Код Безопасности

Средство защиты информации

SECRET NET 7

Руководство администратора

Принципы построения

RU.88338853.501410.015 91 1

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

Оглавление

Список сокращений ... **5**

Введение ... **6**

Общие сведения ... **7**
- Назначение системы ... 7
- Основные функции ... 7
- Состав устанавливаемых компонентов ... 7
- Лицензирование ... 8

Архитектура и средства управления ... **9**
- Основные подсистемы клиента Secret Net ... 9
  - Ядро ... 9
  - Подсистема локального управления ... 10
  - Защитные подсистемы ... 10
  - Модуль входа ... 11
  - Подсистема контроля целостности ... 11
  - Подсистема работы с аппаратной поддержкой ... 11
- Построение системы в сетевом режиме функционирования ... 11
  - Подготовка Active Directory к развертыванию системы ... 12
  - Назначение и функции сервера безопасности ... 12
  - Домены безопасности ... 13
  - Сетевая структура системы Secret Net ... 14
  - Централизованное хранение данных ... 15
- Обзор средств управления ... 15
  - Средства локального управления ... 15
  - Средства централизованного управления ... 22

Защитные механизмы ... **28**
- Управление защитными механизмами ... 28
  - Получение и применение настроек ... 28
  - Защита сетевых обращений к службам каталогов ... 29
- Механизм защиты входа в систему ... 29
  - Идентификация и аутентификация пользователей ... 29
  - Блокировка компьютера ... 30
  - Аппаратные средства защиты ... 31
  - Общие сведения об интеграции Secret Net и комплексов "Соболь" ... 32
- Дискреционное управление доступом к ресурсам файловой системы ... 33
- Разграничение доступа к устройствам ... 35
- Полномочное управление доступом ... 36
- Замкнутая программная среда ... 37
- Защита информации на локальных дисках ... 38
- Затирание информации, удаляемой с дисков ... 39
- Регистрация событий ... 39
- Контроль целостности ... 39
- Контроль подключения и изменения устройств компьютера ... 40
- Теневое копирование выводимых данных ... 41
- Функциональный контроль подсистем ... 42
- Контроль печати ... 42

Приложение ... **44**
- Необходимые права для установки и управления ... 44
  - Установка и удаление компонентов ... 44
  - Настройка механизмов и управление параметрами объектов ... 46
  - Использование программы оперативного управления ... 47
- Рекомендации по настройке для соответствия требованиям к автоматизированным системам ... 49
  - Общие сведения о настройке для соответствия классам защищенности ... 49
  - Использование дополнительных средств защиты загрузки ... 50

Настраиваемые параметры системы Secret Net 51
Документация **63**

Список сокращений

AD	Active Directory
API	Application Programming Interface
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IMAPI	Image Mastering Application Programming Interface
MS	Microsoft
MSDN	Microsoft Developers Network
NTFS	New Technology File System
PCMCIA	Personal Computer Memory Card International Association
PKI	Public Key Infrastructure
SSL	Secure Socket Layer
TLS	Transport Layer Security
UDF	Universal Disk Format
USB	Universal Serial Bus
XML	Extensible Markup Language
XPS	XML Paper Specification
АС	Автоматизированная система
БД	База данных
ЗПС	Замкнутая программная среда
ИС	Информационная система
КЦ	Контроль целостности
НСД	Несанкционированный доступ
ОС	Операционная система
ОУ	Оперативное управление
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
РДУ	Разграничение доступа к устройствам
СБ	Сервер безопасности
СЗИ	Средство или система защиты информации
СУБД	Система управления базами данных
ФСТЭК	Федеральная служба по техническому и экспортному контролю

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net 7" RU.88338853.501410.015 (далее — система Secret Net, Secret Net). В нем содержатся сведения, необходимые администраторам для ознакомления с принципами работы и возможностями применения системы Secret Net.

Условные обозначения

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

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

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

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

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

- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения.

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

Другие источники информации

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

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

Глава 1
Общие сведения

Назначение системы

Система Secret Net предназначена для защиты от несанкционированного доступа к информационным ресурсам компьютеров, функционирующих под управлением операционных систем MS Windows 8/7/Vista/XP и Windows Server 2012/2008/2003.

Основные функции

Защита от несанкционированного доступа (НСД) обеспечивается комплексным применением набора защитных механизмов, расширяющих средства безопасности ОС Windows.

Система Secret Net может функционировать в следующих режимах:

- автономный режим — предусматривает только локальное управление защитными механизмами;
- сетевой режим — предусматривает локальное и централизованное управление защитными механизмами, а также централизованное получение информации и изменение состояния защищаемых компьютеров.

Основные функции, реализуемые системой Secret Net:

- контроль входа пользователей в систему;
- разграничение доступа пользователей к ресурсам файловой системы и устройствам компьютера;
- создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера (замкнутой программной среды);
- разграничение доступа пользователей к конфиденциальным данным;
- контроль потоков конфиденциальной информации в системе;
- контроль вывода на печать и добавление грифов в распечатываемые документы (маркировка документов);
- контроль целостности защищаемых ресурсов;
- контроль подключения и изменения устройств компьютера;
- функциональный контроль ключевых компонентов Secret Net;
- защита содержимого дисков при несанкционированной загрузке;
- уничтожение (затирание) содержимого файлов при их удалении;
- теневое копирование выводимой информации;
- регистрация событий безопасности в журнале Secret Net;
- мониторинг и оперативное управление защищаемыми компьютерами (только в сетевом режиме функционирования);
- централизованный сбор и хранение журналов (только в сетевом режиме функционирования);
- централизованное управление параметрами механизмов защиты (только в сетевом режиме функционирования).

Состав устанавливаемых компонентов

Система Secret Net состоит из следующих отдельно устанавливаемых программных средств:

1. Компонент "Secret Net 7" (далее — клиент).
2. Компонент "Модификатор схемы Active Directory" (далее — модификатор AD). Используется только в сетевом режиме функционирования. Применяется в

случае использования Active Directory для размещения и хранения сведений об объектах централизованного управления.

3. Компонент "Secret Net 7 — Сервер безопасности" (далее — сервер безопасности или СБ). Используется только в сетевом режиме функционирования.
4. Компонент "Secret Net 7 — Программа управления" (далее — программа оперативного управления). Используется только в сетевом режиме функционирования.

Лицензирование

Имеется ряд ограничений на использование системы Secret Net, связанных с политикой лицензирования данного продукта. Лицензируются следующие параметры:

- режим функционирования системы Secret Net;
- разрешенные для использования версии программного обеспечения;
- возможность использования механизма защиты дисков;
- возможность использования терминального доступа;
- количество клиентов в глобальном каталоге (в сетевом режиме функционирования);
- количество клиентов, подключаемых к серверу безопасности (в сетевом режиме функционирования);
- количество компьютеров, с которых возможно одновременное подключение средств управления к серверу безопасности (в сетевом режиме функционирования).

Ограничения на использование Secret Net определяются приобретенными лицензиями.

Глава 2
Архитектура и средства управления

Обобщенная структурная схема взаимодействия основных компонентов системы Secret Net представлена на следующем рисунке.

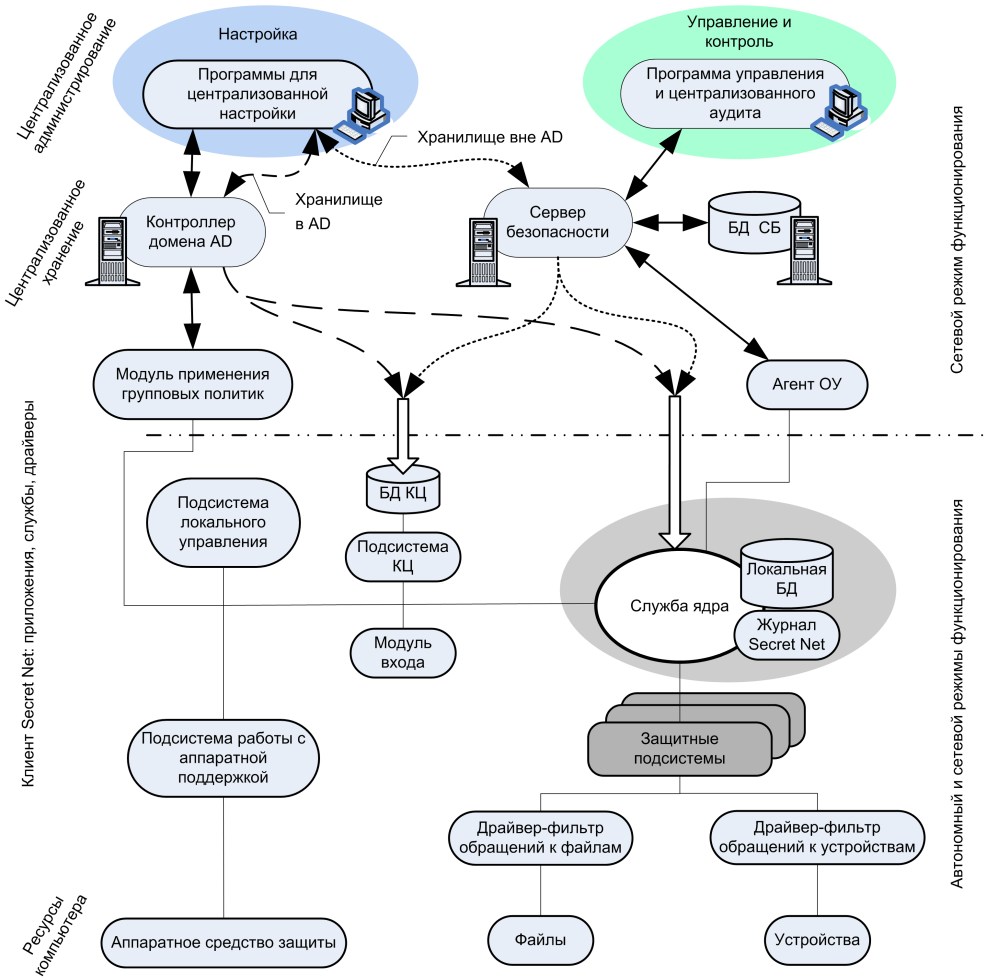


Рис.1 Структурная схема взаимодействия

Основные подсистемы клиента Secret Net

Клиент системы Secret Net включает следующие основные компоненты и подсистемы:

- служба ядра;
- подсистема локального управления;
- защитные подсистемы;
- модуль входа;
- подсистема контроля целостности;
- подсистема работы с аппаратной поддержкой.

