КОД БЕЗОПАСНОСТИ

Средство защиты информации

# Secret Net Studio

## Руководство администратора

Настройка и эксплуатация. Локальная защита

RU.88338853.501400.001 91 5




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

# Оглавление

**Список сокращений** ... **6**

**Введение** ... **7**
Локальная защита ... 7

**Настройка контроля устройств** ... **8**
Общие сведения о разграничении доступа к устройствам ... 8
Список устройств ... 8
Правила наследования параметров в списке устройств ... 9
Возможности управления ... 9
Особенности применения групповых политик со списками устройств ... 10
Начальные параметры использования устройств ... 11
Общий порядок настройки для использования только разрешенных устройств ... 11
Управление списком устройств ... 12
Загрузка списка устройств ... 12
Создание списка устройств в групповой политике ... 13
Добавление и удаление элементов списка устройств ... 14
Контроль подключения и изменения устройств ... 15
Задание и настройка политики контроля устройств ... 15
Утверждение конфигурации ... 16
Избирательное разграничение доступа к устройствам ... 16
Настройка прав доступа к устройствам ... 16
Настройка регистрации событий и аудита операций с устройствами ... 17
Настройка теневого копирования выводимых данных ... 18
Управление функцией теневого копирования для устройств ... 18
Выбор устройств для теневого копирования ... 18

**Настройка контроля печати** ... **20**
Общие сведения о разграничении доступа к принтерам ... 20
Список принтеров ... 20
Возможности управления ... 20
Начальные параметры использования принтеров ... 21
Общий порядок настройки для печати только на разрешенных принтерах ... 21
Управление списком принтеров ... 22
Загрузка списка принтеров ... 22
Создание списка принтеров в групповой политике ... 22
Добавление и удаление элементов в списке принтеров ... 23
Избирательное разграничение доступа к принтерам ... 23
Настройка прав пользователей для печати на принтерах ... 23
Настройка регистрации событий ... 24
Настройка теневого копирования выводимых данных ... 24
Управление функцией теневого копирования для принтеров ... 24
Выбор принтеров для теневого копирования ... 24
Настройка маркировки распечатываемых документов ... 25
Управление режимом маркировки ... 26
Программа редактирования маркеров ... 30

**Настройка замкнутой программной среды** ... **34**
Общие сведения о методах и средствах настройки ... 34
Модель данных ... 34
Объекты модели по умолчанию ... 35
Программа управления КЦ-ЗПС ... 36
Синхронизация центральной и локальной баз данных ... 37
Начальная настройка механизма ... 38
Подготовка к построению модели данных ... 38
Общий порядок настройки ... 39
Формирование новой модели данных ... 39
Добавление задач в модель данных ... 40
Добавление заданий и включение в них задач ... 42
Включение мягкого режима ЗПС и формирование заданий по журналу ... 43

Установка связей субъектов с заданиями ЗПС ... 45
Подготовка ресурсов для замкнутой программной среды ... 45
Включение и настройка изоляции процессов ... 47
Расчет эталонов ... 48
Предоставление привилегии при работе в ЗПС ... 51
Включение жесткого режима ЗПС ... 52
Сохранение и загрузка модели данных ... 53
Сохранение ... 53
Оповещение об изменениях ... 53
Настройка автоматического запуска синхронизации ... 53
Принудительный запуск полной синхронизации ... 56
Загрузка и восстановление модели данных ... 56
Экспорт ... 56
Импорт ... 58
Внесение изменений в модель данных ... 61
Изменение параметров объектов ... 61
Добавление объектов ... 64
Удаление объектов ... 73
Связи между объектами ... 74
Запрет использования локальных заданий ... 75
Поиск зависимых модулей ... 75
Замена переменных окружения ... 76
**Полномочное управление доступом ... 77**
Общие сведения о полномочном разграничении доступа ... 77
Категории конфиденциальности ресурсов ... 77
Уровни допуска и привилегии пользователей ... 78
Режим контроля потоков механизма полномочного управления доступом ... 79
Настройка полномочного разграничения доступа ... 80
Общий порядок настройки ... 80
Настройка категорий конфиденциальности ... 81
Назначение уровней допуска и привилегий пользователям ... 82
Присвоение категорий конфиденциальности ресурсам ... 83
Настройка регистрации событий ... 84
Настройка использования принтеров для печати документов ... 84
Дополнительная настройка для работы в режиме контроля потоков ... 84
Рекомендуемый порядок настройки ... 84
Программа настройки для режима контроля потоков ... 85
Выбор уровней конфиденциальности для сетевых интерфейсов ... 86
Включение и отключение режима контроля потоков ... 86
Порядок настройки совместного функционирования с прикладным ПО ... 87
Правила работы с конфиденциальными ресурсами ... 90
**Настройка защиты хранимых данных ... 94**
Дискреционное управление доступом к каталогам и файлам ... 94
Предоставление привилегии для изменения прав доступа к ресурсам ... 94
Назначение администраторов ресурсов ... 94
Настройка регистрации событий и аудита операций с ресурсами ... 94
Затирание удаляемой информации ... 95
Защита локальных дисков ... 96
Включение механизма защиты дисков ... 96
Включение и отключение защиты логических разделов ... 99
Отключение механизма защиты дисков ... 99
Шифрование данных в криптоконтейнерах ... 100
Предоставление привилегии для создания криптоконтейнеров ... 100
Настройка регистрации событий ... 100
Управление криптографическими ключами пользователей ... 100
**Особенности настройки для защиты терминальных подключений ... 104**
Использование идентификаторов в терминальных сессиях ... 104
Отключение предварительной аутентификации ... 104
Программные методы обработки идентификаторов ... 106
Ограничение использования локальных устройств и ресурсов ... 106

Управление перенаправлением буфера обмена ... 106
Управление перенаправлением локальных устройств терминального клиента ... 107
Управление перенаправлением принтеров ... 108
Защита конфиденциальной информации при терминальных подключениях ... 109
**Приложение** ... **110**
Список групп и классов для контроля устройств ... 110
Примеры настройки использования подключаемых съемных дисков ... 111
Локальное присвоение пользователям определенных съемных дисков ... 111
Централизованное формирование списка используемых съемных дисков ... 112
Резервное копирование БД КЦ-ЗПС с использованием командной строки ... 113
Общие сведения о программе настройки для режима контроля потоков ... 114
Автоматическая настройка ... 114
Настройка вручную ... 115
Аварийное снятие защиты локальных дисков ... 125
Работа с мастером аварийного восстановления ... 125
Использование загрузочного диска аварийного восстановления ... 126
**Документация** ... **127**

# Список сокращений

| | |
|---|---|
| **AD** | Active Directory |
| **BIOS** | Basic Input/Output System |
| **FAT** | File Allocation Table |
| **GPT** | GUID Partition Table |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **LFN** | Long File Name |
| **MBR** | Master Boot Record |
| **MMC** | Microsoft Management Console |
| **NTFS** | New Technology File System |
| **PCMCIA** | Personal Computer Memory Card International Association |
| **PIN** | Personal Identification Number |
| **PKI** | Public Key Infrastructure |
| **ReFS** | Resilient File System |
| **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 |
| **ОС** | Операционная система |
| **ПАК** | Программно-аппаратный комплекс |
| **ПО** | Программное обеспечение |
| **ЦБД** | Центральная база данных |

# Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio" RU.88338853.501400.001 (далее — Secret Net Studio, система защиты, изделие). В нем содержатся сведения, необходимые администраторам для настройки и управления следующими механизмами защиты:

- дискреционное управление доступом;
- затирание удаляемой информации;
- контроль подключения и изменения устройств;
- замкнутая программная среда;
- полномочное управление доступом;
- контроль печати;
- защита информации на локальных дисках;
- шифрование данных в криптоконтейнерах.

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

## Условные обозначения

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

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

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

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.

- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.

- Эта пиктограмма сопровождает информацию предостерегающего характера.

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

## Другие источники информации

**Сайт в интернете.** Вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

**Учебные курсы.** Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

## Локальная защита

К группе локальной защиты относятся подсистемы, реализующие применение следующих механизмов защиты:

- контроль устройств;
- контроль печати;
- замкнутая программная среда;
- полномочное управление доступом;
- дискреционное управление доступом к ресурсам файловой системы;
- затирание данных;
- защита информации на локальных дисках;
- шифрование данных в криптоконтейнерах.

# Глава 1
# Настройка контроля устройств

## Общие сведения о разграничении доступа к устройствам

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.

### 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.

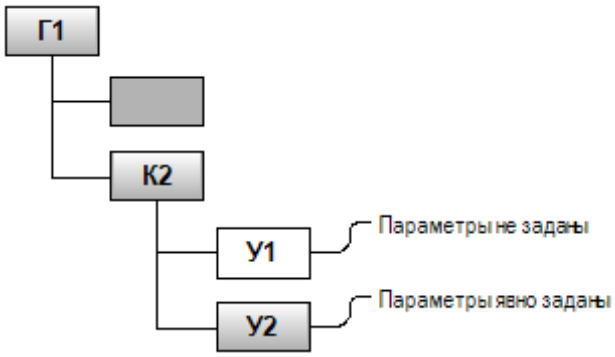
Полный список групп и классов устройств приведен в приложении на стр.**110**.

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

Для централизованного управления устройствами на компьютерах с клиентом в сетевом режиме функционирования 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.

## Правила наследования параметров в списке 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".

## Возможности управления

Управление устройствами осуществляется в программе управления Secret Net Studio, которая может устанавливаться как отдельный компонент "Secret Net Studio — Центр управления" — для работы в централизованном режиме или как составная часть клиента Secret Net Studio — для работы в локальном режиме. Сведения о работе с программой управления см. в документах [**3**], [**4**].

Предусмотрены следующие методы управления устройствами:

- управление с использованием только локальной политики каждого компьютера;
- управление с использованием групповых политик для элементов верхнего уровня (групп, классов и моделей устройств) и локальной политики каждого компьютера для конкретных устройств;
- управление с использованием групповых политик для всех элементов списка устройств.

Для компьютеров с установленным клиентом в автономном режиме функционирования недоступны возможности управления с использованием групповых политик.

Редактирование параметров групповых политик осуществляется на рабочем месте администратора безопасности в программе управления в централизованном режиме работы. Параметры локальной политики можно настраивать как в централизованном режиме работы, так и в локальном.

### Управление с использованием групповых политик для элементов верхнего уровня

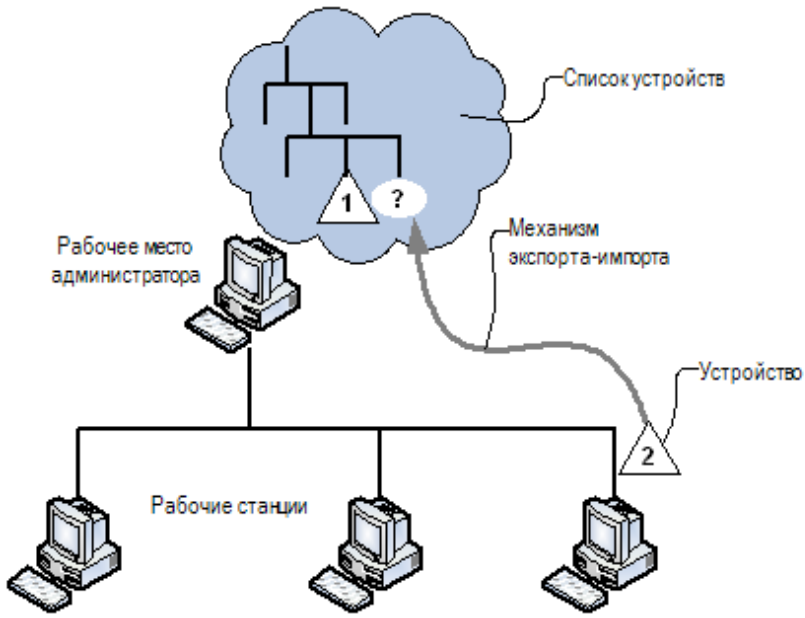
Данный вариант является предпочтительным, когда требуется обеспечить общие принципы контроля устройств на защищаемых компьютерах и нет необходимости централизованной настройки для отдельных устройств. Администратору безопасности достаточно настроить параметры использования для групп, классов и моделей устройств в нужных групповых политиках — например, в политике организационного подразделения. Параметры групповой политики будут применяться на компьютерах независимо от того, какие параметры заданы для этих элементов в локальной политике каждого компьютера. При этом настройка параметров использования конкретных устройств выполняется в локальной политике каждого компьютера.

### Управление с использованием групповых политик для всех элементов списка устройств

Если на нескольких компьютерах требуется применить одинаковые параметры использования конкретных устройств, можно выполнить их настройку в политике домена, организационного подразделения или сервера безопасности.

Устройства, параметры которых нужно настроить, должны быть добавлены в список групповой политики. В список устройств политики можно добавить сведения об устройствах, подключенных к какому-либо компьютеру с установленным клиентским ПО системы Secret Net Studio.

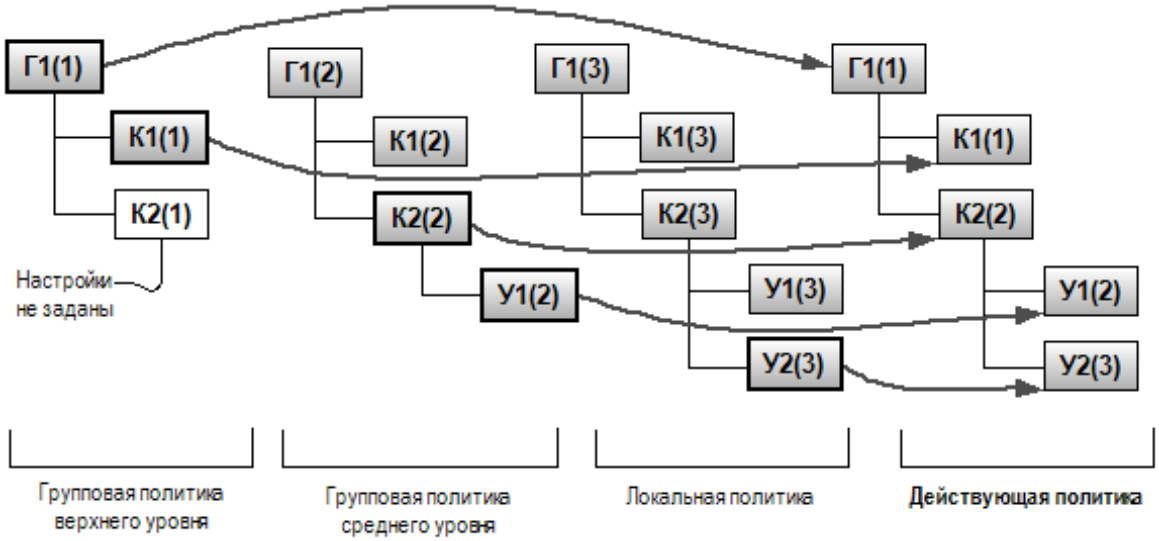
Описание предусмотренных возможностей для добавления устройств см. на стр.**14**.




## Особенности применения групповых политик со списками устройств

При входе пользователя в систему значения параметров контроля и доступа к устройствам устанавливаются в соответствии с действующей политикой. Действующая политика определяется при применении заданных параметров групповых политик с учетом их приоритета. Наименьший приоритет имеют параметры локальной политики. Они могут действовать только в случае отсутствия таких параметров в групповых политиках других уровней (в политиках доменов,

организационных подразделений и серверов безопасности). Наивысший приоритет имеет групповая политика корневого сервера безопасности. Частный пример применения параметров групповых политик для групп (Г), классов (К) и отдельных устройств (У) показан на рисунке:




## Начальные параметры использования устройств

После установки системы защиты в локальной политике заданы следующие правила использования устройств, 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".
- Теневое копирование отключено для всех устройств.
- 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.
- Регистрируются все события категорий "Контроль аппаратной конфигурации" и "Разграничение доступа к устройствам".
- Разрешается использование локальных устройств и ресурсов в терминальных сессиях.

## Общий порядок настройки для использования только разрешенных устройств

Чтобы обеспечить подключение и использование на компьютере только разрешенных устройств, выполните настройку в следующем порядке:

1. После установки системы защиты подключите к компьютеру все устройства, которые будут использоваться. Устройства будут зарегистрированы в системе

с разрешающими правами доступа и параметрами контроля от вышестоящих элементов списка (моделей, классов и групп).

2. Настройте параметры использования устройств для текущей аппаратной конфигурации:
   - политика контроля (см. стр.**15**);
   - разграничение доступа пользователей (см. стр.**16**);
   - теневое копирование (см. стр.**18**);
   - полномочное разграничение доступа (см. стр.**83** и стр.**86**).
3. Чтобы ограничить использование устройств в терминальных подключениях, включите запрет перенаправления (см. стр.**107**).
4. Отключите наследование параметров конкретных устройств от вышестоящих элементов списка и отключите разрешающие права для соответствующих моделей, классов и групп (см. стр.**15**). Например, разрешающие права можно отключить для группы "Устройства Secure Digital".

В результате пользователь сможет подключать и использовать только разрешенные устройства, а другие устройства будут запрещены. В дальнейшем можно удаленно разрешать использование новых устройств с помощью программы управления. Для этого по запросу пользователя администратор безопасности предлагает подключить нужное устройство (например USB-флеш-накопитель) 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. Администратор на своем рабочем месте в программе управления загружает параметры локальной политики соответствующего компьютера и выполняет необходимые действия для разрешения использования устройства.

**Примечание.**
Отдельные инструкции для настройки использования подключаемых съемных дисков приведены в приложении на стр.111.

# Управление списком устройств

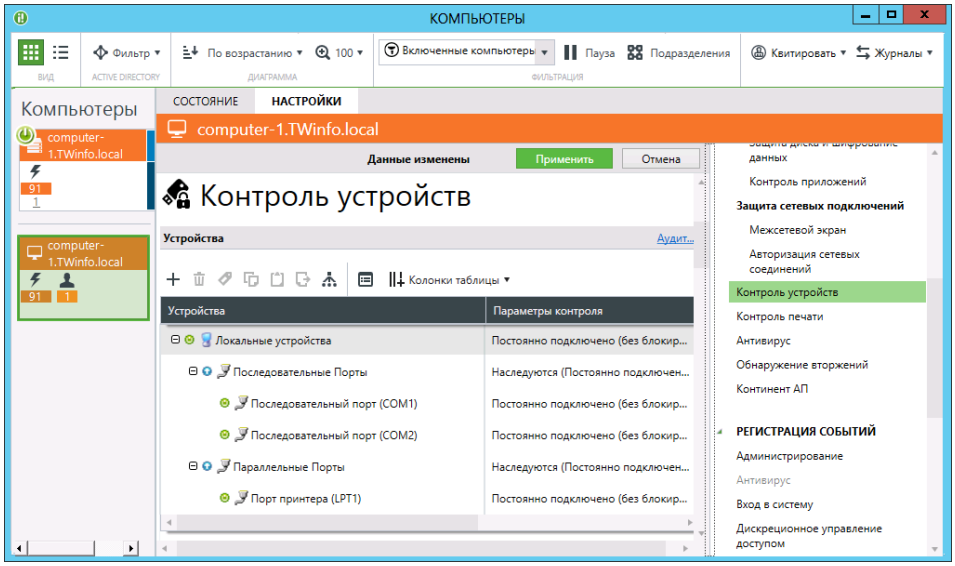
## Загрузка списка устройств

Ниже приводится описание процедуры загрузки списка устройств при работе с программой управления в централизованном режиме. Загрузка списка устройств локально выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для загрузки списка устройств:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль устройств / Устройства".

   Пример списка представлен на следующем рисунке.




В локальной политике в список устройств автоматически добавляются все обнаруженные устройства компьютера. Также в этот список помещаются сведения об устройствах, подключенных на терминальных клиентах данного компьютера во время терминальных сессий (при условии, что эти устройства разрешены для использования — см. стр. **107**). 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 Studio. 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 |

## Создание списка устройств в групповой политике

При установке системы Secret Net Studio список устройств формируется отдельно для каждого компьютера в локальной политике. Для централизованного управления списками устройств могут использоваться групповые политики доменов, организационных подразделений и серверов безопасности.

По умолчанию в групповых политиках отсутствуют списки устройств. Поэтому для реализации централизованного управления необходимо создать список устройств в нужной групповой политике. Настройка групповых политик осуществляется в программе управления (см. документ [**4**]).

## Добавление и удаление элементов списка устройств

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

Предусмотрены следующие способы добавления устройств:

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

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

### Использование мастера импорта устройств

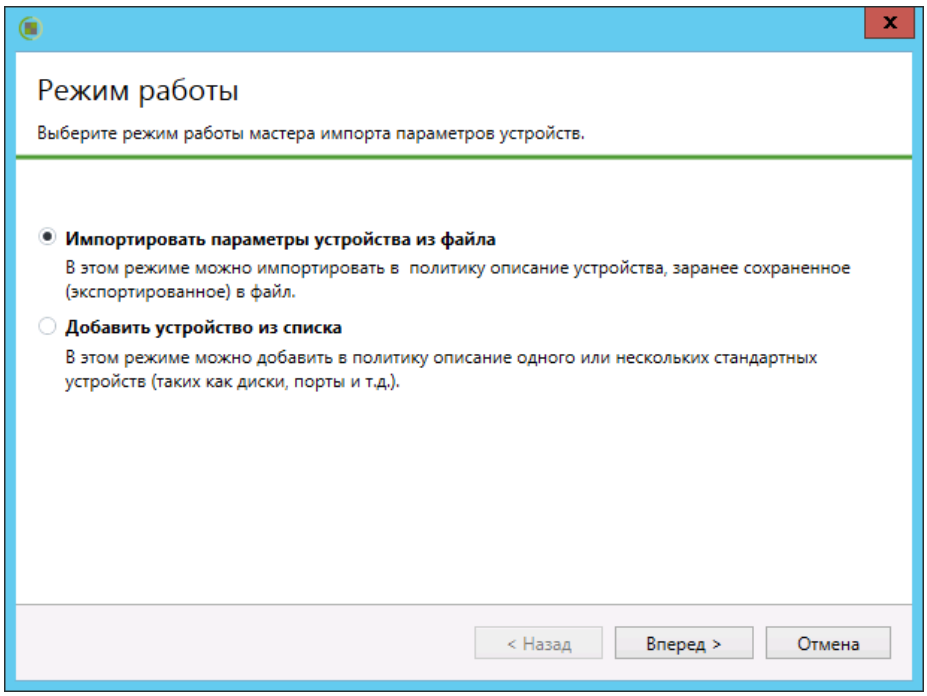
Мастер импорта предоставляет следующие возможности:

- импорт устройства из файла, в котором сохранены (экспортированы) сведения об устройстве;
- добавление стандартного устройства из предопределенного списка (например, порт ввода/вывода).

**Для импорта устройств в список групповой политики:**

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

   На экране появится стартовый диалог мастера импорта устройств.




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

### Экспорт сведений об устройствах из списка устройств

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

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

**Для экспорта сведений:**

1. Вызовите контекстное меню нужного устройства или модели и выберите команду "Экспорт".

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

### Использование буфера обмена для добавления устройств

Сведения об устройстве можно скопировать в буфер обмена из списка устройств другой политики.

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

### Удаление устройств

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

# Контроль подключения и изменения устройств

## 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.

По умолчанию на компьютерах действуют параметры контроля устройств, заданные в локальной политике. Для компьютеров с установленным клиентом в сетевом режиме функционирования можно задать политику контроля устройств в групповых политиках (см. стр.13).

**Для настройки политики контроля устройств:**

1. Загрузите список устройств (см. стр.12).
2. Выберите строку с нужным элементом списка (группа, класс, модель или устройство).
3. При необходимости введите дополнительные сведения об элементе в ячейке колонки "Комментарий". Для этого нажмите кнопку в правой части ячейки.

   **Примечание.**
   По умолчанию колонка "Комментарий" не отображается. Для включения отображения нажмите кнопку "Колонки таблицы", которая расположена над списком устройств.
   Дополнительные сведения, указанные для устройства, сохраняются в журнале при регистрации событий, связанных с этим устройством.
4. Укажите нужные параметры в ячейке колонки "Параметры контроля". Для этого нажмите кнопку в правой части ячейки. Если для данного объекта требуется отключить наследование параметров от вышестоящего объекта и явно задать 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 регистрируется событие тревоги как попытка несанкционированного доступа, и система ожидает утверждение изменений аппаратной конфигурации администратором безопасности.<br>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". Разблокировать компьютер сможет 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.<br>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 тревоги.<br>Параметр присутствует только для тех устройств, для которых отслеживается процесс подключения и можно запретить использование |

5. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

### 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 тревоги. 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 изменений аппаратной конфигурации выполняется в программе управления. Описание процедуры см. в документе [**4**].

