужный размер хранилища в процентах от дискового пространства.
5. Выберите вариант поведения системы при переполнении хранилища (если размер хранилища достигает максимального уровня):
 - чтобы разрешить вывод данных — установите отметку в поле "автоматически перезаписывать старые данные при переполнении хранилища". В этом случае копии выводимых данных будут замещать в хранилище наиболее старые копии, помещенные в хранилище;
 - чтобы запретить вывод данных — удалите отметку из поля. При достижении максимального размера хранилища новые попытки вывода данных будут блокироваться системой.

Настройка контроля запускаемых приложений

В журнале Secret Net могут регистрироваться события запуска и завершения работы приложений (процессов) для обеспечения возможности аудита отслеживания процессов средствами системы защиты. Регистрация может выполняться в следующем объеме:

- события, относящиеся к работе только тех приложений, запуск которых выполнен пользователем компьютера;
- события запуска и завершения для всех процессов системы — не только пользовательских приложений, но и системных.

Примечание.

Регистрация событий для всех процессов системы может существенно увеличить нагрузку на ядро Secret Net и способствовать быстрому переполнению журнала записями о таких событиях. В большинстве случаев данный режим регистрации не является необходимым, поэтому по умолчанию включена регистрация событий, относящихся только к пользовательским приложениям.

Для настройки контроля приложений:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 13).
2. Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.

3. Вызовите контекстное меню для параметра "Контроль приложений: Режим аудита" и выберите в нем команду "Свойства".
На экране появится диалог настройки параметра.
4. Чтобы включить режим регистрации событий для всех процессов системы, установите отметку в поле "аудит пользовательских и системных приложений". Если достаточно регистрации только для приложений, запущенных пользователем компьютера, — оставьте отмеченным поле "аудит пользовательских приложений".
5. Закройте диалог настройки параметра и выберите папку "Регистрация событий".
В правой части окна появится список регистрируемых событий.
6. Укажите, какие события категории "Контроль приложений" будут регистрироваться в журнале Secret Net. Описание процедуры настройки списка регистрируемых событий см. на стр. [151](#).

Предоставление прав доступа к журналам

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

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

Привилегии для работы с локальными журналами

Для использования программы просмотра локальных журналов предоставляются следующие привилегии:

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

Примечание.

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

Для предоставления привилегий:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. [13](#)).
2. Выберите папку "Привилегии".
В правой части окна появится список привилегий.
3. Выберите элемент "Журнал: Просмотр журнала системы защиты" и вызовите диалог настройки параметра.
4. В диалоге отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия, и нажмите кнопку "ОК".
5. Выберите элемент "Журнал: Управление журналом системы защиты" и вызовите диалог настройки параметра.
6. В диалоге отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия, и нажмите кнопку "ОК".

Привилегии для работы с централизованными журналами

Для загрузки записей централизованных журналов используется программа оперативного управления. Описание предусмотренных привилегий для работы с программой см. в документе [\[4\]](#).

Глава 8

Вспомогательные средства администрирования

Формирование отчетов

В Secret Net 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).

Электронные идентификаторы. Отчет содержит сведения о электронных идентификаторах, зарегистрированных в системе Secret Net.

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.



Внимание!

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

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 в программе оперативного управления. Описание процедуры централизованного формирования отчета см. в документе [4].

Для локального формирования отчета "Паспорт ПО":

1. Выполните запуск программы "Контроль программ и данных" в локальном режиме работы (см. стр. 71).
2. Выберите 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) и укажите название организации. Для этого нажмите кнопку "Дополнительно...", в появившемся диалоге настройте 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"

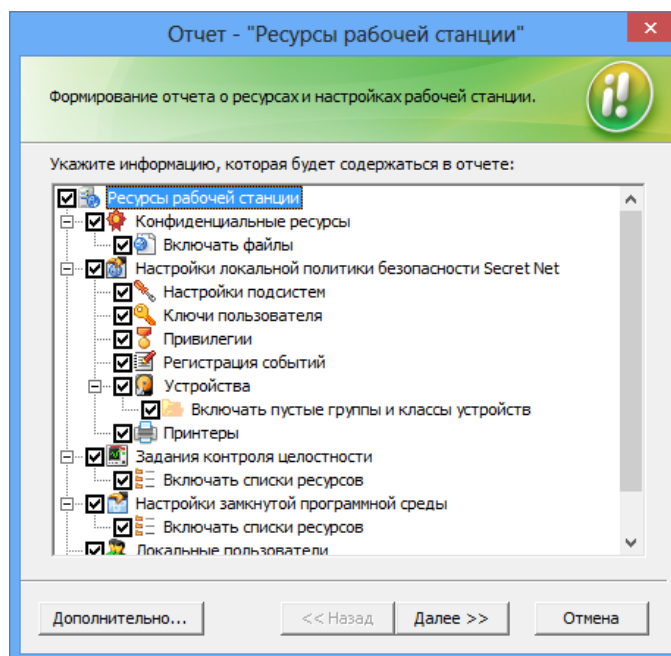
В отчете содержатся следующие сведения о компьютере:

- учетная информация компьютера (имя компьютера, название подразделения, к которому относится компьютер, номер системного блока и др.);
- общие сведения о клиенте Secret Net (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 в программе оперативного управления. Описание процедуры централизованного формирования отчета см. в документе [4].

Для локального формирования отчета "Ресурсы рабочей станции":

1. Выполните запуск программы "Контроль программ и данных" в локальном режиме работы (см. стр. 71).
2. Выберите 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, 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 в автономном режиме функционирования или в сетевом режиме, если процедура формирования отчета выполняется на контроллере домена).

- **Список файловых ресурсов с явно заданными правами доступа.**
Чтобы сохранить список, отметьте элемент "Дискреционное управление доступом".
- 4. При необходимости настройте параметры нумерации страниц отчета (расположение номеров и отображение общего количества страниц) и укажите название организации. Для этого нажмите кнопку "Дополнительно...", в появившемся диалоге настройте 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 (см. ниже) или в программе оперативного управления. Описание процедуры формирования отчета в программе оперативного управления см. в документе [4].

Для формирования отчета "Допуск пользователей к ПАК "Соболь"" в программе "Контроль программ и данных":

1. Выполните запуск программы "Контроль программ и данных" в централизованном режиме работы (см. стр. 71).
2. Выберите команду "Сервис | Отчеты | Пользователи ПАК "Соболь"".
На экране появится стартовый диалог мастера формирования отчета.
3. Если требуется, чтобы отчет содержал сведения по всем компьютерам (не только на которых установлен ПАК "Соболь"), установите отметку в поле "Добавить в отчет рабочие станции без ПАК "Соболь"". При необходимости настройте параметры нумерации страниц отчета (расположение номеров и отображение общего количества страниц) и укажите название организации. Для этого нажмите кнопку "Дополнительно...", в появившемся диалоге настройте параметры и нажмите кнопку "ОК".
4. Нажмите кнопку "Далее >".
Программа начнет процесс получения и обработки данных, и на экране появится соответствующее сообщение.

Отчет "Электронные идентификаторы"

В отчете содержатся сведения о электронных идентификаторах, присвоенных пользователям.

Отчет формируется централизованно в программе оперативного управления. Описание процедуры формирования отчета приводится в документе [4].

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 локальных журналов. Описание процедуры формирования отчета приводится 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 реализована возможность экспорта и импорта параметров политик, параметров пользователей и параметров механизмов КЦ и ЗПС.

Экспорт/импорт параметров политик

Экспорт параметров системы Secret Net 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. 13).
2. Вызовите контекстное меню раздела "Параметры Secret Net" и выберите 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. 13).
2. Вызовите контекстное меню раздела "Параметры Secret Net" и выберите 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

В автономном режиме функционирования система Secret Net предоставляет возможности экспорта и импорта параметров пользователей (локальных и зарегистрированных доменных пользователей). Экспорт выполняется в файлы формата XML (*.xml).

**Примечание.**

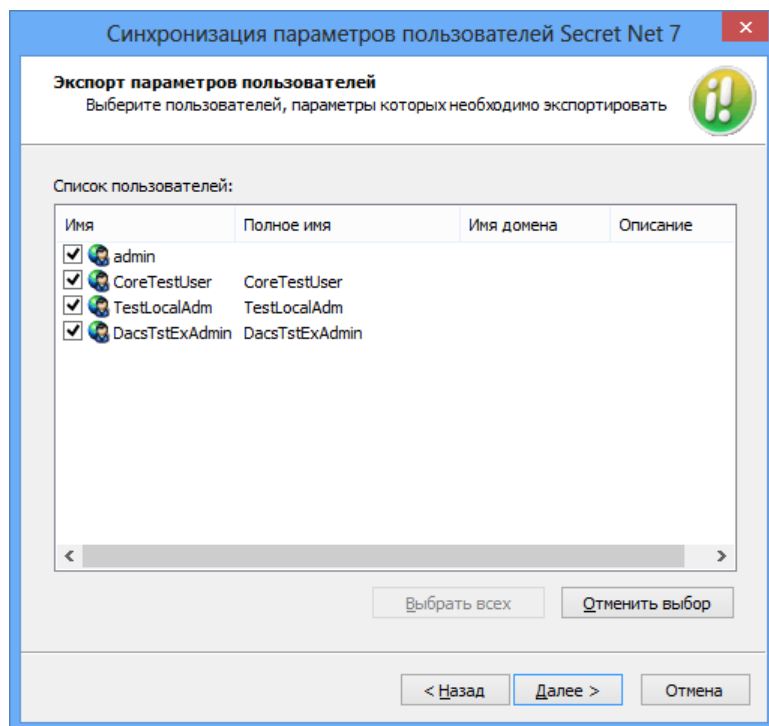
При экспорте и импорте параметров пользователя осуществляется и экспорт/импорт параметров электронных идентификаторов пользователя.

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. Откройте оснастку "Управление компьютером". Для этого выполните соответствующее действие в зависимости от версии установленной операционной системы:
 - на компьютере под управлением ОС Windows 8 или Windows Server 2012 загрузите начальный экран "Пуск" и выберите элемент "Управление компьютером" (относится к группе "Код безопасности");
 - на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код безопасности | Secret Net | Управление компьютером".
2. Перейдите к разделу "Управление компьютером (локальным) | Служебные программы".
3. В зависимости от того, параметры каких пользователей необходимо экспортировать, вызовите контекстное меню для папки "Локальные пользователи и группы | Пользователи" или "Доменные пользователи" и выберите соответствующую команду:
 - "Все задачи | Экспорт/Импорт параметров" — для папки "Пользователи";
 - "Экспорт/Импорт параметров" — для папки "Доменные пользователи".
 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. **86**.

Редактирование учетной информации компьютера

Учетная информация компьютера указывается при установке клиентского ПО системы Secret Net. 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 и используются в отчетах "Паспорт ПО" (см. стр. **157**) и "Ресурсы рабочей станции" (см. стр. **158**).

При необходимости учетную информацию можно изменить.

Для редактирования учетной информации:

1. В Панели управления Windows выберите ярлык "Управление Secret Net 7".
На экране появится диалоговое окно "Управление Secret Net 7".
2. Перейдите к диалогу "Учетная информация".
3. Введите сведения о компьютере в соответствующих полях.
4. Нажмите кнопку "Применить" или "ОК".

Локальное оповещение о событиях НСД

Событиями НСД считаются события, которые имеют тип "Аудит отказов" и регистрируются в журнале Secret Net или штатном журнале безопасности ОС Windows. При возникновении на компьютере таких событий система защиты может локально оповещать об этом текущего пользователя компьютера. В качестве локального оповещения осуществляется подача звукового сигнала и

кратковременный вывод пиктограммы предупреждения в правом верхнем углу экрана.

Режим локального оповещения о событиях НСД можно включать и отключать для всех пользователей компьютера (компьютеров) или предоставить пользователям возможность управлять режимом самостоятельно.

Для управления режимом локального оповещения о событиях НСД:

1. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net" (см. стр. 13).
2. Выберите папку "Настройки подсистем".
В правой части окна появится список параметров.
3. Вызовите контекстное меню для параметра "Администрирование: Локальное оповещение об НСД" и выберите в нем команду "Свойства".
На экране появится диалог настройки параметра.
4. Для включения или отключения режима установите отметку в соответствующем поле. Чтобы предоставить пользователям возможность самостоятельного управления режимом установите отметку в поле "определяется пользователем".



Примечание.

Переключение режима локального оповещения пользователем осуществляется с помощью команды "Уведомления о НСД" в контекстном меню пиктограммы Secret Net в Панели задач.

Локальная регистрация серийных номеров

В локальной базе данных системы Secret Net хранятся следующие серийные номера:

- серийный номер клиента (СНК) — содержит лицензию на использование клиентского ПО системы защиты на компьютере. Наличие серийного номера обеспечивает работоспособность программного обеспечения определенной версии (версий);
- серийный номер подсистемы защиты дисков — содержит лицензию на использование механизма защиты дисков. Наличие серийного номера обеспечивает возможность работы механизма в составе клиентского ПО;
- серийный номер разрешения терминальных подключений — содержит лицензию на использование терминального доступа к компьютеру. Наличие серийного номера обеспечивает возможность определенного количества терминальных подключений с других компьютеров, на которых не установлено клиентское ПО системы Secret Net.

При необходимости можно ввести новый или сменить зарегистрированный серийный номер в локальной базе данных компьютера. Регистрация серийного номера необходима в следующих случаях:

- чтобы сменить демонстрационную лицензию на бессрочную (для СНК);
- чтобы активировать действие механизма защиты дисков (для серийного номера подсистемы защиты дисков);
- чтобы активировать возможность терминальных подключений (для серийного номера разрешения терминальных подключений);
- чтобы восстановить серийный номер в локальной базе данных при повреждении или удалении.

В сетевом режиме функционирования ввод серийных номеров можно выполнять локально или централизованно на рабочем месте администратора в программе оперативного управления (см. документ [4]). В автономном режиме функционирования доступна возможность только локального ввода серийных номеров (см. ниже).

Для локальной регистрации серийного номера:

1. В Панели управления Windows выберите ярлык "Управление Secret Net 7".