Ядро

Служба ядра автоматически запускается на защищаемом компьютере при его включении и функционирует на протяжении всего времени работы компьютера. Она осуществляет управление подсистемами и компонентами и обеспечивает их взаимодействие.

Ядро выполняет следующие функции:

- обеспечивает обмен данными между компонентами клиента и обработку поступающих команд;
- обеспечивает доступ других компонентов системы к информации, хранящейся в локальной базе данных Secret Net;
- обрабатывает поступающую информацию о событиях, происходящих на компьютере и связанных с безопасностью системы, и регистрирует их в журнале Secret Net.

Подсистема регистрации является одним из элементов ядра клиента и предназначена для управления регистрацией событий, связанных с работой системы защиты. Такие события регистрируются в журнале Secret Net. Эта информация поступает от подсистем Secret Net, которые следят за происходящими событиями. Перечень событий Secret Net, подлежащих регистрации, устанавливается администратором безопасности.

В локальной БД Secret Net хранится информация о настройках системы защиты, необходимых для работы защищаемого компьютера. Локальная БД размещается в реестре ОС Windows и специальных файлах.

Доступ подсистем и компонентов системы защиты к данным, хранящимся в БД Secret Net, обеспечивается службой ядра.

Подсистема локального управления

Подсистема локального управления обеспечивает:

- управление объектами защиты (устройствами, файлами, каталогами);
- управление параметрами пользователей и защитных механизмов;
- взаимодействие с локальной БД Secret Net;
- формирование заданий на контроль целостности;
- просмотр локальных журналов.

Защитные подсистемы

Со службой ядра взаимодействуют следующие защитные подсистемы:

- **Замкнутая программная среда** — предотвращает запуск неразрешенного программного обеспечения (ПО).
- **Затирание данных** — обеспечивает затирание содержимого удаленных файлов.
- **Защита дисков** — обеспечивает защиту информации на локальных дисках при несанкционированной загрузке компьютера.
- **Разграничение доступа к устройствам** — обеспечивает разграничение доступа к заданным устройствам компьютера (портам, USB-устройствам, локальным дискам и др.).
- **Теневое копирование** — сохраняет в специальном хранилище копии выводимых данных (например, файлов).
- **Полномочное управление доступом** — обеспечивает хранение категорий конфиденциальности ресурсов, разграничение доступа к этим ресурсам и контроль потоков конфиденциальной информации в системе.
- **Контроль печати** — обеспечивает контроль вывода документов на печать (в том числе и конфиденциальных).
- **Дискреционное управление доступом** — обеспечивает хранение прав доступа к ресурсам файловой системы и разграничение доступа пользователей к этим ресурсам.

При обращении пользователя к ресурсам компьютера (файлам, каталогам или устройствам) специальные модули перехватывают это обращение. Далее управление переходит к драйверам защитных подсистем, которые выполняют профильные действия, соответствующие цели обращения пользователя к ресурсу.

Информацию для выполнения действий драйверы защитных подсистем получают от ядра при инициализации подсистемы, при входе пользователя и в определенные моменты работы системы. Информация может быть получена драйверами как в процессе инициализации подсистем при загрузке компьютера, так и по запросу защитной подсистемы при обработке обращения пользователя к ресурсу. Загрузку необходимой информации через API защитных подсистем при инициализации и по запросу осуществляет служба ядра.

Модуль входа

Совместно с ОС Windows модуль входа в систему обеспечивает:

- обработку входа пользователя в систему (проверка возможности входа, оповещение остальных модулей о начале или завершении работы пользователя);
- блокировку работы пользователя;
- функциональный контроль работоспособности системы;
- загрузку данных с персональных идентификаторов пользователя;
- усиленную аутентификацию пользователя при входе в систему.

При обработке входа пользователя в систему осуществляется формирование контекста пользователя: определение его привилегий, уровня допуска и др.

Подсистема контроля целостности

Подсистема контроля целостности обеспечивает проверку неизменности ресурсов (каталогов, файлов, ключей и значений реестра) компьютера. Хотя данная подсистема и выполняет контролирующие функции, она не включена в состав защитных подсистем, так как выполняет контроль не при обращении пользователя к ресурсам, а при наступлении определенных событий в системе (загрузка, вход пользователя, контроль по расписанию).

Подсистема работы с аппаратной поддержкой

Подсистема обеспечивает взаимодействие с устройствами аппаратной поддержки системы Secret Net и состоит из следующих компонентов:

- модуль, обеспечивающий единый интерфейс обращения ко всем поддерживаемым устройствам;
- модули работы с устройствами (каждый модуль обеспечивает работу с конкретным устройством);
- драйверы устройств аппаратной поддержки (если они необходимы).

Построение системы в сетевом режиме функционирования

Сетевой режим функционирования системы Secret Net предполагает использование компонентов, обеспечивающих возможность централизованного управления защищаемыми компьютерами. Для централизованного управления в системе должны быть установлены следующие программные средства:

- компонент "Secret Net 7 — Сервер безопасности". Для функционирования компонента требуется наличие системы управления базами данных (СУБД), реализуемой сервером СУБД Oracle или MS SQL. Сервер безопасности и сервер СУБД могут быть установлены на разных компьютерах (рекомендуется) или на одном компьютере;
- компонент "Secret Net 7" в сетевом режиме функционирования — на всех защищаемых компьютерах. На рабочих местах администраторов при установке компонента необходимо выбрать вариант с установкой средств централизованной настройки;
- компонент "Secret Net 7 — Программа управления" — на рабочих местах администраторов, в задачи которых входит конфигурирование сетевой структуры системы Secret Net, мониторинг, оперативное управление или работа с централизованными журналами.

Кроме того, если для централизованного управления параметрами групповых политик и/или параметрами доменных пользователей будут использоваться стандартные средства ОС Windows — дополнительно необходимо установить соответствующие компоненты ОС. Сведения о составе требуемых компонентов в зависимости от версии ОС приведены в документе [**3**].

Подготовка Active Directory к развертыванию системы

На начальном этапе развертывания системы Secret Net необходимо определиться с возможностью внесения изменений в конфигурационные хранилища Active Directory. Система Secret Net может функционировать в различных вариантах интеграции в структуру AD. Порядок установки компонентов зависит от того, где будет размещаться хранилище объектов централизованного управления Secret Net: в базе данных доменных служб Active Directory или в отдельной базе вне AD.

Для максимальной интеграции в структуру AD хранилище объектов централизованного управления Secret Net следует разместить в базе данных доменных служб Active Directory. В этом случае до установки компонентов системы Secret Net необходимо модифицировать схему AD для добавления в нее нужных классов и атрибутов и регистрации конфигурационных данных в разделе конфигурации каталога AD. Модификация выполняется с использованием компонента "Модификатор схемы Active Directory". Процедура модификации не затрагивает имеющиеся в AD объекты и связи и поэтому не может оказать влияние на работоспособность существующей доменной структуры. Для модификации схемы в дополнение к правам на изменение конфигурации каталога AD требуются права для модификации схемы AD. По умолчанию такие права предоставлены пользователям, включенным соответственно в группы "Администраторы предприятия" (Enterprise Admins) и "Администраторы схемы" (Schema Admins).

Если максимальная интеграция в структуру AD не требуется, хранилище объектов централизованного управления Secret Net можно сформировать в отдельной базе данных вне Active Directory. При этом имеется возможность реализовать управление параметрами Secret Net для доменных пользователей с использованием стандартных оснасток ОС Windows. Для этого достаточно расширить конфигурацию каталога AD путем импорта (регистрации) нужных конфигурационных данных для поддержки управляющих модулей системы Secret Net. Добавлять в схему AD новые классы и атрибуты не требуется. Регистрация конфигурационных данных осуществляется однократно в лесу доменов при установке сервера безопасности. Для выполнения процедуры требуются права на изменение конфигурации каталога AD. По умолчанию такие права предоставлены пользователям группы "Администраторы предприятия" (Enterprise Admins). Для случаев, когда невозможно выполнить установку сервера безопасности пользователем с такими правами, предусмотрена альтернативная возможность регистрации конфигурационных данных администратором домена путем запуска командного файла sn7-modify-AD.cmd из каталога \Tools\Infosec\ModifyAD\ на установочном компакт-диске системы Secret Net.

Если установка выполнена без расширения конфигурации каталога AD — управление параметрами Secret Net для доменных пользователей будет возможно только с помощью программы управления пользователями из состава средств централизованной настройки системы Secret Net.

Назначение и функции сервера безопасности

Сервер безопасности является основным элементом в сетевой структуре системы Secret Net. Этот компонент обеспечивает взаимодействие объектов управления, реализует функции контроля и управления, а также осуществляет обработку, хранение и передачу информации.

Основные функции сервера безопасности:

- получение информации от агентов на защищаемых компьютерах о текущем состоянии рабочих станций и сессиях работы пользователей;
- оперативное получение и передача сведений о событиях НСД, зарегистрированных на защищаемых компьютерах;
- отправка команд управления на защищаемые компьютеры;
- получение информации о состоянии защитных подсистем на компьютерах и отправка команд на изменение состояния защитных подсистем;
- получение и передача на защищаемые компьютеры параметров групповых политик, заданных в программе оперативного управления системы Secret Net;
- контроль действительности лицензий на использование компонентов системы Secret Net;
- получение локальных журналов с защищаемых компьютеров и передача содержимого журналов в базу данных сервера безопасности;
- обработка запросов к базе данных;
- архивирование и восстановление содержимого журналов в базе данных;
- протоколирование обращений к серверу.

Домены безопасности

В системе Secret Net реализация централизованного управления компьютерами и синхронизации параметров защиты базируется на концепции доменов безопасности. Домены безопасности в системе Secret Net формируются из объектов, включенных в определенные контейнеры Active Directory: в организационных подразделениях (Organizational Unit) или во всем домене AD. По аналогии с доменами Active Directory несколько доменов безопасности (со своими серверами безопасности) могут образовывать лес доменов.