## Избирательное разграничение доступа к устройствам

При настройке разграничения доступа пользователей к устройствам выполняются действия:

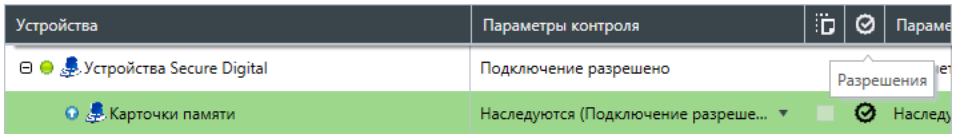
1. Настройка прав доступа пользователей к устройствам.
2. Настройка регистрации событий и аудита операций с устройствами.

### Настройка прав доступа к устройствам

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

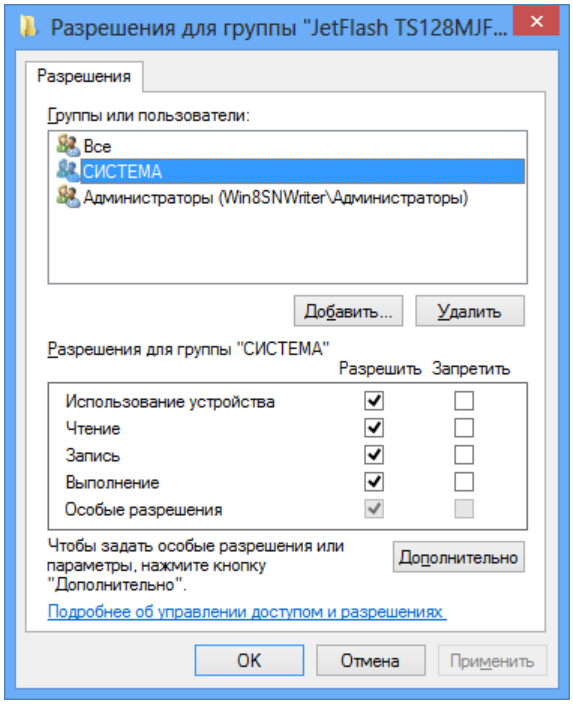
**Для настройки прав доступа к устройствам:**

1. Загрузите список устройств (см. стр.**12**).
2. Выберите строку с нужным элементом списка (класс или устройство).
3. Подведите указатель к ячейке колонки "Разрешения" и нажмите левую кнопку мыши.




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).




4. При необходимости отредактируйте список учетных записей в верхней части диалога.
5. 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.
6. После закрытия диалога "Разрешения..." нажмите кнопку "Применить" в верхней части вкладки "Настройки".

## 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. Настройка выполняется в программе управления. События, для которых можно включить или отключить регистрацию, представлены на вкладке "Настройки" панели свойств объектов в разделе "Регистрация событий", группа "Контроль устройств". Переход к параметрам регистрации можно выполнить из соответствующей группы параметров в разделе "Политики" (см. стр. 12) — для этого используйте ссылку "Аудит" в правой части заголовка группы "Настройки" или группы "Устройства".

### Настройка аудита успехов и отказов

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

**Для настройки аудита:**

1. Загрузите список устройств (см. стр. 12).

2. Выберите строку с нужным элементом списка (класс или устройство).
3. Подведите указатель к ячейке колонки "Разрешения" и нажмите левую кнопку мыши.

   На экране появится диалог ОС Windows "Разрешения...".
4. Нажмите кнопку "Дополнительно".

   На экране появится диалоговое окно настройки дополнительных параметров.
5. Перейдите к диалогу "Аудит" и настройте параметры аудита ОС Windows.
6. После закрытия диалога "Разрешения..." нажмите кнопку "Применить" в верхней части вкладки "Настройки".

# Настройка теневого копирования выводимых данных

## Управление функцией теневого копирования для устройств

Функцию теневого копирования можно отключить для всех устройств, подключаемых к системе в качестве дисков. Если функция теневого копирования включена, будут действовать заданные параметры для устройств.

Ниже приводится описание процедуры централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для общего управления функцией теневого копирования:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль устройств / Настройки".
3. Для параметра "Теневое копирование" укажите нужное значение:
   - "Отключено для всех устройств" — теневое копирование при записи информации на устройства не выполняется;
   - "Определяется настройками устройства" — теневое копирование выполняется для устройств с включенным режимом теневого копирования .
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

## Выбор устройств 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.

**Для управления режимом сохранения копий в списке устройств:**

1. Загрузите список устройств (см. стр.**12**).
2. Выберите строку с нужным элементом списка (класс или устройство).
3. Измените нужным образом состояние выключателя в ячейке колонки "Теневое копирование":
   - установите отметку — чтобы включить режим сохранения копий;
   - удалите отметку — если нужно отключить режим.


4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

# Глава 2
# Настройка контроля печати

## Общие сведения о разграничении доступа к принтерам

### 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 Studio. Этот список представлен в локальной политике и хранится в локальной базе данных системы Secret Net Studio.

Для централизованного управления принтерами на компьютерах с клиентом в сетевом режиме функционирования можно создать список принтеров в групповой политике.

### Возможности управления

Управление принтерами осуществляется в программе управления Secret Net Studio, которая может устанавливаться как отдельный компонент "Secret Net Studio — Центр управления" — для работы в централизованном режиме или как составная часть клиента Secret Net Studio — для работы в локальном режиме. Сведения о работе с программой управления см. в документах [**3**], [**4**].

Предусмотрены следующие методы управления принтерами:

- управление с использованием только локальной политики каждого компьютера;
- управление с использованием групповых политик для общих параметров по умолчанию и локальной политики каждого компьютера для конкретных принтеров;
- управление с использованием групповых политик для общих параметров по умолчанию и для конкретных принтеров.

Для компьютеров с установленным клиентом в автономном режиме функционирования недоступны возможности управления с использованием групповых политик.

Редактирование параметров групповых политик осуществляется на рабочем месте администратора безопасности в программе управления в централизованном режиме работы. Параметры локальной политики можно настраивать как в централизованном режиме работы, так и в локальном.

#### Управление с использованием групповых политик для общих параметров по умолчанию

Данный вариант является предпочтительным, когда требуется обеспечить общие принципы контроля принтеров на защищаемых компьютерах и нет необходимости централизованной настройки для отдельных устройств. Администратору безопасности достаточно настроить параметры для элемента "Настройки по умолчанию" в нужных групповых политиках — например, в политике организационного подразделения. Параметры групповой политики будут применяться на компьютерах независимо от того, какие параметры заданы для этого элемента в локальной политике каждого компьютера. При этом

настройка параметров использования конкретных принтеров выполняется в локальной политике каждого компьютера.

### Управление с использованием групповых политик для общих параметров по умолчанию и для конкретных принтеров

Если на нескольких компьютерах требуется применить одинаковые параметры использования конкретных принтеров, можно выполнить их настройку в политике домена, организационного подразделения или сервера безопасности.

Для настройки параметров принтера его необходимо включить в список принтеров групповой политики. В список принтеров можно добавить любой доступный принтер.

Описание предусмотренных возможностей для добавления принтеров см. на стр.**23**.

## Начальные параметры использования принтеров

После установки системы защиты в локальной политике по умолчанию заданы следующие правила использования принтеров, которые распространяются на всех пользователей компьютера:

- К принтерам предоставлен доступ стандартным группам пользователей: "Система", "Все" и "Все пакеты приложений".
- Теневое копирование отключено.
- Разрешается печать документов любой категории конфиденциальности.
- Разрешается использование локальных принтеров в терминальных сессиях.

## Общий порядок настройки для печати только на разрешенных принтерах

Чтобы обеспечить возможность печати только на принтерах, разрешенных к использованию на компьютере, выполните настройку в следующем порядке:

1. После установки системы защиты откройте список принтеров операционной системы и проверьте наличие всех принтеров, которые планируется использовать. При отсутствии нужных принтеров выполните процедуры их установки (добавления в список ОС) в соответствии с рекомендациями производителя.

   **Примечание.**
   Необходимо 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 принтера (добавления в список ОС) для каждого способа подключения. Этим будет обеспечена корректная идентификация таких принтеров системой защиты.

2. Добавьте принтеры в список групповой политики (см. стр.**23**).
3. Настройте параметры использования принтеров:
   - разграничение доступа пользователей (см. стр.**23**);
   - теневое копирование (см. стр.**24**);
   - полномочное разграничение доступа (см. стр.**84**).
4. Чтобы ограничить использование принтеров в терминальных подключениях, включите запрет перенаправления (см. стр.**108**).
5. В списке принтеров для элемента "Настройки по умолчанию" установите запрет печати для всех пользователей и включите ограничение печати документов всех категорий конфиденциальности.

В результате пользователь сможет отправлять документы на печать только на разрешенные устройства, а другие принтеры будут недоступны для использования. 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.

# Управление списком принтеров

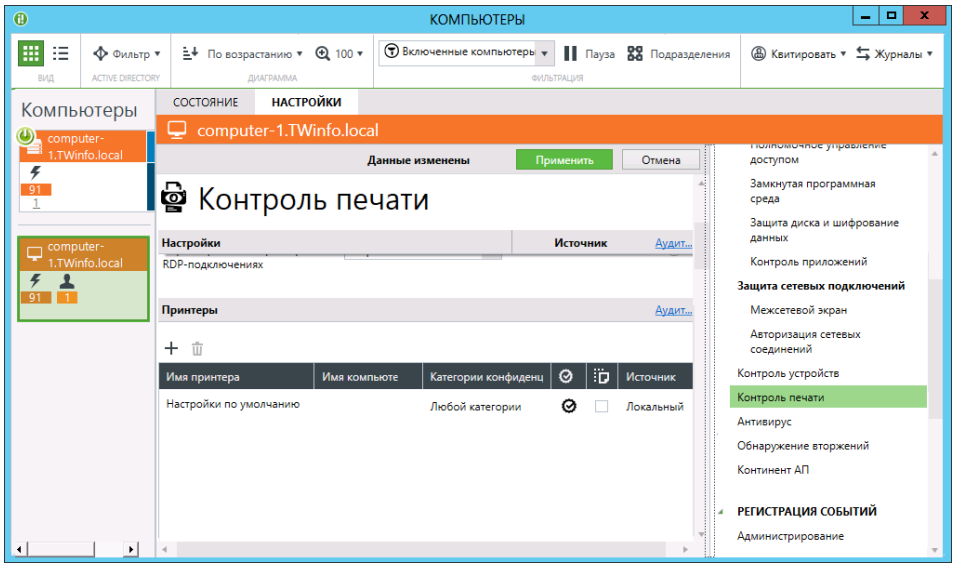
## Загрузка списка принтеров

Ниже приводится описание процедуры загрузки списка принтеров при работе с программой управления в централизованном режиме. Загрузка списка принтеров локально выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для загрузки списка принтеров:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль печати / Принтеры".

   Пример списка представлен на следующем рисунке.




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".

## Создание списка принтеров в групповой политике

Для централизованного управления параметрами принтеров могут использоваться групповые политики доменов, организационных подразделений и серверов безопасности.

По умолчанию в групповых политиках отсутствуют списки принтеров. Поэтому для реализации централизованного управления необходимо создать список принтеров в нужной групповой политике. Настройка групповых политик осуществляется в программе управления (см. документ [**4**]).

## Добавление и удаление элементов в списке принтеров

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

### Использование мастера добавления принтеров

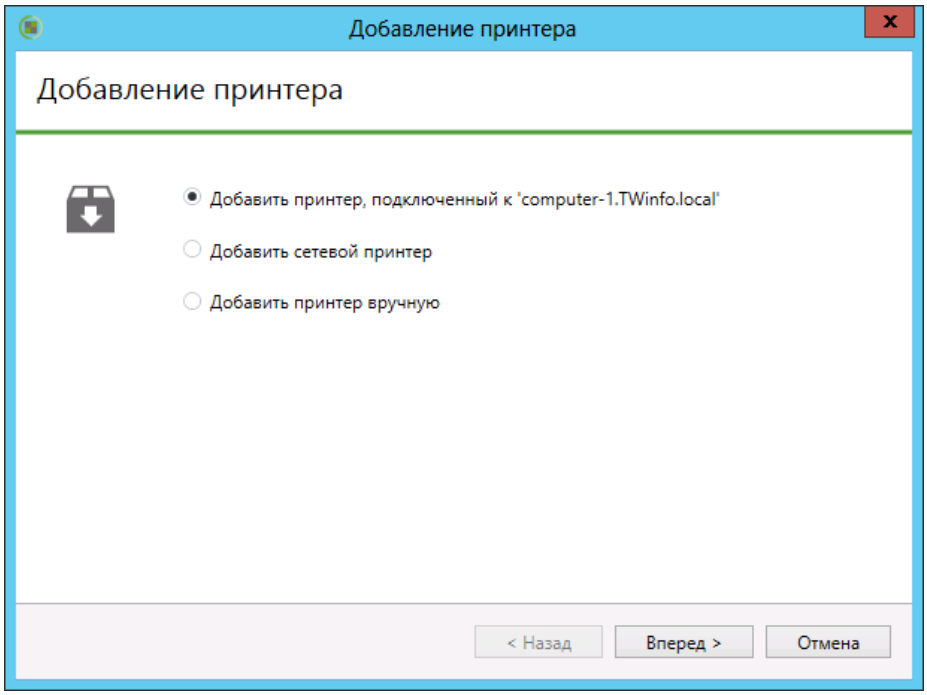
Мастер добавления предоставляет следующие возможности:

- добавление принтера, подключенного к выбранному компьютеру;
- добавление сетевого принтера;
- добавление принтера вручную.

**Для добавления принтера в список групповой политики:**

1. Вызовите контекстное меню любого элемента в списке принтеров и выберите команду "Добавить принтер".

   На экране появится стартовый диалог мастера добавления принтеров.




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

### Удаление принтеров

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

# Избирательное разграничение доступа к принтерам

При настройке разграничения доступа к принтерам выполняются действия:

1. Настройка прав пользователей для печати на принтерах.
2. Настройка регистрации событий.

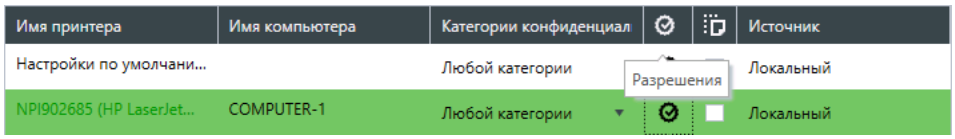
## Настройка прав пользователей для печати на принтерах

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

**Для настройки прав пользователей для печати:**

1. Загрузите список принтеров (см. стр.**20**).

2. Выберите строку с нужным элементом списка.
3. Подведите указатель к ячейке колонки "Разрешения" и нажмите левую кнопку мыши.




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

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

### Настройка регистрации событий

Для отслеживания произошедших событий, связанных с работой механизма контроля печати, необходимо выполнить настройку регистрации событий. Настройка выполняется в программе управления. События, для которых можно включить или отключить регистрацию, представлены на вкладке "Настройки" панели свойств объектов в разделе "Регистрация событий", группа "Контроль печати". Переход к параметрам регистрации можно выполнить из соответствующей группы параметров в разделе "Политики" (см. стр. **22**) — для этого используйте ссылку "Аудит" в правой части заголовка группы "Настройки" или группы "Принтеры".

## Настройка теневого копирования выводимых данных

### Управление функцией теневого копирования для принтеров

Функцию теневого копирования можно отключить для всех принтеров. Если функция теневого копирования включена, при печати документов будут действовать параметры, заданные для принтеров.

Ниже приводится описание процедуры централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для общего управления функцией теневого копирования:**

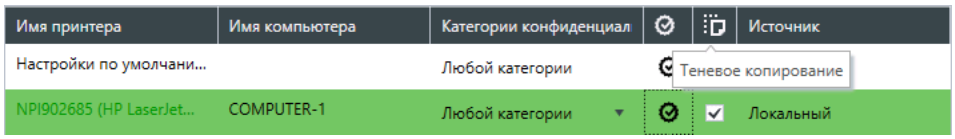
1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль печати / Настройки".
3. Для параметра "Теневое копирование" укажите нужное значение:
   - "Отключено для всех принтеров" — теневое копирование при выводе на печать не выполняется;
   - "Определяется настройками принтера" — теневое копирование выполняется для принтеров с включенным режимом теневого копирования .
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

### Выбор принтеров для теневого копирования

Управлять режимом сохранения копий можно для конкретных принтеров или для элемента "Настройки по умолчанию" в списке принтеров.

**Для управления режимом сохранения копий в списке принтеров:**

1. Загрузите список принтеров (см. стр.**20**).
2. Выберите строку с нужным элементом списка.
3. Измените нужным образом состояние выключателя в ячейке колонки "Теневое копирование":
   - установите отметку — чтобы включить режим сохранения копий;
   - удалите отметку — если нужно отключить режим.

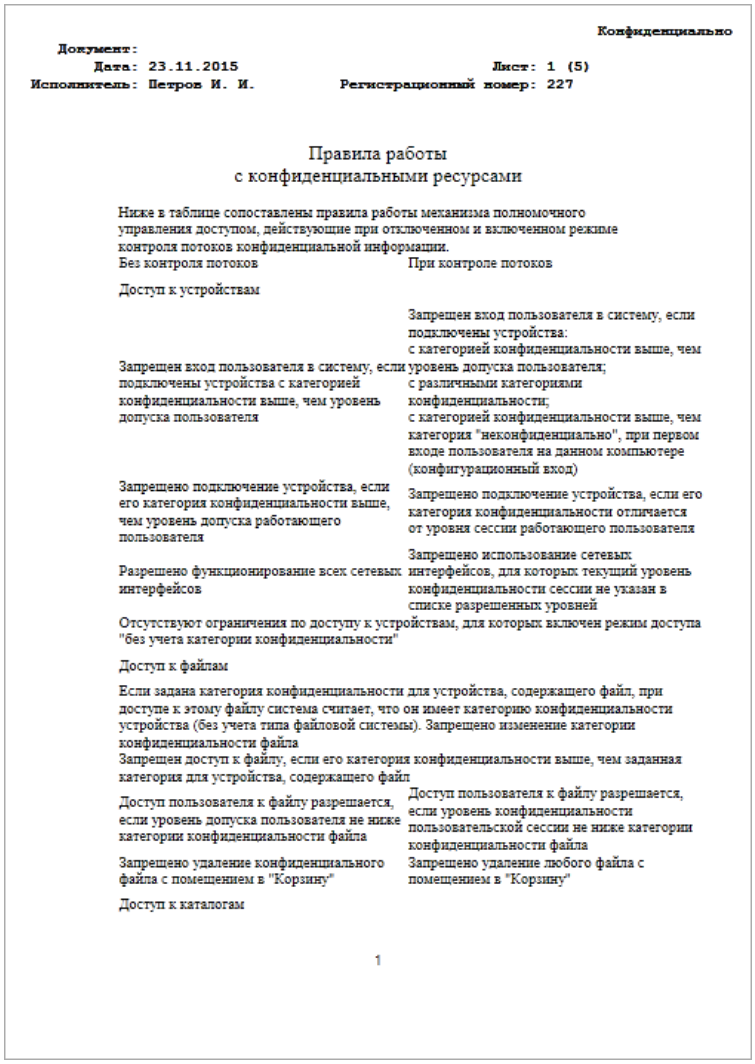



4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

## 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. Пример распечатанной страницы с маркером в верхнем колонтитуле представлен на следующем рисунке.



Конфиденциально

Документ:
Дата: 23.11.2015 Лист: 1 (5)
Исполнитель: Петров И. И. Регистрационный номер: 227

Правила работы
с конфиденциальными ресурсами

Ниже в таблице сопоставлены правила работы механизма полномочного управления доступом, 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:<br>с категорией конфиденциальности выше, чем уровень допуска пользователя;<br>с различными категориями конфиденциальности;<br>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 | |

1

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 предопределенными 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, категорий конфиденциальности) и добавления новых объектов.

## Управление режимом маркировки

Параметры, определяющие действие режима маркировки документов, представлены в списках объектов групповых политик.

**Внимание!**
На компьютерах, входящих в один домен безопасности, должны применяться одинаковые параметры использования маркеров. Рекомендуется задать эти параметры в одной общей групповой политике.

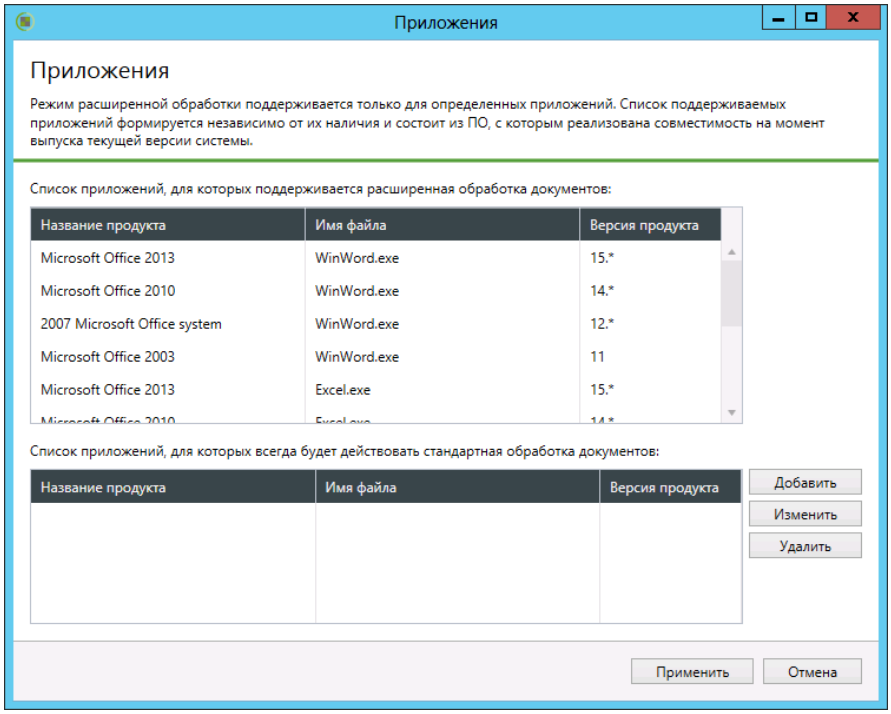
Ниже приводится описание процедуры централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для включения и настройки режима маркировки:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль печати / Настройки".
3. Для параметра "Маркировка документов" укажите нужное значение:
   - "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 Studio регистрируются события начала печати документа, окончания печати документа. При включенном теневом копировании в хранилище сохраняется копия распечатанного фрагмента, а не всего документа;
   - "Расширенная обработка" — режим может использоваться при печати из приложений, с которыми реализована совместимость (см. ниже). 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 Studio 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 Studio осуществляется в зависимости от состояния параметра групповой политики, который определяет действие функции теневого копирования для всех принтеров (см. стр. 24). Если для параметра "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".
4. Настройте параметры использования маркеров. Для этого нажмите кнопку "Редактировать" и выполните настройку в появившемся окне программы редактирования маркеров (описание интерфейса и общий порядок действий при работе с программой приведены на стр. 30). Если требуется вернуть параметры маркировки, заданные по умолчанию, — нажмите кнопку "По умолчанию".
5. Если включен режим "Стандартная обработка" — завершите процедуру, нажав кнопку "Применить" в верхней части вкладки "Настройки".
6. Если включен режим "Расширенная обработка" — проверьте список совместимых приложений и при необходимости укажите программы, в которых должен действовать стандартный режим обработки. Для этого выберите ссылку "Приложения, включенные в расширенную обработку".

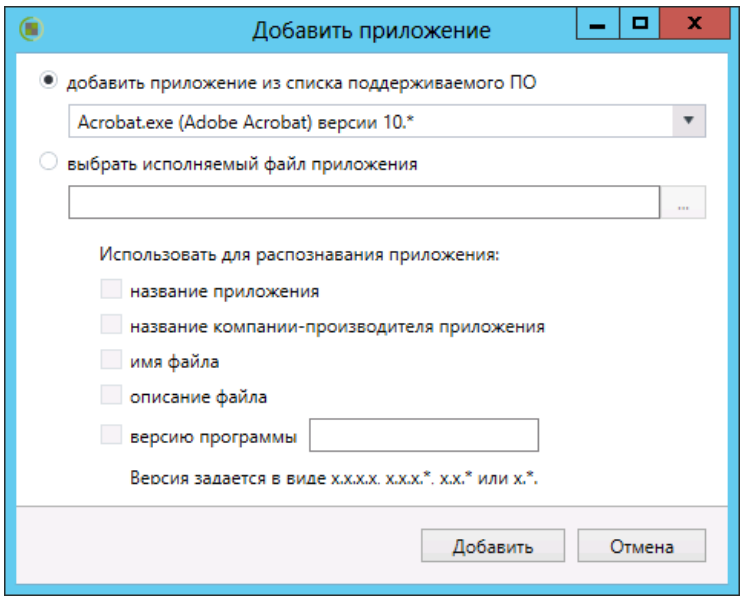
   На экране появится диалог со списками приложений.