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. Укажите тип серийного номера:
 - для ввода серийного номера клиента — установите отметку в поле "Secret Net";
 - для ввода серийного номера подсистемы защиты дисков — установите отметку в поле "защита жесткого диска";
 - для ввода серийного номера разрешения терминальных подключений — установите отметку в поле "терминальный доступ".
4. В поле ввода введите новый серийный номер и нажмите кнопку "ОК". При появлении на экране диалога запроса нажмите кнопку "Да" для продолжения процедуры.
5. 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 7".

Временное отключение защитных механизмов

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

В перечень механизмов, для которых предусмотрено отключение, входят:

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

При соблюдении соответствующих организационных мер некоторые механизмы можно отключать в нормальном режиме работы системы. Например, компьютер контроллера домена не предполагается использовать в качестве файлового сервера или рабочей станции для пользователей. Поэтому при установке клиента на этом компьютере по умолчанию отключены те механизмы, в которых нет необходимости для роли контроллера домена. За счет этого повышается производительность системы в целом.

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



Примечание.

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 выберите ярлык "Управление Secret Net 7".
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.

Внимание!

Для включения режима усиленной защиты трафика при обращениях к службам каталогов установите отметку в поле "шифровать управляющий сетевой трафик". Перед сохранением изменений будет выполнена проверка возможности установки защищенного соединения со службами каталогов, 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 или серверу безопасности будет невозможен для компонентов системы Secret Net. Включать режим усиленной защиты следует только после настройки инфраструктуры открытых ключей в системе.

Включение режима для сервера безопасности выполняется в конфигурационном файле ServerConfig.xml, который расположен в каталоге установки сервера безопасности. Чтобы включить режим, найдите параметр UseSSLConnection и измените значение false на true.

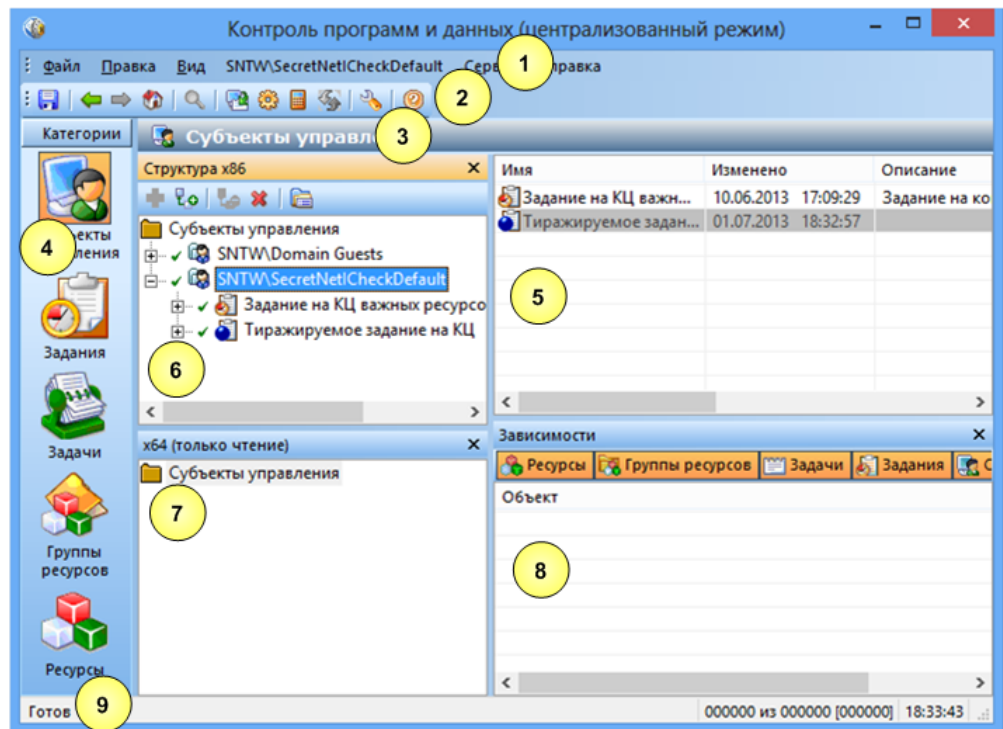
4. Нажмите кнопку "ОК" и перезагрузите компьютер.

Приложение

Общие сведения о программе "Контроль программ и данных"

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, связанных с выбранным элементом в окне структуры. Строка таблицы выделяется соответствующим цветом, если объект находится в одном из следующих состояний:









- объект связан с вышестоящими и нижестоящими объектами — по умолчанию фон текста белый;
- объект не связан с вышестоящими или нижестоящими объектами — по умолчанию фон текста 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. [169](#))

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 выберите команду "Добавить в рабочую модель..."

8 — Окно зависимостей

Содержит список объектов, связанных с выбранным элементом 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. Выберите команду "Сервис | Настройки...".
На экране появится диалог "Настройки приложения".
2. Последовательно выбирая названия групп из списка в левой части диалога, укажите необходимые значения параметров (параметры представлены в правой части). 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 с вышестоящими, и с нижестоящими объектами иерархии
Фон
Определяет цвет фона строки для отображения сведений об объектах, которые связаны 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)
<p>Определяет цвет символов для отображения:</p> <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)
<p>Определяет цвет фона строки для отображения:</p> <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)
<p>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</p>
Фон (нелокальные)
<p>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</p>

Группа параметров "Общие | Интерфейс"

Содержит отдельные параметры интерфейса, не относящиеся к вышеперечисленным группам.

Диалог при подготовке к ЗПС
<p>Если установлено значение "Да", при запуске процедуры подготовки ресурсов для включения их в механизм ЗПС (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)</p>
Диалог расчета эталонов
<p>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)</p>
Сетка в списке
<p>Если установлено значение "Да", в области списка объектов и в дополнительном окне зависимостей отображаются линии, разделяющие ячейки таблиц</p>

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, имеющих 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>`
При централизованном управлении список действует на компьютерах с версией ОС соответствующей разрядности (32- или 64-разрядные версии) и относящихся к субъектам, для которых в параметрах механизма ЗПС действует параметр "Режимы заданы централизованно"

Добавлять модули

Если установлено значение "Да", при поиске выполняемых ресурсов программа 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 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 безопасности, в отношении которых модель данных изменилась, будет отправлено оповещение об изменениях

Группа параметров "Настройки AD | Общие"




Содержит единственный параметр настройки удаления объектов из централизованной модели данных. Используется только в режиме централизованного управления.

Время жизни

Определяет время, в течение которого объект централизованной модели данных, помеченный для удаления, остается в Active Directory и учитывается при синхронизации. Значение параметра задается в часах

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

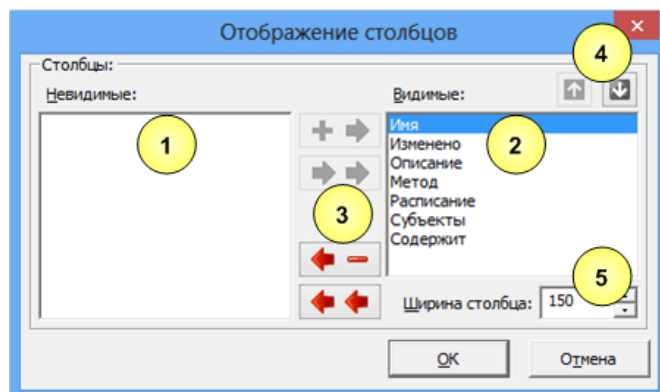
Настройка отображения колонок в таблицах

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 выберите команду "Столбцы...".

На экране появится диалог настройки параметров отображения колонок:

**Пояснение.**

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

2. Настройте параметры отображения колонок.

Для восстановления исходного состояния таблицы:

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

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

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. Выберите 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

При наличии установленной отметки параметр определяет имя колонки (в раскрываемом списке справа), по которой будет выполняться поиск в таблице. Если отметка отсутствует, поиск осуществляется во всех отображаемых колонках в таблице

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. [168](#)).

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 выберите команду "Перейти в дереве".

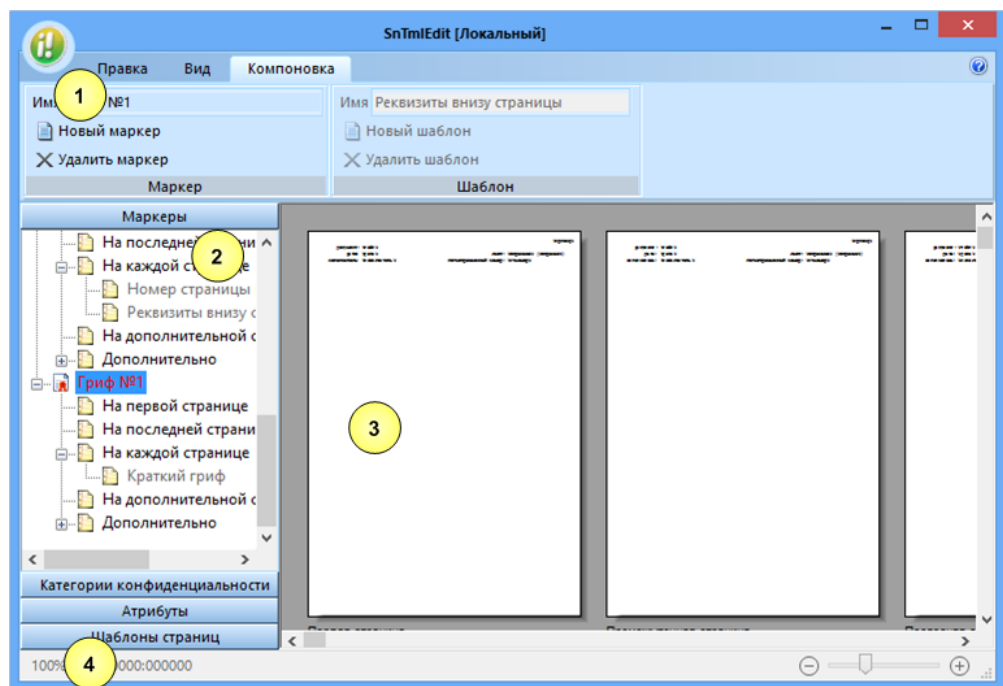
В окне структуры будет раскрыта соответствующая ветвь дерева и выделен искомый объект.

Общие сведения о программе редактирования маркеров

Программа редактирования маркеров предназначена для настройки маркировки документов, выводимых на печать. Запуск программы осуществляется в диалоге настройки параметра групповой политики "Контроль печати: Маркировка документов" (см. стр. [123](#)).

Интерфейс программы

Пример окна программы редактирования маркеров представлен на следующем рисунке:



Окно программы может содержать следующие элементы интерфейса:

1 Лента

Содержит команды управления (инструменты) для выполнения действий в программе. Лента состоит из отдельных вкладок, в которых группируются команды в соответствии с их назначением. Для открытия вкладки используется ее заголовок.

Рабочее пространство в окне программы можно увеличить за счет переключения ленты в режим автоматического сворачивания. В этом режиме отображаются только заголовки вкладок, а разворачивание ленты происходит при выборе заголовка вкладки. Чтобы переключить режим отображения ленты, наведите указатель на заголовок любой вкладки и дважды нажмите левую кнопку мыши

2 Панель выбора объектов

Содержит списки объектов и параметров использования объектов. Объекты и параметры группируются в следующих разделах:

- "Маркеры" — раздел предназначен для формирования списка маркеров (грифов). Для каждого маркера указываются шаблоны оформления определенных страниц при печати документа: первой страницы, последней, некоторых страниц, дополнительной или на обратной стороне листа. Маркер может содержать несколько шаблонов. При этом расположение данных указывается в шаблонах, но не в маркере. Формирование списка маркеров осуществляется с помощью команд группы "Маркер" на вкладке "Компоновка";
- "Категории конфиденциальности" — раздел предназначен для выбора маркеров, которые будут использоваться при печати документов определенных категорий конфиденциальности;
- "Атрибуты" — раздел предназначен для формирования списка атрибутов, которые будут использоваться в оформлении шаблонов страниц. Атрибуты представляют собой переменные, значения которых задаются перед отправкой документа на печать. Сведения для атрибута могут запрашиваться у пользователя или подставляются системой автоматически (например, текущая дата). Атрибуты с возможностью автоматического получения сведений обозначаются специальной пиктограммой. В списке можно добавлять и удалять атрибуты, для которых предусматривается запрос сведений у пользователя. Редактирование списка атрибутов осуществляется с помощью кнопок добавления и удаления элементов на панели инструментов в верхней части раздела "Атрибуты";
- "Шаблоны страниц" — раздел предназначен для формирования списка шаблонов оформления, которые указываются в маркерах для определенных страниц. Шаблон является макетом страницы, который накладывается на содержимое документа при его печати. Формирование списка шаблонов осуществляется с помощью команд группы "Шаблон" на вкладке "Компоновка".