Формирование первого домена безопасности в домене AD происходит при установке первого сервера безопасности. Возможность выбора контейнера Active Directory для формирования домена безопасности зависит от варианта размещения хранилища объектов централизованного управления, указанного при установке сервера безопасности:

- Если хранилище объектов централизованного управления системы Secret Net размещается в БД доменных служб Active Directory, доменом безопасности считается весь домен AD. Возможность создания домена безопасности на базе отдельного организационного подразделения отсутствует. В этом случае сервер безопасности и подчиненные ему компьютеры используют встроенную базу данных каталога AD для сохранения и применения параметров. Синхронизация параметров на компьютерах осуществляется с использованием штатных средств AD. Однако в этих условиях предоставление всех необходимых полномочий администратору безопасности возможно только после включения этого пользователя в группу администраторов домена Active Directory.
- При размещении хранилища объектов централизованного управления вне Active Directory сервер безопасности использует базу данных альтернативной службы каталогов. В зависимости от операционной системы компьютера сервера безопасности вместо доменных служб AD обработку данных осуществляют службы облегченного доступа к каталогам Active Directory (Active Directory Lightweight Directory Services, AD LDS) или компонент режима приложений Active Directory (Active Directory Application Mode, ADAM). В этом варианте для формирования домена безопасности можно выбрать как весь домен AD, так и отдельное организационное подразделение. Контроль получения и применения параметров на защищаемых компьютерах осуществляется самим сервером безопасности.

  Домен безопасности создается как часть структуры леса доменов безопасности. Для леса назначается группа пользователей, которым будут предоставлены права на создание новых доменов безопасности. Эта группа

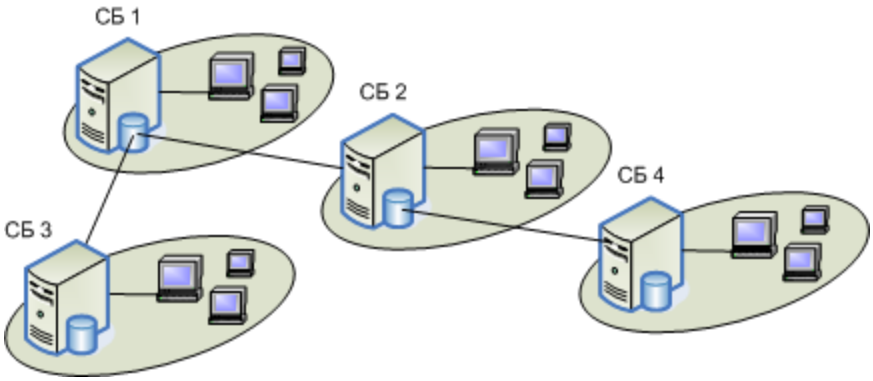
будет являться группой администраторов леса доменов безопасности. При создании домена безопасности назначается группа пользователей, которым будут предоставлены права администрирования домена безопасности — группа администраторов домена безопасности.

Внимание!
Чтобы обеспечить бесперебойное функционирование защищаемых компьютеров, подчиненных серверу безопасности с хранилищем объектов вне AD, следует предусмотреть наличие резервного сервера в этом же домене безопасности. Также необходимо регулярно выполнять резервное копирование (экспорт) хранилища, чтобы иметь возможность его восстановления при переустановке сервера.

Сетевая структура системы Secret Net

Сетевая структура системы Secret Net строится по принципу подчинения защищаемых компьютеров сети серверу безопасности. Для подчинения серверу безопасности компьютер должен быть в составе домена безопасности.

В рамках леса доменов можно организовать функционирование нескольких серверов безопасности с подчинением по иерархическому принципу. При этом иерархия подчинения серверов не обязательно должна соответствовать структуре доменов в лесе. На рисунке представлен пример использования нескольких серверов СБ1 — СБ4.



Каждый сервер контролирует работу своей группы защищаемых компьютеров и имеет свою базу данных. При этом некоторые операции доступны и в отношении объектов, относящихся к подчиненным серверам. Как видно из рисунка, серверы безопасности СБ2 и СБ3 являются подчиненными по отношению к СБ1, а СБ4 — подчиненным по отношению к СБ2.

Сетевую структуру системы Secret Net можно формировать с учетом различных особенностей построения сети и распределения полномочий между администраторами. Одним из основных факторов, влияющих на формирование сетевой структуры системы Secret Net, является вопрос наделения полномочиями администраторов безопасности. Если администраторам безопасности предоставлены права администраторов домена Active Directory, установку серверов безопасности в этом домене целесообразно выполнять с созданием хранилища объектов централизованного управления в БД доменных служб AD. При необходимости разделить полномочия администраторов серверы безопасности следует устанавливать с созданием хранилища вне AD и сформировать домены безопасности на базе организационных подразделений. Такой вариант позволяет в нужном объеме разделить полномочия администраторов безопасности и администраторов домена Active Directory, поскольку в рамках организационного подразделения администратору безопасности могут быть предоставлены все необходимые права на администрирование.

Обмен данными между клиентами и сервером осуществляется в режиме сессий. При передаче данных используется протокол HTTPS. На сервере должен быть установлен сертификат для обеспечения защиты соединений с сервером.

Централизованное хранение данных

Компоненты системы Secret Net используют следующие структуры централизованного хранения данных:

- база данных сервера безопасности на сервере СУБД — содержит централизованные журналы и оперативную информацию для мониторинга системы;
- база данных доменных служб Active Directory или AD LDS/ADAM — содержит параметры системы Secret Net, относящиеся к компьютерам, пользователям и группам пользователей, списки серверов безопасности, списки электронных идентификаторов и других объектов для централизованного управления системой защиты.

Разделение хранилищ обусловлено спецификой обращения к данным. Обращения осуществляют только те компоненты, которым это разрешено. Контроль и разграничение доступа к хранилищам осуществляются самой системой, поэтому от администратора не требуется дополнительных действий для обеспечения защиты обращений.

Обзор средств управления

Управление системой Secret Net осуществляется с помощью специальных программных средств, устанавливаемых при развертывании системы. Средства управления предоставляют возможности для настройки системы и изменения состояния объектов, а также для контроля функционирования защищаемых компьютеров. В зависимости от назначения средства управления могут представлять собой отдельные программы или программные элементы, встраиваемые в другие средства в качестве дополнительных расширений.

Средства локального управления

Средства локального управления используются при работе на защищаемом компьютере. Они предназначены для выполнения действий пользователями или администраторами компьютера в автономном и сетевом режимах функционирования системы Secret Net. В сетевом режиме функционирования средства локального управления используются при невозможности централизованного управления по каким-либо причинам.

В состав средств локального управления входят следующие программные средства:

- диалог "Secret Net" в диалоговом окне настройки свойств ресурса;
- интегрированные средства управления параметрами в оснастке "Локальная политика безопасности";
- интегрированные средства управления пользователями в оснастке "Управление компьютером";
- программа "Контроль программ и данных" в локальном режиме работы;
- программа просмотра локальных журналов;
- программа дополнительной настройки подсистемы полномочного управления доступом;
- диалоговое окно "Управление Secret Net 7" в Панели управления Windows.

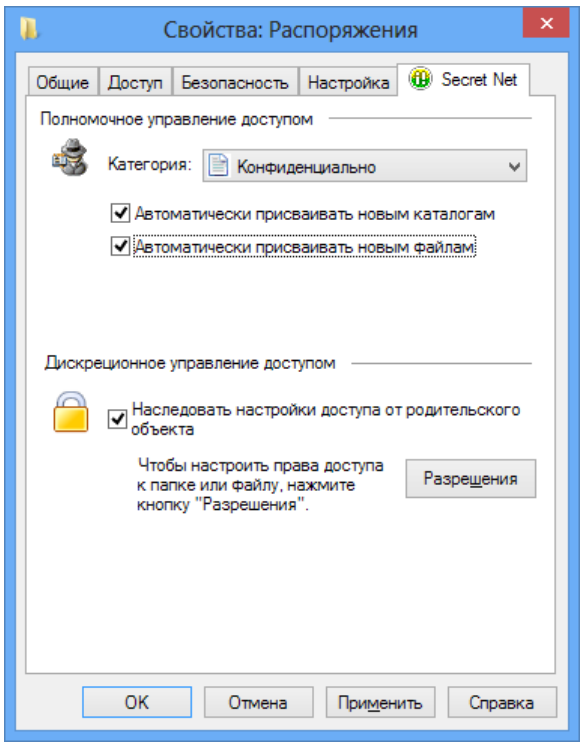
Примечание.
В приведенном списке перечислены регулярно используемые средства управления. Для выполнения частных специфических задач могут использоваться дополнительные программные средства, описание работы с которыми приводится в соответствующих документах.

Диалог "Secret Net" в окне настройки свойств ресурса

Стандартное диалоговое окно настройки свойств ресурса (каталога или файла) ОС Windows содержит дополнительный диалог "Secret Net". В диалоге

выполняются действия по изменению категории конфиденциальности ресурсов для механизма полномочного управления доступом или прав доступа к ресурсам для механизма дискреционного управления доступом. Настройку может выполнять администратор безопасности или пользователи, являющиеся администраторами выбранного ресурса.

Вызов диалогового окна настройки свойств каталога или файла осуществляется стандартным способом в программе "Проводник". На рисунке представлен пример диалога "Secret Net" в диалоговом окне настройки свойств каталога.



Описание процедур использования диалога "Secret Net" приводится в документе [**6**].