7. 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 Studio.
8. Отредактируйте, если требуется, список программ со стандартным режимом обработки и нажмите кнопку "Применить". Для редактирования списка используйте соответствующие кнопки справа:

| 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.

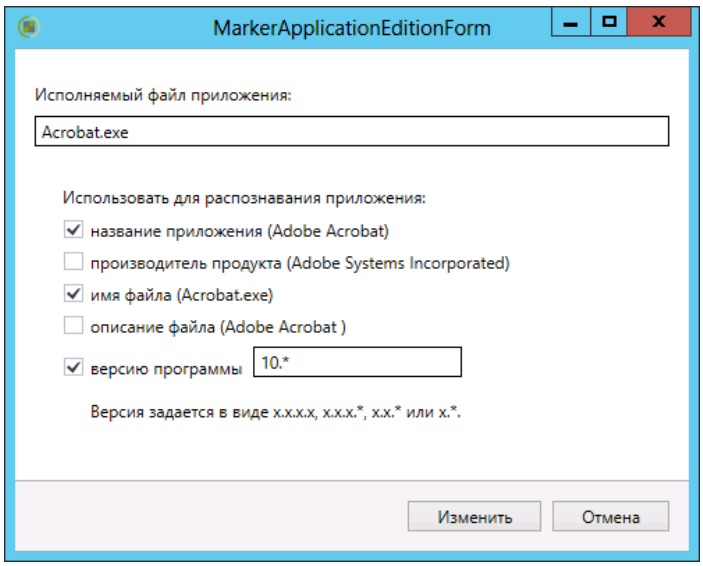


В диалоге выберите вариант добавления приложения, настройте доступные параметры и нажмите кнопку "Добавить". Предусмотрены следующие варианты выбора приложений:

- 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 "Изменить".

9. По окончании работы со списком приложений нажмите кнопку "Применить" в верхней части вкладки "Настройки".

**Для отключения режима маркировки:**

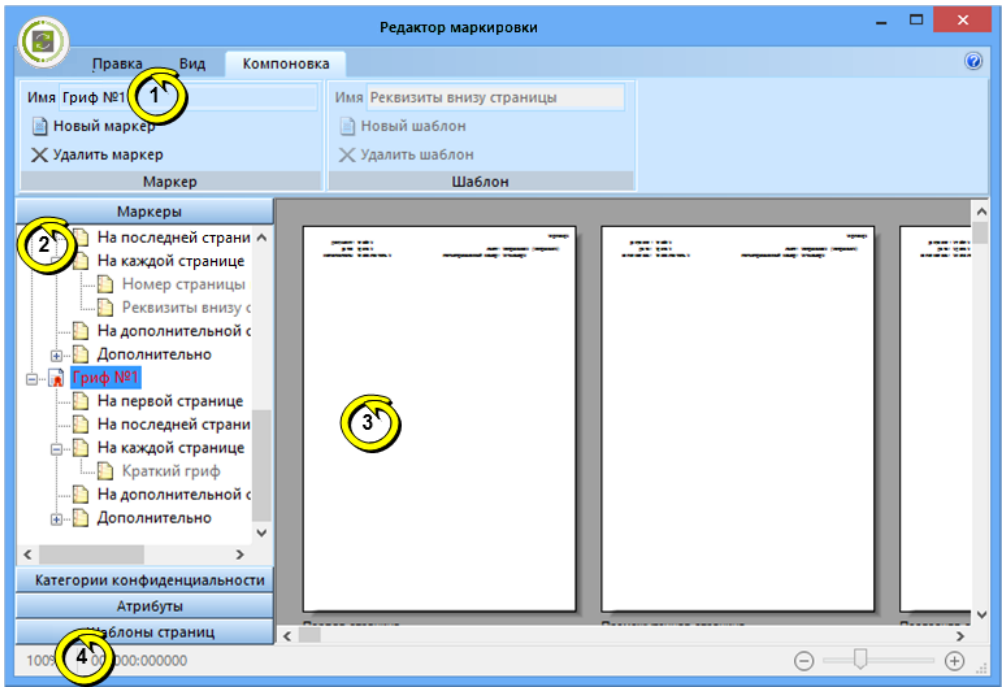
1. Выполните действия **1**–**2** вышеописанной процедуры.
2. Для параметра "Маркировка документов" укажите значение "Отключена".
3. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

# Программа редактирования маркеров

Программа редактирования маркеров предназначена для настройки маркировки документов, выводимых на печать. Запуск программы осуществляется в диалоге настройки параметра групповой политики "Маркировка документов" (см. стр.26).

## Интерфейс программы

Пример окна программы редактирования маркеров представлен на следующем рисунке:




Окно программы может содержать следующие элементы интерфейса:

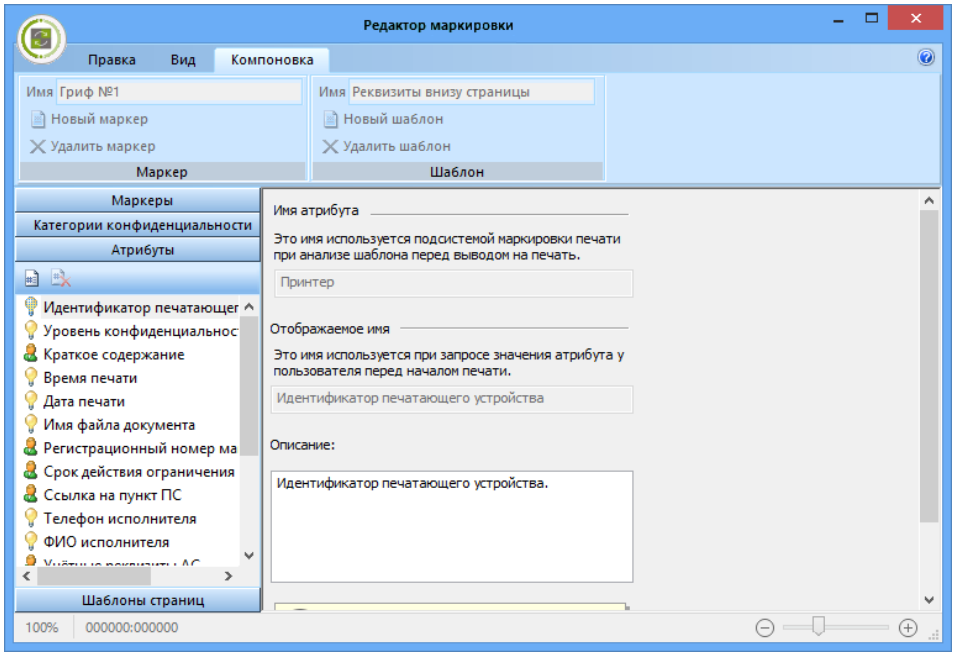
| **1 — Лента** |
|---|
| Содержит команды управления (инструменты) для выполнения действий в программе. Лента состоит из отдельных вкладок, в которых группируются команды в соответствии с их назначением. Для открытия вкладки используется ее заголовок.<br>Рабочее пространство в окне программы можно увеличить 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:<br>• "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";<br>• "Категории конфиденциальности" — раздел предназначен для выбора маркеров, которые будут использоваться при печати документов определенных категорий конфиденциальности;<br>• "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";<br>• "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".<br>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:<br>• при выборе маркера — в области представлен общий вид маркировки всех страниц при печати документов с использованием маркера;<br>• 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;<br>• при выборе атрибута — область редактирования содержит поля с параметрами атрибута: внутреннее и отображаемое имя атрибута, описание и сведения о применении атрибута;<br>• 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

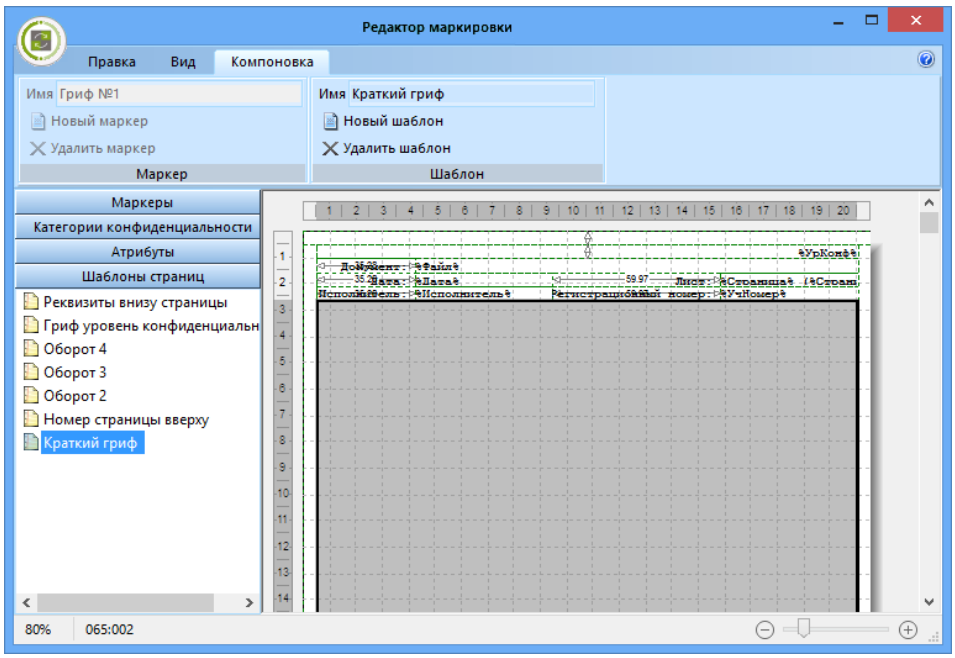
Редактирование маркеров в программе рекомендуется выполнять в следующем порядке:

1. В панели выбора объектов перейдите к разделу "Атрибуты".



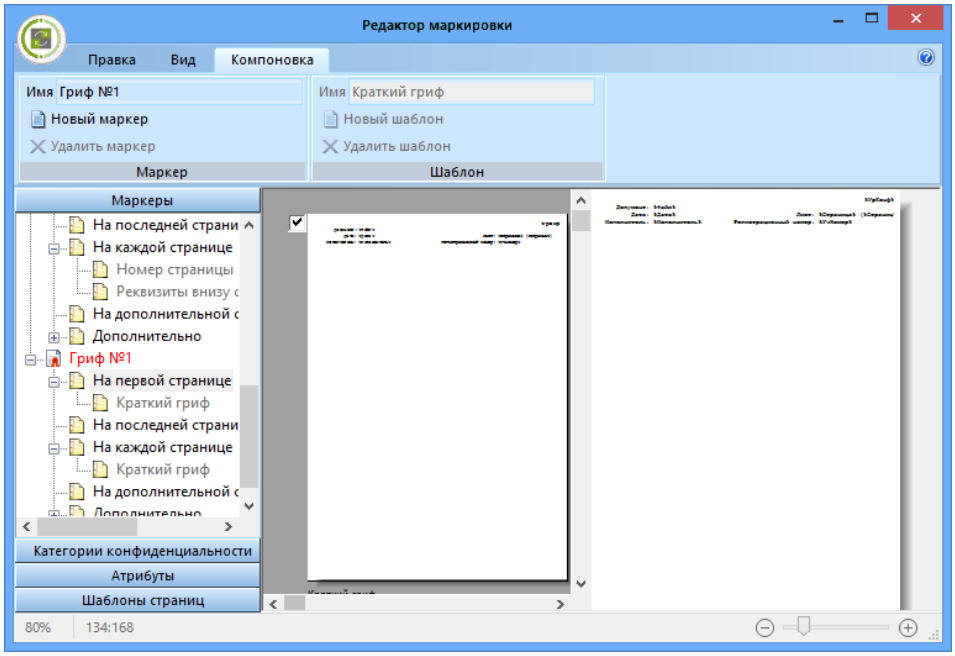

Если в списке отсутствуют нужные атрибуты (позволяющие получать и выводить необходимые сведения при печати документов), измените имеющиеся атрибуты или добавьте новые.

2. В панели выбора объектов перейдите к разделу "Шаблоны страниц".



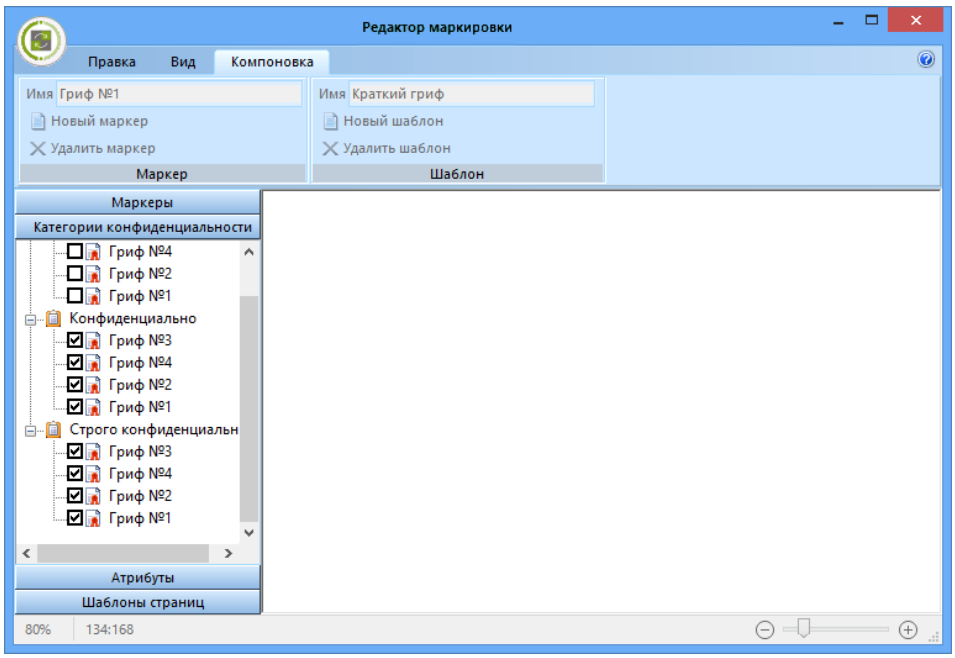

Если в списке отсутствуют нужные шаблоны (с требуемым оформлением и наборами атрибутов), измените имеющиеся шаблоны или добавьте новые. Редактирование элементов оформления шаблонов осуществляется стандартными способами.

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. Сохраните сделанные изменения. Для этого вызовите общее меню программы с помощью кнопки в левом верхнем углу окна и выберите команду "Сохранить описание маркировки".

6. Закройте программу.

# Глава 3
# Настройка замкнутой программной среды

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 (скрипты). Попытки запуска других ресурсов блокируются, и в журнале регистрируются события тревоги.

В системе Secret Net Studio настройка механизма ЗПС может осуществляться совместно с настройкой механизма контроля целостности (КЦ). Для этих механизмов используется общее средство настройки — программа "Контроль программ и данных". В данной главе рассматривается порядок работы с программой для реализации замкнутой программной среды отдельно или совместно с механизмом КЦ. Описание настройки механизма контроля целостности см. в документе [**3**].

## Общие сведения о методах и средствах настройки

### 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 место нахождения контролируемого ресурса и его тип |
| **Группа ресурсов** | Объединяет несколько описаний ресурсов одного типа (файлы, каталоги, объекты системного реестра, исполняемые скрипты). 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 Studio, 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 Studio. В ЛБД КЦ-ЗПС на каждом компьютере хранится модель данных, относящаяся к этому компьютеру.

Для клиентов в сетевом режиме функционирования формируется центральная база данных (ЦБД) КЦ-ЗПС в специальном централизованном хранилище. 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.

В централизованном режиме программы управления КЦ-ЗПС модели данных 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 |

### Формирование модели данных для ЗПС

Модель данных для механизма ЗПС можно сформировать на основе сведений о запускавшихся программах из журнала Secret Net Studio. Для этого при централизованном управлении необходимо создать файл журнала в dvt- или snlog-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 запускавшихся программах можно загрузить непосредственно из локального журнала. Далее на основании этих данных формируются задания ЗПС для субъектов.

## Объекты модели по умолчанию

Во время установки клиентского ПО системы Secret Net Studio проверяется наличие модели данных в БД КЦ-ЗПС. Если модель данных отсутствует, автоматически выполняется ее формирование и наполнение объектами по умолчанию.

При начальном формировании в модель добавляются следующие задания:

- "Задание для контроля ресурсов Secret Net Studio";
- "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 Studio.

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

## Программа управления КЦ-ЗПС

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 Studio. В данной главе рассматриваются методы работы с программой для настройки механизма ЗПС. Описание интерфейса см. в документе [**3**].

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.

Программа управления КЦ-ЗПС может работать в централизованном и локальном режимах. Централизованный режим используется для настройки параметров работы механизмов на компьютерах с установленным клиентом в сетевом режиме функционирования.

Для работы с программой управления КЦ-ЗПС пользователь должен входить в локальную группу администраторов компьютера. Чтобы использовать централизованный режим, пользователь дополнительно должен входить и в группу администраторов домена безопасности.

**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.

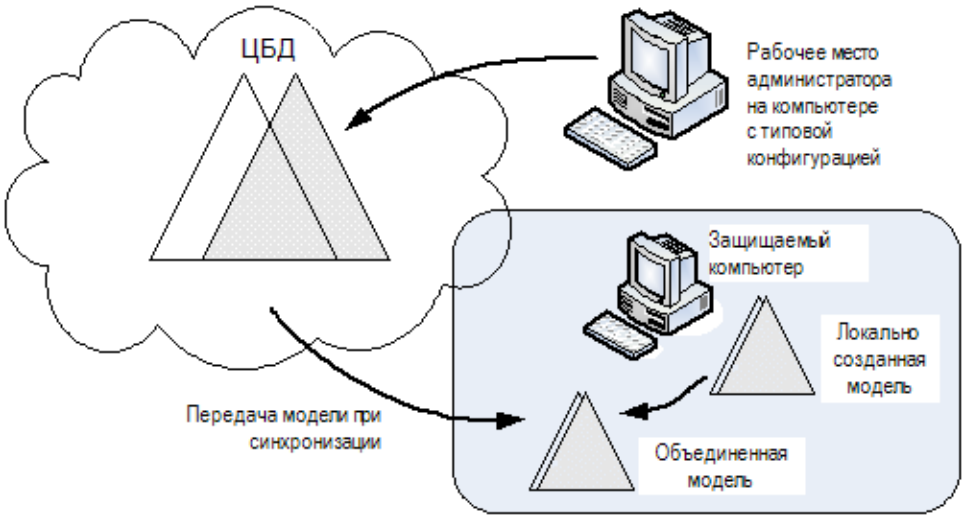
## Синхронизация центральной и локальной баз данных

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;
- после входа (в фоновом режиме во время работы пользователя);
- 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. 53). Для оперативной синхронизации на компьютерах должны быть настроены определенные параметры ОС Windows.

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.

# Начальная настройка механизма

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

## Подготовка к построению модели данных

При подготовке 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.

Из числа компьютеров с установленным клиентом в сетевом режиме функционирования выделяются группы 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.

## Общий порядок настройки

Для использования на компьютерах механизма ЗПС выполните настройку в следующем порядке:

1. Сформируйте новую модель данных с настройкой контроля по умолчанию (см. стр.**39**).
2. Добавьте в модель данных дополнительные объекты:
   - задачи для использования в ЗПС (см. стр.**40**);
   - задания ЗПС (см. стр.**42**).

   **Примечание.**
   Для формирования задач и заданий ЗПС можно использовать метод накопления сведений о действиях пользователей во время работы. Данный метод предусматривает использование мягкого режима работы механизма и получение информации о запуске программ из журнала Secret Net Studio (см. стр.**43**).
3. Установите связи заданий ЗПС с субъектами (см. стр.**45**).
4. Укажите ресурсы для контроля (см. стр.**45**).
5. Включите режим изоляции процессов (см. стр.**47**).
6. Создайте эталоны контролируемых ресурсов (см. стр.**48**).
7. Для пользователей, при работе которых не должны действовать ограничения ЗПС, предоставьте привилегию (см. стр.**51**).
8. Включите жесткий режим работы механизма ЗПС (см. стр.**52**).

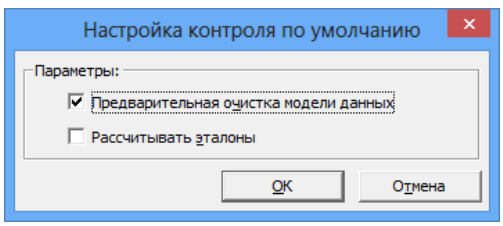
В процессе эксплуатации системы может возникнуть необходимость корректировки или пересмотра модели данных. Если предполагается кардинальная переработка модели, то лучше выполнить ее с нуля. Если переработке будет подвергнута небольшая часть модели, то в этом случае можно применить отдельные процедуры модификации модели (см. стр.**61**).

## Формирование новой модели данных

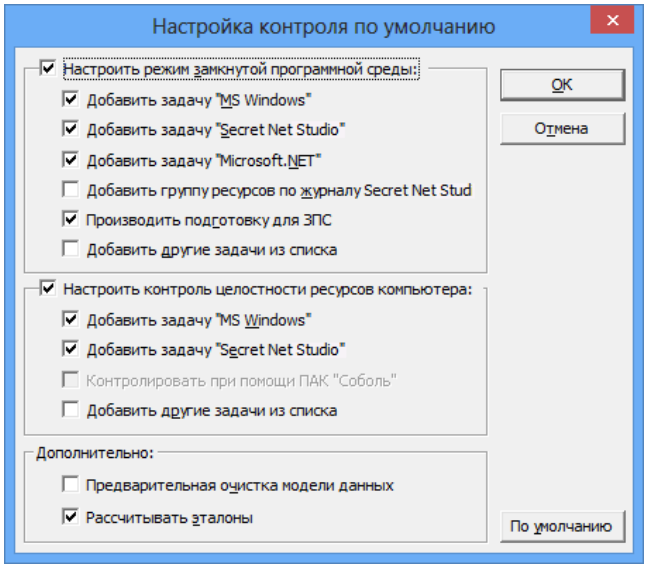
При формировании в модель данных автоматически добавляются описания для важных ресурсов ОС Windows, а также описания ресурсов некоторых прикладных программ. Новая модель данных будет сформирована с настройкой контроля по умолчанию.

**Для формирования новой модели данных:**

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. В зависимости от режима работы программы настройте нужные параметры 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 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.

## 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 Studio). 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.

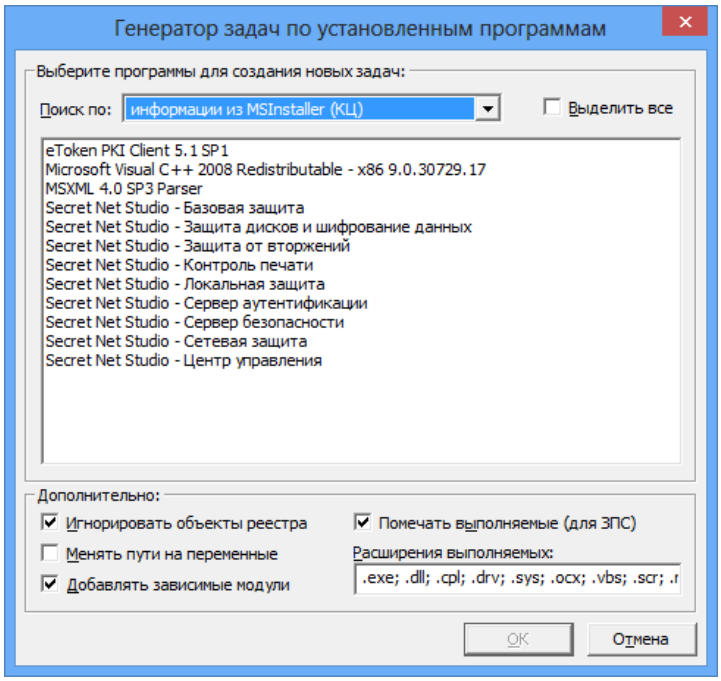
Перед началом генерации администратор безопасности может просмотреть список установленного ПО и наметить те компоненты (программы), для которых должны быть сгенерированы задачи. При этом в задачи будут автоматически включены ресурсы, связанные с исполняемыми модулями выбранного ПО. Можно также задать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

Кроме того, для ЗПС задачи можно добавить, используя способ формирования заданий ЗПС по журналу Secret Net Studio (см. стр.**43**).