Для перехода к нужному разделу используются соответствующие кнопки на панели выбора объектов

3 Область редактирования

Предназначена для отображения и настройки параметров выбранного объекта. В зависимости от типа выбранного объекта область редактирования содержит:

- при выборе маркера — в области представлен общий вид маркировки всех страниц при печати документов с использованием маркера;
- при выборе элемента маркера, соответствующего определенным страницам, — область делится на две части: слева представлен список шаблонов для выбора, а справа — общий вид маркировки страницы при оформлении выбранными шаблонами;
- при выборе атрибута — область редактирования содержит поля с параметрами атрибута: внутреннее и отображаемое имя атрибута, описание и сведения о применении атрибута;
- при выборе шаблона — область редактирования содержит макет страницы для настройки оформления. Настройка выполняется посредством размещения элементов оформления (текста, рамок, значений атрибутов) внутри прямоугольных областей, аналогичных надписям в текстовых редакторах. Управление масштабом и общими параметрами отображения области редактирования осуществляется с помощью команд на вкладке "Вид". Управление элементами оформления и надписями — с помощью команд на вкладке "Правка". Чтобы отредактировать текст в надписи, наведите на нее указатель и дважды нажмите левую кнопку мыши — на экране появится диалог для ввода текста и вставки атрибутов

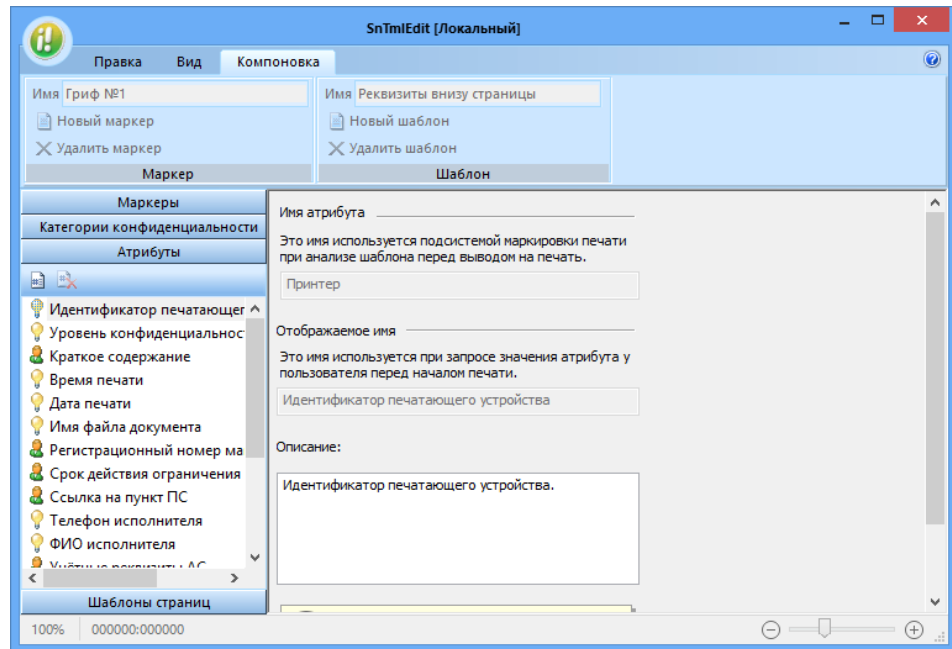
4 Строка состояния

Содержит индикаторы масштаба и положения курсора, используемые при работе с шаблонами страниц

Порядок действий при редактировании маркеров

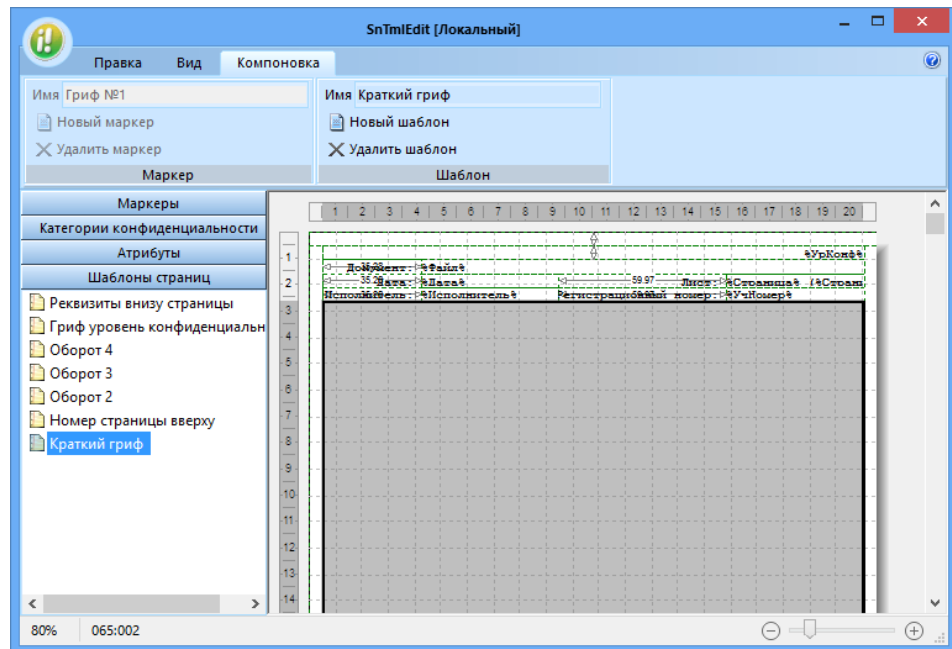
Редактирование маркеров в программе рекомендуется выполнять в следующем порядке:

1. В панели выбора объектов перейдите к разделу "Атрибуты".



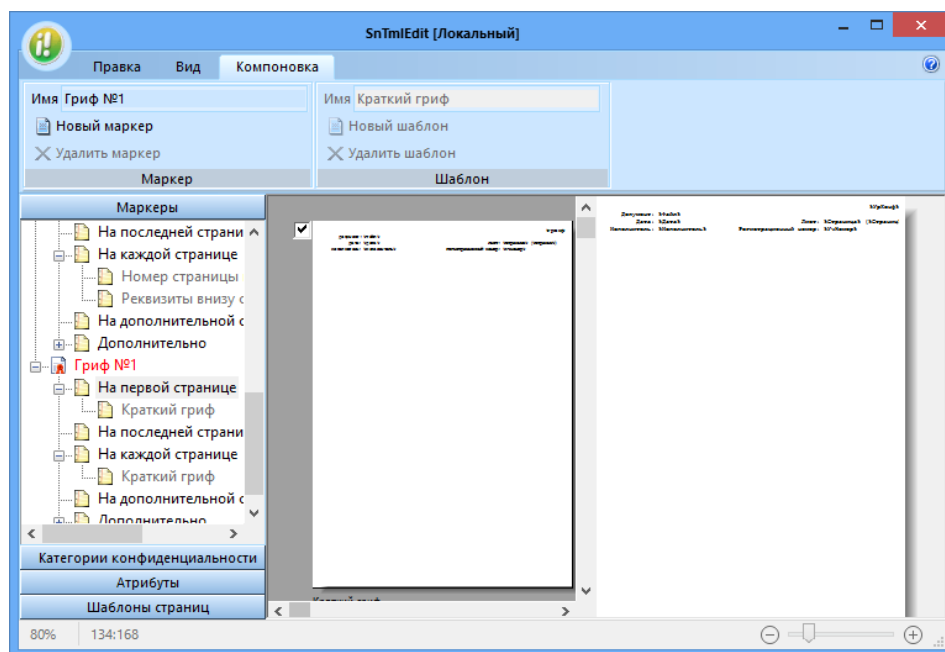
Если в списке отсутствуют нужные атрибуты (позволяющие получать и выводить необходимые сведения при печати документов), измените имеющиеся атрибуты или добавьте новые.

2. В панели выбора объектов перейдите к разделу "Шаблоны страниц".



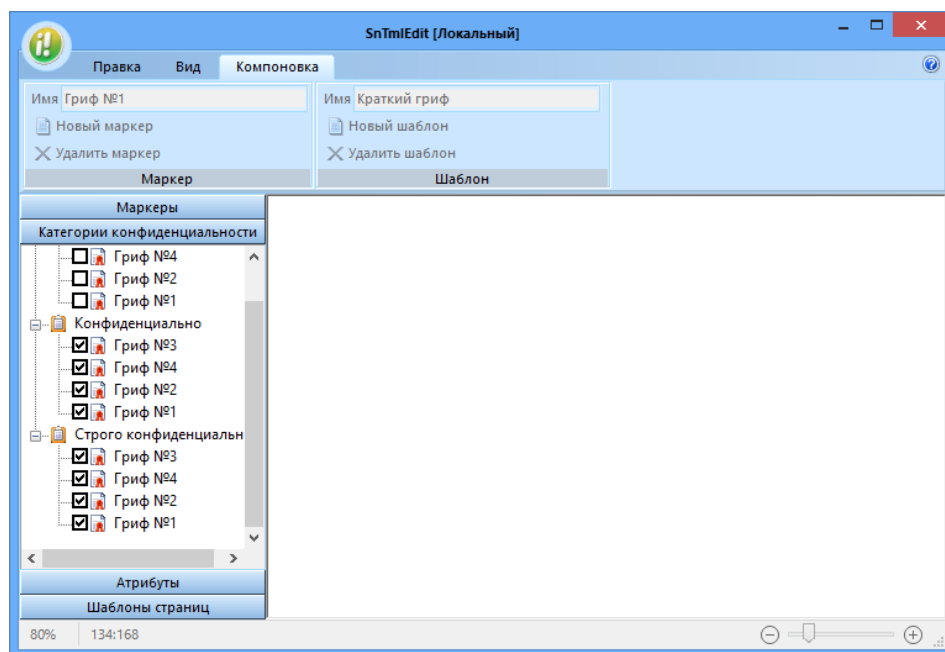
Если в списке отсутствуют нужные шаблоны (с требуемым оформлением и наборами атрибутов), измените имеющиеся шаблоны или добавьте новые. Редактирование элементов оформления шаблонов осуществляется стандартными способами.

3. В панели выбора объектов перейдите к разделу "Маркеры".



Если в списке отсутствуют нужные маркеры (с требуемыми названиями и компоновкой шаблонов), измените имеющиеся маркеры или добавьте новые. Для изменения компоновки шаблонов маркера выберите нужную страницу (диапазон страниц) и в левой части области редактирования отметьте нужные шаблоны.

4. В панели выбора объектов перейдите к разделу "Категории конфиденциальности".



Для каждой категории конфиденциальности отметьте маркеры, которые будут использоваться при печати документов.

5. Закройте программу с сохранением сделанных изменений.



Примечание.

Для промежуточного сохранения изменений в процессе редактирования маркеров можно использовать команду "Сохранить описание маркировки" в общем меню программы, вызов которого осуществляется в левом верхнем углу окна.

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 происходит 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

Резервное копирование БД КЦ-ЗПС с использованием командной строки

Экспорт и импорт модели данных КЦ-ЗПС можно выполнять путем запуска программы "Контроль программ и данных" из командной строки. Для запуска необходимо перейти в каталог установки клиента и запустить на исполнение файл SnICheckAdm.exe с нужными параметрами.

Перечень предусмотренных параметров представлен в таблице.

Параметр	Значение	Описание
HIDE	Отсутствует	Блокирует открытие окна программы
MODE	LOCAL CENTRAL	Локальный режим работы (по умолчанию). Централизованный режим работы
LOAD	Отсутствует	Выполняется загрузка модели данных из БД (ЛБД или ЦБД — зависит от режима работы)
IMPORT	Имя файла в кавычках, например: "C:\Catalog 1\model.xml"	Импорт модели данных из файла
EXPORT	Имя файла в кавычках, например: "C:\Catalog 1\model.xml"	Экспорт модели данных в файл
SAVE	Отсутствует	Выполняется сохранение модели данных в БД (ЛБД или ЦБД — зависит от режима работы)
CALC	Отсутствует	Выполняется расчет эталонов. Модель данных предварительно должна быть сохранена. Реакция на ошибки во время расчета — в соответствии с параметрами, заданными в программе
EXIT	FORCE (необязательно)	Завершает работу программы. Если присутствует значение Force, не выполняется проверка сохранения изменений в БД (и не выводится соответствующий запрос при наличии несохраненных изменений)

Заданные параметры применяются в порядке их следования в командной строке (слева направо). Регистр символов не учитывается.

Перед каждым параметром необходимо добавлять символ "/" или "-". Все элементы строки (параметры, значения) разделяются пробелами.

Пример использования:

```
SnICheckAdm.exe /hide /mode central /load /export "D:\Dir1\Data.xml" /exit force
```

В приведенном примере выполняется запуск программы в централизованном режиме работы без открытия окна. В программу загружается модель данных из ЦБД и затем экспортируется в указанный XML- файл. После экспорта завершается работа программы без проверки несохраненных изменений.

Список групп и классов для контроля устройств

Табл.1 Группы и классы устройств

Группа	Класс
Локальные устройства	Последовательные порты. Параллельные порты. Сменные диски. Оптические диски. Физические диски. Процессоры. Оперативная память. Системная плата. Аппаратная поддержка. Программно-реализованные диски
Устройства USB	Сетевые платы и модемы. Интерфейсные устройства. Сканеры и цифровые фотоаппараты. Принтеры. Устройства хранения. Bluetooth адаптеры. Сотовые телефоны. Электронные идентификаторы и считыватели. Прочие
Устройства PCMCIA	Последовательные порты и модемы. Параллельные порты. Устройства хранения. Сетевые платы. Прочие
Устройства IEEE1394	Устройства хранения. Принтеры. Сканеры и цифровые фотоаппараты. Сетевые устройства. Цифровые видеокамеры. Прочие
Устройства Secure Digital	Карточки памяти
Сеть	Соединение Ethernet. Беспроводное соединение (WiFi). Соединение Bluetooth. Соединение 1394 (FireWire). Инфракрасное соединение (IrDA)

Примеры настройки использования подключаемых съемных дисков

Локальное присвоение пользователям определенных съемных дисков

В данном разделе рассматривается пример локальной настройки системы защиты для разграничения доступа пользователей к устройствам, которые подключаются в качестве съемных дисков. В результате настройки пользователям будут предоставлены возможности подключать и использовать определенные устройства (для каждого пользователя — отдельный съемный диск или несколько дисков), к которым другие пользователи не будут иметь доступа.

1. Подключите устройство.

Примечание.

Подключение требуется, чтобы устройство появилось в списке устройств локальной политики безопасности. Если устройство до этого уже подключалось и сведения о нем присутствуют в списке устройств, подключать устройство не обязательно.

2. Вызовите оснастку для управления параметрами локальной политики безопасности компьютера (см. стр. [13](#)).

3. Перейдите к разделу "Параметры безопасности | Параметры Secret Net" и выберите папку "Устройства".

В правой части окна появится общий список устройств аппаратной конфигурации.

4. Выберите в списке нужное устройство, вызовите контекстное меню и выберите команду "Свойства".

На экране появится диалог для настройки параметров объекта.

5. Перейдите к группе параметров "Настройки".

6. Удалите отметку из поля "Наследовать настройки контроля от родительского объекта" (если отметка установлена).

После этого станут доступны параметры контроля устройства.

7. Отметьте режим контроля "Подключение устройства разрешено" и нажмите кнопку "Разрешения".

На экране появится диалог ОС Windows "Разрешения...".

8. Отредактируйте список учетных записей в верхней части диалога: добавьте учетную запись пользователя, которому будет разрешено использование устройства, и удалите ненужные элементы.

9. Укажите параметры доступа для элементов списка: включите разрешения на выполнение операций для учетной записи пользователя, которому будет разрешено использование устройства, и запреты для других элементов (если они присутствуют в списке).