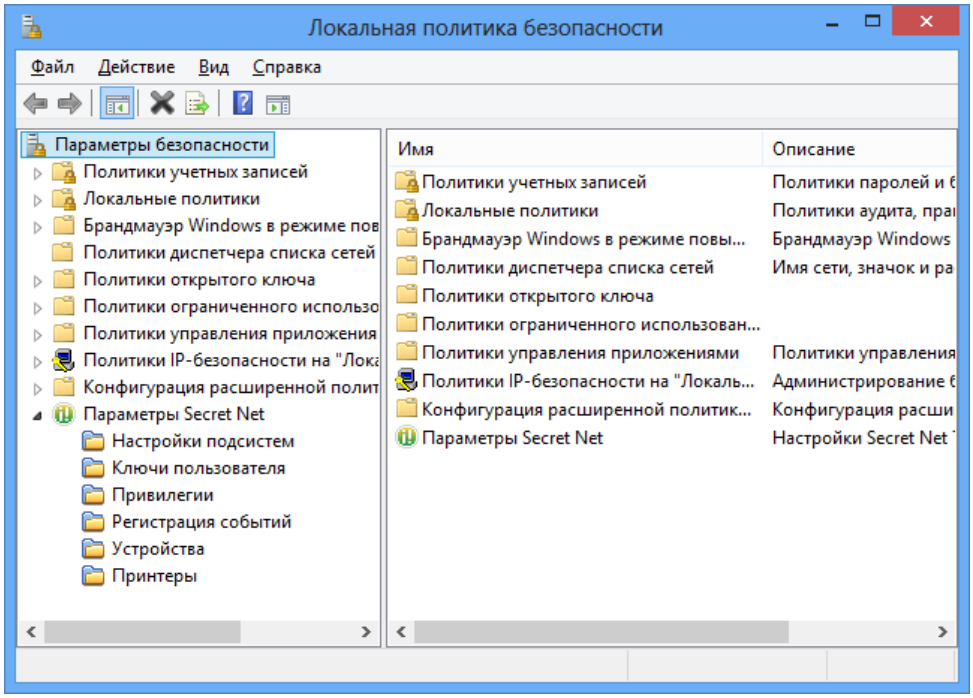
Интегрированные средства управления параметрами в оснастке "Локальная политика безопасности"

Параметры безопасности ОС Windows в стандартной оснастке "Локальная политика безопасности" дополнены разделом "Параметры Secret Net". В данном разделе представлены параметры системы Secret Net, которые применяются на компьютере средствами групповых политик и действуют в рамках локальной политики безопасности (в автономном режиме функционирования системы) или как объединение параметров локальной политики с политикой безопасности домена/организационного подразделения/сервера безопасности (в сетевом режиме функционирования).

Открыть оснастку "Локальная политика безопасности" можно с помощью команды запуска, добавляемой при установке клиента Secret Net. 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 "Локальная политика безопасности" (относится к группе "Код безопасности");
- на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код безопасности | Secret Net | Локальная политика безопасности".

Пример содержимого оснастки представлен на следующем рисунке.



Настройку параметров политики безопасности выполняет администратор. Процедуры настройки параметров Secret Net аналогичны процедурам изменения других стандартных параметров. Описание процедур настройки приводится в документе [**3**].

Интегрированные средства управления пользователями в оснастке "Управление компьютером"

В стандартную оснастку ОС Windows "Управление компьютером" интегрируются специальные средства для локального управления пользователями и их параметрами в системе Secret Net.

В автономном режиме функционирования системы Secret Net оснастка "Управление компьютером" используется для управления как локальными пользователями компьютера, так и доменными. Для управления параметрами доменных пользователей формируется список в отдельном разделе "Доменные пользователи". Если доменный пользователь отсутствует в списке (то есть для него не заданы параметры Secret Net), при входе в систему ему предоставляются минимальные привилегии и уровень допуска, а также считается, что пользователю не присвоен персональный идентификатор (соответственно, вход в систему будет невозможен при включенном режиме усиленной аутентификации или входа только по идентификатору).

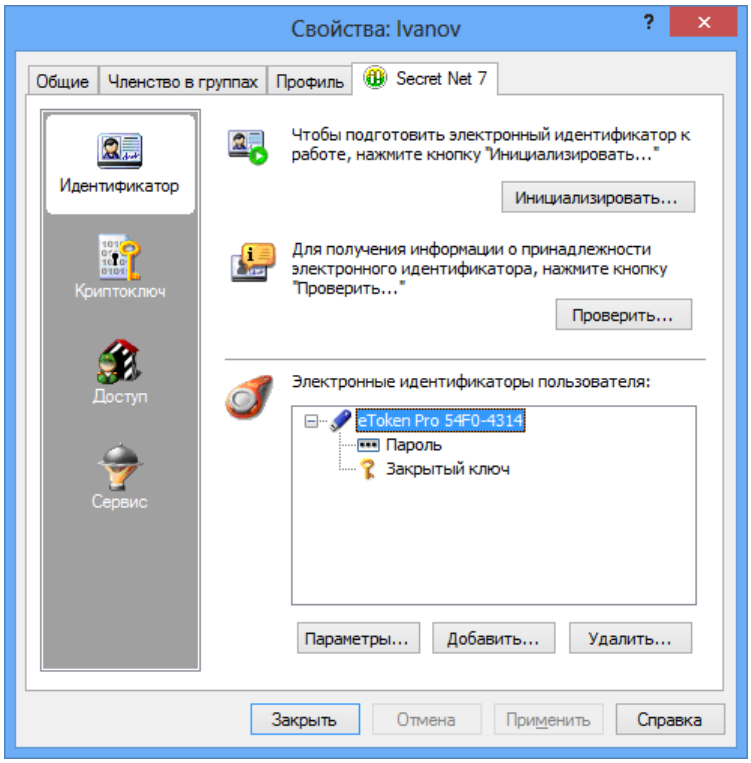
В сетевом режиме функционирования в оснастке "Управление компьютером" осуществляется управление только локальными пользователями.

Открыть оснастку "Управление компьютером" можно с помощью команды запуска, добавляемой при установке клиента Secret Net. Для этого выполните соответствующее действие в зависимости от версии установленной операционной системы:

- на компьютере под управлением ОС Windows 8 или Windows Server 2012 — загрузите начальный экран "Пуск" и выберите элемент "Управление компьютером" (относится к группе "Код безопасности");
- на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код безопасности | Secret Net | Управление компьютером".

Управление параметрами Secret Net для пользователей осуществляется в дополнительном диалоге "Secret Net 7", который добавляется в окно настройки

свойств пользователя. На рисунке представлен пример диалога в окне настройки свойств локального пользователя.



Управление пользователями осуществляется администратором. Описание процедур использования диалога "Secret Net 7" приводится в документе [**3**].

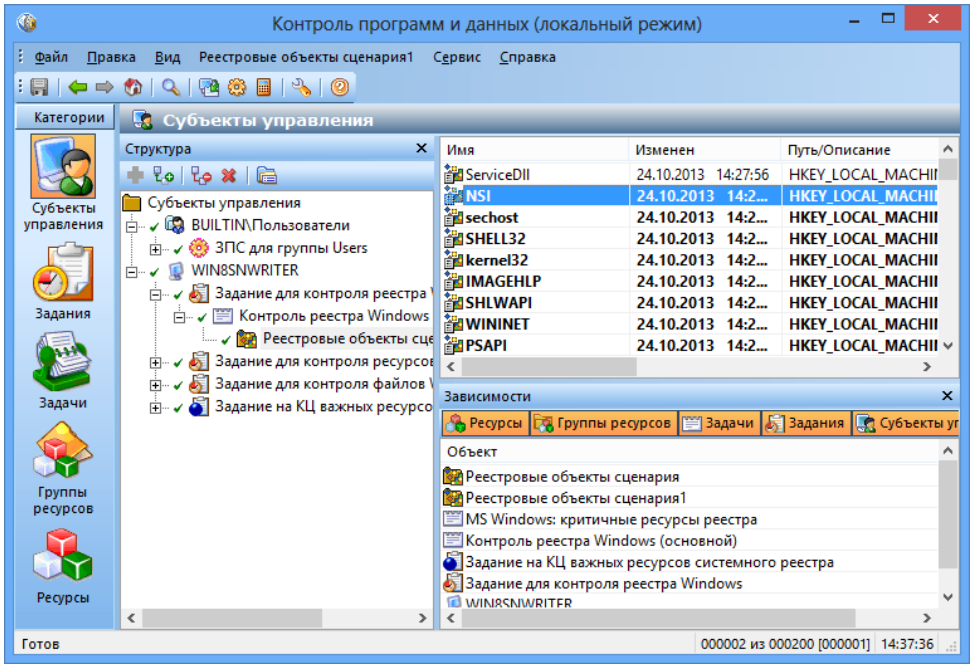
Программа "Контроль программ и данных" в локальном режиме

Программа "Контроль программ и данных" в локальном режиме работы предназначена для настройки механизмов контроля целостности и замкнутой программной среды на компьютере. В ходе настройки для механизма контроля целостности определяются списки контролируемых объектов компьютера, методы и расписание проведения контроля, реакция системы на результат контроля. Для замкнутой программной среды определяются списки программ, запуск которых разрешен пользователям компьютера. Из этих сведений формируется локальная модель данных, представляющая собой иерархию объектов и описание связей между ними.

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".

Пример содержимого окна программы представлен на следующем рисунке.



Настройка механизмов контроля целостности и замкнутой программной среды выполняется администратором. Описание процедур использования программы приводится в документе [**3**].

Программа просмотра локальных журналов

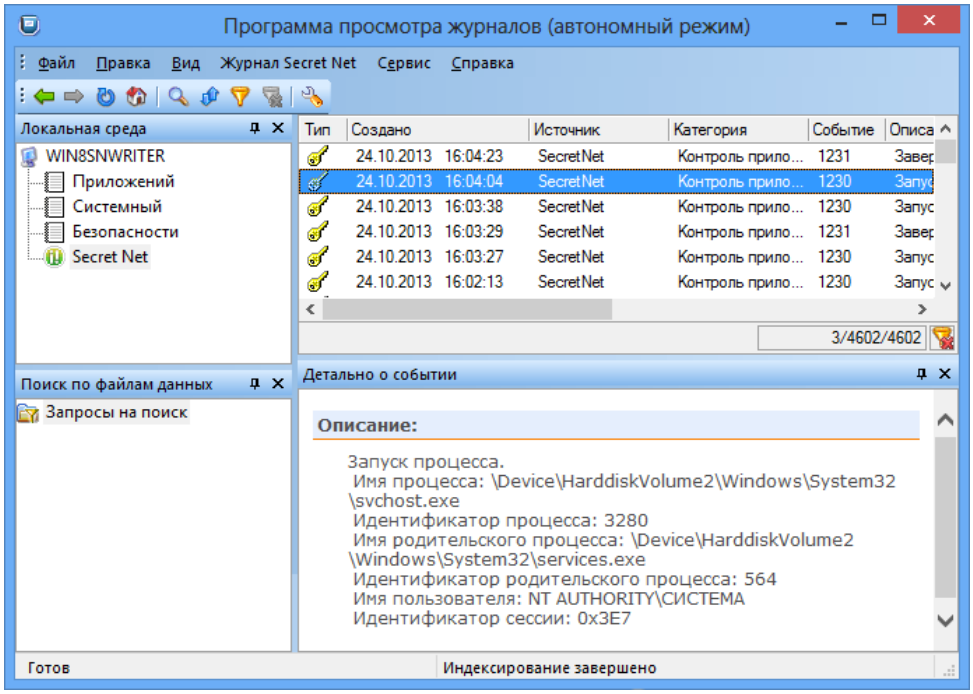
Программа просмотра локальных журналов предназначена для загрузки и работы с записями журналов, которые регистрируются и хранятся на компьютере локально. Загрузку записей можно выполнять из специального журнала Secret Net и из штатных журналов ОС Windows (журнал приложений, системный журнал и журнал безопасности). Также с использованием этой программы осуществляется доступ к дубликатам данных в локальном хранилище теневого копирования.