**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 |
| **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 |

| Условие | Пояснение |
|---|---|
| **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", а также файлы с нетипичными расширениями (список таких файлов формируется в параметрах программы). При необходимости отредактируйте список расширений для применения при этом отборе ресурсов |

**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 "OK".

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

5. Нажмите кнопку "OK" 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).

## Добавление заданий и включение в них задач

Цель данного этапа — сформировать задания на основе задач, созданных на предыдущем этапе.

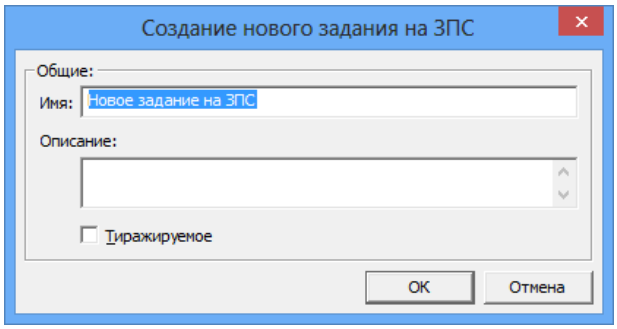
**Для формирования задания:**

1. Выберите категорию "Задания" и в меню "Задания" выберите команду "Создать задание".

   На экране появится диалог выбора типа задания.

2. Выберите тип задания (ЗПС) и нажмите кнопку "OK".

   На экране появится диалог:




   Введите имя задания, его краткое описание и нажмите кнопку "OK".

**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 "OK".

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

## Включение мягкого режима ЗПС и формирование заданий по журналу

При формировании заданий ЗПС на основе сведений из журнала Secret Net Studio действия выполняются в следующем порядке:

| | |
|---|---|
| **1.** | Включение ЗПС в мягком режиме |
| **2.** | Сбор сведений в журнале |
| **3.** | Добавление задач ЗПС, созданных по журналу |

### 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 Studio регистрируются соответствующие события тревоги. В жестком режиме разрешается запуск только тех программ, которые входят в список разрешенных. Запуск других программ блокируется, а в журнале Secret Net Studio регистрируются события тревоги.

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 программах и скриптах в журнале

Модель ЗПС может быть создана на основе данных журнала Secret Net Studio. Чтобы собрать нужные сведения, пользователям разрешается запускать любые программы и скрипты. На это отводится некоторый период времени. Сведения о запускаемых программах и скриптах регистрируются в журнале. На время сбора сведений необходимо включить регистрацию всех событий категории "Замкнутая программная среда" на тех компьютерах, на которых замкнутая программная среда будет использоваться.

По окончании сбора сведений осуществляется формирование задач ЗПС в модели данных на основе сведений о программах и скриптах из журнала Secret Net Studio. Экспорт сведений в модель данных может выполняться непосредственно из локального журнала Secret Net Studio или из файла, в который предварительно были сохранены записи журнала. Описание процедур сохранения записей журнала в файл приводится в документе [**4**].

### Добавление задач ЗПС, созданных по журналу

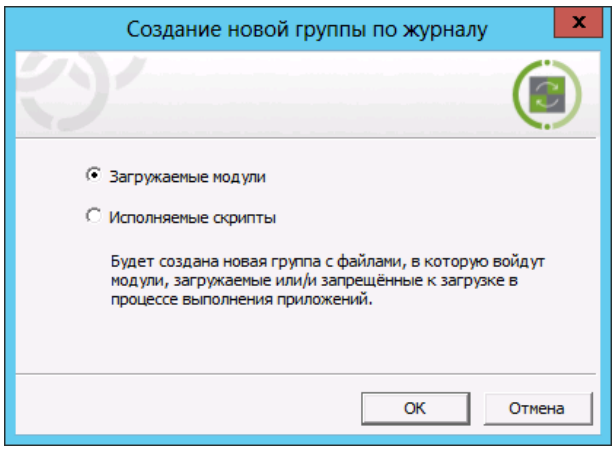
На этой стадии на основании данных из журнала Secret Net Studio формируются задачи, добавляемые к заданиям ЗПС.

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

**Для добавления задач ЗПС, созданных по журналу:**

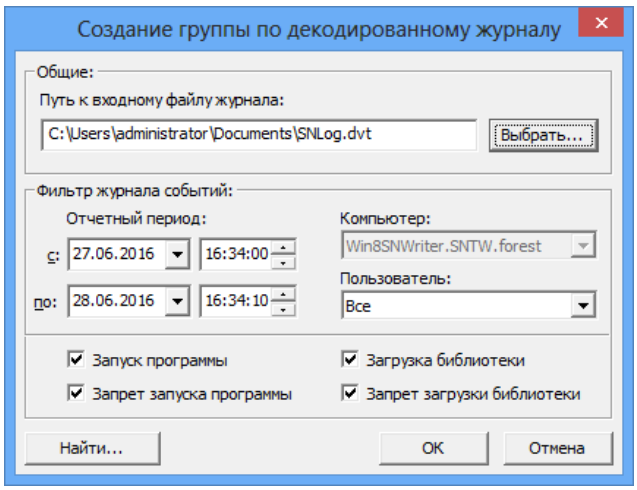
1. В основном окне программы управления КЦ-ЗПС выберите нужный субъект.
2. Выберите ранее созданное задание ЗПС, связанное с выбранным субъектом, или создайте новое задание ЗПС.
3. Вызовите контекстное меню и выберите в нем "Добавить задачи/группы | Новую группу по журналу".

   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 "OK".

   На экране появится диалог, подобный следующему:



6. Укажите необходимые значения параметров (путь к dvt- или snlog-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.

## 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 централизованной 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 типа субъектов (в централизованном режиме) или стандартный диалог ОС Windows для выбора пользователей и групп пользователей (в локальном режиме).
3. Укажите тип добавляемых объектов и затем найдите и выберите нужные объекты из числа существующих или, если добавляется группа компьютеров, укажите имя группы, ее описание и сформируйте список относящихся к ней компьютеров.
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 замкнутой программной среды

Чтобы ресурсы контролировались 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.

Также для каждого ресурса, которому установлен признак "выполняемый", может выполняться поиск зависимых модулей (см. стр. **75** ). Найденные зависимые модули добавляются в модель данных в те же группы ресурсов, в

которые входят исходные модули. Им также присваивается признак "выполняемый".

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 Studio начнет контролировать запуск программ пользователем и регистрировать соответствующие события в журнале.

При построении модели данных с помощью автоматизированных средств (см. стр.**40**) 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:

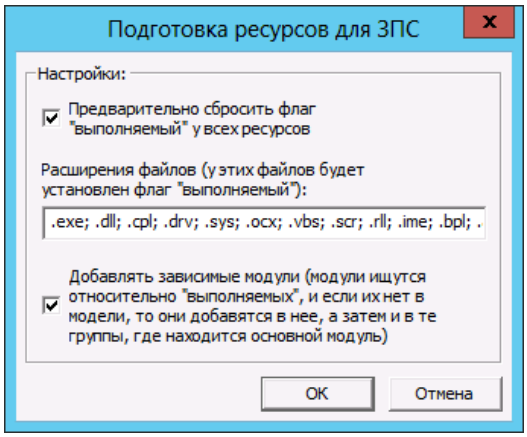
- Перед началом выполнения процедуры можно сбросить признак "выполняемый" у всех ресурсов в модели данных, у которых он имеется. В этом случае будут анализироваться все ресурсы, включенные в модель.
- Необходимо выполнить поиск зависимых модулей. В этом случае для каждого ресурса, которому будет установлен 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.

**Примечание.**
В централизованном режиме работы программы для выполнения процедуры подготовки ресурсов необходимо наличие в модели данных хотя бы одного задания ЗПС с ресурсами для контроля.

**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 "OK".

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.

## Включение и настройка изоляции процессов

При необходимости обеспечить изолированную среду для определенных процессов (запретить обмен данными с другими процессами) действия выполняются в следующем порядке:

| | |
|---|---|
| **1.** | Включение режима изоляции процессов |
| **2.** | Добавление файлов изолируемых процессов в список ресурсов |
| **3.** | Включение изоляции для ресурсов |

### Включение режима изоляции процессов

По умолчанию режим изоляции процессов отключен. Включение режима выполняется для субъекта управления.

**Для включения режима изоляции:**

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 поле "Изоляция процессов включена".
4. Нажмите кнопку "OK".

Для выбранного компьютера (или группы) начнет действовать режим изоляции процессов.

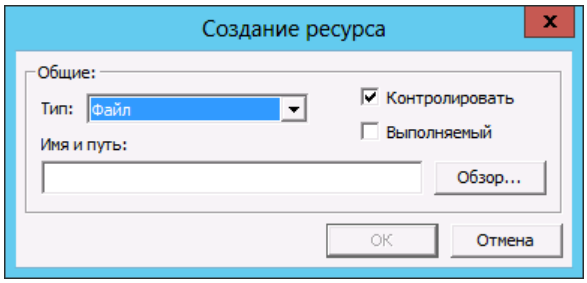
### Добавление файлов изолируемых процессов в список ресурсов

В списки ресуров заданий для ЗПС необходимо добавить исполняемые файлы процессов, которые будут изолированными. Изоляцию можно включить для файлов с расширением .exe (например, файл запуска редактора "Блокнот" notepad.exe), а также для файлов, перечисленных в списке "Имена исполняемых модулей процессов" в параметрах программы.

**Для добавления файла процесса в список ресурсов:**

1. Вызовите контекстное меню группы ресурсов для файлов и каталогов в задании ЗПС и выберите в нем "Добавить ресурсы | Новый одиночный".

   Появится диалог для настройки параметров ресурса.




2. Укажите параметры добавляемого ресурса (см. таблицу ниже) и нажмите кнопку "OK".

| Параметр | Пояснение |
|---|---|
| **Тип** | Укажите тип добавляемого ресурса: файл |
| **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.<br>Если контроль данного ресурса не требуется, удалите отметку. В этом случае описание ресурса сохранится в модели данных и его можно будет поставить на контроль позднее |
| **Выполняемый** | Параметр используется для обозначения исполняемых файлов, которые формируют списки программ, разрешенных для запуска при включенной замкнутой программной среде |

Ресурс появится в списке основного окна программы.

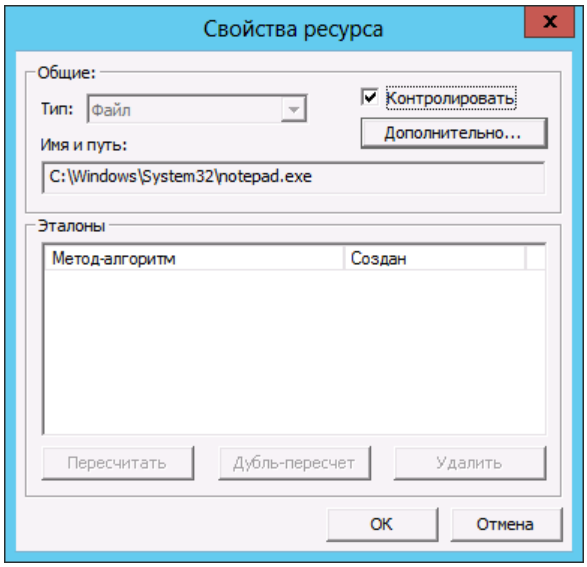
### Включение изоляции для ресурсов

После добавления файлов процессов в список ресурсов выполняется процедура включения изоляции для каждого ресурса.

**Для включения изоляции для ресурса:**

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

   Появится диалог настройки параметров ресурса.




2. Нажмите кнопку "Дополнительно". В появившемся диалоге "Дополнительные свойства приложения" установите отметку в поле "Изолировать процесс" и нажмите кнопку "OK".
3. Нажмите кнопку "OK" в диалоге настройки параметров ресурса.

## 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.**39** ). Если построение модели осуществляется с использованием генератора задач или вручную, расчет эталонов должен выполняться отдельно.

На этапе настройки 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.

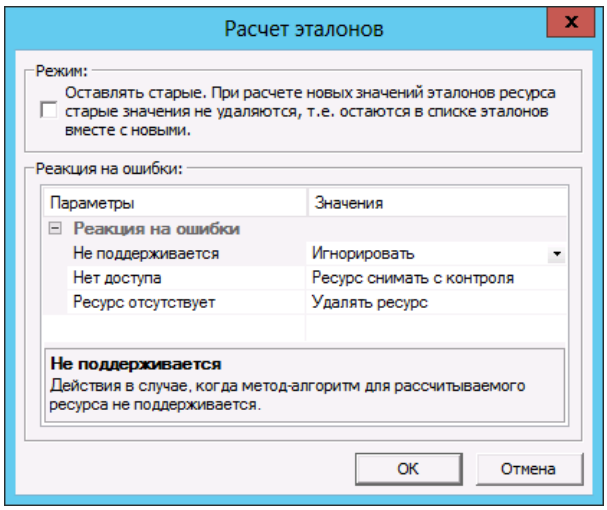
В локальном режиме расчет эталонов может быть выполнен для всех ресурсов, имеющихся в локальной модели данных. Исключение составляют те ресурсы, эталоны которых рассчитаны централизованно (ресурсы входят в тиражируемые задания).

В централизованном режиме используются различные методы для расчета эталонов 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 "Эталоны | 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.

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 "OK".

   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 тревоги 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 "OK".

**Для расчета эталонов тиражируемых заданий (в централизованном режиме):**

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".

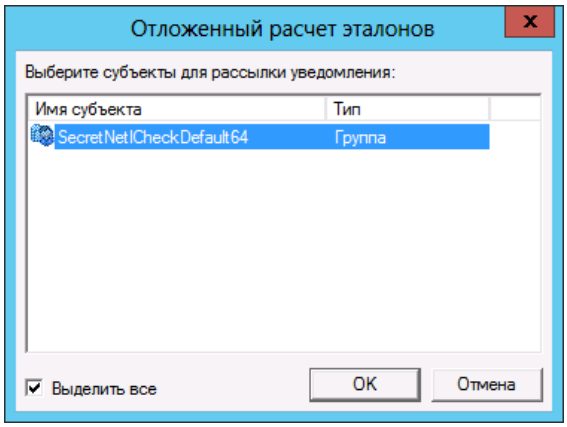
   На экране появится диалог "Расчет эталонов".

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

**Для расчета эталонов нетиражируемого задания (в централизованном режиме):**

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 "OK".

**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.

## Предоставление привилегии при работе в ЗПС

В Secret Net Studio предусмотрена привилегия, которая отменяет ограничения ЗПС для пользователя. На пользователей, которым предоставлена данная привилегия, действие механизма замкнутой программной среды не распространяется.

По умолчанию привилегией обладают пользователи, входящие в локальную группу администраторов.

Ниже приводится описание процедуры централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для предоставления привилегии:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Замкнутая программная среда".

3. Для параметра "Учетные записи, на которые не действуют правила замкнутой программной среды" отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия.
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

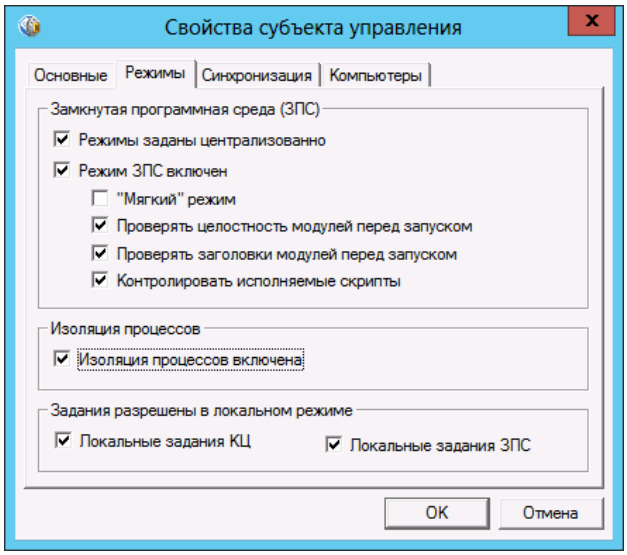
## Включение жесткого режима ЗПС

В жестком режиме работы механизма ЗПС возможен запуск только разрешенных программ, библиотек и сценариев. Запуск других ресурсов блокируется, а в журнале Secret Net Studio регистрируются события тревоги как попытки несанкционированного доступа.

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 |

| Параметр | Пояснение |
|---|---|
| **Контролировать исполняемые скрипты** | Блокируется выполнение сценариев (скриптов), не входящих в перечень разрешенных для запуска и не зарегистрированных в базе данных системы Secret Net Studio |

6. Нажмите кнопку "OK".

# 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.**56**, стр.**58**).

## Оповещение об изменениях

Сведения об изменениях в модели данных, выполненных в централизованном режиме, распространяются на включенные компьютеры домена в соответствии с настройкой параметра группы "Оповещения" (описание процедуры настройки параметров программы см. в документе [**3**]). Функция действует для клиентов в сетевом режиме функционирования.

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.

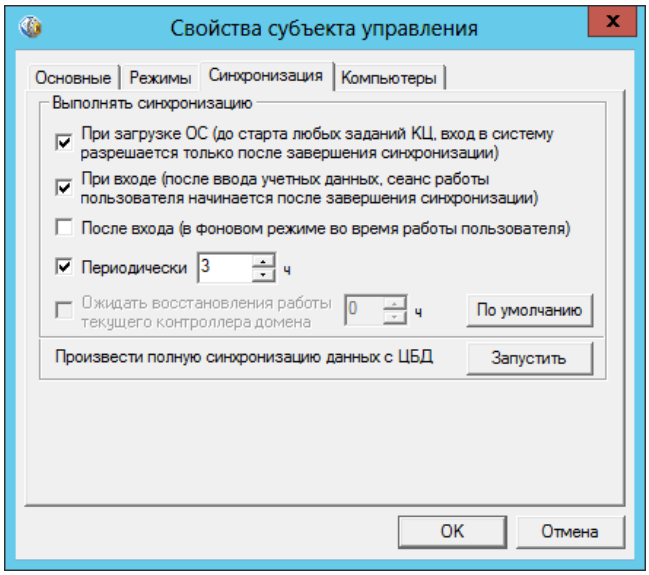
Настройка параметров запуска синхронизации осуществляется в централизованном режиме работы программы. Параметры могут быть заданы как для отдельных компьютеров, так и для групп. При этом действуют приоритеты применения параметров: наивысший приоритет имеют параметры компьютеров, затем параметры групп, 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.<br>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.<br>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.<br>Действие данного параметра может приводить к задержкам входа при изменении в ЦБД объемных заданий и при низкой пропускной способности каналов связи |

| Параметр | Пояснение |
|---|---|
| **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) |
| **Ожидать восстановления работы текущего контроллера домена** | *В текущей версии не используется* |

**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.

4. Нажмите кнопку "OK".

**Для проверки и корректировки параметров запуска синхронизации в группах:**

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

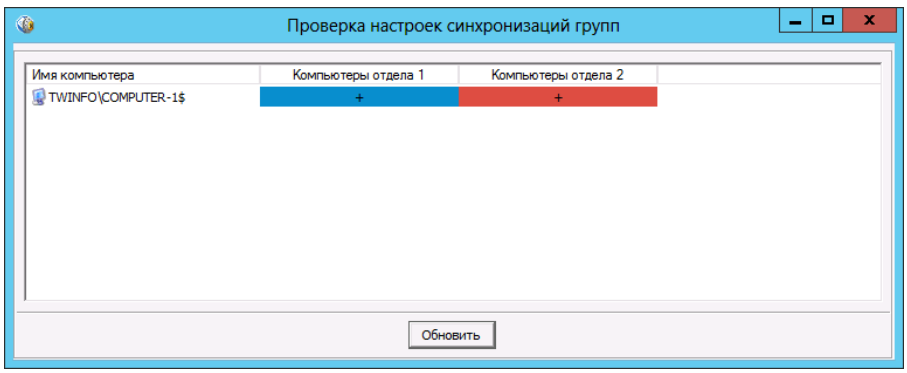
**Примечание.**
Команда недоступна, если список субъектов в модели данных содержит только одну группу по умолчанию SecretNetICheckDefault.

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

- Сообщение об отсутствии обнаруженных конфликтов — если для всех компьютеров в группах отсутствуют несовпадающие параметры запуска синхронизации.

  **Примечание.**
  Не считается конфликтной ситуация, когда компьютер, включенный в группы с различными параметрами, также присутствует в модели и как отдельный субъект. В этом случае, в соответствии с приоритетом применения параметров, для этого компьютера будут применяться параметры, заданные для него как субъекта (независимо от того, какие параметры заданы для групп, в которые он входит).

- Список компьютеров с конфликтующими параметрами:




  В списке перечислены компьютеры и указаны группы, в которых заданы несовпадающие параметры запуска синхронизации для этих компьютеров.

2. Если в результате проверки выведен список компьютеров с конфликтующими параметрами, переместите или сверните окно со списком. В основном окне программы выполните действия для устранения конфликтов (например, отредактируйте списки компьютеров в группах или добавьте указанные компьютеры в качестве отдельных субъектов со своими параметрами). Для повторной проверки снова перейдите в окно со списком и нажмите кнопку "Обновить".

## Принудительный запуск полной синхронизации

Запуск синхронизации изменений ЦБД КЦ-ЗПС на компьютерах может выполняться автоматически в соответствии с заданными параметрами (см. стр.**53**). 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:

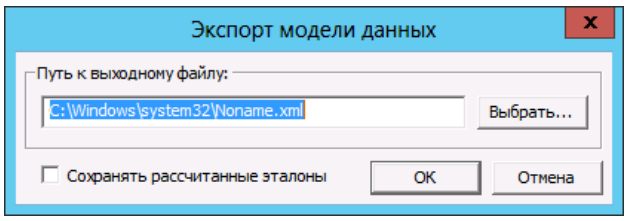
- экспортирование всей модели данных;
- выборочное экспортирование объектов определенных категорий (не применяется к объектам категории "Субъекты управления").

**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.**113**.

**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 "OK" в диалоге настройки параметров экспортирования.

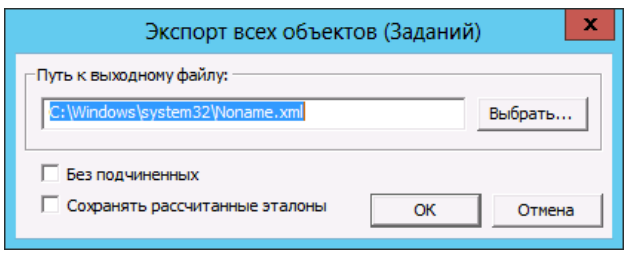
**Для выборочного экспортирования объектов:**

1. На панели категорий выберите категорию, в которой содержатся нужные объекты для экспортирования (кроме категории "Субъекты управления").
2. В окне структуры или в области списка объектов найдите экспортируемые объекты.

   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 содержимого папки" 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 "OK" 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.

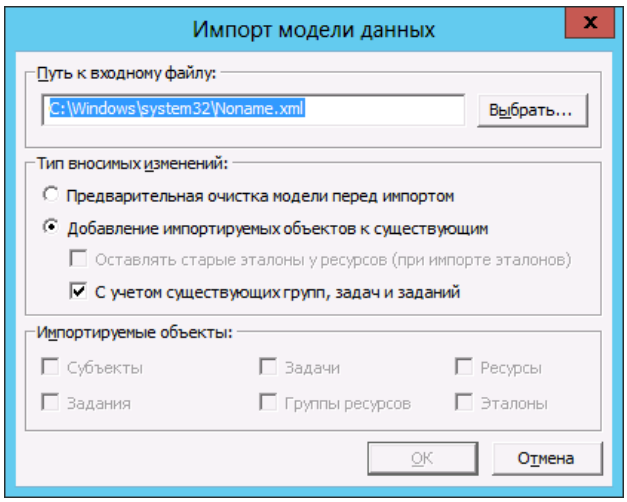
Импортом из файла с сохраненной моделью данных добавляются списки ресурсов, экспортированные из другой модели данных. Данный способ используется при переносе настроек защитных механизмов с одного компьютера на другой. Компьютеры должны иметь сходные конфигурации и использовать одинаковое программное обеспечение.