10. Закройте диалоги с сохранением изменений и при необходимости повторите процедуру для других устройств.

Централизованное формирование списка используемых съемных дисков

Система защиты позволяет ограничить подключение устройств (в том числе подключаемых съемных дисков) и разрешить использование только того оборудования, которое указано администратором безопасности. Для этих целей могут применяться следующие методы:

- метод формирования списков устройств в локальных политиках безопасности на компьютерах (описан в разделе "Настройки по умолчанию" — см. стр. [51](#));
- метод централизованного формирования списка используемых устройств в групповых политиках безопасности доменов или организационных подразделений.

Если устройства преимущественно подключаются к одним и тем же компьютерам, для формирования списков устройств рекомендуется использовать средства локальных политик безопасности на этих компьютерах (первый метод). Для случаев, когда требуется составить единый список подключаемых устройств для всех компьютеров домена или организационного подразделения, можно использовать средства соответствующей групповой политики безопасности. Однако не следует помещать в такой список слишком много устройств (несколько сотен и более), так как это может привести к длительным задержкам при обновлении групповых политик на компьютерах.

Формирование списка подключаемых устройств в групповой политике осуществляется следующим образом:

1. Задайте политику контроля устройств в нужной групповой политике (политике безопасности домена или организационного подразделения). Описание процедуры задания политики контроля см. на стр. [56](#).
2. В список устройств групповой политики добавьте нужные устройства. Описание возможностей для добавления см. на стр. [57](#).
3. Для добавленных устройств включите режим контроля "Подключение устройства разрешено". В параметрах моделей и/или классов, к которым принадлежат добавленные устройства, включите режим контроля "Подключение устройства запрещено". Описание процедуры настройки политики контроля устройств см. на стр. [60](#).

События, регистрируемые в журнале Secret Net

Табл.2 События категории "Вход/выход"

Название	ID	Тип	Описание
Компьютер заблокирован системой защиты	1016	Аудит отказов	Блокировка компьютера была автоматически включена по одной из следующих причин: <ul style="list-style-type: none"> • нарушена аппаратная конфигурация компьютера; • нарушена целостность объектов контроля. Причина блокировки указана в поле "Описание"
Компьютер разблокирован	1017	Аудит успехов	Блокировка компьютера отключена администратором безопасности
Ошибка выполнения функционального контроля	1018	Аудит отказов	При загрузке компьютера обнаружены сбои в работе функциональных модулей системы защиты. Причины сбоев указаны в поле "Описание"
Успешное завершение функционального контроля	1019	Аудит успехов	Выполнена проверка работы функциональных модулей системы защиты. Сбои не обнаружены
Запрет входа пользователя	1201	Аудит отказов	Пользователю отказано во входе в систему. Причина запрета указывается в поле "Описание"
Вход пользователя в систему	1202	Аудит успехов	В систему успешно вошел пользователь. В поле "Описание" указываются: <ul style="list-style-type: none"> • имя пользователя; • тип сессии (локальная или терминальная); • идентификатор сессии; • режим входа (стандартный, смешанный или по идентификатору); • режим аутентификации при входе (стандартная или усиленная); • назначенный уровень допуска пользователя; • назначенный уровень конфиденциальности для сессии работы пользователя
Пользователь возобновил сеанс работы на компьютере	1203	Аудит успехов	Пользователь продолжил работу в текущем сеансе (ранее приостановленном). Например, разблокировал рабочую станцию или снова подключился к незавершенному сеансу терминальной сессии
Система инициировала блокировку сессии пользователя	1204	Информация	Блокировка сессии была автоматически включена по одной из следующих причин: <ul style="list-style-type: none"> • истек период неактивности сессии; • был изъят электронный идентификатор
Идентификатор не зарегистрирован	1206	Аудит отказов	Предъявленный персональный идентификатор (при входе пользователя в систему или при разблокировании компьютера) не сопоставлен ни с одним пользователем. В поле "Описание" указываются: <ul style="list-style-type: none"> • тип идентификатора (полный); • номер идентификатора
Пользователь приостановил сеанс работы на компьютере	1207	Аудит успехов	Пользователь прервал работу, не завершая сеанс. Событие регистрируется, например, при блокировке рабочей станции, при смене пользователя или при закрытии окна терминальной сессии без завершения сеанса. В поле "Описание" указывается: <ul style="list-style-type: none"> • имя пользователя; • идентификатор сессии

Название	ID	Тип	Описание
Завершение работы пользователя	1208	Аудит успехов	Сеанс работы пользователя в системе завершен. Имя пользователя, тип входа (локальный или терминальный) и идентификатор сессии указаны в поле "Описание"
Пароль пользователя не соответствует требованиям безопасности	1095	Предупреждения	Пользователю отказано в доступе к системе по причине несоответствия правилам парольной политики. В поле "Описание" указывается имя пользователя

Табл.3 События категории "Регистрация"

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

Табл.4 События категории "Контроль печати"

Название	ID	Тип	Описание
Печать документа	1286	Аудит успехов	Выполнена печать документа. В поле "Описание" указываются: <ul style="list-style-type: none"> • имя процесса, осуществляющего печать; • идентификатор процесса; • принтер, на котором производится печать; • идентификатор задания печати; • название документа; • категория конфиденциальности документа; • полный путь файла документа
Запрет прямого обращения к принтеру	1285	Аудит отказов	Пользователю отказано в печати документа посредством прямого обращения к порту принтера (например, из командной строки или с помощью DOS-программы). Причина запрета — включен режим контроля печати. В поле "Описание" указываются: <ul style="list-style-type: none"> • имя принтера или порта; • идентификатор процесса; • имя процесса

Название	ID	Тип	Описание
Начало печати документа	1036	Аудит успехов	Запущен процесс печати документа. В поле "Описание" указываются: <ul style="list-style-type: none"> имя процесса, осуществляющего печать (полный путь); идентификатор процесса; принтер, на котором производится печать; идентификатор задания печати; название документа; категория конфиденциальности документа; полный путь файла документа; краткое содержание документа (наименование, вид, код, шифр); общее количество экземпляров документа; номер первого экземпляра, печатаемого в данном задании; количество страниц для печати
Успешное завершение печати документа	1037	Аудит успехов	Печать документа успешно завершена. В поле "Описание" указываются: <ul style="list-style-type: none"> имя процесса, осуществляющего печать (полный путь); идентификатор процесса; идентификатор задания печати; количество фактически напечатанных экземпляров
Ошибка при печати документа	1038	Аудит отказов	Во время печати документа произошла ошибка. В поле "Описание" указываются: <ul style="list-style-type: none"> имя процесса, осуществляющего печать (полный путь); идентификатор процесса; идентификатор задания печати; описание ошибки; количество фактически напечатанных экземпляров (включая неполные)
Запрет печати документа	1082	Аудит отказов	Пользователю отказано в выводе документа на печать. В поле "Описание" указываются: <ul style="list-style-type: none"> имя процесса, осуществляющего печать (полный путь); идентификатор процесса; принтер, на котором производится печать; название документа; категория конфиденциальности документа; полный путь файла документа; описание причины запрета печати
Начало печати экземпляра документа	1039	Аудит успехов	Запущен процесс печати экземпляра документа. В поле "Описание" указываются: <ul style="list-style-type: none"> имя процесса, осуществляющего печать (полный путь); идентификатор процесса; идентификатор задания печати; номер экземпляра документа
Успешное завершение печати экземпляра документа	1280	Аудит успехов	Экземпляр документа успешно напечатан. В поле "Описание" указываются: <ul style="list-style-type: none"> имя процесса, осуществляющего печать (полный путь); идентификатор процесса; идентификатор задания печати; количество фактически отпечатанных страниц (включая дополнительные)

Название	ID	Тип	Описание
Ошибка при печати экземпляра документа	1281	Аудит отказов	Во время печати экземпляра документа произошла ошибка. В поле "Описание" указываются: <ul style="list-style-type: none"> имя процесса, осуществляющего печать (полный путь); идентификатор процесса; идентификатор задания печати; описание ошибки; количество фактически отпечатанных страниц (включая дополнительные)
Сохранение копии напечатанного документа	1283	Аудит успехов	Система отправляет копию файла напечатанного документа в хранилище. В поле "Описание" указываются: <ul style="list-style-type: none"> имя процесса, осуществляющего печать (полный путь); идентификатор процесса; принтер, на котором производится печать; идентификатор задания печати; название документа; категория конфиденциальности документа; полный путь файла документа; идентификатор копии в хранилище (папка, в которой находится файлы XPS-образа документа и задания. Имена файлов совпадают, расширения .xps и .xjb соответственно)

Табл.5 События категории "Полномочное управление доступом"

Название	ID	Тип	Описание
Изменение параметров конфиденциальности ресурса	1270	Аудит успехов	Изменены параметры конфиденциальности файла или каталога. В поле "Описание" указываются: <ul style="list-style-type: none"> имя процесса; идентификатор процесса (PID); имя процесса, выполнившего действие; имя ресурса (файла, каталога), для которого произведены изменения; новая категория конфиденциальности; новое значение признака наследования; старая категория конфиденциальности; старое значение признака наследования
Запрет изменения параметров конфиденциальности ресурса	1271	Аудит отказов	Пользователю отказано в изменении категории конфиденциальности файла или каталога (например, если пользователь не имеет соответствующей привилегии или файлу присваивается более высокая категория, чем у каталога). В поле "Описание" указываются: <ul style="list-style-type: none"> имя процесса; идентификатор процесса (PID); имя ресурса; текущие параметры конфиденциальности; запрошенные параметры конфиденциальности; причина запрета

Название	ID	Тип	Описание
Доступ к конфиденциальному ресурсу	1272	Аудит успехов	<p>Выполнено открытие конфиденциального файла. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • идентификатор процесса (PID); • действующее значение категории конфиденциальности ресурса; • источник категории конфиденциальности (файл/устройство); • режим работы подсистемы полномочного управления; • запрошенный доступ
Запрет доступа к конфиденциальному ресурсу	1273	Аудит отказов	<p>Выполнена попытка открытия конфиденциального файла. Из-за недостаточного уровня допуска к конфиденциальной информации пользователю отказано в открытии ресурса. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • идентификатор процесса (PID); • имя ресурса; • действующее значение категории конфиденциальности ресурса; • источник категории конфиденциальности (файл/устройство); • режим работы подсистемы полномочного управления; • запрошенный доступ
Вывод конфиденциальной информации на внешний носитель	1274	Аудит успехов	<p>Выполнено сохранение конфиденциального файла или каталога на внешний носитель при включенном режиме контроля потоков. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • идентификатор процесса (PID); • имя ресурса; • действующее значение категории конфиденциальности ресурса
Запрет вывода конфиденциальной информации на внешний носитель	1275	Аудит отказов	<p>Выполнена попытка сохранения конфиденциального файла или каталога на внешний носитель при включенном режиме контроля потоков. Из-за отсутствия соответствующей привилегии пользователю отказано в сохранении ресурса. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • идентификатор процесса (PID); • имя ресурса; • действующее значение категории конфиденциальности ресурса; • причина запрета
Перемещение конфиденциального ресурса	1276	Аудит успехов	<p>Выполнено перемещение конфиденциального файла или каталога. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • идентификатор процесса (PID); • новые параметры ресурса (имя, категория конфиденциальности, значение признака наследования); • предыдущие параметры ресурса (имя, категория конфиденциальности, значение признака наследования)

Название	ID	Тип	Описание
Запрет перемещения конфиденциального ресурса	1277	Аудит отказов	<p>Выполнена попытка перемещения конфиденциального файла или каталога. Из-за недостаточного уровня допуска к конфиденциальной информации пользователю отказано в перемещении ресурса.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • идентификатор процесса (PID); • имя ресурса; • категория конфиденциальности ресурса; • значение признака наследования; • запрошенное имя ресурса; • причина запрета
Удаление конфиденциального ресурса	1278	Аудит успехов	<p>Выполнено удаление конфиденциального файла или каталога.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • идентификатор процесса (PID); • имя ресурса; • значение категории конфиденциальности; • значение признака наследования
Конфликт категорий конфиденциальности	1279	Аудит отказов	<p>Выполнена попытка открытия конфиденциального файла или каталога. Из-за несовпадения значений категорий конфиденциальности доступ к ресурсу пользователю запрещен.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • идентификатор процесса (PID); • имя ресурса; • значение категории конфиденциальности; • описание конфликта; • значение категории конфликтующего объекта
Использование механизма исключений	1300	Предупреждения	<p>При работе в режиме контроля потоков приложением был использован механизм исключений для сохранения служебного ресурса (определенного при настройке механизма) с категорией конфиденциальности ниже, чем уровень сессии.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • идентификатор процесса (PID); • имя ресурса; • значение категории конфиденциальности; • уровень сессии пользователя

Табл.6 События категории "Замкнутая программная среда"

Название	ID	Тип	Описание
Запрет запуска программы	1050	Аудит отказов	<p>Произошла попытка запуска программы, которая не входит в список разрешенных для запуска программ, или нарушена целостность исполняемого файла программы. Пользователю отказано в запуске программы.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя программы; • имя процесса, выполнившего действие; • режим работы механизма замкнутой программной среды; • причины отказа