В сетевом режиме функционирования системы Secret Net содержимое локальных журналов может передаваться в централизованное хранилище. После передачи записей происходит очистка локальных журналов, поэтому становится невозможной загрузка этих записей в программе просмотра локальных журналов.

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

- на компьютере под управлением ОС Windows 8 или Windows Server 2012 — загрузите начальный экран "Пуск" и выберите элемент "Журналы" (относится к группе "Код безопасности");
- на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код безопасности | Secret Net | Журналы".

Пример содержимого окна программы представлен на следующем рисунке.



Доступ к содержимому локальных журналов предоставлен администраторам. Описание процедур использования программы приводится в документе [**5**].

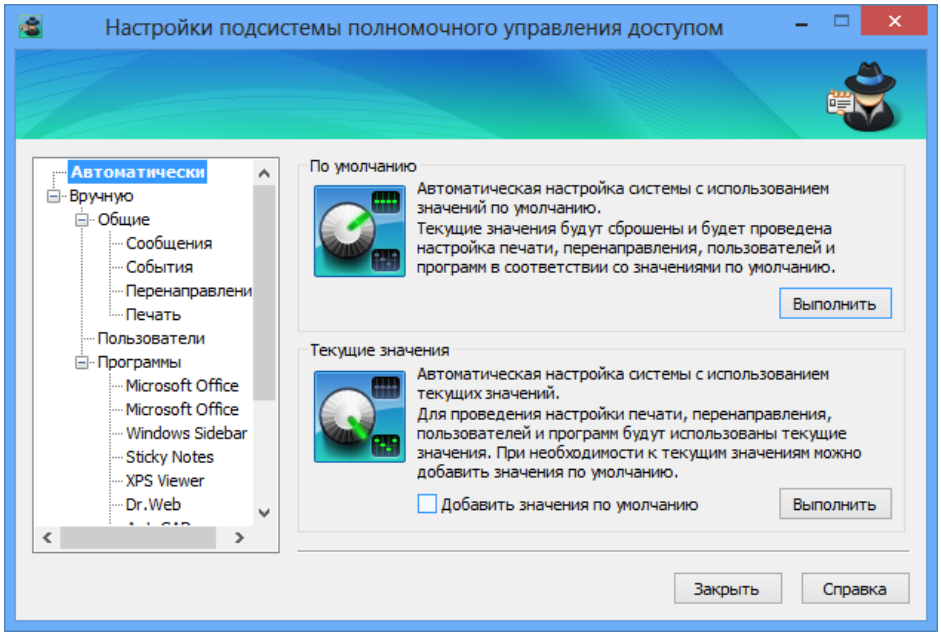
Программа настройки подсистемы полномочного управления доступом

Программа настройки подсистемы полномочного управления доступом предназначена для дополнительной настройки системы при необходимости использования режима контроля потоков. Также с помощью программы можно отключить вывод предупреждающих сообщений и регистрацию событий для случаев, когда такие оповещения не требуются.

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".

Пример содержимого окна программы представлен на следующем рисунке.

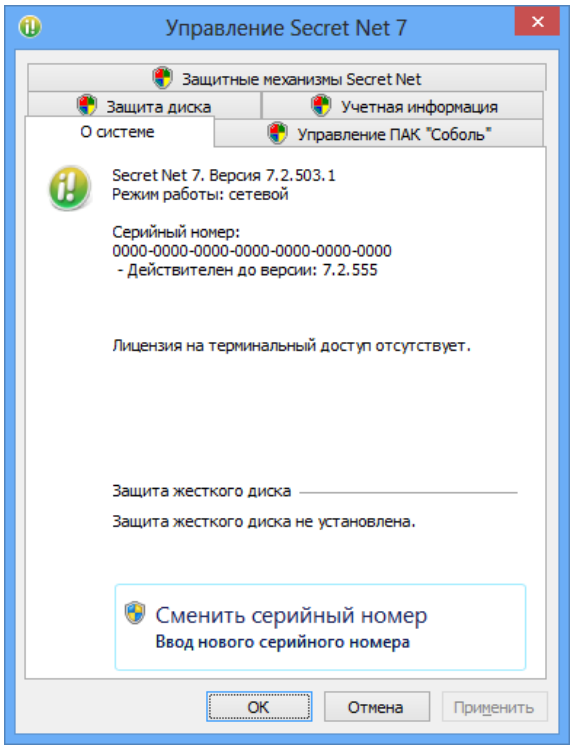


Настройка подсистемы полномочного управления доступом выполняется администратором. Описание процедур использования программы приводится в документе [**3**].

Диалоговое окно "Управление Secret Net 7" в Панели управления Windows

Диалоговое окно "Управление Secret Net 7" предназначено для просмотра и редактирования общей информации о системе, для локального управления серийными номерами лицензий, а также для управления функционированием защитных механизмов и аппаратных средств защиты.

Вызов диалогового окна осуществляется из Панели управления ОС Windows.



Описание процедур использования окна "Управление Secret Net 7" приводится в документе [**3**].

Средства централизованного управления

Средства централизованного управления используются на рабочих местах администраторов для централизованной настройки параметров и для контроля функционирования защищаемых компьютеров. Применение средств централизованного управления невозможно для компьютеров, на которых система Secret Net установлена в автономном режиме функционирования.

В состав средств централизованного управления входят следующие программные средства:

- интегрированные средства управления параметрами в оснастке редактирования объектов групповой политики;
- интегрированные средства управления пользователями в оснастке "Active Directory — пользователи и компьютеры";
- программа управления пользователями;
- программа "Контроль программ и данных" в централизованном режиме работы;
- программа оперативного управления.

Примечание.
В приведенном списке перечислены регулярно используемые средства управления. Для выполнения частных специфических задач могут использоваться дополнительные программные средства, описание работы с которыми приводится в соответствующих документах.

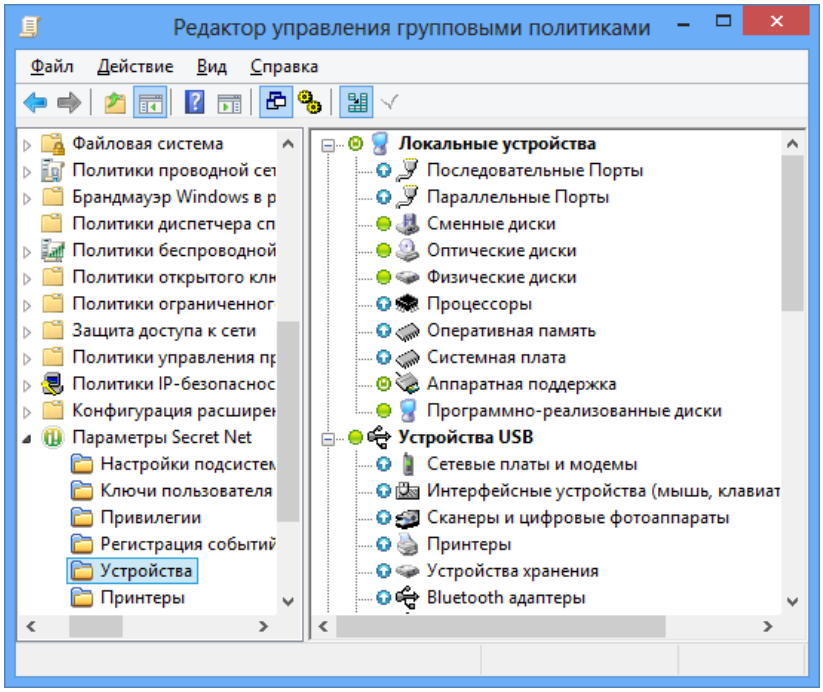
Интегрированные средства управления параметрами в оснастке групповой политики

В состав параметров групповых политик, применяемых на компьютерах, добавляются параметры системы Secret Net. В оснастке управления групповой политики домена или организационного подразделения эти параметры представлены в разделе "Конфигурация компьютера | Политики | Конфигурация Windows | Параметры безопасности | Параметры Secret Net". Применение параметров осуществляется в соответствии с их приоритетом: параметры политики организационного подразделения имеют более высокий приоритет для компьютеров этого подразделения, чем параметры политики домена.

Примечание.
Настройку параметров групповых политик также можно осуществлять в программе оперативного управления (см. стр.26). При этом приоритет параметров, заданных в программе, выше параметров политик в оснастках ОС Windows. Заданные в программе параметры применяются на компьютерах в следующей последовательности: сначала применяются параметры доменов и организационных подразделений (начиная от вышестоящих элементов иерархии к нижестоящим), а затем параметры серверов безопасности — начиная от сервера, которому компьютеры подчинены непосредственно, и далее до корневого сервера в иерархии. Таким образом, параметры политик, заданные для корневого сервера безопасности, имеют наивысший приоритет.

Для редактирования параметров групповых политик в оснастках ОС Windows необходимо на рабочем месте администратора установить стандартные средства централизованного управления ОС Windows. Версии средств централизованного управления и процедуры вызова оснасток различаются в зависимости от версии операционной системы. Сведения о необходимых средствах и используемых методах вызова оснасток приводятся в документе [**3**].

На рисунке представлен пример оснастки групповой политики.



Процедуры настройки параметров Secret Net аналогичны процедурам изменения других стандартных параметров. Описание процедур настройки приводится в документе [**3**].