> **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.<br>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.<br>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.<br>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".

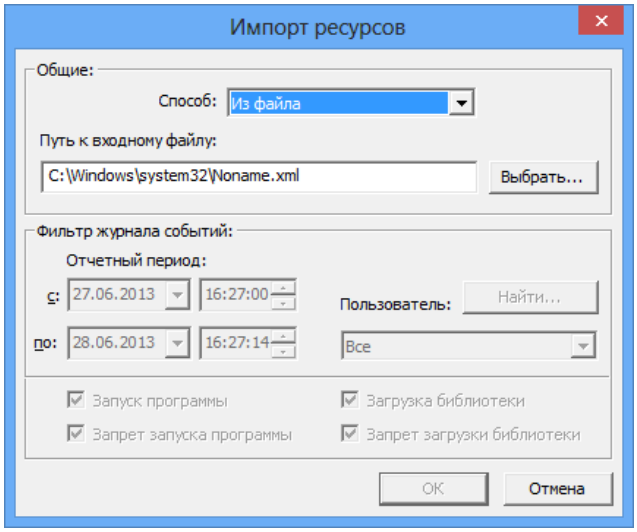
7. Нажмите кнопку "OK" в диалоге настройки параметров импортирования.

**Для импортирования объектов текущей категории:**

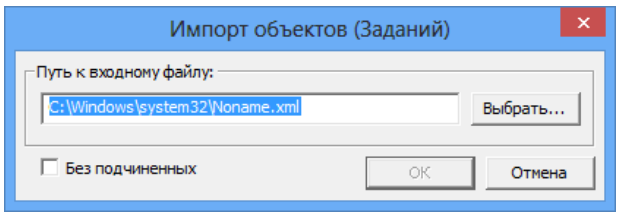
1. На панели категорий выберите категорию, в которую нужно импортировать объекты (кроме категории "Субъекты управления").
2. В окне структуры выберите корневой элемент. Откройте меню с названием выбранного элемента (например, "Задание") и выберите команду "Импорт и добавление".

   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 "OK".

   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 Studio в модель можно вносить изменения. Необходимость изменений, как правило, обусловливается 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.

## 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);
- признак "контролировать";
- эталоны;
- дополнительные параметры.

Значения параметров "тип" и "имя и 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. 76).

Эталоном 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.

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.

Для исполняемых файлов процессов (файлы с расширением .exe, а также файлы, перечисленные в списке "Имена исполняемых модулей процессов" в параметрах программы — см. документ [**3**]) можно настраивать следующие дополнительные параметры:

- параметры исключений, которые будут применяться во время действия механизма ЗПС — 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 CS6 и SolidWorks;
- параметры изоляции процесса — позволяют обеспечить изолированную среду для процесса (запретить обмен данными с другими процессами).

**Для изменения параметров ресурса:**

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

Появится диалог настройки параметров ресурса.

2. При необходимости измените состояние признака "Контролировать".
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 ресурс является исполняемым файлом, настройте дополнительные параметры исключений для механизма ЗПС и изоляции процесса. Для этого нажмите кнопку "Дополнительно" и в появившемся диалоге выполните следующие действия:
   - чтобы разрешить выполнение процессом любых скриптов, установите отметку в поле "Разрешить выполнять любые скрипты";
   - чтобы разрешить процессу запуск файлов из определенных каталогов, установите отметку в поле "Разрешить 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 "-";
   - чтобы включить изоляцию процесса, установите отметку в поле "Изолировать процесс";
   - нажмите кнопку "ОК".
7. Нажмите кнопку "ОК" в диалоге настройки параметров ресурса.

### 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 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.**70**).
3. Внесите изменения в поля "Имя" и "Описание" и нажмите кнопку "ОК".

### Параметры задания

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".

   Появится диалог для настройки параметров задания.
2. Настройте доступные для изменения параметры и нажмите кнопку "OK".

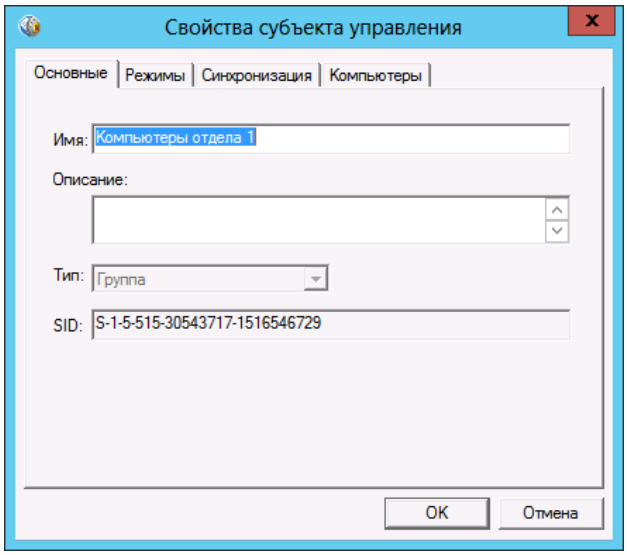
### Параметры субъектов

Свойства субъекта управления определяют основные параметры (имя, тип и пр.), а также в зависимости от типа субъекта можно настраивать дополнительные параметры применения режимов, синхронизации данных и списки компьютеров для групп.

**Для изменения параметров субъекта:**

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

   Появится диалоговое окно, подобное представленному на следующем рисунке:




   В зависимости от типа субъекта и режима работы программы могут быть представлены следующие диалоги:

   - "Основные" — содержит основные параметры субъекта (имя, описание, тип и идентификатор субъекта).
   - "Режимы" — диалог представлен для компьютеров и групп компьютеров и содержит следующие параметры:
     - способ задания режима ЗПС (централизованно или локально);
     - состояние механизма ЗПС (включен или отключен);
     - режим работы механизма ЗПС (жесткий или мягкий);
     - режимы дополнительной проверки целостности модулей и их заголовков перед запуском и контроля выполнения сценариев (скриптов);
     - состояние режима изоляции процессов;
     - разрешение или запрет выполнения заданий КЦ и ЗПС, созданных в локальных моделях данных.

- "Синхронизация" — диалог представлен для компьютеров и групп компьютеров в централизованном режиме работы программы и содержит параметры синхронизации ЦБД и ЛБД.
- "Компьютеры" — диалог представлен для групп компьютеров и предназначен для просмотра и редактирования состава группы (возможность редактирования отсутствует для групп по умолчанию SecretNetICheckDefault).

2. Настройте доступные для изменения параметры и нажмите кнопку "OK".

## 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 группу ресурсов. Группа ресурсов должна быть включена в задачу, а задача — в задание (также допускается включить группу ресурсов непосредственно в задание). Наконец, задание необходимо связать с одним из субъектов — компьютером, пользователем, группой пользователей или 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:<br>• файл с сохраненной моделью данных (см. стр.**58**);<br>• журнал безопасности ОС Windows или журнал Secret Net Studio на данном компьютере, либо сохраненный журнал в файле (см. далее) |
| **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 "OK".

   Появится диалог для настройки параметров ресурса.

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

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.<br>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:

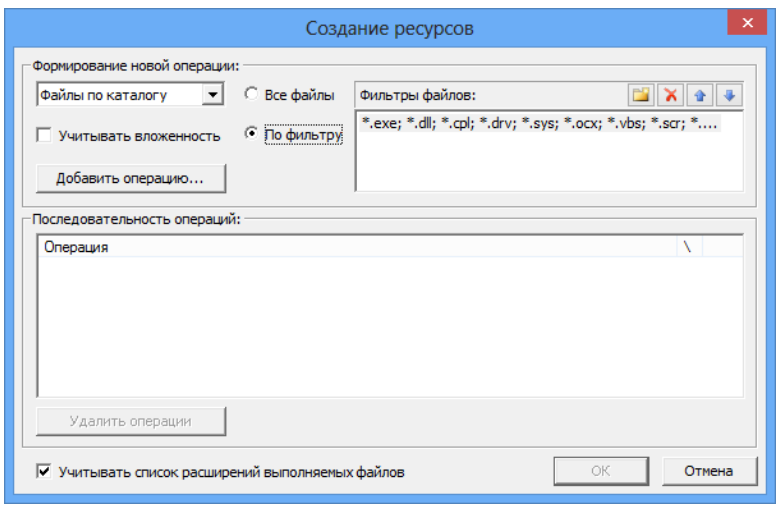
| Параметр | Пояснение |
|---|---|
| **Имя** | Введите имя ресурса, уникальное для списка ресурсов. В качестве имени ресурса можно указать, например, имя файла, из которого загружен сценарий (скрипт) |
| **Описание** | Введите дополнительные сведения о ресурсе |
| **Содержимое** | Введите текст сценария (скрипта) — последовательность исполняемых команд и/или действий, обрабатываемых по технологии Active Scripts.<br>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 (группа "Формирование новой операции") предназначена для указания варианта отбора ресурсов и задания дополнительных условий. Дополнительные условия задаются в зависимости от выбранного варианта. Одному варианту можно задать несколько условий для добавления ресурсов с использованием фильтров. Чтобы выполнить операцию, необходимо выбрать вариант, задать дополнительные условия и затем нажать кнопку "Добавить операцию".

Нижняя часть диалога (группа "Последовательность операций") предназначена для отображения последовательности выполненных операций.

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

| Параметр | Пояснение |
|---|---|
| **Вариант отбора ресурсов** | Предусмотрены следующие варианты:<br>• Выбранные файлы (стандартная процедура выбора файлов, дополнительные условия недоступны).<br>• Файлы по каталогу (добавляются файлы, входящие в указанный каталог, учитывается вложенность, можно использовать фильтр).<br>• Каталоги с файлами (учитывается вложенность, можно использовать фильтр).<br>• Каталоги по каталогу (учитывается вложенность).<br>• Переменные по ключу (выбираются переменные по ключу реестра, учитывается вложенность).<br>• 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** | Устанавливается признак "выполняемый" для файлов, которые имеют определенные расширения или имена, заданные параметрами "Расширения выполняемых" и "Имена исполняемых модулей процессов" в параметрах программы (см. документ [**3**]). 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; *.rll; *.ime; *.bpl; *.ax; *.acm; *.com; *.ppl; *.cmd; *.bat. При необходимости его можно изменить или добавить в список новые фильтры. Расширения файлов в строке разделяются точкой с запятой, запятой или пробелом.

- Для изменения фильтра выберите строку, нажмите клавишу <F2> 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. Для этого выберите нужный вариант в раскрывающемся списке: "Выбранные файлы", "Файлы по каталогу", "Каталоги с файлами", "Каталоги по каталогу", "Переменные по ключу" или "Ключи с переменными".

3. Если выбран вариант "Выбранные файлы", нажмите кнопку "Добавить операцию". Для остальных вариантов — перейдите к выполнению действия **5**.

   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".

   Если другие ресурсы добавлять не требуется, перейдите к действию **9**.

5. Если выбран вариант "Файлы по каталогу", "Каталоги с файлами" или "Каталоги по каталогу", настройте дополнительные параметры (при использовании фильтра выберите его в списке) и нажмите кнопку "Добавить операцию". Для остальных вариантов — перейдите к выполнению действия **7**.

   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".

   Если другие ресурсы добавлять не требуется, перейдите к действию **9**.

7. Если выбран вариант "Переменные по ключу" или "Ключи с переменными", отметьте при необходимости поле "Учитывать вложенность" и нажмите кнопку "Добавить операцию".

   Появится стандартный диалог ОС Windows для просмотра реестра.

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

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

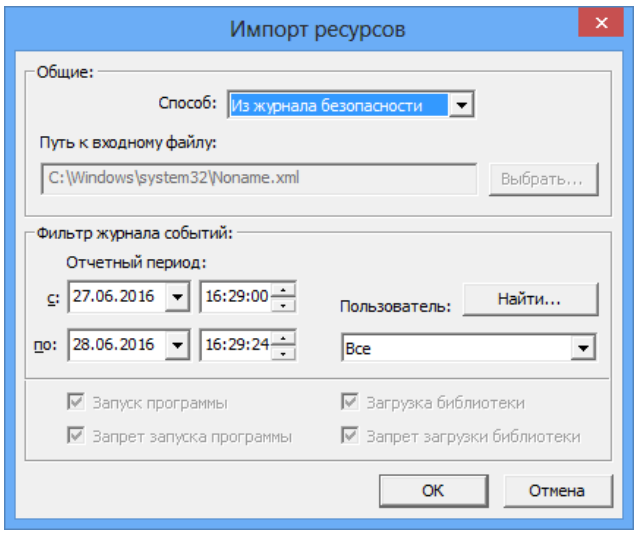
9. Проверьте список выполненных операций и, если он содержит все ресурсы, которые планировалось включить в модель данных, нажмите кнопку "ОК".

   Диалог "Создание ресурсов" закроется, 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 Studio:**

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 Studio".

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

   **Примечание.**
   Из журнала Secret Net Studio импортируется информация о ресурсах, связанных с 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.**59**), из журнала безопасности или журнала Secret Net Studio (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 файл, в который предварительно были экспортированы сведения из журнала. В локальном режиме источником может быть журнал безопасности или журнал Secret Net Studio.

**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 "OK". 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 "OK".

   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 "OK".

   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 "OK".

   На экране появится диалог настройки.
5. В централизованном режиме нажмите кнопку "Выбрать" и выберите файл, в который предварительно были экспортированы сведения из журнала (в формате snlog или dvt).

В локальном режиме выберите способ (журнал безопасности или журнал Secret Net Studio).

В зависимости от режима и выбранного способа станут доступными настройки фильтра журнала событий.

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

   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.**58**).

## Добавление задач

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

- вручную;
- вручную со сценарием;
- с помощью генератора задач (см. стр.**40**);
- с помощью средств импорта (см. стр.**58**).

**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 "OK".

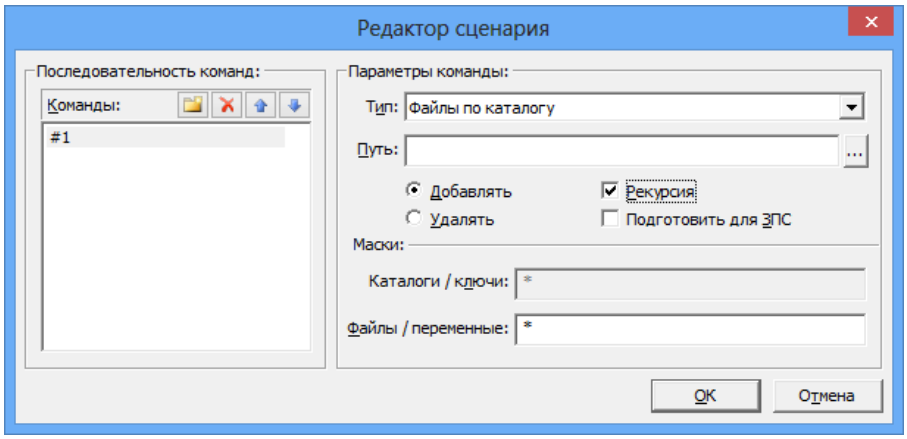
   В модели данных появится новая задача, не связанная с другими объектами.

**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 ресурсов и укажите путь.

   Предусмотренные типы перечислены в следующей таблице.

| Тип ресурсов | 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 Secret Net Studio** | Отбираются ресурсы из состава ПО клиента системы Secret Net Studio |
| **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 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 действия для команды.

   Параметр "Добавлять" используется для добавления отбираемых ресурсов в общий список ресурсов задачи. Параметр "Удалять" — для удаления ресурсов из общего списка, сформированного предыдущими командами.

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

8. Если выбран тип "Файлы по каталогу" или "Каталоги с файлами", при необходимости используйте возможность добавления в список зависимых модулей (см. стр.**75**). Для добавления зависимых модулей установите отметку в поле "Подготовить для ЗПС". В этом случае автоматически будут также выбраны все зависимые модули для файлов, указанных с помощью маски. Они будут добавлены в модель и помечены как исполняемые. То есть результат будет таким же, как при выполнении процедуры поиска и добавления зависимых модулей, но не на данном компьютере, а на всех, где будет выполнен создаваемый сценарий.

9. В зависимости от выбранного типа ресурсов 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 типа ресурсов "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 "OK". Затем нажмите кнопку "OK" в диалоге свойств задачи.

    В основном окне программы появится задача с пиктограммой  .

### Добавление заданий

Процедуры добавления задания подробно описаны на стр.**42**.

### Добавление субъектов

В централизованном режиме в модель данных можно добавлять компьютеры и группы, включающие в себя компьютеры. В локальном режиме добавляются пользователи и группы пользователей. После добавления субъекты отмечены в списке знаком  (как не связанные с другими объектами).

**Для добавления компьютеров (централизованный режим):**

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

   Появится диалог для выбора типа добавляемых субъектов.
3. Установите отметку в поле "Компьютер" и нажмите кнопку "OK".

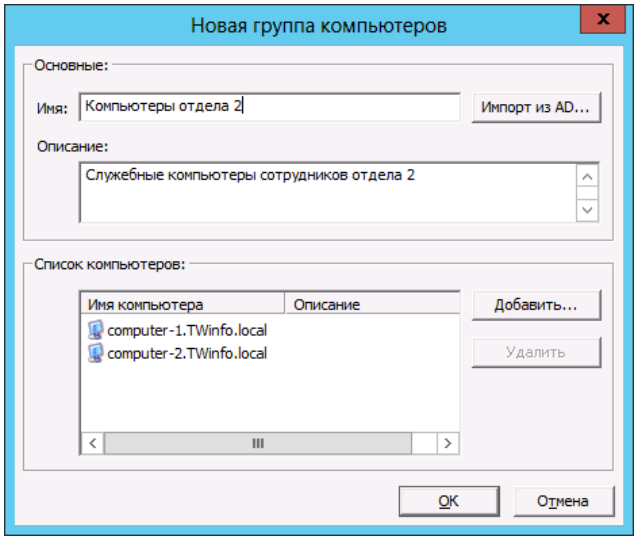
   Появится диалог со списком компьютеров домена безопасности с установленным клиентским ПО Secret Net Studio.
4. Выберите в списке нужные компьютеры и нажмите кнопку "OK".

**Для добавления группы компьютеров (централизованный режим):**

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

   Появится диалог для выбора типа добавляемых субъектов.
3. Установите отметку в поле "Группа компьютеров" и нажмите кнопку "OK".

   Появится диалог для настройки создаваемой группы.




4. Если в Active Directory имеется группа, которая содержит нужные компьютеры для создания группы в модели данных, можно импортировать из AD сведения об этом объекте. Для этого нажмите кнопку "Импорт из AD" и выберите нужную группу компьютеров в появившемся диалоге ОС Windows.
5. Введите имя и дополнительные сведения о создаваемой группе в соответствующих полях.
6. Сформируйте список компьютеров группы. Для добавления и удаления элементов списка используйте кнопки справа.
7. Нажмите кнопку "OK".

**Для добавления пользователей и групп пользователей (локальный режим):**

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

   Появится диалог ОС Windows для выбора пользователей и групп.
3. Найдите и выберите нужные объекты и нажмите кнопку "OK".

## 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 нельзя удалить группу по умолчанию SecretNetICheckDefault или SecretNetICheckDefault64 (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 категории:**

1. Выберите нужную категорию ("Субъекты управления", "Задания", "Задачи" или "Группы ресурсов"), 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 добавить: в задание — задачу, в задачу — группу ресурсов, а в группу — ресурс.

**Для связывания объектов:**

1. Выберите категорию объекта, вызовите контекстное меню для нужного объекта и 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".

## 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

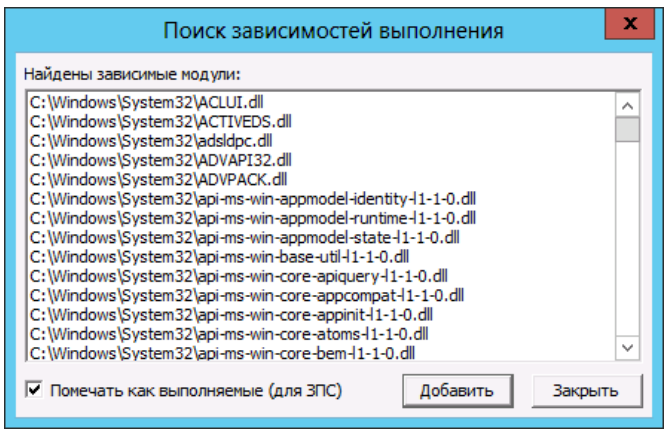
При работе пользователя с приложениями запуск исполняемых файлов может сопровождаться запуском модулей (драйверов и библиотек), не входящих непосредственно в приложения. Такие модули называются зависимыми.

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".

# Глава 4
# Полномочное управление доступом

## Общие сведения о полномочном разграничении доступа

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.

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 Studio 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. **9** ) 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 путем наследования категории родительского каталога. Автоматическое присвоение осуществляется, если для каталога включены признаки "Автоматически присваивать новым каталогам" и/или "Автоматически присваивать новым файлам". При этом возможность изменения признаков доступна пользователю с привилегией на управление категориями конфиденциальности.

## Уровни допуска и привилегии пользователей

### Уровни допуска

Доступ пользователя к конфиденциальной информации осуществляется, 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.**82**.

### Привилегии пользователей

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

| Привилегия | Описание |
|---|---|
| **Управление категориями конфиденциальности** | Пользователь может:<br>• изменять категории конфиденциальности каталогов и файлов в рамках своего уровня допуска;<br>• управлять режимом наследования категорий конфиденциальности каталогов (см. стр.**83**) |
| **Печать конфиденциальных документов** | Используется для разрешения пользователю выводить на принтер конфиденциальные документы. Привилегия применяется при включенном механизме контроля печати |
| **Вывод конфиденциальной информации** | Пользователю разрешается выводить конфиденциальную информацию на внешние носители при включенном режиме контроля потоков. Внешними носителями в системе Secret Net Studio считаются сменные диски, для которых включен режим доступа "без учета категории конфиденциальности" |

Привилегии предоставляются администратором безопасности пользователям, уполномоченным управлять конфиденциальностью ресурсов, распечатывать и копировать конфиденциальную информацию (см. стр.**82**). 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. По умолчанию режим отключен. Для корректной работы системы перед включением режима необходимо выполнить дополнительную настройку. Основные действия для настройки выполняются локально с помощью специальной программы из состава клиентского ПО Secret Net Studio.

### Уровень конфиденциальности сессии

При включенном режиме контроля потоков возможность использования устройств и доступа к конфиденциальным файлам определяется уровнем конфиденциальности сессии, который устанавливается при входе пользователя в систему. Уровень сессии не может быть выше уровня допуска пользователя. Сессия заканчивается вместе с сеансом работы пользователя на компьютере. Уровень сессии нельзя изменить до ее окончания.

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.

Например, пользователь при входе в систему 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.

Из-за особенностей работы в конфиденциальных сессиях все действия, связанные с изменением конфигурации системы, необходимо выполнять в неконфиденциальной сессии или при отключенном режиме контроля потоков. В частности, конфиденциальную сессию нельзя использовать для настройки программного обеспечения, изменения режимов, а также для выполнения первичного входа пользователя на компьютер (когда формируется профиль учетной записи). Уровень конфиденциальности сессии, отличный от неконфиденциального, следует выбирать только для обработки конфиденциальных данных.

### Назначение сессии уровня конфиденциальности

В зависимости от заданных параметров присвоение сессии определенного уровня конфиденциальности может выполняться по выбору пользователя или автоматически системой. Автоматическое назначение уровня выполняется в следующих случаях:

- при включенном параметре "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);
- при включенном параметре "автоматический выбор максимального уровня сессии". Если параметр включен, уровень конфиденциальности сессии принудительно устанавливается равным уровню допуска пользователя.

### Использование устройств и сетевых интерфейсов

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 полномочного разграничения доступа

## 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.**82**).
3. Присвойте ресурсам категории конфиденциальности (см. стр.**83**).
4. Настройте перечень регистрируемых событий (см. стр.**84**).
5. Для добавления маркеров в распечатываемые документы настройте и включите режим маркировки (см. стр.**26**).
6. Для ограничения вывода конфиденциальных документов на печать настройте использование принтеров (см. стр.**84**).
7. Для использования режима контроля потоков настройте и включите режим (см. стр.**84**).

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

Перед началом использования механизма разъясните пользователям правила работы с конфиденциальными ресурсами.