Название	ID	Тип	Описание
Запуск программы	1051	Аудит успехов	<p>Выполнен запуск программы, которая удовлетворяет заданным условиям механизма замкнутой программной среды — программа входит в список разрешенных для запуска программ и целостность исполняемого файла программы не нарушена.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя программы; • имя процесса, выполнившего действие; • режим работы механизма замкнутой программной среды
Запрет загрузки библиотеки	1052	Аудит отказов	<p>Произошла попытка загрузки динамической библиотеки (DLL), файл которой не входит в список разрешенных для запуска программ, или нарушена целостность файла библиотеки. Процессу отказано в загрузке библиотеки.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя библиотеки; • имя процесса, выполнившего действие; • режим работы механизма замкнутой программной среды; • причины отказа
Загрузка библиотеки	1053	Аудит успехов	<p>Выполнена загрузка динамической библиотеки (DLL), которая удовлетворяет заданным условиям механизма замкнутой программной среды — файл библиотеки входит в список разрешенных для запуска программ и его целостность не нарушена.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя файла библиотеки; • имя процесса, выполнившего действие; • режим работы механизма замкнутой программной среды
Исполнение скрипта	1054	Аудит успехов	<p>Разрешено выполнение сценария (последовательность исполняемых команд и/или действий в текстовом виде, скрипт), который удовлетворяет заданным условиям механизма замкнутой программной среды — сценарий зарегистрирован в БД КЦ-ЗПС, и его исполнение разрешено (сценарий включен в задание ЗПС).</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя файла сценария (если есть) или название сценария; • сведения о сценарии, хранящиеся в БД; • имя файла сценария, сохраненного в хранилище системы защиты; • имя процесса, выполнившего действие; • режим работы механизма замкнутой программной среды
Запрет исполнения неизвестного скрипта	1055	Аудит отказов	<p>Произошла попытка выполнения сценария (последовательность исполняемых команд и/или действий в текстовом виде, скрипт), который не зарегистрирован в БД КЦ-ЗПС. Процессу отказано в исполнении сценария.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя файла сценария (если есть) или название сценария; • имя файла сценария, сохраненного в хранилище системы защиты; • имя процесса, выполнившего действие; • режим работы механизма замкнутой программной среды; • причины отказа

Табл.7 События категории "Расширение групповой политики"

Название	ID	Тип	Описание
Групповые политики успешно применены	1060	Аудит успехов	Новые заданные параметры групповых политик вступили в силу
Ошибка применения групповых политик	1061	Предупреждения	При попытке применения параметров групповых политик произошла ошибка. Код ошибки указан в поле "Описание"
Предупреждение при применении групповых политик	1062	Предупреждения	<p>При попытке применения параметров групповых политик обнаружено несоответствие версий шаблона групповой политики безопасности и клиента системы защиты. Для устранения несоответствия требуется синхронизировать версии (в зависимости от ситуации обновить шаблон на контроллере домена или обновить ПО клиента).</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> код предупреждения; имя групповой политики

Табл.8 События категории "Служба репликации"

Название	ID	Тип	Описание
Ошибка создания контекста пользователя	1065	Предупреждения	<p>При входе пользователя в систему произошла ошибка формирования контекста пользователя для работы в системе защиты. В текущем сеансе работы пользователю предоставляются минимальные права или привилегии на работу в системе (в зависимости от того, при чтении каких данных произошла ошибка).</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> имя пользователя; раздел данных контекста, при получении которых произошла ошибка (параметры полномочного доступа, открытый ключ пользователя, привилегии пользователя); код ошибки

Табл.9 События категории "Контроль целостности"

Название	ID	Тип	Описание
Начало обработки задания на контроль целостности	1100	Аудит успехов	На компьютере началась проверка целостности ресурсов, входящих в задание на контроль целостности. Имя задания указано в поле "Описание"
Успешное завершение задания на контроль целостности	1101	Аудит успехов	На компьютере завершена проверка целостности ресурсов, входящих в задание на контроль целостности. Целостность всех проверенных ресурсов не нарушена. Имя задания указано в поле "Описание"

Название	ID	Тип	Описание
Обнаружено нарушение целостности при обработке задания	1102	Аудит отказов	<p>На компьютере завершена проверка целостности ресурсов, входящих в задание на контроль целостности. В процессе проверки обнаружено нарушение целостности одного или нескольких ресурсов, входящих в задание.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> имя задания; тип реакции на отказ при контроле целостности, заданный для задания (блокировка компьютера, восстановление ресурса, принятие нового значения объекта в качестве эталонного)
Успешная проверка целостности ресурса	1103	Аудит успехов	<p>При проверке целостности ресурса не обнаружено нарушений.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> тип ресурса (файл, каталог, ключ реестра и пр.); имя ресурса; имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); название алгоритма расчета контрольных сумм (CRC7, ЭЦП, хэш и пр.), если в качестве метода контроля используется проверка содержимого; имя связанной с заданием задачи, к которой относится ресурс; имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием; дополнительное описание процедуры проверки целостности (в случае необходимости). Например, параметры использованного эталонного значения для контроля целостности ресурса, если имеется несколько эталонов
Нарушение целостности ресурса	1104	Аудит отказов	<p>При проверке целостности ресурса обнаружено нарушение целостности.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> тип ресурса (файл, каталог, ключ реестра и пр.); имя ресурса; имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); название алгоритма расчета контрольных сумм (CRC7, ЭЦП, хэш и пр.), если в качестве метода контроля используется проверка содержимого; имя связанной с заданием задачи, к которой относится ресурс; имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием; дополнительное описание процедуры проверки целостности (в случае необходимости). Например, текущие и предыдущие параметры ресурса, когда это возможно отследить

Название	ID	Тип	Описание
Для ресурса отсутствует эталонное значение	1105	Аудит отказов	<p>Проверка целостности ресурса не была выполнена из-за отсутствия эталонного значения для контроля (например, если после формирования задания не были рассчитаны эталонные значения контролируемых параметров).</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> тип ресурса (файл, каталог, ключ реестра и пр.); имя ресурса; имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); название алгоритма расчета контрольных сумм (CRC7, ЭЦП, хэш и пр.), если в качестве метода контроля используется проверка содержимого; имя связанной с заданием задачи, к которой относится ресурс; имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием
Удаление устаревших эталонных значений	1106	Аудит успехов	<p>Системой автоматически удалены "устаревшие" эталонные значения для контроля целостности ресурса. Под устаревшими подразумеваются значения, имеющие более раннее время создания, чем то эталонное значение, с которым совпал результат проверки целостности ресурса.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> тип ресурса (файл, каталог, ключ реестра и пр.); имя ресурса; имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); название алгоритма расчета контрольных сумм (CRC7, ЭЦП, хэш и пр.), если в качестве метода контроля используется проверка содержимого; имя связанной с заданием задачи, к которой относится ресурс; имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием; время создания эталонного значения, с которым совпал полученный результат проверки целостности ресурса

Название	ID	Тип	Описание
Текущее значение ресурса принято в качестве эталонного	1107	Аудит успехов	<p>Полученное при контроле целостности значение контролируемого параметра ресурса сохранено в качестве эталонного значения. Событие происходит, если в параметрах задания, в состав которого входит ресурс, определена реакция принятия новых значений контролируемых параметров в качестве эталонных.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> тип ресурса (файл, каталог, ключ реестра и пр.); имя ресурса; имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); название алгоритма расчета контрольных сумм (CRC7, ЭЦП, хэш и пр.), если в качестве метода контроля используется проверка содержимого; имя связанной с заданием задачи, к которой относится ресурс; имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием
Ресурс восстановлен по эталонному значению	1108	Аудит успехов	<p>Ресурс, у которого обнаружено нарушение целостности, был восстановлен с использованием эталонного значения. Событие происходит при условии физической возможности операции восстановления (например, невозможно восстановить файл, если контроль целостности осуществляется методом проверки существования).</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> тип ресурса (файл, каталог, ключ реестра и пр.); имя ресурса; имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); название алгоритма расчета контрольных сумм (CRC7, ЭЦП, хэш и пр.), если в качестве метода контроля используется проверка содержимого; имя связанной с заданием задачи, к которой относится ресурс; имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием; дополнительное описание процедуры восстановления (в случае необходимости)

Название	ID	Тип	Описание
Ошибка при восстановлении ресурса по эталонному значению	1109	Ошибки	<p>При попытке восстановления ресурса с использованием эталонного значения произошла ошибка (например, файл занят другим процессом). В поле "Описание" указываются:</p> <ul style="list-style-type: none"> тип ресурса (файл, каталог, ключ реестра и пр.); имя ресурса; имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); название алгоритма расчета контрольных сумм (CRC7, ЭЦП, хэш и пр.), если в качестве метода контроля используется проверка содержимого; имя связанной с заданием задачи, к которой относится ресурс; имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием; дополнительное описание процедуры восстановления (в случае необходимости)
Ошибка при открытии базы данных контроля целостности	1110	Ошибки	<p>При попытке обращения к локальной базе данных контроля целостности произошла ошибка (например, если база данных повреждена). Место нахождения базы данных указано в поле "Описание"</p>
Ошибка при принятии текущего значения ресурса в качестве эталонного	1112	Ошибки	<p>При попытке принять полученное значение контролируемого параметра ресурса в качестве эталонного значения произошла ошибка (например, если ресурс отсутствует). Событие регистрируется при контроле целостности, если в параметрах задания, в состав которого входит ресурс, определена реакция принятия новых значений объектов в качестве эталонных. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> тип ресурса (файл, каталог, ключ реестра и пр.); имя ресурса; имя обрабатываемого задания на контроль целостности, в состав которого входит ресурс; название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); название алгоритма расчета контрольных сумм (CRC7, ЭЦП, хэш и пр.), если в качестве метода контроля используется проверка содержимого; имя связанной с заданием задачи, к которой относится ресурс; имя группы ресурсов, содержащей ресурс. Группа ресурсов может быть включена непосредственно в обрабатываемое задание либо может входить в структуру задачи, связанной с заданием; дополнительное описание процедуры проверки целостности (в случае необходимости)
Исправление ошибок в базе данных	1113	Предупреждения	<p>Обнаружены и автоматически исправлены ошибки в базе данных подсистемы контроля целостности и замкнутой программной среды (например, если обнаружены связи с отсутствующими объектами, эти связи удаляются). Местонахождение базы данных указано в поле "Описание"</p>

Название	ID	Тип	Описание
Установка задания КЦ на контроль	1150	Аудит успехов	В программе управления (в режиме работы с локальной БД) установлена связь между заданием на контроль целостности и субъектом (компьютером). Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: <ul style="list-style-type: none"> имя задания; параметры расписания выполнения задания
Снятие задания КЦ с контроля	1151	Аудит успехов	В программе управления (в режиме работы с локальной БД) удалена связь между заданием на контроль целостности и субъектом (компьютером). Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: <ul style="list-style-type: none"> имя задания; параметры расписания выполнения задания
Добавление учетной записи к заданию ЗПС	1152	Аудит успехов	В программе управления (в режиме работы с локальной БД) установлена связь между заданием замкнутой программной среды и субъектом (пользователем). Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: <ul style="list-style-type: none"> имя задания; имя учетной записи, с которой связано задание
Удаление учетной записи из задания ЗПС	1153	Аудит успехов	В программе управления (в режиме работы с локальной БД) удалена связь между заданием замкнутой программной среды и субъектом (пользователем). Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: <ul style="list-style-type: none"> имя задания; имя учетной записи, с которой было связано задание
Создание задания	1154	Аудит успехов	В программе управления (в режиме работы с локальной БД) создан объект "Задание". Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: <ul style="list-style-type: none"> имя задания; название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); название алгоритма расчета контрольных сумм (CRC7, ЭЦП, хэш и пр.), если в качестве метода контроля используется проверка содержимого; параметры расписания выполнения задания; тип реакции при успешном выполнении контроля целостности (включена или нет регистрация событий); тип реакции на отказ при контроле целостности (блокировка компьютера, восстановление ресурса и т. п.)
Удаление задания	1155	Аудит успехов	В программе управления (в режиме работы с локальной БД) удален объект "Задание". Событие регистрируется после сохранения модели данных программы. Имя задания указано в поле "Описание"

Название	ID	Тип	Описание
Изменение задания	1156	Аудит успехов	В программе управления (в режиме работы с локальной БД) изменены параметры объекта "Задание". Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: <ul style="list-style-type: none"> имя задания (то, которое было до изменения параметров); перечень измененных параметров; новое имя задания (если имя было изменено)
Создание задачи	1157	Аудит успехов	В программе управления (в режиме работы с локальной БД) создан объект "Задача". Событие регистрируется после сохранения модели данных программы. Имя задачи указано в поле "Описание"
Удаление задачи	1158	Аудит успехов	В программе управления (в режиме работы с локальной БД) удален объект "Задача". Событие регистрируется после сохранения модели данных программы. Имя задачи указано в поле "Описание"
Изменение задачи	1159	Аудит успехов	В программе управления (в режиме работы с локальной БД) изменены параметры объекта "Задача". Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: <ul style="list-style-type: none"> имя задачи (то, которое было до изменения параметров); перечень измененных параметров; новое имя задачи (если имя было изменено)
Создание группы ресурсов	1160	Аудит успехов	В программе управления (в режиме работы с локальной БД) создан объект "Группа ресурсов". Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: <ul style="list-style-type: none"> имя группы ресурсов; какие типы ресурсов могут включаться в группу (файлы/каталоги или объекты реестра)
Удаление группы ресурсов	1161	Аудит успехов	В программе управления (в режиме работы с локальной БД) удален объект "Группа ресурсов". Событие регистрируется после сохранения модели данных программы. Имя группы ресурсов указано в поле "Описание"
Изменение группы ресурсов	1162	Аудит успехов	В программе управления (в режиме работы с локальной БД) изменены параметры объекта "Группа ресурсов". Событие регистрируется после сохранения модели данных программы. В поле "Описание" указываются: <ul style="list-style-type: none"> имя группы ресурсов (то, которое было до изменения параметров); перечень измененных параметров; новое имя группы ресурсов (если имя было изменено)
Синхронизация локальной базы данных с центральной	1163	Аудит успехов	Выполнена синхронизация локальной и центральной базы данных контроля целостности и замкнутой программной среды (КЦ-ЗПС)
Ошибка синхронизации локальной базы данных с центральной	1164	Ошибки	При попытке синхронизации локальной и центральной базы данных КЦ-ЗПС произошла ошибка. Сведения об ошибке указаны в поле "Описание"

Название	ID	Тип	Описание
Ошибка при расчете эталона	1165	Ошибки	<p>При расчете эталонного значения ресурса во время синхронизации локальной и центральной баз данных КЦ-ЗПС произошла ошибка.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя ресурса; • название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); • название алгоритма расчета контрольных сумм (CRC7, ЭЦП, хэш и пр.), если в качестве метода контроля используется проверка содержимого; • дополнительное описание процедуры расчета (в случае необходимости)

Табл.10 События категории "ЦУ КЦ-ЗПС"