Интегрированные средства управления пользователями в оснастке "Active Directory — пользователи и компьютеры"

В стандартную оснастку ОС Windows "Active Directory — пользователи и компьютеры" могут быть интегрированы специальные средства для управления параметрами доменных пользователей в системе Secret Net. Данные средства можно использовать при следующих условиях:

- установка системы Secret Net выполнена с модификацией схемы Active Directory или зарегистрированы конфигурационные данные Secret Net в разделе конфигурации каталога AD (при установке сервера безопасности или с использованием специального командного файла). Сведения о порядке установки компонентов системы Secret Net для сетевого режима функционирования см. в документе [**2**];
- на рабочем месте администратора безопасности установлены средства централизованной настройки системы Secret Net (при установке клиента в сетевом режиме функционирования). Сведения об установке клиента системы Secret Net в сетевом режиме функционирования см. в документе [**2**];
- на рабочем месте администратора безопасности установлены стандартные средства централизованного управления ОС Windows. Сведения о необходимых средствах см. в документе [**3**].

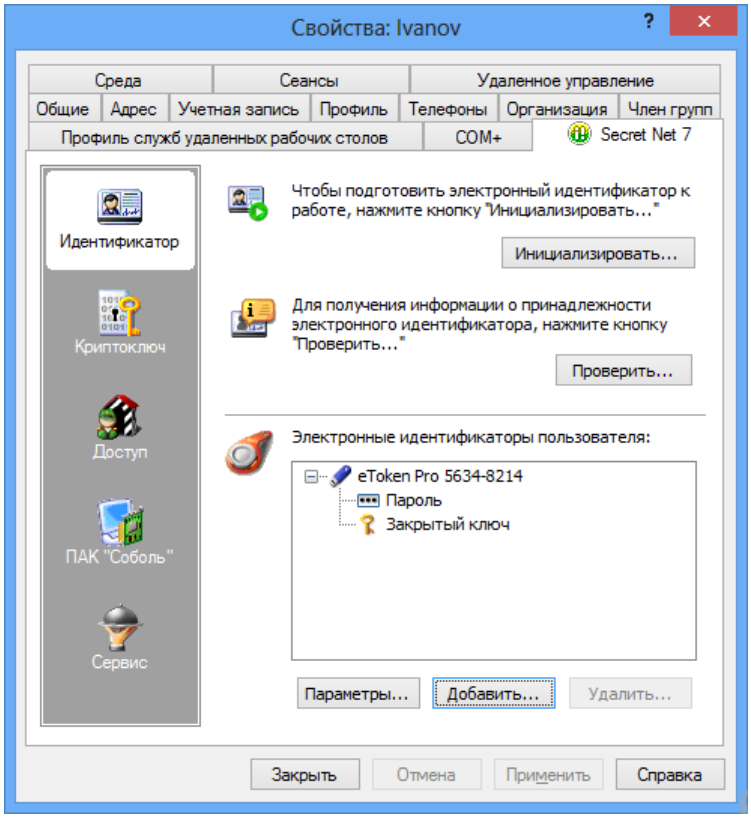
Для открытия оснастки "Active Directory — пользователи и компьютеры" выполните соответствующее действие в зависимости от версии установленной операционной системы:

- на компьютере под управлением ОС Windows 8 или Windows Server 2012 — загрузите начальный экран "Пуск", выберите элемент "Администрирование" и в открывшемся окне выберите ярлык "Пользователи и компьютеры Active Directory";
- на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Администрирование | Active Directory — пользователи и компьютеры".

Управление параметрами Secret Net для пользователей осуществляется в дополнительном диалоге "Secret Net 7", который добавляется в окно настройки

свойств пользователя. Стандартные параметры доменных пользователей хранятся в Active Directory. Параметры Secret Net могут храниться или в AD, или в отдельной базе данных — в зависимости от выбранного варианта при установке сервера безопасности.

На рисунке представлен пример диалога в окне настройки свойств доменного пользователя.



Описание процедур использования диалога "Secret Net 7" приводится в документе [**3**].

Программа управления пользователями

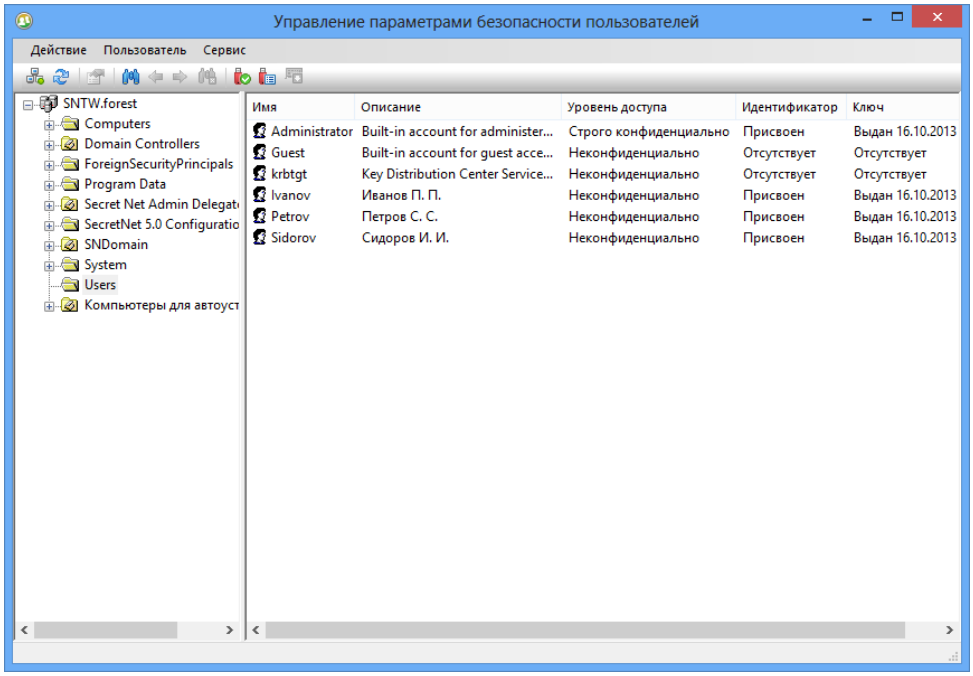
Программа управления пользователями, входящая в состав средств централизованной настройки системы Secret Net, предназначена для настройки параметров работы пользователей в системе защиты. Программа реализует те же функции, которые представлены в оснастке ОС Windows "Active Directory — пользователи и компьютеры" с интегрированными средствами управления системы Secret Net. В части настройки параметров пользователей администратор безопасности может использовать только эту программу или осуществлять настройку совместно со средствами оснастки ОС Windows.

Программу управления пользователями следует использовать только на компьютерах администраторов безопасности. На компьютерах рядовых пользователей рекомендуется устанавливать клиентское ПО Secret Net без установки средств централизованной настройки.

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 "Управление пользователями" (относится к группе "Код безопасности");
- на компьютере под управлением другой ОС — нажмите кнопку "Пуск" и в меню вызова программ выберите команду "Код безопасности | Secret Net | Управление пользователями".

Пример содержимого окна программы представлен на следующем рисунке.



Управление параметрами пользователей осуществляется аналогично оснастке ОС Windows "Active Directory — пользователи и компьютеры" с интегрированными средствами управления системы Secret Net. Описание процедур использования программы приводится в документе [**3**].

Программа "Контроль программ и данных" в централизованном режиме

Программа "Контроль программ и данных" в централизованном режиме работы предназначена для формирования централизованной модели данных с описаниями объектов, контролируемых на защищаемых компьютерах. Централизованная модель данных применяется на компьютерах совместно с локальными моделями, если они заданы. При этом приоритет имеют параметры централизованной модели.

При наличии в системе компьютеров с версиями ОС Windows различной разрядности формируются две модели данных — для компьютеров под управлением 32-разрядных версий и для компьютеров с 64-разрядными версиями операционных систем. Администратор с помощью программы может редактировать только одну централизованную модель данных, разрядность которой совпадает с разрядностью версии ОС Windows компьютера администратора. Поэтому при необходимости редактирования централизованной модели другой разрядности администратору следует использовать компьютер с версией ОС той же разрядности.

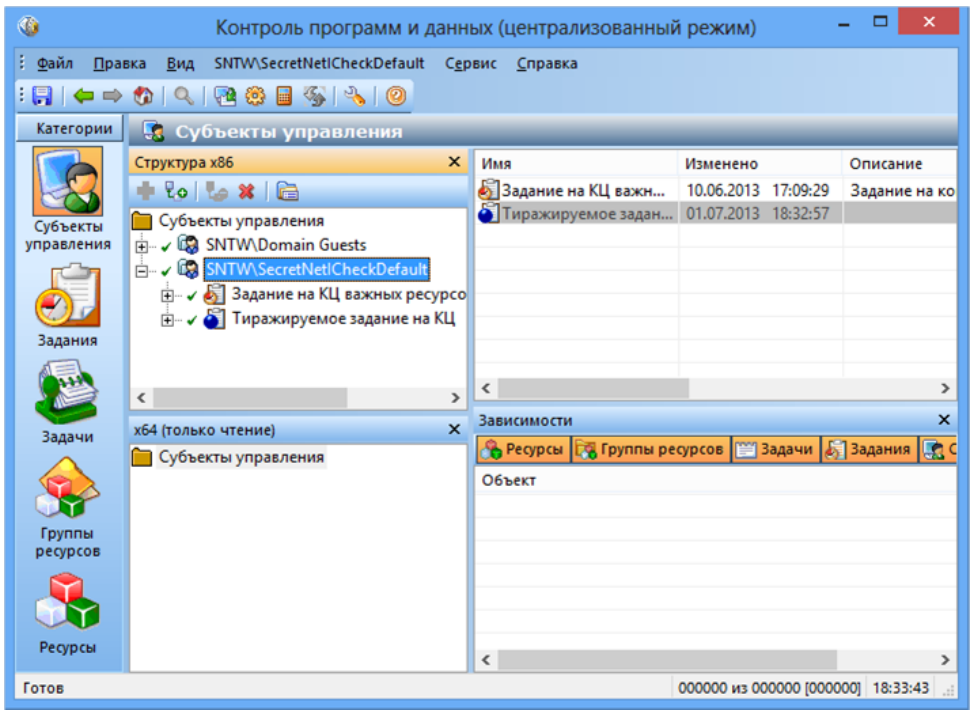
Программные модули, обеспечивающие возможность работы с программой в централизованном режиме, должны быть установлены только на компьютерах администраторов. На компьютерах рядовых пользователей рекомендуется устанавливать клиентское ПО Secret Net без установки средств централизованной настройки (в состав которых входят указанные программные модули).

Для запуска программы в централизованном 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 (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)".