## Настройка категорий конфиденциальности

**Внимание!**

Для компьютеров с клиентом в сетевом режиме функционирования, чтобы избежать конфликтов в названиях категорий конфиденциальности, количество и названия для категорий должны быть заданы в одной общей групповой политике, применяемой на компьютерах. В программе управления рекомендуется настроить одну из следующих групповых политик (перечислены в порядке возрастания приоритета применения параметров):

- политика домена — для всех компьютеров, входящих в домен;
- политика организационного подразделения — для всех компьютеров, входящих в это организационное подразделение;
- политика, заданная для сервера безопасности, — применяется на всех компьютерах, подчиненных этому серверу безопасности.

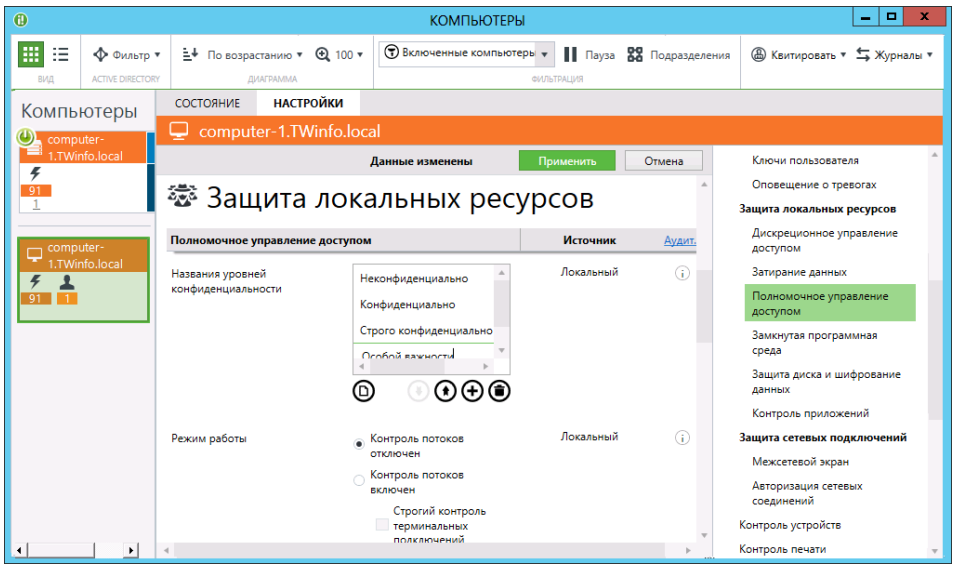
Например, все компьютеры, на которых будет обрабатываться конфиденциальная информация, можно включить в отдельное организационное подразделение и настроить категории в политике для этого подразделения.

Ниже приводится описание процедуры централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для настройки количества и названий категорий конфиденциальности:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Полномочное управление доступом".

   Пример содержимого группы параметров представлен на следующем рисунке.




3. Для параметра "Названия уровней конфиденциальности" сформируйте список категорий конфиденциальности. Для добавления, удаления или перемещения элементов используйте соответствующие кнопки под списком. Чтобы переименовать категорию, наведите на нее указатель и дважды нажмите левую кнопку мыши. При необходимости восстановить исходный набор категорий нажмите кнопку "По умолчанию".

**Примечание.**
Список упорядочен по степени важности категорий с точки зрения конфиденциальности информации. Наименьший уровень (приоритет) имеет первый элемент списка, наибольший уровень — у последнего элемента. 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.

4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

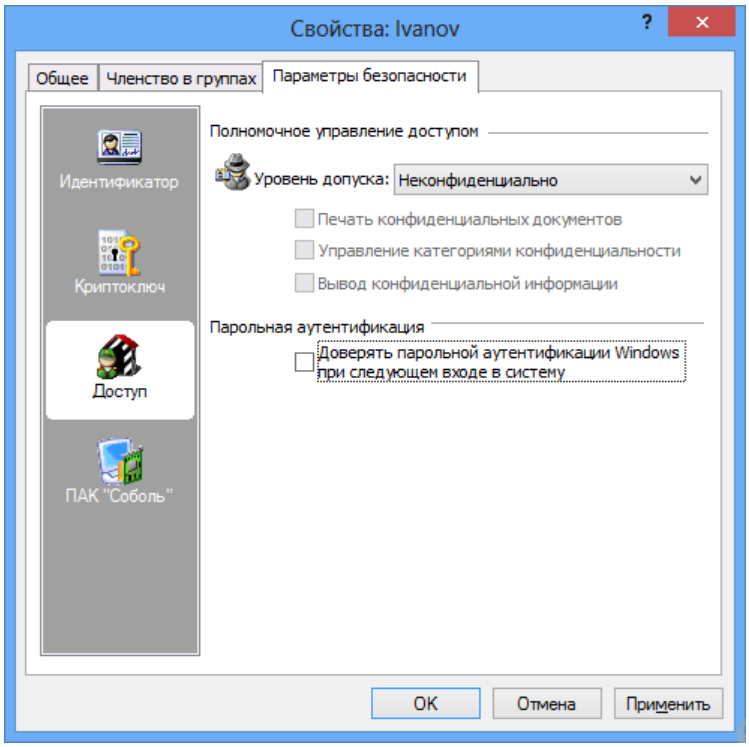
## Назначение уровней допуска и привилегий пользователям

Уровень допуска и привилегии назначаются администратором безопасности каждому пользователю индивидуально.

Привилегию можно предоставить только тем пользователям, которым назначен уровень допуска.

**Для назначения уровня допуска и привилегий:**

1. Запустите программу управления пользователями (см. документ [**3**]).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Параметры безопасности".
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.

### 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. Загрузите список устройств (см. стр.12).
2. Выберите строку с нужным элементом списка (группа, класс, модель или устройство).
3. Укажите нужные параметры в ячейке колонки "Параметры доступа". Для этого нажмите кнопку в правой части ячейки. 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". 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 "Без учета категории".
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

### Присвоение категорий конфиденциальности каталогам и файлам

Присвоение ресурсам категорий конфиденциальности выполняется уполномоченными пользователями, имеющими привилегию "Управление категориями конфиденциальности".

Описание процедур изменения категорий конфиденциальности каталогов и файлов см. в документе [**9**].

**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 непроизвольного 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. Настройка выполняется в программе управления. События, для которых можно включить или отключить регистрацию, представлены на вкладке "Настройки" панели свойств объектов в разделе "Регистрация событий", группа "Полномочное управление доступом". Переход к параметрам регистрации можно выполнить из соответствующей группы параметров в разделе "Политики" (см. стр.**81** ) — для этого используйте ссылку "Аудит" в правой части заголовка группы.

### 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.**23**).

**Для настройки использования принтеров:**

1. Загрузите список принтеров (см. стр.**20**).
2. Выберите строку с нужным элементом списка.
3. Укажите нужные параметры в ячейке колонки "Категории конфиденциальности". Для этого нажмите кнопку в правой части ячейки. Отметьте нужные уровни конфиденциальности.
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

## Дополнительная настройка для работы в режиме контроля потоков

### Рекомендуемый порядок настройки

Для корректного функционирования системы при использовании механизма полномочного управления доступом в режиме контроля потоков рекомендуется выполнить настройку в следующем порядке:

1. Учетной записи администратора безопасности предоставьте возможность управления механизмом полномочного управления доступом. Для этого:
   - назначьте учетной записи наивысший уровень допуска к конфиденциальной информации и предоставьте привилегию "Управление категориями конфиденциальности" (см. стр.**82**);
   - включите администратора безопасности в локальные группы администраторов компьютеров.
2. На каждом компьютере выполните следующие действия:
   - создайте профили всех пользователей, которые будут работать на компьютере. Профиль пользователя автоматически формируется операционной системой при первом входе в систему (если ранее пользователь не выполнял вход на данном компьютере);
   - выполните запуск приложений, которые будут использоваться, и настройте параметры работы приложений;
   - запустите программу настройки для режима контроля потоков (см. стр.**85**), включите режим автоматической настройки для нужных приложений и выполните автоматическую настройку.
3. Укажите уровни конфиденциальности для сетевых интерфейсов (см. стр.**86**).

4. Включите режим контроля потоков (см. стр.**86**).
5. Проверьте на компьютерах корректность функционирования приложений в конфиденциальных сессиях. При возникновении ошибок выполните действия для настройки совместного функционирования с прикладным ПО (см. стр.**87**).

## Программа настройки для режима контроля потоков

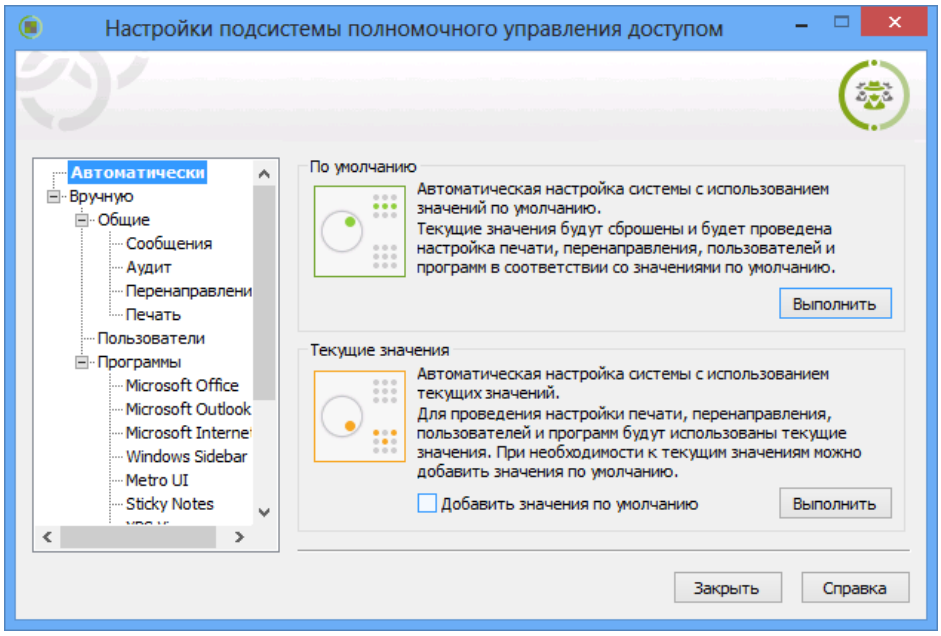
Чтобы обеспечить функционирование механизма полномочного управления доступом при включенном режиме контроля потоков, требуется выполнить дополнительную настройку локально на компьютере. Для этого используется программа настройки подсистемы полномочного управления доступом для режима контроля потоков (далее — программа настройки для режима контроля потоков, программа настройки). Настройка выполняется перед включением режима контроля потоков, а также в процессе эксплуатации системы при добавлении новых пользователей, программ, принтеров, для оптимизации функционирования 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".

**Примечание.**
Запуск программы невозможен в следующих случаях:
- если текущий пользователь не входит в локальную группу администраторов;
- если механизм полномочного управления доступом отключен.

Пример содержимого окна программы представлен на следующем рисунке.




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.

В программе реализованы средства как для автоматической настройки, так и для конфигурирования вручную. При автоматической настройке выполняется базовый набор действий, после которых обеспечивается функционирование механизма и совместимость со стандартным и наиболее распространенным программным обеспечением. Средства запуска автоматической настройки представлены в окне программы по умолчанию. Настройка вручную предусмотрена для выполнения специфических действий — например, чтобы обеспечить совместную работу с ПО, которое не входит в список для автоматической настройки.

Подробные сведения о работе с программой приведены в приложении на стр.**114**.

## 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. Загрузите список устройств (см. стр.**12**).
2. В группе "Сеть" выберите строку с нужным элементом списка (группа, класс или сетевой интерфейс).
3. Укажите нужные параметры в ячейке колонки "Параметры доступа". Для этого нажмите кнопку в правой части ячейки. 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". Отметьте нужные уровни конфиденциальности. Если устройство должно функционировать независимо от уровня конфиденциальности сессии, удалите отметки для всех уровней.
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

## Включение и отключение режима контроля потоков

Ниже приводятся описания процедур централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для включения режима контроля потоков:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Полномочное управление доступом".
3. Для параметра "Режим работы" установите отметку в поле "Контроль потоков включен" и 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.

4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

**Для отключения режима контроля потоков:**

1. Выполните вход в систему в неконфиденциальной сессии.
2. Выполните действия **1**–**2** вышеописанной процедуры.
3. Для параметра "Режим работы" установите отметку в поле "Контроль потоков отключен".
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

## Порядок настройки совместного функционирования с прикладным ПО

При работе механизма полномочного управления доступом в режиме контроля потоков могут происходить сбои запуска или функционирования некоторых приложений прикладного программного обеспечения. Если сбои проявляются только при работе с приложением в конфиденциальных сессиях (с уровнем выше, чем "Неконфиденциально"), это может происходить по причине запрета обращения к файлам приложения со стороны механизма.

Чтобы обеспечить корректную работу приложений, для режима контроля потоков предусмотрена функция перенаправления вывода служебных файлов. Для применения функции создаются копии отдельных служебных каталогов приложений с различными категориями конфиденциальности. В зависимости от уровня конфиденциальности сессии файловые операции прикладного ПО автоматически перенаправляются в каталог-копию с соответствующей категорией конфиденциальности. Таким образом, для приложения реализуется возможность работы со служебными каталогами, и при этом данные сохраняются с нужной категорией конфиденциальности.

Если после включения режима контроля потоков приложение перестает корректно функционировать, выполните следующие действия для диагностики и настройки совместного функционирования:

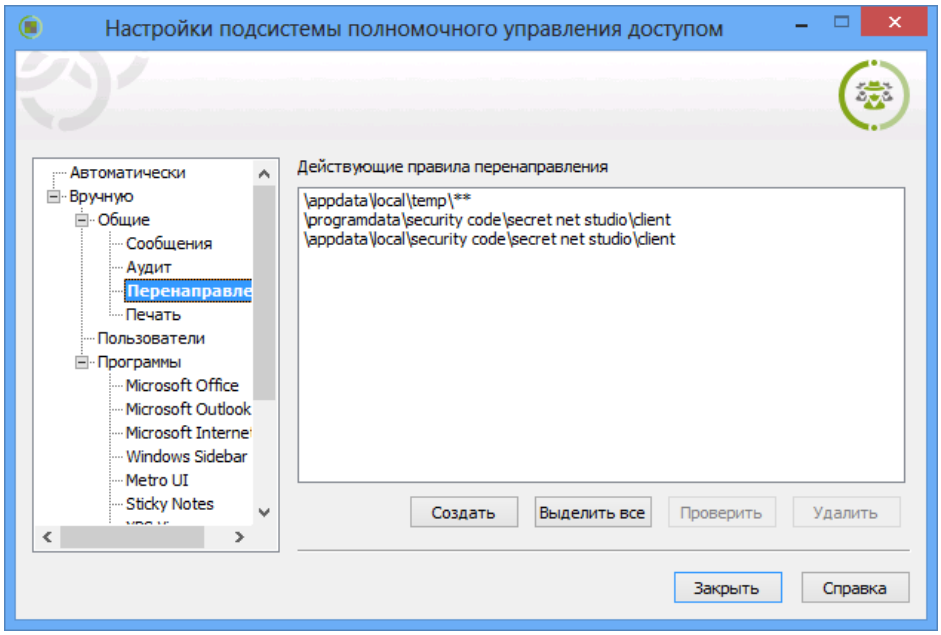
1. Проверьте наличие готового шаблона настройки для работы данного приложения. Для этого запустите программу настройки (см. стр. **85**) и перейдите к разделу "Вручную | Программы". Если приложение присутствует в списке, включите для него режим автоматической настройки и затем выполните автоматическую настройку с текущими значениями параметров. При отсутствии приложения перейдите к следующим действиям для диагностики и настройки.

> **Примечание.**
> Список приложений в программе настройки предназначен для применения готовых шаблонов настройки совместной работы. По умолчанию режим автоматической настройки отключен для большинства элементов списка (например, для ПО AutoCAD, Photoshop и др.). Поэтому для применения шаблона данный режим необходимо включить. Подробные сведения о работе с программой приведены в приложении на стр. **114**.

2. Выполните вход в систему с отключенным режимом контроля потоков или в неконфиденциальной сессии. Запустите программу управления в локальном режиме и выполните очистку локального журнала Secret Net Studio.
3. Завершите сеанс, включите режим контроля потоков и выполните вход в конфиденциальной сессии.
4. Запустите приложение. Если запуск выполняется успешно, воспроизведите действия, которые приводят к ошибкам в работе ПО.
5. Завершите сеанс, выполните вход в неконфиденциальной сессии и отключите режим контроля потоков.
6. Запустите программу управления в локальном режиме и загрузите записи журнала Secret Net Studio. Найдите записи о событиях запрета доступа категории "Полномочное управление доступом". В дополнительных описаниях событий определите процессы, относящиеся к приложению, и пути, по которым выполнялись обращения.
7. Проанализируйте полученные пути и по возможности классифицируйте их, исходя из назначения каталогов. Каталоги, в которых могут происходить сбои при обращении к файлам:

| **Каталоги с документами пользователей** |
|---|
| В каталогах хранятся файлы рабочих документов пользователей. Например, каталог \Documents в профиле пользователя.<br>Вероятные причины запрета доступа — не соблюдаются общие рекомендации по присвоению категорий каталогам и файлам (см. стр.**83**) или действуют правила работы с конфиденциальными ресурсами (см. стр.**90**).<br>Применять перенаправление для таких каталогов не рекомендуется. Для обеспечения доступа следует установить корректные категории конфиденциальности ресурсов (обеспечить соответствие категорий каталогов и хранящихся в них файлов) |
| **Каталоги временных данных приложения** |
| Каталоги используются приложением для записи и чтения временных данных в течение одного сеанса работы. После завершения сеанса созданные файлы, как правило, удаляются.<br>Вероятная причина запрета доступа — произошла попытка создания файла в каталоге, для которого установлена категория конфиденциальности ниже, чем уровень сессии.<br>В большинстве случаев перенаправление для таких каталогов не требуется. Достаточно установить максимальную категорию конфиденциальности без автоматического присвоения категории для создаваемых объектов. За счет этого приложению будет разрешено создание файлов в сессиях любых уровней конфиденциальности |
| **Каталоги с параметрами настройки приложения** |
| В каталогах хранятся конфигурационные файлы, которые формируются приложением при первом запуске и настройке и в дальнейшем не изменяются при обычной работе приложения. Доступ к таким файлам во всех следующих сеансах осуществляется только на чтение для загрузки параметров приложения.<br>Вероятная причина запрета доступа — произошла попытка создания или модификации конфигурационных файлов в каталоге, который был создан при настройке параметров приложения.<br>В большинстве случаев перенаправление для таких каталогов не требуется. При необходимости изменить конфигурационные файлы выполните настройку приложения в неконфиденциальной сессии |
| **Каталоги с рабочими данными приложения** |
| Каталоги используются приложением для записи и чтения служебных данных в каждом сеансе работы. Файлы не удаляются после завершения сеанса и могут перезаписываться в следующих сеансах.<br>Корректная работа с файлами в таких каталогах обеспечивается с помощью функции перенаправления (см. ниже) |

**8.** Для создания правил перенаправления запустите программу настройки и перейдите к разделу "Вручную | Общие | Перенаправление".




Добавление правил осуществляется с помощью кнопки "Создать". Каждое правило перенаправления должно содержать часть пути, которая идентифицирует перенаправляемые каталоги. Например, значение \AppData\Local\Temp** соответствует временному каталогу в профиле пользователя. Каталоги, у которых часть пути совпадает с указанным значением, будут перенаправляться в конфиденциальных сессиях. В приведенном примере правило обеспечивает перенаправление временных каталогов (со всеми подкаталогами) всех пользователей компьютера.

**Рекомендации для формирования списка правил перенаправления**

- По возможности избегайте копирования больших объемов данных из исходных каталогов в каталоги перенаправления. При настройке функции перенаправления из исходных каталогов вместо дублирования всего содержимого можно копировать только подкаталоги без файлов или только вложенные файлы без каталогов. Такое копирование осуществляется, если в правиле перенаправления в конце пути указана шаблонная подстрока "**" (с двумя символами "звездочка") или "*" (с одним символом "звездочка") соответственно.
- Часть пути в правиле перенаправления следует задать с оптимальной точностью для идентификации каталогов. Обычно достаточно указать каталоги двух- трех уровней вложенности. Слишком короткая часть пути может привести к перенаправлению каталогов, не относящихся к нужному приложению. Излишне подробное значение может вызвать необходимость создания отдельных правил (например, для каждого пользователя). Это усложнит настройку, а также повлияет на скорость обработки данных подсистемой.

**9.** Включите режим контроля потоков, выполните вход в конфиденциальной сессии и убедитесь в корректном функционировании приложения. Если данное приложение будет использоваться на других компьютерах с включенным режимом контроля потоков, выполните локальную настройку использования тех же каталогов (см. действия **7**–**8**).

# 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.

<table>
<tr><th>Без контроля потоков</th><th>При контроле потоков</th></tr>
<tr><td colspan="2">Доступ к устройствам</td></tr>
<tr><td>Запрещен вход пользователя в систему, если подключены устройства с категорией конфиденциальности выше, чем уровень допуска пользователя</td><td>Запрещен вход пользователя в систему, если подключены устройства:<ul><li>с категорией конфиденциальности выше, чем уровень допуска пользователя;</li><li>с различными категориями конфиденциальности;</li><li>с категорией конфиденциальности выше, чем категория "неконфиденциально", при первом входе пользователя на данном компьютере (конфигурационный вход)</li></ul></td></tr>
<tr><td>Запрещено подключение устройства, если его категория конфиденциальности выше, чем уровень допуска работающего пользователя</td><td>Запрещено подключение устройства, если его категория конфиденциальности отличается от уровня сессии работающего пользователя</td></tr>
<tr><td>Разрешено функционирование всех сетевых интерфейсов</td><td>Запрещено использование сетевых интерфейсов, для которых текущий уровень конфиденциальности сессии не указан в списке разрешенных уровней</td></tr>
<tr><td colspan="2">Отсутствуют ограничения по доступу к устройствам, для которых включен режим доступа "без учета категории конфиденциальности"</td></tr>
<tr><td colspan="2">Доступ к файлам</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">Запрещен доступ к файлу, если его категория конфиденциальности выше, чем заданная категория для устройства, содержащего файл</td></tr>
<tr><td>Доступ пользователя к файлу разрешается, если уровень допуска пользователя не ниже категории конфиденциальности файла</td><td>Доступ пользователя к файлу разрешается, если уровень конфиденциальности пользовательской сессии не ниже категории конфиденциальности файла</td></tr>
<tr><td>Запрещено удаление конфиденциального файла с помещением в "Корзину"</td><td>Запрещено удаление любого файла с помещением в "Корзину"</td></tr>
<tr><td colspan="2">Доступ к каталогам</td></tr>
<tr><td colspan="2">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</td></tr>
<tr><td colspan="2">Запрещен доступ к каталогу, если его категория конфиденциальности выше, чем заданная категория для устройства, содержащего каталог</td></tr>
<tr><td colspan="2">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"</td></tr>
</table>

| 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.<br>Ограничение: устанавливаемая категория конфиденциальности должна быть равна текущему уровню конфиденциальности сессии |
| Если отключен режим автоматического присвоения категории конфиденциальности:<br>• при создании, сохранении или копировании подкаталогу/файлу присваивается категория "неконфиденциально";<br>• 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 | Если отключен режим автоматического присвоения категории конфиденциальности:<br>• при создании, сохранении или копировании подкаталогу/файлу присваивается категория, соответствующая уровню конфиденциальности сессии, но не выше категории конфиденциальности каталога;<br>• 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 конфиденциальности | |
| **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:<br>• повысить категорию конфиденциальности каталогов и файлов, но не выше уровня допуска пользователя;<br>• понизить категорию конфиденциальности каталогов и файлов, текущая категория конфиденциальности которых не выше уровня допуска пользователя;<br>• 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:<br>• повысить категорию конфиденциальности каталогов и файлов, но не выше текущего уровня сессии;<br>• понизить категорию конфиденциальности каталогов и файлов, текущая категория конфиденциальности которых не выше текущего уровня сессии;<br>• изменять состояние режима автоматического присвоения категории конфиденциальности каталога, если текущая категория конфиденциальности каталога не выше текущего уровня сессии |
| **Печать конфиденциальных документов** | |
| Если включен механизм контроля печати:<br>• пользователь, **не** обладающий привилегией "Печать конфиденциальных документов", может распечатывать только неконфиденциальные документы;<br>• пользователь, обладающий привилегией "Печать конфиденциальных документов", может распечатывать конфиденциальные документы с категорией конфиденциальности, не превышающей уровень допуска пользователя | Если включен механизм контроля печати:<br>• пользователь, **не** обладающий привилегией "Печать конфиденциальных документов", может распечатывать только неконфиденциальные документы (при условии, что документ не редактировался);<br>• пользователь, обладающий привилегией "Печать конфиденциальных документов", может распечатывать конфиденциальные документы с категорией конфиденциальности, не превышающей текущий уровень сессии |
| Если отключен механизм контроля печати, 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 | |
| **Вывод на внешние носители** | |

| Без контроля потоков | При контроле потоков |
|---|---|
| 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. Внешними носителями в системе Secret Net Studio считаются сменные диски, для которых включен режим доступа "без учета категории конфиденциальности" |

# Глава 5
# Настройка защиты хранимых данных

## 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 "Управление правами доступа". Привилегия, в частности, позволяет назначить администраторов ресуров, 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.