Название	ID	Тип	Описание
Установка задания КЦ на контроль	1210	Аудит успехов	<p>В программе управления (в режиме работы с центральной БД) установлена связь между заданием на контроль целостности и субъектом.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя задания; • тип субъекта (компьютер или группа, включающая компьютеры); • SID учетной записи субъекта; • параметры расписания выполнения задания
Снятие задания КЦ с контроля	1211	Аудит успехов	<p>В программе управления (в режиме работы с центральной БД) удалена связь между заданием на контроль целостности и субъектом.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя задания; • тип субъекта (компьютер или группа, включающая компьютеры); • SID учетной записи субъекта; • параметры расписания выполнения задания
Добавление учетной записи к заданию ЗПС	1212	Аудит успехов	<p>В программе управления (в режиме работы с центральной БД) установлена связь между заданием замкнутой программной среды и субъектом.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя задания; • тип субъекта (компьютер или группа, включающая компьютеры); • SID учетной записи субъекта
Удаление учетной записи из задания ЗПС	1213	Аудит успехов	<p>В программе управления (в режиме работы с центральной БД) удалена связь между заданием замкнутой программной среды и субъектом.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя задания; • тип субъекта (компьютер или группа, включающая компьютеры); • SID учетной записи субъекта

Название	ID	Тип	Описание
Создание задания	1214	Аудит успехов	В программе управления (в режиме работы с центральной БД) создан объект "Задание". В поле "Описание" указываются: <ul style="list-style-type: none"> имя задания; тип задания (тиражируемое/нетиражируемое); название метода контроля (проверка существования, проверка содержимого, проверка атрибутов и пр.); название алгоритма расчета контрольных сумм (CRC7, ЭЦП, хэш и пр.), если в качестве метода контроля используется проверка содержимого; параметры расписания выполнения задания; тип реакции при успешном выполнении контроля целостности (включена или нет регистрация событий); тип реакции на отказ при контроле целостности (блокировка компьютера, восстановление ресурса, принятие нового значения объекта в качестве эталонного)
Удаление задания	1215	Аудит успехов	В программе управления (в режиме работы с центральной БД) удален объект "Задание". Имя задания указано в поле "Описание"
Изменение задания	1216	Аудит успехов	В программе управления (в режиме работы с центральной БД) изменены параметры объекта "Задание". В поле "Описание" указываются: <ul style="list-style-type: none"> имя задания (то, которое было до изменения параметров); перечень измененных параметров; новое имя задания (если имя было изменено)
Создание задачи	1217	Аудит успехов	В программе управления (в режиме работы с центральной БД) создан объект "Задача". Имя задачи указано в поле "Описание"
Удаление задачи	1218	Аудит успехов	В программе управления (в режиме работы с центральной БД) удален объект "Задача". Имя задачи указано в поле "Описание"
Изменение задачи	1219	Аудит успехов	В программе управления (в режиме работы с центральной БД) изменены параметры объекта "Задача". В поле "Описание" указываются: <ul style="list-style-type: none"> имя задачи (то, которое было до изменения параметров); перечень измененных параметров; новое имя задачи (если имя было изменено)
Создание группы ресурсов	1220	Аудит успехов	В программе управления (в режиме работы с центральной БД) создан объект "Группа ресурсов". В поле "Описание" указываются: <ul style="list-style-type: none"> имя группы ресурсов; какие типы ресурсов могут включаться в группу (файлы/каталоги или объекты реестра)
Удаление группы ресурсов	1221	Аудит успехов	В программе управления (в режиме работы с центральной БД) удален объект "Группа ресурсов". Имя группы ресурсов указано в поле "Описание"

Название	ID	Тип	Описание
Изменение группы ресурсов	1222	Аудит успехов	В программе управления (в режиме работы с центральной БД) изменены параметры объекта "Группа ресурсов". В поле "Описание" указываются: <ul style="list-style-type: none"> имя группы ресурсов (то, которое было до изменения параметров); перечень измененных параметров; новое имя группы ресурсов (если имя было изменено)
Добавление субъекта	1223	Аудит успехов	В программе управления (в режиме работы с центральной БД) добавлен субъект управления. В поле "Описание" указываются: <ul style="list-style-type: none"> SID учетной записи субъекта; тип субъекта (компьютер или группа, включающая компьютеры); заданные параметры субъекта
Удаление субъекта	1224	Аудит успехов	В программе управления (в режиме работы с центральной БД) удален субъект управления. В поле "Описание" указываются: <ul style="list-style-type: none"> SID учетной записи субъекта; тип субъекта (компьютер или группа, включающая компьютеры)
Изменение субъекта	1225	Аудит успехов	В программе управления (в режиме работы с центральной БД) изменены параметры субъекта управления. В поле "Описание" указываются: <ul style="list-style-type: none"> SID учетной записи субъекта; тип субъекта (компьютер или группа, включающая компьютеры); перечень измененных параметров

Табл.11 События категории "Контроль конфигурации"

Название	ID	Тип	Описание
Успешное завершение контроля аппаратной конфигурации	1290	Аудит успехов	Завершена процедура контроля аппаратной конфигурации при загрузке компьютера. Состояние контролируемых устройств не изменилось. Новые устройства не обнаружены
Ошибка при контроле аппаратной конфигурации	1291	Аудит отказов	Завершена процедура контроля аппаратной конфигурации при загрузке компьютера. Текущая конфигурация не соответствует сохраненному списку устройств компьютера (т. е. обнаружены факты изменения состояния устройств или добавления новых)
Обнаружено новое устройство	1292	Аудит отказов	При контроле аппаратной конфигурации компьютера обнаружено новое подключенное устройство, которое относится к модели/классу/группе с установленным режимом контроля "Устройство постоянно подключено к компьютеру" или "Подключение устройства запрещено". В поле "Описание" указывается категория конфиденциальности устройства. Полная информация об устройстве сохраняется в разделе двоичных данных

Название	ID	Тип	Описание
Устройство удалено из системы	1293	Аудит отказов	При контроле аппаратной конфигурации не было найдено устройство, входящее в список устройств компьютера. В поле "Описание" указывается категория конфиденциальности устройства. Полная информация об устройстве сохраняется в разделе двоичных данных
Изменены параметры устройства	1294	Аудит отказов	При контроле аппаратной конфигурации при загрузке компьютера обнаружено изменение физического параметра устройства, установленного на контроль (например, объем памяти). В поле "Описание" указываются: <ul style="list-style-type: none"> • название измененного параметра; • текущее значение параметра; • предыдущее значение параметра. Полная информация об устройстве сохраняется в разделе двоичных данных
Утверждение аппаратной конфигурации компьютера	1131	Аудит успехов	Текущая аппаратная конфигурация компьютера утверждена администратором. С этого момента данная аппаратная конфигурация считается эталонной
Переход в спящий режим	1295	Аудит успехов	Изменен режим работы компьютера. Администратор системы оповещается о переходе компьютера в спящий режим
Выход из спящего режима	1296	Аудит успехов	Изменен режим работы компьютера. Администратор системы оповещается о включении нормального режима

Табл.12 События категории "Разграничение доступа к устройствам"

Название	ID	Тип	Описание
Подключение устройства	1134	Аудит успехов	На компьютере произошло подключение разрешенного устройства. В поле "Описание" указывается категория конфиденциальности устройства. Полная информация об устройстве сохраняется в разделе двоичных данных
Отключение устройства	1135	Аудит успехов	На компьютере произошло отключение разрешенного устройства. В поле "Описание" указываются: <ul style="list-style-type: none"> • категория конфиденциальности устройства; • причина отключения устройства. Полная информация об устройстве сохраняется в разделе двоичных данных
Запрет подключения устройства	1136	Аудит отказов	На компьютере произошла попытка подключения запрещенного устройства. В поле "Описание" указываются: <ul style="list-style-type: none"> • категория конфиденциальности устройства; • причина запрета подключения устройства. Полная информация об устройстве сохраняется в разделе двоичных данных
Несанкционированное отключение устройства	1137	Аудит отказов	На компьютере произошло отключение постоянно подключенного устройства. Категория конфиденциальности указывается в поле "Описание". Полная информация об устройстве сохраняется в разделе двоичных данных

Название	ID	Тип	Описание
Доступ к устройству	1138	Аудит успехов	Во время работы пользователя на компьютере было использовано устройство. Пользователь обладает разрешением на доступ к данному устройству. В поле "Описание" указываются: <ul style="list-style-type: none"> имя процесса, выполнившего обращение; идентификатор процесса (PID); описание запрошенного доступа; дополнительная информация (при обращении к диску — полный путь к объекту, к которому был осуществлен доступ). Полная информация об устройстве сохраняется в разделе двоичных данных
Запрет доступа к устройству	1139	Аудит отказов	Во время работы пользователя на компьютере произошла попытка использования устройства. Пользователь не обладает разрешением на доступ к данному устройству. В поле "Описание" указываются: <ul style="list-style-type: none"> имя процесса, выполнившего обращение; идентификатор процесса (PID); описание запрошенного доступа; описание разрешенного доступа (эффективные права); дополнительная информация (при обращении к диску — полный путь к объекту, к которому была осуществлена попытка доступа). Полная информация об устройстве сохраняется в разделе двоичных данных

Табл.13 События категории "Сетевые подключения"

Название	ID	Тип	Описание
Запрет сетевого подключения под другим именем	1242	Аудит отказов	Произошла попытка запуска команды или сетевого подключения с вводом учетных данных пользователя, который не выполнил интерактивный вход в систему. Действие заблокировано системой защиты. В поле "Описание" указываются: <ul style="list-style-type: none"> сведения о сетевом ресурсе; имя пользователя

Табл.14 События категории "Управление"

Название	ID	Тип	Описание
Добавлен пользователь	1140	Аудит успехов	Пользователь добавлен в локальную базу данных системы защиты. SID добавленного пользователя указывается в поле "Описание"
Удален пользователь	1141	Аудит успехов	Пользователь удален из локальной базы данных системы защиты. SID удаленного пользователя указывается в поле "Описание"
Изменены параметры пользователя	1142	Аудит успехов	Изменены параметры или привилегии пользователя. В поле "Описание" указываются: <ul style="list-style-type: none"> SID измененного пользователя; разделы параметров пользователя, в которых сделаны изменения (параметры полномочного доступа, привилегии пользователя, параметры электронных идентификаторов)

Название	ID	Тип	Описание
Изменен ключ пользователя	1143	Аудит успехов	Выполнена смена ключа пользователя. В поле "Описание" указываются: <ul style="list-style-type: none"> SID пользователя, у которого изменен ключ; инициатор смены ключа (администратор безопасности или сам пользователь); сведения о предыдущем ключе
Изменены параметры действующей политики безопасности	1144	Аудит успехов	Изменены параметры системы защиты в консоли локальной политики безопасности. В поле "Описание" указываются названия разделов, в которых сделаны изменения (настройки подсистемы контроля печати, настройки подсистемы полномочного управления доступом, привилегии пользователей и групп, настройки политики аудита и др.)
Удален ключ пользователя	1145	Аудит успехов	Ключ пользователя удален. В поле "Описание" указываются: <ul style="list-style-type: none"> SID пользователя; дата выдачи ключа
Включена защитная подсистема	1146	Аудит успехов	Включен механизм защиты системы Secret Net. В поле "Описание" указываются: <ul style="list-style-type: none"> название механизма; имя процесса, выполнившего действие
Отключена защитная подсистема	1147	Аудит успехов	Отключен механизм защиты системы Secret Net. В поле "Описание" указываются: <ul style="list-style-type: none"> название механизма; имя процесса, выполнившего действие
Установлена защита для диска	1148	Аудит успехов	Включен режим защиты для логического раздела локального диска. Сведения о логическом разделе указываются в поле "Описание"
Отключена защита для диска	1149	Аудит успехов	Отключен режим защиты для логического раздела локального диска. Сведения о логическом разделе указываются в поле "Описание"
Изменен пароль пользователя	1094	Аудит успехов	Выполнена смена пароля пользователя. В поле "Описание" указываются: <ul style="list-style-type: none"> SID пользователя, у которого изменен пароль; инициатор смены пароля (кем выполнена процедура)

Табл.15 События категории "ПАК "Соболь""¹

Название	ID	Тип	Описание
Соболь: вход пользователя	1170	Аудит успехов	Программно-аппаратным комплексом "Соболь" успешно выполнены идентификация и аутентификация пользователя. Вход пользователя в систему разрешен. В поле "Описание" указываются: <ul style="list-style-type: none"> номер предъявленного персонального электронного идентификатора; имя пользователя

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

Название	ID	Тип	Описание
Соболь: изменение режима работы	1172	Аудит успехов	<p>ПАК "Соболь" переведен пользователем в другой режим работы (автономный или сетевой). В автономном режиме управление работой ПАК "Соболь" осуществляется только средствами администрирования программно-аппаратного комплекса. При этом регистрация событий категории "ПАК "Соболь"" в журнале Secret Net прекращается. В сетевом режиме ПАК "Соболь" функционирует совместно с СЗИ Secret Net и часть функций управления передается средствам управления системы защиты.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> номер предъявленного персонального электронного идентификатора; имя пользователя; описание включенного режима работы
Соболь: очистка журнала	1173	Аудит успехов	<p>Пользователем выполнена очистка системного журнала ПАК "Соболь".</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> номер предъявленного персонального электронного идентификатора; имя пользователя
Соболь: ошибка синхронизации параметров	1174	Ошибки	<p>Обнаружена ошибка при обработке запроса, поступившего к ПАК "Соболь". Запрос не был обработан.</p> <p>Ошибка может быть вызвана тем, что запрос поступил от внешней программы, не относящейся к СЗИ Secret Net</p>
Соболь: смена аутентификатора	1176	Аудит успехов	<p>Выполнена смена аутентификатора пользователя.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> номер предъявленного персонального электронного идентификатора; имя пользователя
Соболь: запрет входа пользователя	1177	Аудит отказов	<p>Пользователю отказано во входе в систему.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> номер предъявленного персонального электронного идентификатора; имя пользователя; причина запрета (предъявлен незарегистрированный идентификатор, введен неправильный пароль, пользователь заблокирован)
Соболь: нарушена целостность ресурса	1178	Аудит отказов	<p>При проверке целостности контролируемого объекта средствами ПАК "Соболь" обнаружено несовпадение полученных и эталонных значений контрольных сумм или не найдены файлы шаблонов для контроля целостности.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> номер предъявленного персонального электронного идентификатора; имя пользователя; тип ресурса (сектор диска или файл); имя ресурса; дополнительные сведения
Соболь: синхронизация параметров	1179	Аудит успехов	<p>Обработан запрос, поступивший к ПАК "Соболь", или изменен список пользователей программно-аппаратного комплекса (добавлены или удалены пользователи). Сведения о выполненном действии указаны в поле "Описание"</p>