Пример содержимого окна программы представлен на следующем рисунке.



Описание процедур использования программы приводится в документе [**3**].

Программа оперативного управления

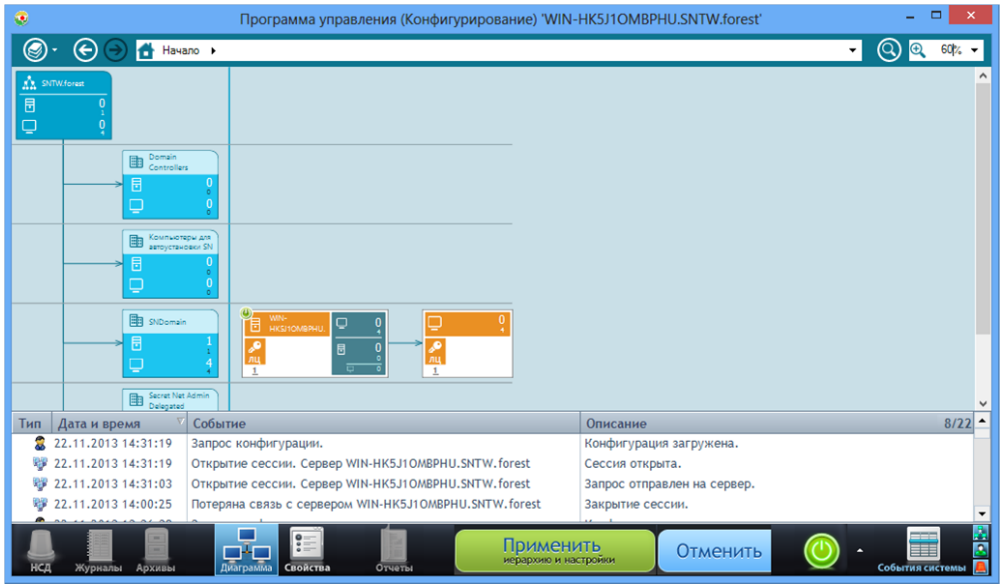
Программа оперативного управления предназначена для конфигурирования сетевой структуры, централизованного управления защищаемыми компьютерами и для работы с записями журналов, поступивших на хранение в базу данных сервера безопасности. Программа устанавливается на рабочих местах администраторов. При работе осуществляется взаимодействие с сервером безопасности, который обрабатывает все управляющие команды администратора.

Соединение с сервером безопасности может устанавливаться в одном из двух режимов: режим управления компьютерами и работы с централизованными журналами или режим конфигурирования сетевой структуры. Также предусмотрена возможность запуска программы в режиме без соединения с сервером безопасности — для работы с записями журналов, сохраненных в файлах. Выбор режима осуществляется при запуске программы. Режим работы нельзя изменить до окончания сеанса работы с программой.

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 "Программа 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 | Программа управления".

Перед началом работы на экране появляется стартовый диалог программы, предназначенный для выбора режима работы и сервера безопасности для подключения. После выбора нужного режима происходит открытие основного окна программы. На рисунке представлен пример основного окна программы в режиме конфигурирования сетевой структуры.



Описание процедур использования программы приводится в документе [**4**].

Глава 3
Защитные механизмы

Управление защитными механизмами

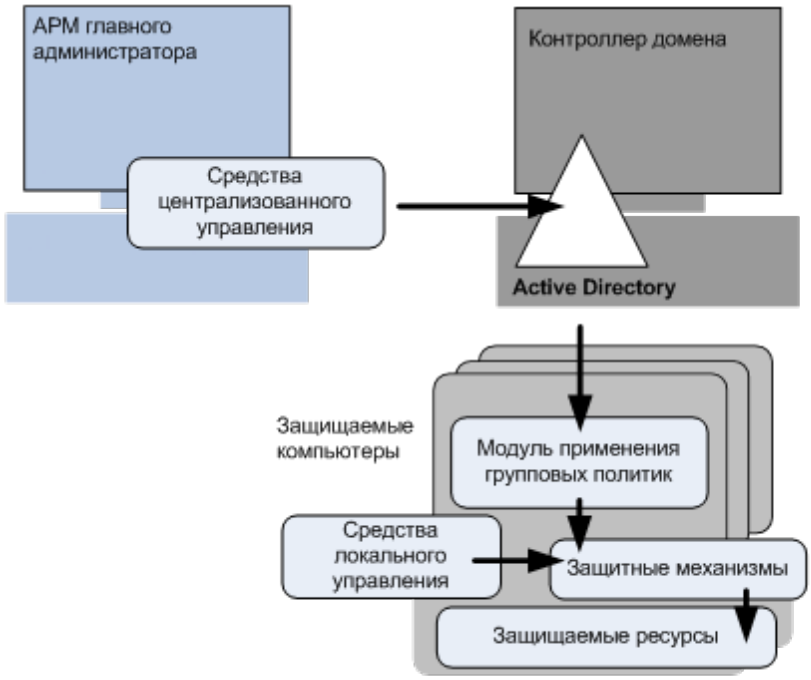
Настройка защитных механизмов может выполняться средствами локального управления, а в сетевом режиме функционирования системы — также и средствами централизованного управления.

Получение и применение настроек

При входе пользователя в систему осуществляется формирование контекста пользователя и сохранение полученных настроек в памяти компьютера. Поэтому после изменения параметров пользователя они в большинстве случаев вступают в силу только при следующем входе пользователя в систему. При выходе пользователя из системы информация удаляется из памяти.

Защитные подсистемы загружают параметры из локальной базы обычно при загрузке или при оповещении об изменении действующей политики безопасности.

Параметры из хранилища объектов централизованного управления запрашиваются с рабочей станции по мере необходимости (например, при загрузке компьютера или входе пользователя). Действующая политика безопасности формируется из параметров локальной и групповых политик в процессе их применения на рабочей станции. Инициатором процесса выступает операционная система, используя модуль применения групповых политик. Сначала создается список всех объектов-политик, имеющих отношение к данной рабочей станции, в порядке увеличения их приоритета: от локальной политики (она имеет самый низкий приоритет), далее политики домена и организационного подразделения, заданные в стандартных оснастках ОС Windows, затем аналогичные политики, заданные в программе оперативного управления системы Secret Net, и завершают список политики серверов безопасности, к которым относится компьютер (наивысший приоритет у политики корневого сервера в иерархии). Настройки всех политик с учетом их приоритетов последовательно объединяются в локальной политике. После этого сформированные настройки сохраняются в локальной базе данных.



Защита сетевых обращений к службам каталогов

В сетевом режиме функционирования системы Secret Net предусмотрен режим усиленной защиты доступа к службам каталогов. В этом режиме сетевые обращения к службам каталогов, выполняемые компонентами системы Secret Net, осуществляются с использованием протоколов Secure Socket Layer/Transport Layer Security (SSL/TLS). Данные протоколы предусматривают проверку подлинности компьютера, на котором развернута служба каталогов (контроллер домена или сервер безопасности), и реализуют функции установки безопасного соединения с использованием сертификатов.

Для использования режима защиты доступа к службам каталогов в системе должна быть организована и настроена инфраструктура открытых ключей (Public Key Infrastructure — PKI). Для внедрения PKI могут применяться стандартные средства ОС Windows или ПО сторонних производителей — например, ПО "КриптоПро". Сведения о настройке защищенного соединения со службами каталогов с применением стандартных средств ОС приведены в документе [**3**].

Механизм защиты входа в систему

Защита входа в систему обеспечивает предотвращение доступа посторонних лиц к компьютеру. К механизму защиты входа относятся следующие средства:

- средства для идентификации и аутентификации пользователей;
- средства блокировки компьютера;
- аппаратные средства защиты от загрузки ОС со съемных носителей.

Идентификация и аутентификация пользователей

Идентификация и аутентификация пользователя выполняются при каждом входе в систему. Штатная для ОС Windows процедура входа предусматривает ввод имени и пароля пользователя или использование аппаратных средств, поддерживаемых операционной системой.

В системе Secret Net идентификация пользователей может выполняться в следующих режимах:

- "По имени" — пользователь может войти в систему, выполнив ввод имени и пароля или используя аппаратные средства, стандартные для ОС Windows;
- "Смешанный" — пользователь может войти в систему, выполнив ввод имени и пароля, а также использовать персональный идентификатор, поддерживаемый системой Secret Net;
- "Только по идентификатору" — каждый пользователь для входа в систему должен обязательно использовать персональный идентификатор, поддерживаемый системой Secret Net.

Для обеспечения защиты входа в Secret Net могут применяться средства идентификации и аутентификации на базе идентификаторов eToken, iKey, Rutoken, JaCarta или iButton. Такие устройства должны быть зарегистрированы (присвоены пользователям) средствами системы защиты. Кроме того, предусмотрены режимы усиленной аутентификации, основанные на дополнительной проверке подлинности предъявленной ключевой информации пользователя или его пароля системой Secret Net. Носителями ключевой информации могут являться идентификаторы или сменные носители, такие как дискеты, флеш-карты, флеш-накопители и т. п. Генерация ключевой информации выполняется средствами системы Secret Net.

Усилить защиту компьютеров можно с помощью следующих режимов:

- режим разрешения интерактивного входа только для доменных пользователей — в этом режиме блокируется вход в систему локальных пользователей (под локальными учетными записями);
- режим запрета вторичного входа в систему — в этом режиме блокируется запуск команд и сетевых подключений с вводом учетных данных другого пользователя (не выполнившего интерактивный вход в систему).

В сетевом режиме функционирования системы Secret Net предусмотрена возможность взаимодействия со средством защиты информации TrustAccess при совместном использовании этих продуктов. При взаимодействии обеспечивается синхронизация учетных данных доменных пользователей в базе данных TrustAccess с помощью средств системы Secret Net. За счет этого пользователи при входе в систему автоматически авторизуются и в домене TrustAccess, что обеспечивает более удобное использование функций указанного средства защиты (при этом домен TrustAccess должен соответствовать домену безопасности Secret Net). Для взаимодействия с СЗИ TrustAccess в системе Secret Net необходимо включить режим интеграции с TrustAccess и включить режим синхронизации учетных данных для нужных пользователей (включение режима синхронизации учетных данных доступно после включения режима интеграции с TrustAccess).

Блокировка компьютера

Средства блокировки компьютера предназначены для предотвращения несанкционированного использования компьютера. В этом режиме блокируются устройства ввода (клавиатура и мышь) и экран монитора.