Ниже приводится описание процедуры централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для предоставления привилегии:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Дискреционное управление доступом".
3. Для параметра "Учетные записи с привилегией управления правами доступа" отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия.
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

### 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 [**9**].

### 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. Настройка выполняется в программе управления. События, для которых можно включить или отключить регистрацию, представлены на вкладке "Настройки" панели свойств объектов в разделе "Регистрация событий", группа "Дискреционное управление доступом". Переход к параметрам регистрации можно выполнить из соответствующей группы параметров в разделе "Политики" (см. стр.**94** ) — для этого используйте ссылку "Аудит" в правой части заголовка группы.

### 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 [**9**].

## Затирание удаляемой информации

Система Secret Net Studio может выполнять затирание областей памяти, в которых остаются данные от удаленных объектов. Это предотвращает возможность восстановления данных после удаления и обеспечивает безопасность повторного использования носителей информации. Затирание может выполняться автоматически на устройствах определенных типов (локальные и сменные диски, оперативная память) или для файловых объектов, выбранных пользователем.

**Внимание!**

Затирание файла подкачки виртуальной памяти выполняется стандартными средствами ОС Windows при выключении компьютера. Если в Secret Net Studio включен режим затирания оперативной памяти, рекомендуется дополнительно включить действие стандартного параметра безопасности Windows "Завершение работы: очистка файла подкачки виртуальной памяти".

Не осуществляется затирание файлов при их перемещении в папку "Корзина", так как во время нахождения в этой папке файлы не удаляются с диска. Затирание таких файлов происходит после очистки содержимого "Корзины".

Ниже приводится описание процедуры централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для настройки механизма:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Затирание данных".
3. Укажите нужные значения для параметров затирания:
   - "Количество циклов затирания на локальных дисках";
   - "Количество циклов затирания на сменных носителях";
   - "Количество циклов затирания оперативной памяти";
   - "Количество циклов затирания по команде "Удалить безвозвратно".

   **Примечание.**

   Если параметру присвоено значение "0", затирание не выполняется. Для гарантированного уничтожения данных в большинстве случаев достаточно двух проходов затирания.
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

# 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 Studio. Все другие способы загрузки ОС считаются несанкционированными с точки зрения функционирования механизма (например, загрузка с внешнего носителя или загрузка другой ОС, установленной на компьютере).

Процедура настройки механизма защиты дисков состоит из следующих этапов:

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

## Включение механизма защиты дисков

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

При включении механизма 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.

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.

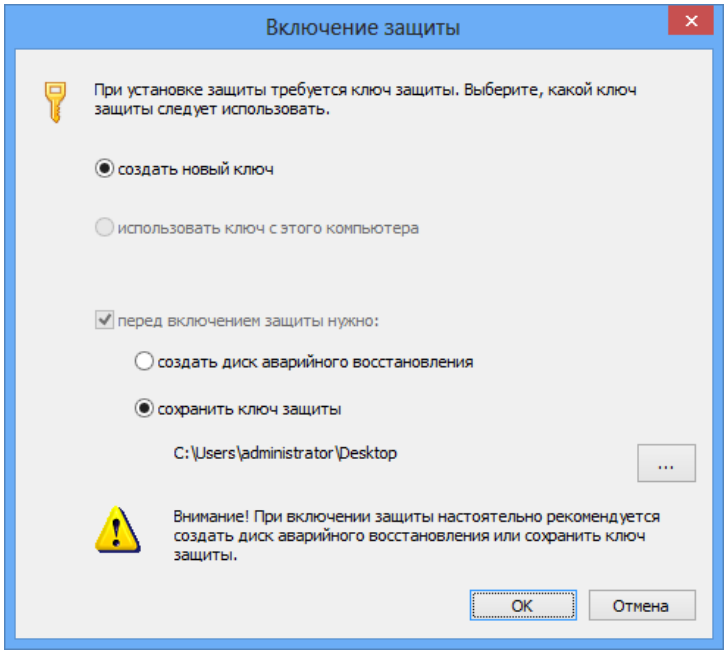
**Внимание!**
Если системный диск (физический диск, с которого выполняется загрузка ОС) использует основную загрузочную запись (Master Boot Record — MBR), в настройках BIOS компьютера должна быть отключена функция проверки загрузочных вирусов. Для отключения функции установите значение "Disabled" для параметра "Boot Virus Detection" (наличие данной функции и название параметра зависит от используемой версии BIOS).

**Для включения механизма защиты дисков:**

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

   На экране появится одноименное диалоговое окно.
2. Перейдите к диалогу "Защита диска" и нажмите кнопку "Включить защиту". Если на компьютере установлен ПАК "Соболь", на экране появится запрос на продолжение операции. Нажмите кнопку "Да" в диалоге запроса.

   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 и дождитесь завершения процесса загрузки ОС.

**Примечание.**
Если на компьютере установлен ПАК "Соболь", в котором включен контроль целостности физических секторов жесткого диска, после включения механизма защиты дисков ПАК "Соболь" может зафиксировать нарушение целостности загрузочного сектора. В этом случае для устранения ошибок КЦ необходимо средствами ПАК "Соболь" выполнить новый расчет эталонных значений.

### 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.**125**).

**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.

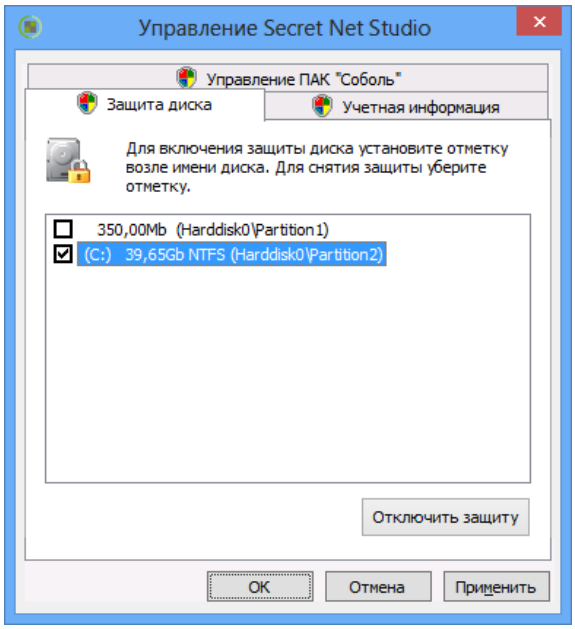
Механизм обеспечивает защиту до 128 логических разделов при общем количестве физических дисков до 32. Логические разделы, для которых устанавливается режим защиты, должны иметь файловую систему FAT, NTFS или ReFS. Поддерживаются физические диски с основной загрузочной записью (MBR) или с таблицей разделов 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 Studio".

   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 "OK" и перезагрузите компьютер.

## Отключение механизма защиты дисков

При отключении механизма защиты дисков происходит снятие защиты со всех логических разделов и возвращение первоначального состояния загрузочной области 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 Studio".

   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.

# Шифрование данных в криптоконтейнерах

## Предоставление привилегии для создания криптоконтейнеров

В механизме шифрования данных в криптоконтейнерах создание криптоконтейнеров доступно пользователям, которым предоставлена привилегия "Создание криптоконтейнера".

По умолчанию привилегией на создание криптоконтейнеров обладают пользователи, входящие в локальную группу администраторов и в группу "Пользователи".

Ниже приводится описание процедуры централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для предоставления привилегии:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Защита диска и шифрование данных".
3. Для параметра "Учетные записи с привилегией на создание криптоконтейнера" отредактируйте список пользователей и групп пользователей, которым предоставлена привилегия.
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

## Настройка регистрации событий

Для отслеживания произошедших событий, связанных с работой механизма шифрования данных в криптоконтейнерах, необходимо выполнить настройку регистрации событий. Настройка выполняется в программе управления. События, для которых можно включить или отключить регистрацию, представлены на вкладке "Настройки" панели свойств объектов в разделе "Регистрация событий", группа "Защита диска и шифрование данных". Переход к параметрам регистрации можно выполнить из соответствующей группы параметров в разделе "Политики" (см. выше) — для этого используйте ссылку "Аудит" в правой части заголовка группы.

## Управление криптографическими ключами пользователей

Для работы с зашифрованными данными в криптоконтейнерах пользователям необходимо загружать криптографические ключи (ключевую информацию) со своих ключевых носителей. Ключевая информация может храниться в присвоенном пользователю персональном идентификаторе или сменном носителе.

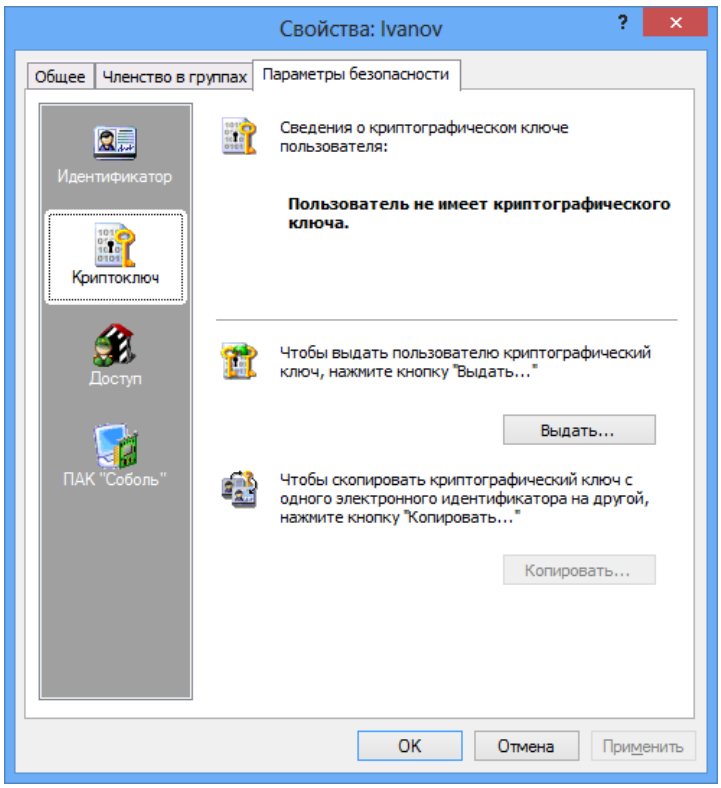
### Выдача и смена ключей

Генерация ключевой информации и запись закрытого ключа на ключевой носитель может выполняться при присвоении пользователю персонального идентификатора. Описание процедуры присвоения см. в документе [**3**]. Если пользователю присвоен идентификатор, но ключевая информация не была сгенерирована или требуется сменить имеющиеся ключи, администратор может выполнить процедуру выдачи/смены ключей.

**Для выдачи/смены ключей:**

1. Запустите программу управления пользователями (см. документ [**3**]).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Параметры безопасности".
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"). Кнопка активна, если пользователю присвоен хотя бы один идентификаторр.

   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, содержащий старый закрытый ключ данного пользователя.

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

**Примечание.**
Продолжение процедуры без устранения ошибки невозможно.

7. Если возникла ошибка, нажмите кнопку "Повторить" для повторного выполнения операции. После устранения ошибки 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 "Закрыть".

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 возникли. Для этого нажмите кнопку "< Назад" и повторно выполните операцию. После устранения ошибок нажмите кнопку "Готово".

**Внимание!**

Настоятельно рекомендуется исправлять ошибки, произошедшие при записи ключей в идентификаторы. После успешного завершения всех предусмотренных операций для каждой из них должно быть указано состояние "Выполнено".

### Копирование ключей

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

**Для копирования ключей:**

1. Запустите программу управления пользователями (см. документ [**3**]).
2. Вызовите окно настройки свойств пользователя и перейдите к диалогу "Параметры безопасности".
3. В панели выбора групп параметров выберите группу "Криптоключ".
4. Нажмите кнопку "Копировать". Кнопка активна, если пользователю присвоены хотя бы два идентификатора.

   На экране появится диалог "Предъявите идентификатор".

5. Предъявите идентификатор, 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 Studio:

- 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 [**9**]). Смена ключевой информации самим пользователем возможна только по истечении минимального срока действия ключа.

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

Ниже приводится описание процедуры централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для настройки параметров:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Ключи пользователя".
3. Укажите нужные значения для параметров "Максимальный срок действия ключа", "Минимальный срок действия ключа" и "Предупреждение об истечении срока действия ключа".

   **Примечание.**
   Если установлено нулевое значение, параметр не применяется.

4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

# Глава 6
# Особенности настройки для защиты терминальных подключений

## Использование идентификаторов в терминальных сессиях

Присвоенные пользователям персональные идентификаторы могут использоваться для терминального входа в подключениях удаленного доступа. Для этого на компьютере, который является терминальным сервером, должен быть включен любой из следующих режимов идентификации (см. документ [**3**]):

- "Смешанный" (включен по умолчанию);
- "Только по идентификатору".

При этом в средствах подключения к удаленному рабочему столу (Remote Desktop Connection) версии 6.0 и выше (в составе ОС Windows 7 и выше) по умолчанию требуется предварительная аутентификация пользователя. Предварительная аутентификация осуществляется путем ввода учетных данных пользователя (имя и пароль) до подключения к терминальному серверу. Из-за этого проявляются следующие особенности установки соединения:

- Если на терминальном сервере включен режим идентификации "Смешанный" — после предварительной аутентификации на терминальном клиенте сразу осуществляется терминальный вход по указанным учетным данным пользователя. Терминальный сервер не ожидает предъявление идентификатора.
- Если на терминальном сервере включен режим идентификации "Только по идентификатору" — при удаленном подключении сначала выполняется предварительная аутентификация (пользователь вводит имя и пароль для инициирования подключения), а затем при соединении с терминальным сервером пользователю необходимо предъявить свой персональный идентификатор.

При отключенной предварительной аутентификации обеспечивается вход пользователя в терминальную сессию по идентификатору без предварительного запроса имени и пароля.

### Отключение предварительной аутентификации

Требование предварительной аутентификации в средствах подключения к удаленному рабочему столу может действовать как на стороне терминального клиента, так и на стороне терминального сервера. Если запрос учетных данных пользователя отключен на стороне клиента, терминальный вход с этого компьютера будет возможен только на сервер с отключенным требованием предварительной аутентификации. При отключении требования на терминальном сервере удаленные подключения разрешаются для любых клиентов — и с включенной, и с отключенной предварительной аутентификацией.

#### Отключение на терминальном клиенте

Отключение предварительной аутентификации на стороне терминального клиента предусмотрено в средствах подключения к удаленному рабочему столу версии 6.0 и выше. Средства указанных версий установлены по умолчанию в ОС Windows 7 и выше. Для получения сведений об используемой версии вызовите контекстное меню заголовка окна "Подключение к удаленному рабочему столу" (Remote Desktop Connection) и активируйте команду "О программе" (About).

**Для отключения предварительной аутентификации на стороне терминального клиента:**

1. Войдите в систему с учетными данными пользователя, который будет открывать терминальные сессии на этом компьютере.
2. В текстовом редакторе (например, Блокнот) загрузите файл Default.rdp из папки документов пользователя.

   **Пояснения.**
   Файл Default.rdp является скрытым системным файлом. Он автоматически создается в системной папке документов пользователя (%USERPROFILE%\Documents или %USERPROFILE%\My Documents) после первого терминального входа с этого компьютера и далее обновляется при изменении параметров подключения.
   Чтобы загрузить файл, в стандартном диалоге открытия файлов выберите системную папку документов (ярлык папки присутствует в левой части диалога) и в поле ввода имени файла введите Default.rdp.
3. Проверьте в тексте наличие строки с параметром enablecredsspsupport. Если параметр отсутствует, добавьте строку:

   enablecredsspsupport:i:0

   **Примечание.**
   При наличии указанного параметра проверьте заданное значение и при необходимости отредактируйте его.
4. Сохраните изменения.

### Отключение на терминальном сервере

**Для отключения предварительной аутентификации на стороне терминального сервера:**

1. В Панели управления Windows перейдите к разделу "Система" (System) и в левой части окна выберите ссылку "Настройка удаленного доступа" (Remote settings).

   На экране появится диалоговое окно настройки свойств системы, в котором будет открыта вкладка с параметрами удаленного доступа.
2. Удалите отметку из поля, разрешающего подключения только с проверкой подлинности на уровне сети ("с сетевой проверкой подлинности", with Network Level Authentication). Для этого отметьте поле "Разрешить удаленные подключения к этому компьютеру" ("Разрешать подключения от компьютеров с любой версией удаленного рабочего стола", Allow connections from computers running any version of Remote Desktop).

   **Примечание.**
   Изменение поля, разрешающего подключения только с проверкой подлинности на уровне сети, может быть заблокировано действующей групповой политикой. В этом случае откройте соответствующую оснастку управления групповыми политиками и измените состояние параметра "Требовать проверку подлинности пользователя для удаленных подключений путем проверки подлинности на уровне сети" (Require user authentication for remote connections by using Network Level Authentication). Параметр представлен в группе политик конфигурации компьютера, раздел "Административные шаблоны / Компоненты Windows / Службы удаленных рабочих столов / Узел сеансов удаленных рабочих столов / Безопасность" (Administrative Templates / Windows Components / Remote Desktop Services / Remote Desktop Session Host / Security).
3. Закройте диалоговое окно с сохранением сделанных изменений.

### Программные методы обработки идентификаторов

В терминальных сессиях могут применяться различные методы обработки персональных идентификаторов, подключенных на терминальных клиентах. Предусмотрены следующие методы (перечислены в порядке приоритета использования):

1. Метод виртуальных каналов. Применяется в случае, если на терминальном клиенте установлено ПО клиента Secret Net Studio или СЗИ Secret Net, начиная с версии 7.0. Метод не требует дополнительной настройки и доступен всегда (не отключается).
2. Метод на базе протокола RPC (Remote Procedure Call). Применяется в случае, если на терминальном клиенте установлено ПО клиента Secret Net Studio или СЗИ Secret Net, начиная с версии 5.0. Для использования требуется дополнительная настройка TCP-портов для сетевых соединений (см. документ [**3**]). Данный метод по умолчанию отключен. Для включения метода необходимо на компьютере терминального сервера в ключе системного реестра HKLM\Software\Infosec\Secret Net 5\HwSystem указать нулевое значение для параметра NoRemoteConnect.
3. Метод с использованием режима "Смарт-карты". Применяется в случае отсутствия установленного клиентского ПО на терминальном клиенте. Для использования метода необходимо включать режим "Смарт-карты" в параметрах удаленного подключения. Чтобы заблокировать возможность использования метода, в системном реестре терминального сервера в ключе HKLM\Software\Infosec\Secret Net 5\HwSystem создайте параметр NoSCRedirection типа REG_DWORD со значением 1.

## Ограничение использования локальных устройств и ресурсов

Система Secret Net Studio предоставляет возможность заблокировать использование (перенаправление) локальных устройств и ресурсов компьютеров в терминальных подключениях по протоколу Remote Desktop Protocol (RDP). Блокировка осуществляется при включении запрета перенаправления определенных типов локальных устройств и ресурсов. Если в системе Secret Net Studio включен запрет перенаправления, пользователи не смогут использовать соответствующие локальные устройства и ресурсы своих компьютеров в терминальных сессиях (независимо от заданных параметров удаленного подключения).

Запрет перенаправления может действовать в зависимости от роли компьютера в удаленном подключении. Использование устройств и ресурсов можно блокировать на стороне терминального сервера (чтобы запрет действовал для всех "входящих" терминальных сессий), на стороне терминального клиента (для всех "исходящих" сессий) или независимо от роли компьютера в удаленном подключении.

### Управление перенаправлением буфера обмена

По умолчанию перенаправление буфера обмена в терминальных подключениях не запрещается. В удаленных сеансах действуют параметры использования буфера обмена, заданные в соответствии со стандартными политиками перенаправления в ОС Windows.

Ниже приводится описание процедуры централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для включения и отключения запрета перенаправления буфера обмена:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели

свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.

2. В разделе "Политики" перейдите к группе параметров "Контроль приложений".
3. Для параметра "Перенаправление буфера обмена в RDP-подключениях" выберите нужное значение в раскрывающемся списке:
   - "Разрешено" — пользователям предоставляется возможность самостоятельно настраивать использование буфера обмена в параметрах удаленного подключения. При этом возможность настройки присутствует независимо от того, какие параметры заданы в стандартных политиках ОС Windows;
   - "Запрещено подключать удаленные буферы обмена к компьютеру" — блокирует использование буфера обмена на стороне терминального сервера (запрет действует для всех "входящих" терминальных сессий);
   - "Запрещено использовать буфер обмена компьютера удаленно" — блокирует использование буфера обмена на стороне терминального клиента (запрет действует для всех "исходящих" терминальных сессий);
   - "Запрещено" — блокирует перенаправление буфера обмена независимо от роли компьютера в удаленном подключении (терминальный клиент или сервер);
   - "Определяется политиками Windows" — пользователи могут настраивать использование буфера обмена в параметрах удаленного подключения, если эти действия разрешены в стандартных политиках перенаправления в ОС Windows.
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

## Управление перенаправлением локальных устройств терминального клиента

Управление перенаправлением предусмотрено для локальных устройств следующих типов подключения:

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

По умолчанию перенаправление локальных устройств, подключаемых к компьютеру терминального клиента, не запрещается. В удаленных сеансах действуют параметры использования портов, дисков и других устройств Plug and Play, заданные в соответствии со стандартными политиками перенаправления в ОС Windows.

Ниже приводится описание процедуры централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для включения и отключения запрета перенаправления локальных устройств:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль устройств / Настройки".

3. Для параметра "Перенаправление устройств в RDP-подключениях" выберите нужное значение в раскрывающемся списке каждого типа подключения устройств:
   - "Разрешено" — пользователям предоставляется возможность самостоятельно настраивать использование устройств в параметрах удаленного подключения. При этом возможность настройки присутствует независимо от того, какие параметры заданы в стандартных политиках ОС Windows;
   - "Запрещено подключать удаленные устройства к компьютеру" — блокирует использование устройств на стороне терминального сервера (запрет действует для всех "входящих" терминальных сессий);
   - "Запрещено использовать устройства компьютера удаленно" — блокирует использование устройств на стороне терминального клиента (запрет действует для всех "исходящих" терминальных сессий);
   - "Запрещено" — блокирует перенаправление устройств независимо от роли компьютера в удаленном подключении (терминальный клиент или сервер);
   - "Определяется политиками Windows" — пользователи могут настраивать использование устройств в параметрах удаленного подключения, если эти действия разрешены в стандартных политиках перенаправления в ОС Windows.

   **Примечание.**
   Запрет перенаправления устройств Plug and Play поддерживается только на стороне терминального сервера ("Запрещено подключать удаленные устройства к компьютеру").
4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

## Управление перенаправлением принтеров

По умолчанию перенаправление принтеров, установленных на компьютере терминального клиента, не запрещается. В удаленных сеансах действуют параметры использования принтеров, заданные в соответствии со стандартными политиками перенаправления в ОС Windows.

Ниже приводится описание процедуры централизованной настройки при работе с программой управления в централизованном режиме. Локальная настройка выполняется аналогично с использованием программы управления в локальном режиме. Сведения об использовании программы управления см. в документе [**4**].