Название	ID	Тип	Описание
Соболь: смена пароля	1180	Аудит успехов	Пароль пользователя был изменен. В поле "Описание" указываются: <ul style="list-style-type: none"> номер персонального электронного идентификатора, принадлежащего пользователю, которому сменили пароль; имя пользователя, сменившего пароль; имя пользователя, пароль которого изменен
Соболь: подключение ПАК	1181	Аудит успехов	Средствами администрирования системы Secret Net включен режим совместной работы с ПАК "Соболь"
Соболь: ошибка подключения ПАК	1182	Ошибки	При попытке включения режима совместной работы ПАК "Соболь" и системы Secret Net произошла ошибка. Сведения об ошибке указаны в поле "Описание"
Соболь: отключение ПАК	1183	Аудит успехов	Средствами администрирования системы Secret Net отключен режим совместной работы с ПАК "Соболь"
Соболь: ошибка отключения ПАК	1184	Ошибки	При попытке отключения режима совместной работы ПАК "Соболь" и системы Secret Net произошла ошибка. Сведения об ошибке указаны в поле "Описание"
Соболь: ошибка КС в памяти идентификатора	1185	Ошибки	Обнаружена ошибка при проверке контрольной суммы содержимого персонального идентификатора (например, из-за неисправности идентификатора). В поле "Описание" указываются: <ul style="list-style-type: none"> номер предъявленного персонального электронного идентификатора; имя пользователя
Соболь: изменены параметры загрузочного диска	1186	Аудит успехов	На компьютере произошла смена основного загрузочного диска (например, если выполнена загрузка с внешнего носителя)
Соболь: не рассчитаны контрольные суммы	1187	Ошибки	Для контролируемых объектов не были рассчитаны эталонные значения контрольных сумм при настройке подсистемы контроля целостности. Если используется "мягкий" режим контроля целостности, загрузка компьютера разрешается, несмотря на это событие. В "жестком" режиме вход пользователя в систему будет заблокирован
Соболь: автоматический перерасчет контрольных сумм	1188	Аудит успехов	Выполнен расчет эталонных значений контрольных сумм для контролируемых объектов. Запуск процедуры инициирован по запросу, поступившему от СЗИ Secret Net
Соболь: ручной перерасчет контрольных сумм	1189	Аудит успехов	Выполнен расчет эталонных значений контрольных сумм для контролируемых объектов. Запуск процедуры инициирован по команде администратора ПАК "Соболь"

Табл.16 События категории "Взаимодействие с Trust Access"

Название	ID	Тип	Описание
Синхронизация учетной информации с TrustAccess	1192	Аудит успехов	Выполнена синхронизация учетных данных пользователя в БД TrustAccess. В поле "Описание" указываются: <ul style="list-style-type: none"> имя компьютера; имя домена; выполняемая операция; имя пользователя

Название	ID	Тип	Описание
Ошибка синхронизации учетной информации с TrustAccess	1193	Ошибки	<p>При попытке синхронизации учетных данных пользователя в БД TrustAccess произошла ошибка. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя компьютера; • имя домена; • выполняемая операция; • имя пользователя; • описание ошибки

Табл.17 События категории "Теневое копирование"

Название	ID	Тип	Описание
Начата запись на сменный диск	1260	Аудит успехов	<p>Начинается процесс записи информации на сменный диск. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • ID процесса; • имя файла; • имя файла в хранилище
Запись на сменный диск завершена	1261	Аудит успехов	<p>Запись информации на сменный диск закончена. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • ID процесса; • имя файла; • имя файла в хранилище
Ошибка записи на сменный диск	1262	Ошибки	<p>Обнаружена ошибка при записи информации на сменный диск. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • ID процесса; • имя файла; • имя файла в хранилище; • код ошибки
Запрет записи на сменный диск	1263	Аудит отказов	<p>Пользователю запрещена запись информации на сменный диск. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • ID процесса; • имя файла; • имя файла в хранилище; • причина запрета
Начата запись образа CD/DVD/BD	1264	Аудит успехов	<p>Записывается образ CD/DVD/BD. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • ID процесса; • имя образа в хранилище
Закончена запись образа CD/DVD/BD	1265	Аудит успехов	<p>Запись образа CD/DVD/BD завершена. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • ID процесса; • имя образа в хранилище
Ошибка записи образа CD/DVD/BD	1266	Ошибки	<p>При попытке записи образа CD/DVD/BD произошла ошибка. В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • ID процесса; • имя образа в хранилище; • код ошибки

Название	ID	Тип	Описание
Запрет записи образа CD/DVD/BD	1267	Аудит отказов	Пользователю запрещена запись образа CD/DVD/BD. В поле "Описание" указываются: <ul style="list-style-type: none"> • имя процесса; • ID процесса; • причина запрета

Табл.18 События категории "Контроль приложений"

Название	ID	Тип	Описание
Запуск процесса	1230	Аудит успехов	Произошел запуск процесса (исполняемого модуля). В поле "Описание" указываются: <ul style="list-style-type: none"> • имя процесса (исполняемого модуля); • ID процесса; • имя родительского процесса; • ID родительского процесса; • имя пользователя, под которым работает процесс; • идентификатор сессии пользователя (LUID), под которой работает процесс
Завершение процесса	1231	Аудит успехов	Завершена работа процесса (исполняемого модуля). В поле "Описание" указываются: <ul style="list-style-type: none"> • имя процесса (исполняемого модуля); • ID процесса; • имя пользователя, под которым работал процесс

Табл.19 События категории "Дискреционный доступ"

Название	ID	Тип	Описание
Доступ к файлу или каталогу	1310	Аудит успехов	Выполнен запрошенный доступ к файлу или каталогу на чтение, запись, исполнение или удаление. В поле "Описание" указываются: <ul style="list-style-type: none"> • имя процесса; • идентификатор процесса (PID); • имя ресурса; • запрошенный доступ
Запрет доступа к файлу или каталогу	1311	Аудит отказов	Выполнена попытка доступа к файлу или каталогу на чтение, запись, исполнение или удаление. Из-за отсутствия необходимых прав пользователю отказано в выполнении операции. В поле "Описание" указываются: <ul style="list-style-type: none"> • имя процесса; • идентификатор процесса (PID); • имя ресурса; • запрошенный доступ; • разрешенные права доступа к ресурсу для пользователя

Название	ID	Тип	Описание
Изменение прав доступа	1312	Аудит успехов	<p>Изменены права доступа для файла или каталога: режим наследования, разрешения и запреты, параметры аудита операций.</p> <p>В поле "Описание" указываются:</p> <ul style="list-style-type: none"> • имя процесса; • идентификатор процесса (PID); • имя ресурса; • новые значения прав доступа; • старые значения прав доступа

Табл.20 События категории "Общие события"

Название	ID	Тип	Описание
Событие	1000	Аудит успехов	Некоторое событие, зарегистрированное системой, которое означает успешное выполнение определенного действия. В поле "Описание" указывается информация о процессе, зарегистрировавшем событие, и другие необходимые данные
Несанкционированное действие	1001	Аудит отказов	Некоторое событие, зарегистрированное системой при возникновении на рабочей станции НСД, которое зафиксировано системой защиты, но не относится к какой-либо конкретной защитной подсистеме. В поле "Описание" указывается информация о процессе, зарегистрировавшем событие, и другие необходимые данные
Ошибка	1002	Ошибки	Некоторое событие, зарегистрированное системой, которое означает возникшие неполадки при выполнении определенного действия. В поле "Описание" указывается информация о процессе, зарегистрировавшем событие, и другие необходимые данные
Предупреждение	1003	Предупреждения	Некоторое событие, зарегистрированное системой, которое предупреждает о создавшейся угрозе для безопасности системы. В поле "Описание" указывается информация о процессе, зарегистрировавшем событие, и другие необходимые данные
Информационное событие	1004	Информация	Некоторое событие, зарегистрированное системой, которое содержит дополнительную информацию о функционировании системы защиты. В поле "Описание" указывается информация о процессе, зарегистрировавшем событие, и другие необходимые данные
Нарушение лицензионной политики	1005	Аудит отказов	Обнаружено несоответствие перечня используемых функций и текущего варианта применения системы Secret Net, определенного лицензией

Использование TCP-портов для сетевых соединений

Некоторые модули системы Secret Net используют определенные TCP-порты для сетевого взаимодействия. При установке клиентского ПО системы защиты на компьютере автоматически изменяются следующие параметры ОС Windows:

1. В список исключений или в список правил брандмауэра Windows добавляются элементы, разрешающие использование TCP-портов:
 - "Secret Net: Удаленная работа с идентификаторами" — разрешает использование порта 21326 для работы с электронными идентификаторами при терминальном доступе;
 - "Secret Net: Управление контролем целостности и ЗПС" — разрешает использование порта 21327 для оперативной синхронизации централизованно заданных заданий КЦ-ЗПС.
2. Разрешаются RPC-вызовы от неаутентифицированных клиентов. Для этого в ключе реестра HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC создается параметр RestrictRemoteClients с нулевым значением.
3. Разрешаются анонимные соединения с именованным каналом. Для этого в ключе HKLM\System\CurrentControlSet\Services\LanManServer\Parameters создается параметр NullSessionPipes со значениями SnIcheckSrv и SnHwSrv.

Перечисленные изменения достаточны для сетевого взаимодействия с использованием транспорта TCP. Также предусмотрена альтернативная возможность установки связи через именованные каналы — для этого в брандмауэре Windows необходимо вручную включить действие стандартных правил "Общий доступ к файлам и принтерам", разрешающих использование портов 139 и 445.

Необходимым условием установки соединения является разрешение использования портов 137 и 138 на защищаемых компьютерах. Данные порты открыты по умолчанию в операционной системе. В случае отказов в установке соединений проверьте состояние стандартных правил брандмауэра Windows, разрешающих использование указанных портов, и при необходимости включите их действие.

Устройства, контролирующие сетевой трафик между компьютерами, не должны блокировать использование перечисленных портов.

Рекомендации по настройке Secret Net на кластере

Кластерные технологии позволяют объединить группу компьютеров (узлов), независимо работающих под управлением своих ОС, в единый сервер. При настройке клиентов системы Secret Net, 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 необходимо установить на всех узлах кластера тождественные настройки доменных пользователей. В противном случае работа системы Secret Net 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 и их значения хранятся в специальных файлах-шаблонах. При развертывании системы Secret Net эти файлы-шаблоны помещаются в каталог %WINDIR%\SYSVOL контроллера домена. Наряду с другими параметрами в файле-шаблоне хранится информация о текущей установленной версии Secret Net.

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

При корректном обновлении Secret Net автоматически происходит преобразование файлов-шаблонов и запись номера новой версии. Если обновление Secret Net было выполнено не в полном объеме или не произошло преобразование файла шаблона, это может привести к ошибкам редактирования и применения групповых политик из-за несоответствия версий компонентов.

В случае несовпадения версии установленного клиентского ПО Secret Net и номера версии в файле шаблона возможны следующие ситуации:

- При попытке загрузки содержимого раздела "Параметры безопасности | Параметры Secret Net" в оснастке редактирования групповой политики появляются сообщения о несоответствии версий:
 - если номер версии в файле шаблона старый, а номер версии клиентского ПО новый — выводится запрос на преобразование шаблона к актуальной версии (то есть к версии клиентского ПО). В диалоге рекомендуется нажать кнопку "Да", чтобы преобразовать файл шаблона для соответствия текущей (новой) версии ПО. При отказе от преобразования (кнопка "Нет" в диалоге запроса) редактирование параметров Secret Net в групповой политике на данном компьютере будет невозможно;
 - если номер версии в файле шаблона новый, а номер версии клиентского ПО старый — в оснастке выводится сообщение об ошибке, и редактирование параметров на данном компьютере будет возможно только после обновления клиентского ПО Secret Net.
- При попытке применения на компьютере параметров групповых политик:
 - если номер версии в файле шаблона старый, а номер версии клиентского ПО новый — 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 регистрируется предупреждение о несовпадении версий файла шаблона и версии клиентского ПО. Файл шаблона остается без изменений;
 - если номер версии в файле шаблона новый, а номер версии клиентского ПО старый — групповая политика не применяется. В журнале регистрируется предупреждение о попытке применения более новой версии шаблона политики.

Аварийное снятие защиты локальных дисков

Для отключения режима защиты логических разделов предусмотрены штатные процедуры (см. стр. 149). В тех случаях, когда такие процедуры по каким-либо причинам не могут быть выполнены, можно использовать средства аварийного снятия защиты дисков:

- мастер аварийного восстановления;
- загрузочный диск аварийного восстановления.

Работа с мастером аварийного восстановления

Программа-мастер аварийного восстановления предоставляет следующие возможности:

- восстановление исходного состояния основной загрузочной записи на физическом диске;
- восстановление исходного состояния загрузочных секторов логических разделов, для которых установлен режим защиты;
- вызов мастера создания загрузочного диска аварийного восстановления.

Мастер аварийного восстановления может функционировать независимо от текущего состояния механизма защиты локальных дисков Secret Net. Для выполнения действий необходимо загрузить ключ, с использованием которого установлена защита дисков компьютера.



Предупреждение.

Программу-мастер аварийного восстановления рекомендуется использовать только в тех случаях, когда невозможно снять защиту дисков с помощью штатных процедур (см. стр. 149).

Для отключения защиты дисков:

1. В каталоге установки клиентского ПО Secret Net (по умолчанию \Program Files\Secret Net\Client\) запустите файл TblRescue.exe.
На экране появится стартовый диалог мастера аварийного восстановления.
2. Нажмите кнопку "Далее".
На экране появится диалог для выбора режима работы.
3. Оставьте отмеченным поле "снятие защиты с дисков этого компьютера" и нажмите кнопку "Далее".
На экране появится диалог для загрузки и проверки ключа.
4. Чтобы загрузить ключ, нажмите кнопку "Указать" и выберите нужный файл в стандартном диалоге открытия файла. Имя файла должно содержать расширение .RK.
После загрузки ключа в диалоге мастера появятся сведения о доступных операциях, которые можно выполнить с использованием данного ключа.
5. Нажмите кнопку "Далее >".
Программа выполнит перечисленные операции, после чего на экране появится завершающий диалог мастера.
6. Нажмите кнопку "Готово".