**Для включения и отключения запрета перенаправления принтеров:**

1. В программе управления откройте панель "Компьютеры" и выберите объект, для которого необходимо настроить параметры. Включите отображение панели свойств с помощью команды в контекстном меню объекта. В панели свойств перейдите на вкладку "Настройки" и загрузите параметры с сервера безопасности.
2. В разделе "Политики" перейдите к группе параметров "Контроль печати / Настройки".
3. Для параметра "Перенаправление принтеров в RDP-подключениях" выберите нужное значение в раскрывающемся списке:
   - "Разрешено" — пользователям предоставляется возможность самостоятельно настраивать использование принтеров в параметрах удаленного подключения. При этом возможность настройки присутствует независимо от того, какие параметры заданы в стандартных политиках ОС Windows;
   - "Запрещено подключать удаленные принтеры к компьютеру" — блокирует использование принтеров на стороне терминального сервера (запрет действует для всех "входящих" терминальных сессий);

- "Запрещено использовать принтеры компьютера удаленно" — блокирует использование принтеров на стороне терминального клиента (запрет действует для всех "исходящих" терминальных сессий);
- "Запрещено" — блокирует перенаправление принтеров независимо от роли компьютера в удаленном подключении (терминальный клиент или сервер);
- "Определяется политиками Windows" — пользователи могут настраивать использование принтеров в параметрах удаленного подключения, если эти действия разрешены в стандартных политиках перенаправления в ОС Windows.

4. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

## Защита конфиденциальной информации при терминальных подключениях

В режиме контроля потоков механизма полномочного управления доступом можно включить автоматическое назначение уровня конфиденциальности для терминальных сессий. За счет этого будет обеспечиваться равенство уровней для сессий конфиденциальности на терминальном клиенте и на терминальном сервере.

Настройка параметров автоматического назначения уровней конфиденциальности для сессий пользователей выполняется при включении режима контроля потоков (см. стр.**86**).

# Приложение

## Список групп и классов для контроля устройств

**Табл.1 Группы и классы устройств**

| Группа | Класс |
|---|---|
| **Локальные устройства** | Последовательные порты.<br>Параллельные порты.<br>Сменные диски.<br>Оптические диски.<br>Физические диски.<br>Процессоры.<br>Оперативная память.<br>Системная плата.<br>Аппаратная поддержка.<br>Программно-реализованные диски |
| **Устройства USB** | Сетевые платы и модемы.<br>Интерфейсные устройства (мышь, клавиатура, ИБП и др.)<br>Сканеры и цифровые фотоаппараты.<br>Принтеры.<br>Устройства хранения.<br>Bluetooth адаптеры.<br>Сотовые телефоны (смартфоны, КПК).<br>Электронные идентификаторы и считыватели.<br>Прочие |
| **Устройства PCMCIA** | Последовательные порты и модемы.<br>Параллельные порты.<br>Устройства хранения.<br>Сетевые платы.<br>Прочие |
| **Устройства IEEE1394** | Устройства хранения.<br>Принтеры.<br>Сканеры и цифровые фотоаппараты.<br>Сетевые устройства.<br>Цифровые видеокамеры.<br>Прочие |
| **Устройства Secure Digital** | Карточки памяти |
| **Сеть** | Соединение Ethernet.<br>Беспроводное соединение (WiFi).<br>Соединение Bluetooth.<br>Соединение 1394 (FireWire).<br>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. Если устройство до этого уже подключалось и сведения о нем присутствуют в списке устройств, подключать устройство не обязательно.

2. Запустите программу управления в локальном режиме. 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 "Локальный центр управления" (относится к группе "Код Безопасности");
   - на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код Безопасности | Secret Net Studio| Локальный центр управления".
3. В программе управления откройте панель "Компьютер" и перейдите на вкладку "Настройки".
4. В разделе "Политики" перейдите к группе параметров "Контроль устройств / Устройства".
5. Выберите строку с подключенным устройством.
6. В ячейке колонки "Параметры контроля" удалите отметку из поля "Наследовать настройки контроля от родительского объекта" (если отметка установлена) и отметьте режим контроля "Подключение устройства разрешено.
7. Подведите указатель к ячейке колонки "Разрешения" и нажмите левую кнопку мыши.

   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.
11. Нажмите кнопку "Применить" в верхней части вкладки "Настройки".

## 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 списка устройств на отдельном компьютере (см. стр.**11**);
- метод централизованного формирования списка используемых устройств в групповых политиках (доменов, организационных подразделений или сервера безопасности).

Если устройства преимущественно подключаются к одним и тем же компьютерам, для формирования списков устройств рекомендуется использовать первый метод. Для случаев, когда требуется составить единый список подключаемых устройств для компьютеров домена, организационного подразделения или подчиненных серверу безопасности, можно использовать средства соответствующей групповой политики в программе управления. 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 (см. стр.**13**).
2. В список устройств групповой политики добавьте нужные устройства (см. стр.**14**).
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.**15**.

# 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<br>CENTRAL | Локальный режим работы (по умолчанию).<br>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.

# Общие сведения о программе настройки для режима контроля потоков

Программа настройки для режима контроля потоков предназначена для настройки параметров, обеспечивающих функционирование механизма полномочного управления доступом в режиме контроля потоков. Сведения о запуске программы и условиях работы с ней см. на стр.**85**.

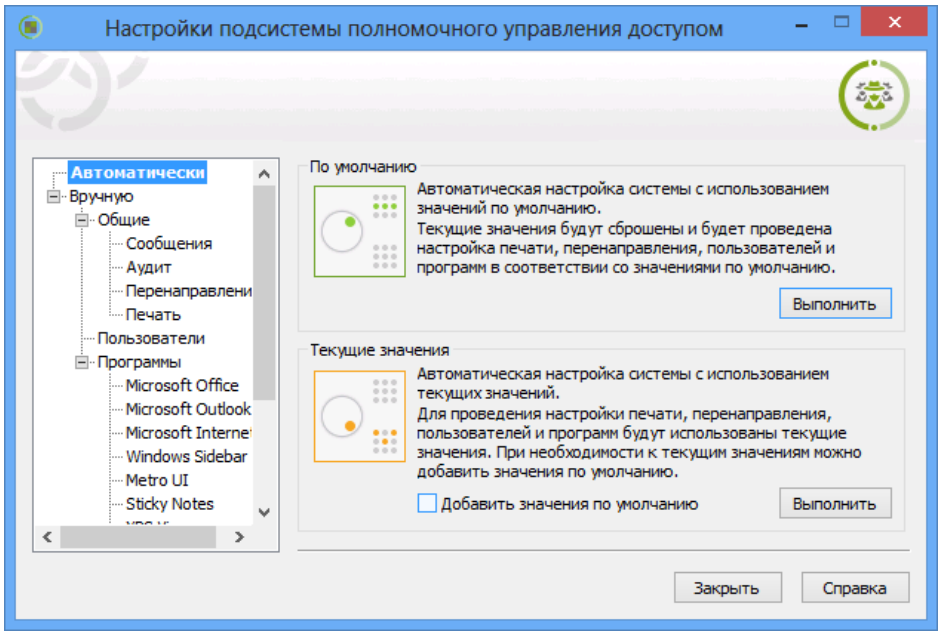
## Автоматическая настройка

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:

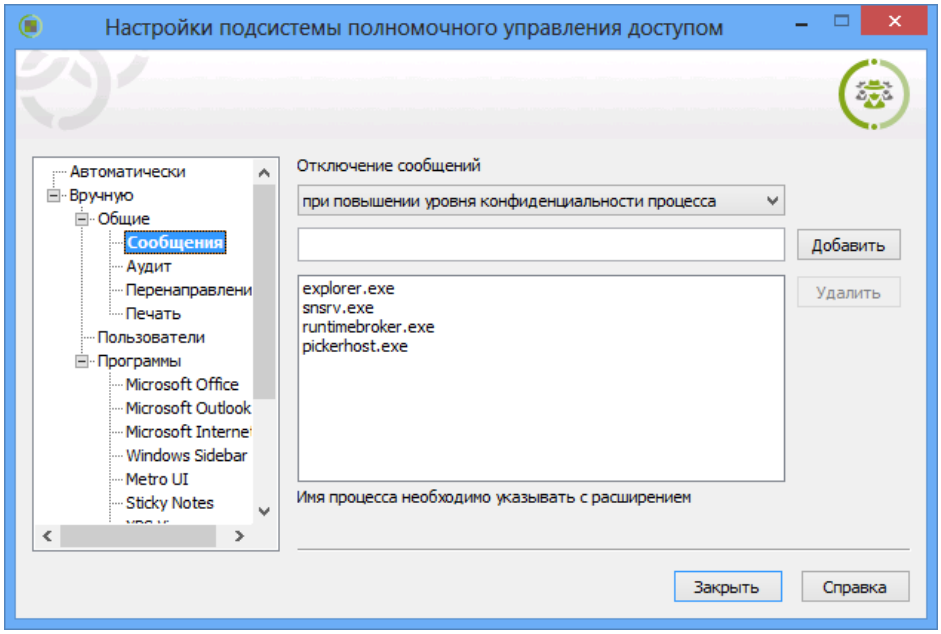
- "Общие" — для настройки общих параметров работы пользователей и приложений;
- "Пользователи" — для настройки параметров, относящихся к профилям пользователей;
- "Программы" — для настройки параметров, относящихся к приложениям.

### 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:**

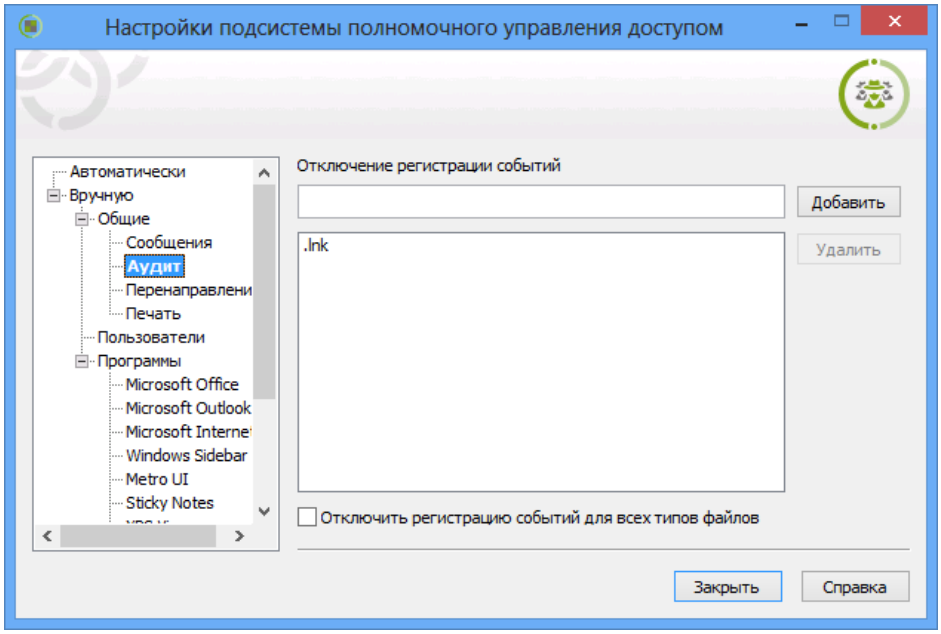
1. В поле "Отключение сообщений" укажите значение "при выводе конфиденциальной информации (по расширению)".

   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 Studio 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 | Аудит".




**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 которых служебным файлам 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.

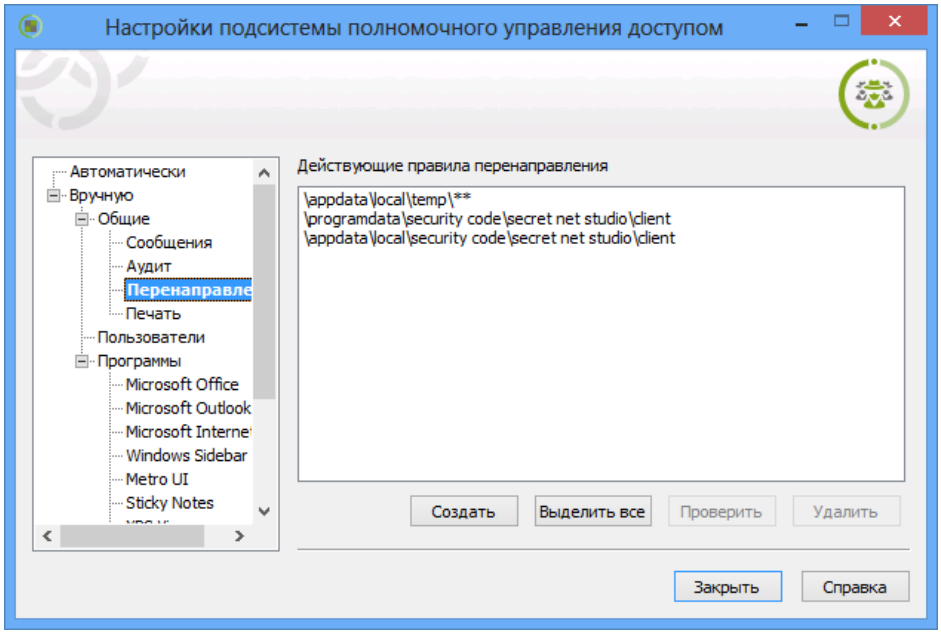
При настройке параметров перенаправления вывода файлов формируется список путей к каталогам с общими файлами, для которых должны быть созданы дополнительные каталоги с различными категориями конфиденциальности. В

этих каталогах будут храниться файлы, используемые в сессиях соответствующих уровней конфиденциальности. Например, для обслуживания обращений приложения MS Word русской версии в списке должна присутствовать запись \AppData\Roaming\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.

**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 "строго 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. **114** ) 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 в формате LFN (Long File Name) 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;
- если в каталоги перенаправления не требуется копировать файлы из исходного каталога — добавьте в конце пути шаблонную подстроку "**" (с двумя символами "звездочка"). В этом случае в каталогах перенаправления будет создана структура подкаталогов исходного каталога без файлов. Например, данный вариант применяется по умолчанию для каталогов временных файлов пользователей;
- если в каталоги перенаправления не требуется копировать подкаталоги исходного каталога — добавьте в конце пути шаблонную подстроку "*" (с одним символом "звездочка"). В этом случае в каталогах перенаправления будут созданы только копии файлов исходного каталога.

- 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 исходных каталогов (в зависимости от указанных шаблонных подстрок). 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 из- за этого могут возникнуть 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 приложение может функционировать некорректно. 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.

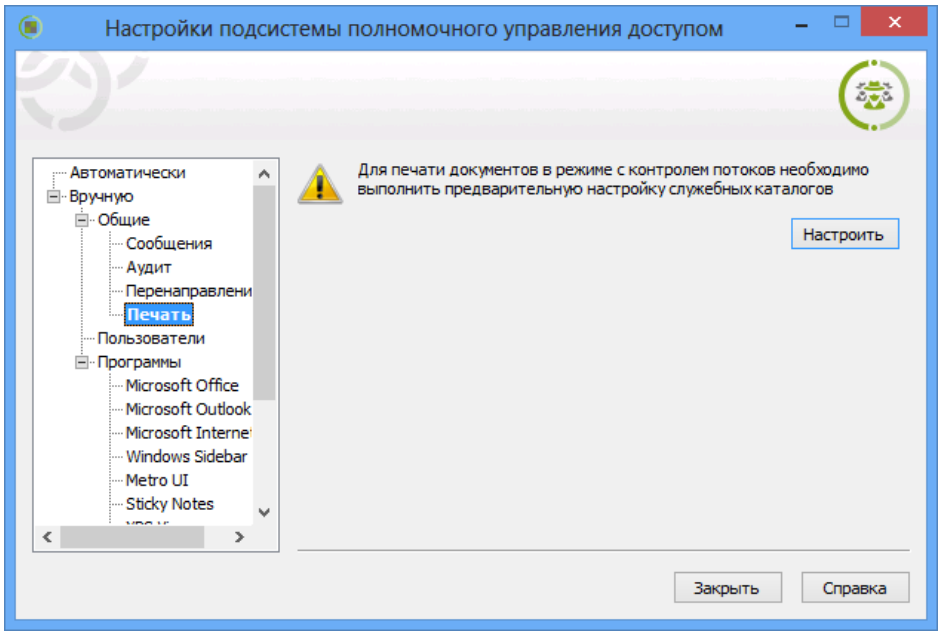
### Настройка системы для печати на принтер

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.114).

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

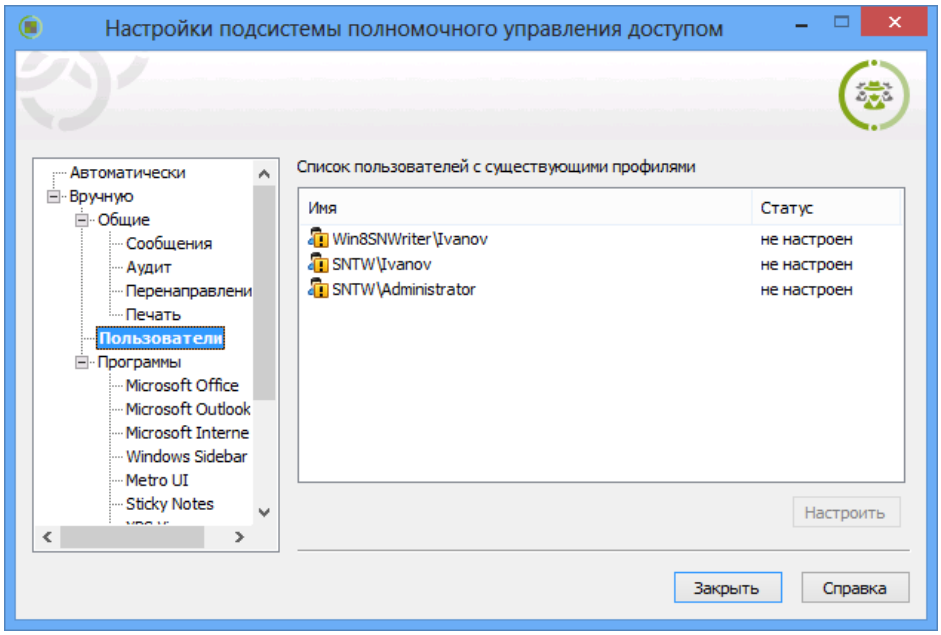
Для работы пользователя в режиме контроля потоков (в конфиденциальных сессиях) должна быть выполнена настройка параметров, относящихся к профилю этого пользователя. Настройка заключается в создании структуры каталогов перенаправления вывода файлов для временных каталогов пользователя и установке соответствующих 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.114). 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

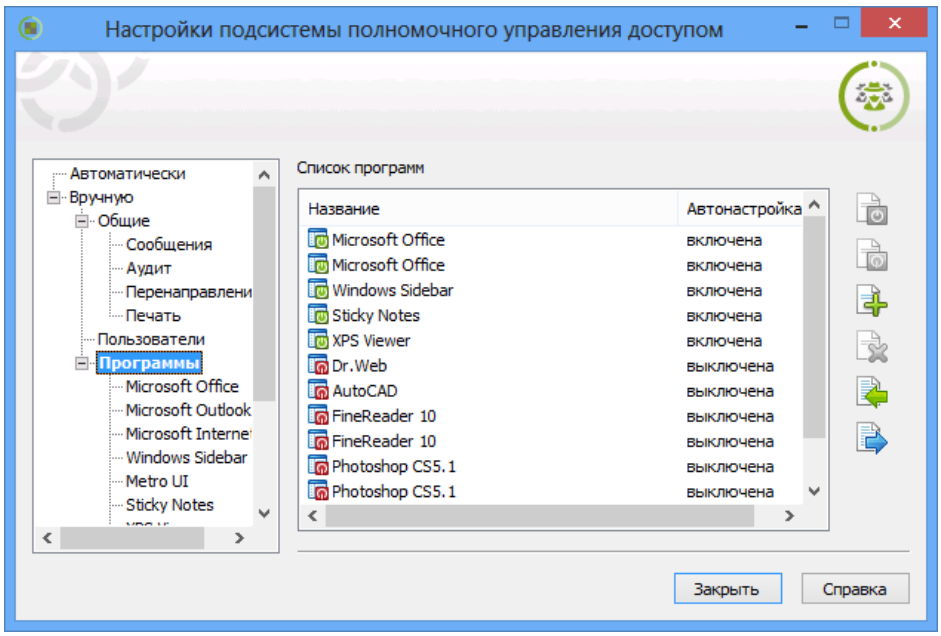
Некоторые приложения не полностью совместимы с механизмом полномочного управления доступом в режиме контроля потоков. Для корректного функционирования таких приложений требуется дополнительная настройка параметров, относящихся к приложению.

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 Studio.

Настройка параметров, относящихся к приложениям, может осуществляться при общей автоматической настройке (см. стр. 114). 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.

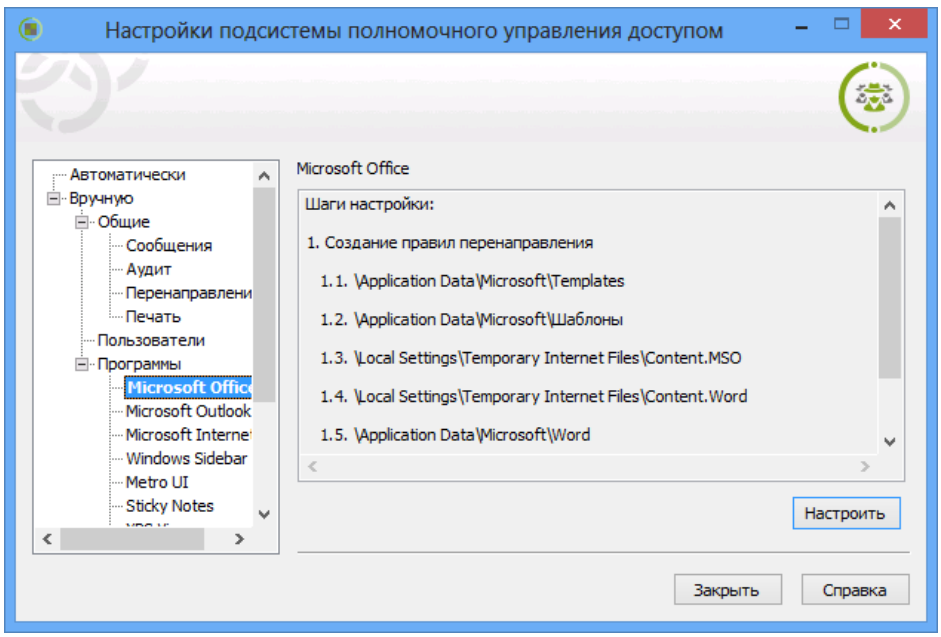
   Выбранные приложения будут незамедлительно удалены из списка.

### 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.

# Аварийное снятие защиты локальных дисков

Для отключения режима защиты логических разделов предусмотрены штатные процедуры (см. стр. 99). 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:

- возвращение первоначального состояния загрузочной области на физическом диске, с которого осуществляется загрузка ОС;
- возвращение первоначального 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 Studio. 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. 99).

**Для отключения защиты дисков:**

1. В каталоге установки клиентского ПО Secret Net Studio 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 Studio 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.**98**).

## Использование загрузочного диска аварийного восстановления

Загрузочный диск аварийного восстановления используется при невозможности загрузки ОС штатным способом с системного диска. Например, если происходит сбой при раскодировании модифицированных данных системного диска, что приводит к блокировке загрузки.

С помощью загрузочного диска можно восстановить первоначальное состояние загрузочной области на физическом диске, с которого осуществляется загрузка ОС, и/или загрузочных секторов логических разделов. Процедура создания диска аварийного восстановления описана на стр.**98**.

**Внимание!**

Для загрузки с диска аварийного восстановления на компьютере должна быть включена функция загрузки с внешних носителей. Например, для загрузки с USB-флеш-накопителя может потребоваться включение режима эмуляции Floppy или Forced FDD в BIOS компьютера.

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 соответствующих областей системного диска. Чтобы вернуть первоначальное состояние объекта, нажмите в диалоге запроса кнопку "Да".

# Документация

| | |
|---|---|
| **1.** Средство защиты информации Secret Net Studio. Руководство администратора. Принципы построения | RU.88338853.501400.001 91 1 |
| **2.** Средство защиты информации Secret Net Studio. Руководство администратора. Установка, обновление, удаление | RU.88338853.501400.001 91 2 |
| **3.** Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация | RU.88338853.501400.001 91 3 |
| **4.** Средство защиты информации Secret Net Studio. Руководство администратора. Централизованное управление, мониторинг и аудит | RU.88338853.501400.001 91 4 |
| **5.** Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Локальная защита | RU.88338853.501400.001 91 5 |
| **6.** Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Сетевая защита | RU.88338853.501400.001 91 6 |
| **7.** Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Антивирус и средство обнаружения вторжений | RU.88338853.501400.001 91 7 |
| **8.** Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Шифрование сетевого трафика | RU.88338853.501400.001 91 8 |
| **9.** Средство защиты информации Secret Net Studio. Руководство пользователя | RU.88338853.501400.001 92 |