Для вызова мастера создания диска аварийного восстановления:

1. В каталоге установки клиентского ПО Secret Net (по умолчанию \Program Files\Secret Net\Client\) запустите файл TblRescue.exe.
На экране появится стартовый диалог мастера аварийного восстановления.
2. Нажмите кнопку "Далее".
На экране появится диалог для выбора режима работы.
3. Установите отметку в поле "создание загрузочного диска аварийного снятия защиты" и нажмите кнопку "Далее".
На экране появится диалог для выбора варианта загрузки ключа.

4. Выполните действия, описанные в процедуре создания загрузочного диска аварийного восстановления (см. стр. [149](#)).

Использование загрузочного диска аварийного восстановления

Механизм защиты локальных дисков модифицирует основную загрузочную запись на физическом диске, с которого выполняется загрузка операционной системы. Кроме того, если включен режим защиты для логического раздела со служебными файлами ОС, на этом разделе также модифицируется загрузочный сектор.

При невозможности раскодирования модифицированных данных загрузка ОС не осуществляется. В этом случае необходимо вернуть к первоначальному состоянию основную загрузочную запись физического диска и/или загрузочные секторы логических разделов. Для этого можно использовать специально созданный загрузочный диск аварийного восстановления. Процедура создания диска описана на стр. [149](#).



Внимание!

Для загрузки с диска аварийного восстановления в настройках BIOS компьютера должна быть включена функция загрузки с внешних носителей. Если загрузка с USB-флеш-накопителя не выполняется, включите в BIOS режим эмуляции Floppy или Forced FDD.

При загрузке с диска аварийного восстановления автоматически запускается программа, которая проверяет возможность восстановления дисков. Если найдены модифицированные диски, которые можно восстановить с помощью ключа на загрузочном диске, на экране появляются запросы на снятие защиты с логических разделов и восстановление основной загрузочной записи. Чтобы вернуть данные к первоначальному состоянию, нажмите в диалоге запроса кнопку "Да".

Восстановление системы после сбоев питания компьютера

В большинстве случаев внезапное отключение питания компьютера не приводит к потере работоспособности системы Secret Net при следующих запусках. Однако возможны ситуации, 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;
- программные модули системы Secret Net.

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, в список исключений из проверки антивирусом. Если описанные действия не приводят к устранению проблем, переустановите на компьютере ПО системы Secret Net (см. документ [2]). При дальнейших проявлениях нештатного поведения системы обратитесь в отдел технической поддержки компании "Код Безопасности".

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 7", 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 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 7".
3. Последовательно введите команды del *.chk, del *.log и del *.edb.
4. Введите команду esentutl /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 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. [161](#)). Импорт параметров из файла резервной копии позволяет существенно упростить процесс восстановления.

Сведения о настройке защищенного соединения со службами каталогов

В сетевом режиме функционирования системы Secret Net предусмотрен режим усиленной защиты доступа к хранилищу объектов централизованного управления Secret Net. В этом режиме сетевые обращения к службам каталогов Active Directory или AD LDS/ADAM, выполняемые компонентами системы Secret Net, осуществляются с использованием протоколов Secure Socket Layer/Transport Layer Security (SSL/TLS). Данные протоколы предусматривают проверку подлинности компьютера, на котором развернута служба каталогов (контроллер домена или сервер безопасности), и реализуют функции установки безопасного соединения с использованием сертификатов.

Для использования режима усиленной защиты в системе должна быть организована и настроена инфраструктура открытых ключей (PKI). Реализация PKI может обеспечиваться стандартными средствами ОС Windows или ПО сторонних производителей. Ниже в данном разделе приводятся общие сведения о порядке организации и настройки PKI с применением стандартных средств ОС.

Защита взаимодействия с Active Directory

Если хранилище объектов централизованного управления системы Secret Net размещается в БД доменных служб Active Directory, настройка PKI выполняется в следующем порядке:

1. В доверенном центре сертификации (Certification Authority, ЦС) запросите сертификат для контроллера домена. Для сертификата необходимо указать полное доменное имя контроллера домена и метод использования "Проверка подлинности сервера" (Server Authentication). Полученный сертификат сохраните в хранилище в контексте компьютера, раздел "Личное" (или "Личные").

Примечание.

Если в системе отсутствует ЦС, для организации защищенных соединений можно использовать самозаверенный сертификат, созданный на контроллере домена. Этот сертификат в дальнейшем применяется и как сертификат компьютера, и как сертификат ЦС.

2. На контроллере домена установите сертификат центра сертификации в качестве сертификата доверенного ЦС и скопируйте этот сертификат из пользовательского хранилища в хранилище в контексте компьютера. Копирование сертификата выполняется в оснастке "Сертификаты", которую следует загрузить в режиме управления сертификатами текущего пользователя и в режиме управления сертификатами компьютера (т. е. загружаются две оснастки "Сертификаты"). Сертификат ЦС копируется из раздела "Доверенные корневые центры сертификации" оснастки с сертификатами текущего пользователя в такой же раздел оснастки с сертификатами компьютера.
3. На компьютерах домена поместите сертификат центра сертификации в раздел "Доверенные корневые центры сертификации" хранилища в контексте компьютера. Распространение сертификата можно выполнить, например, с помощью групповых политик. Для этого используется файл с этим сертификатом (если файл отсутствует, его можно создать путем экспорта сертификата из хранилища). Файл с сертификатом импортируется в оснастку "Политика безопасности домена" в раздел "Параметры безопасности | Политики открытого ключа | Доверенные корневые центры сертификации".
4. По окончании настройки PKI включите режим усиленной защиты трафика на компьютерах:

- Чтобы включить режим для сервера безопасности, откройте конфигурационный файл ServerConfig.xml, который размещается в каталоге установки сервера безопасности. Найдите параметр UseSSLConnection и измените значение false на true. После сохранения файла перезагрузите компьютер.
- Чтобы включить режим для клиента, в Панели управления Windows вызовите диалоговое окно "Управление Secret Net 7". Перейдите к диалогу "Защитные механизмы Secret Net" и установите отметку в поле "шифровать управляющий сетевой трафик". После закрытия диалогового окна перезагрузите компьютер.

Защита взаимодействия с AD LDS/ADAM

При размещении хранилища объектов централизованного управления системы Secret Net вне Active Directory настройка PKI выполняется в следующем порядке:

1. В доверенном центре сертификации (Certification Authority, ЦС) запросите сертификат для сервера безопасности, который установлен с размещением хранилища объектов ЦУ вне AD. Для сертификата необходимо указать полное доменное имя компьютера сервера безопасности и метод использования "Проверка подлинности сервера" (Server Authentication). Полученный сертификат сохраните в хранилище в контексте компьютера, раздел "Личное" (или "Личные").

Примечание.

Если в системе отсутствует ЦС, для организации защищенных соединений можно использовать самозаверенный сертификат, созданный на сервере безопасности. Этот сертификат в дальнейшем применяется и как сертификат компьютера, и как сертификат ЦС.

2. Установите полученный сертификат в IIS. Для этого запустите диспетчер служб IIS (IIS Manager) и в зависимости от версии ОС выполните соответствующие действия:
 - если сервер безопасности установлен на компьютере под управлением ОС Windows Server 2012/2008 — в иерархическом списке раскройте раздел сайтов, вызовите контекстное меню элемента "Default Web Site" и выберите команду "Изменить привязки" (Edit Bindings). В появившемся списке привязок сайта вызовите диалог настройки для элемента с типом "https" и выберите полученный сертификат в списке SSL-сертификатов. После установки сертификата выполните перезапуск IIS с помощью соответствующей команды управления в контекстном меню элемента "Default Web Site";
 - если сервер безопасности установлен на компьютере под управлением ОС Windows Server 2003 — в иерархическом списке раскройте раздел сайтов и вызовите диалоговое окно настройки свойств для элемента "Default Web Site". В диалоговом окне перейдите на вкладку "Безопасность каталога" и в группе элементов "Безопасные подключения" нажмите кнопку "Сертификат" — произойдет запуск специального мастера, с помощью которого выполняется установка сертификата. После установки сертификата выполните перезапуск IIS с помощью соответствующей команды управления в контекстном меню элемента "Default Web Site".
3. Предоставьте необходимые разрешения для доступа к файлу ключа сертификата. Для этого в программе Проводник перейдите к каталогу по умолчанию, в котором хранятся ключи. Местоположение каталога в ОС Windows Server 2012: %ProgramData%\Microsoft\Crypto\RSA\MachineKeys. В других версиях ОС: %ALLUSERSPROFILE%\Application Data\Microsoft\Crypto\RSA\MachineKeys. В каталоге вызовите окно настройки свойств файла ключа сертификата (определить нужный файл в списке можно по дате и времени создания), перейдите на вкладку "Безопасность" и добавьте в список нужную учетную запись с разрешениями по умолчанию. Имя добавляемой учетной записи зависит от того, на каком компьютере установлен сервер безопасности:

- если сервер безопасности установлен на контроллере домена под управлением ОС Windows Server 2012 — учетная запись с именем SecretNetLDS;
 - если сервер безопасности установлен на контроллере домена под управлением другой ОС — учетная запись с именем SecretNetLDS\$;
 - если сервер безопасности установлен на любом другом компьютере — учетная запись с именем NETWORK SERVICE.
4. На компьютере сервера безопасности поместите сертификат сервера в раздел "Личное" (или "Личные") хранилищ в контексте экземпляров служб SecretNet и SecretNet-GC. Для этого загрузите оснастку "Сертификаты" в режиме управления сертификатами компьютера и в режиме управления сертификатами каждой службы (т. е. загружаются три оснастки). Выполните экспорт сертификата сервера вместе с закрытым ключом из раздела "Личное" (или "Личные") оснастки с сертификатами компьютера и затем импорт в разделы "ADAM_SecretNet\Личное" и "ADAM_SecretNet-GC\Личное" (или "ADAM_SecretNet\Личные" и "ADAM_SecretNet-GC\Личные") оснасток с сертификатами служб. После этого предоставьте разрешения для доступа к файлам ключей импортированных сертификатов (см. действие 3).

Примечание.

На компьютере под управлением ОС Windows Server 2008/2003 вместо процедур экспорта и импорта можно выполнить копирование сертификата вместе с закрытым ключом непосредственно в оснастке "Сертификаты". Сертификат копируется из раздела "Личное" (или "Личные") оснастки с сертификатами компьютера в разделы "ADAM_SecretNet\Личное" и "ADAM_SecretNet-GC\Личное" (или "ADAM_SecretNet\Личные" и "ADAM_SecretNet-GC\Личные") оснасток с сертификатами служб. После этого не требуется выполнять процедуру предоставления разрешений доступа к файлам ключей сертификатов.

5. На компьютерах, подчиненных серверу безопасности, поместите сертификат центра сертификации в раздел "Доверенные корневые центры сертификации" хранилища в контексте компьютера. Распространение сертификата можно выполнить, например, с помощью групповых политик. Для этого используется файл с этим сертификатом (если файл отсутствует, его можно создать путем экспорта сертификата из хранилища). Файл с сертификатом импортируется в оснастке групповой политики в раздел "Параметры безопасности | Политики открытого ключа | Доверенные корневые центры сертификации".
6. Если имеется еще один сервер безопасности, выполните вышеперечисленные действия применительно к этому серверу.
7. На каждом сервере безопасности выполните следующие действия:
- Загрузите программу управления сертификатами сервера безопасности (с помощью элемента "Сертификаты" в разделе основного меню "Код безопасности") и выполните синхронизацию сертификата, установленного в IIS, с сертификатом сервера безопасности. Для этого в диалоговом окне настройки перейдите на вкладку "Сервис" и нажмите кнопку "Синхронизировать".
 - Откройте конфигурационный файл ServerConfig.xml, который размещается в каталоге установки сервера безопасности. Найдите параметр UseSSLConnection и измените значение false на true. В параметре Name (расположен ниже) измените значение на полное доменное имя компьютера сервера безопасности. Сохраните изменения и перезагрузите компьютер.
8. Включите режим усиленной защиты трафика на компьютерах с установленным ПО клиента. Для этого в Панели управления Windows вызовите диалоговое окно "Управление Secret Net 7", перейдите к диалогу "Защитные механизмы Secret Net" и установите отметку в поле "шифровать управляющий сетевой трафик". После закрытия диалогового окна перезагрузите компьютер.

Терминологический справочник

А	
Администратор безопасности	Лицо или группа лиц, ответственных за обеспечение безопасности системы, реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты
Алгоритм контроля	Используемый алгоритм для проверки содержимого ресурса (например, файла) при контроле целостности по методу "Содержимое": CRC7, ЭЦП, хэш, имитовставка, полное совпадение или встроенная ЭЦП
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 пользователя
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 работы	Режим работы механизма системы Secret Net, 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
Интервал неактивности	Время, в течение которого не используются устройства ввода (мышь, клавиатура и т. п.)
К	

Категория объекта модели данных	В модели данных используются категории 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 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 механизмах контроля целостности и замкнутой программной среды — список объектов и описание связей между ними. Модель данных — это подробная инструкция для системы Secret Net, 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 в качестве персональных идентификаторов могут использоваться идентификаторы eToken, iKey, Rutoken, JaCarta и 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 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 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, то есть 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 7. Руководство администратора. Принципы построения	RU.88338853.501410.015 91 1
2. Средство защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление	RU.88338853.501410.015 91 2
3. Средство защиты информации Secret Net 7. Руководство администратора. Настройка механизмов защиты	RU.88338853.501410.015 91 3
4. Средство защиты информации Secret Net 7. Руководство администратора. Работа с программой оперативного управления	RU.88338853.501410.015 91 4
5. Средство защиты информации Secret Net 7. Руководство администратора. Локальная работа с журналами регистрации	RU.88338853.501410.015 91 5
6. Средство защиты информации Secret Net 7. Руководство пользователя	RU.88338853.501410.015 92