Блокировка при неудачных попытках входа в систему

Для пользователей могут быть установлены ограничения на количество неудачных попыток входа в систему. В дополнение к стандартным возможностям ОС Windows (блокировка учетной записи пользователя после определенного числа попыток ввода неправильного пароля) система Secret Net может контролировать неудачные попытки входа в систему при включенном режиме усиленной аутентификации по ключу или по паролю. Если пользователь определенное количество раз предъявляет неверную ключевую информацию или вводит пароль, который не был сохранен в БД Secret Net, — система блокирует компьютер. Разблокирование компьютера осуществляется администратором. Счетчик неудачных попыток обнуляется при удачном входе пользователя или после разблокирования компьютера.

Временная блокировка компьютера

Режим временной блокировки включается в следующих случаях:

- если пользователь выполнил действие для включения блокировки;
- если истек заданный интервал неактивности (простоя) компьютера.

Для включения блокировки пользователь может применить стандартный способ блокировки рабочей станции или изъять свой идентификатор из считывателя. Чтобы выполнялась блокировка при изъятии идентификатора, администратору необходимо настроить реакцию на это действие в групповой политике. Блокировка при изъятии идентификатора выполняется при условии, если пользователь выполнил вход в систему с использованием этого идентификатора.

Блокировка по истечении заданного интервала неактивности осуществляется автоматически и распространяется на всех пользователей компьютера.

Для снятия временной блокировки необходимо указать пароль текущего пользователя или предъявить его идентификатор.

Блокировка компьютера при работе защитных подсистем

Блокировка компьютера предусмотрена и в алгоритмах работы защитных подсистем. Такой тип блокировки используется в следующих ситуациях:

- при нарушении функциональной целостности системы Secret Net;
- при изменениях аппаратной конфигурации компьютера;
- при нарушении целостности контролируемых объектов.

Разблокирование компьютера в перечисленных случаях осуществляется администратором.

Блокировка компьютера администратором оперативного управления

В сетевом режиме функционирования блокировка и разблокирование защищаемого компьютера могут осуществляться удаленно по команде пользователя программы оперативного управления.

Аппаратные средства защиты

В Secret Net поддерживается работа с аппаратными средствами, перечисленными в следующей таблице.

Аппаратные средства	Основные решаемые задачи
Средства идентификации и аутентификации на базе идентификаторов eToken, iKey, Rutoken и JaCarta	• Идентификация и аутентификация во время входа пользователя после загрузки ОС. • Идентификация и аутентификация во время входа пользователя с удаленного компьютера. • Снятие временной блокировки компьютера. • Хранение в идентификаторе пароля и криптографического ключа
Устройства Secret Net Card и Secret Net Touch Memory Card PCI 2	• Идентификация и аутентификация во время входа пользователя после загрузки ОС. • Идентификация и аутентификация во время входа пользователя с удаленного компьютера. • Запрет загрузки ОС со съемных носителей. • Снятие временной блокировки компьютера. • Хранение в идентификаторе пароля и криптографического ключа

Аппаратные средства	Основные решаемые задачи
Программно-аппаратные комплексы (ПАК) "Соболь" версий 3.0 и 2.1	• Идентификация и аутентификация пользователей до загрузки ОС. • Идентификация и аутентификация во время входа пользователя после загрузки ОС. • Идентификация и аутентификация во время входа пользователя с удаленного компьютера. • Запрет загрузки ОС со съемных носителей. • Контроль целостности программной среды компьютера до загрузки ОС. • Снятие временной блокировки компьютера. • Хранение в идентификаторе пароля и криптографического ключа

Для идентификации и аутентификации пользователей могут применяться следующие средства:

- идентификаторы iButton (поддерживаемые типы DS1992 — DS1996). Считывающее устройство iButton подключается к разъему платы ПАК "Соболь", Secret Net Card или Secret Net Touch Memory Card PCI 2;
- USB-ключи eToken PRO, eToken PRO (Java), iKey 2032, Rutoken, Rutoken S, Rutoken ЭЦП, Rutoken Lite, JaCarta PKI, JaCarta ГОСТ;
- контактные смарт-карты eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta ГОСТ и USB-считыватель Athena ASEDrive.

Общие сведения об интеграции Secret Net и комплексов "Соболь"

ПАК семейства "Соболь" обеспечивают защиту от НСД к информационным ресурсам автономных компьютеров, сетевых рабочих станций и серверов, на которые устанавливается система Secret Net. ПАК семейства "Соболь" могут функционировать как автономно, так и совместно с Secret Net.

В автономном режиме работы ПАК "Соболь" реализуют свои основные функции до старта операционной системы независимо от Secret Net. Любым внешним программам при этом запрещается доступ к энергонезависимой памяти комплекса. Управление пользователями, журналом регистрации событий, настройка общих параметров осуществляются средствами администрирования комплекса без ограничений.

В режиме совместного использования (интеграции) внешним программам, входящим в состав Secret Net, разрешается доступ к энергонезависимой памяти комплекса. В этом случае значительная часть функций управления комплексом осуществляется с помощью средств администрирования Secret Net. Перечень функций представлен в следующей таблице.

Функция	Описание
Управление входом пользователя Secret Net в комплекс "Соболь" с помощью идентификатора, инициализированного и присвоенного пользователю в системе Secret Net	Пользователю предоставляются права на автоматический вход в комплекс и далее в систему при однократном предъявлении идентификатора. Также для входа может использоваться пароль, записанный в память персонального идентификатора
Управление работой подсистемы контроля целостности ПАК "Соболь"	Для ПАК "Соболь" задания на контроль целостности файлов жесткого диска формируются средствами администрирования Secret Net
Автоматическая передача записей журнала регистрации событий ПАК "Соболь" в журнал Secret Net	Передача записей и их преобразование осуществляются автоматически при загрузке подсистемы аппаратной поддержки Secret Net

Подробные сведения о реализации этих функций содержатся в документе [**3**].

Внимание!
В режиме интеграции системы Secret Net и комплекса "Соболь" идентификатор iButton DS1992 не используется. Рекомендуется использовать идентификаторы DS1995, DS1996 или USB-ключи и смарт-карты, поддерживаемые ПАК "Соболь".

Для обеспечения защиты данных в процессе централизованного управления ПАК "Соболь" в Secret Net реализован ряд криптографических преобразований на основе ГОСТ 28147–89, ГОСТ Р34.10–2001. Ниже в таблице представлен перечень используемых ключей шифрования и их назначение.

Наименование ключа	Назначение	Место хранения
Симметричный ключ ЦУ	Шифрование аутентификаторов[1] в хранилище объектов централизованного управления Secret Net. Расчет имитовставки для списка доступных пользователю компьютеров	Персональный идентификатор администратора
Закрытый ключ ЦУ	Расчет сессионного ключа компьютера при выполнении операций администрирования	Персональный идентификатор администратора
Открытый ключ ЦУ	Расчет сессионного ключа компьютера при выполнении операций синхронизации	Локальная база данных управляемого компьютера
Закрытый ключ компьютера	Расчет сессионного ключа компьютера при выполнении операций синхронизации	Локальная база данных управляемого компьютера
Открытый ключ компьютера	Расчет сессионного ключа компьютера при выполнении операций администрирования	Служба каталогов
Сессионный ключ компьютера	Шифрование информации, предназначенной для защищаемого компьютера	Не хранится (вычисляется в процессе работы)
Ключ преобразования паролей комплексов "Соболь"	Шифрование информации в закрытой памяти платы комплексов "Соболь". Шифрование информации, хранящейся в локальной базе данных защищаемого компьютера	Закрытая память платы комплексов "Соболь"

Дискреционное управление доступом к ресурсам файловой системы

В состав системы Secret Net входит механизм дискреционного управления доступом к ресурсам файловой системы. Этот механизм обеспечивает:

- разграничение доступа пользователей к каталогам и файлам на локальных дисках на основе матрицы доступа субъектов (пользователей, групп) к объектам доступа;
- контроль доступа к объектам как при локальных, так и при сетевых обращениях, включая обращения от имени системной учетной записи;
- невозможность доступа к объектам в обход установленных прав доступа с использованием стандартных средств ОС или прикладных программ (не использующих собственные драйверы для работы с файловой системой);
- независимость действия от встроенного механизма избирательного разграничения доступа ОС Windows. То есть установленные права доступа к

[1] Аутентификатор — структура данных, хранящаяся в службе каталогов, которая совместно с паролем пользователя используется в процедуре его аутентификации.

файловым объектам в системе Secret Net не влияют на аналогичные права доступа в ОС Windows и наоборот.

Аналогично реализации в ОС Windows матрица доступа в системе Secret Net представляет собой списки файловых объектов, в которых определены пользователи и группы пользователей с установленными правами доступа в виде разрешений или запретов на выполнение операций. Перечень предусмотренных прав доступа представлен в следующей таблице.

Право доступа	Действие для каталога	Действие для файла
Чтение (R)	Разрешает или запрещает просмотр имен файлов и подкаталогов	Разрешает или запрещает чтение данных
	Разрешает или запрещает просмотр атрибутов файлового объекта	
Запись (W)	Разрешает или запрещает создание подкаталогов и файлов	Разрешает или запрещает внесение изменений
	Разрешает или запрещает смену атрибутов файлового объекта	
Выполнение (X)	Разрешает или запрещает перемещение по структуре подкаталогов	Разрешает или запрещает выполнение
Удаление (D)	Разрешает или запрещает удаление файлового объекта	
Изменение прав доступа (P)	Разрешает или запрещает изменение прав доступа к файловому объекту. Пользователь, имеющий разрешение на изменение прав доступа к ресурсу, условно считается администратором ресурса	

Права доступа для файлового объекта могут быть заданы явно или наследоваться от вышестоящего элемента иерархии. Явно заданные права имеют более высокий приоритет по сравнению с наследуемыми правами. Права доступа считаются заданными явно, если для объекта отключен режим наследования прав.

Для обеспечения возможности управления списками доступа к любым файловым объектам предусмотрена специальная привилегия "Дискреционное управление доступом: Управление правами доступа". Пользователи, обладающие этой привилегией, могут изменять права доступа для всех каталогов и файлов на локальных дисках (независимо от установленных прав доступа к объектам).

По умолчанию привилегией на управление правами доступа обладают пользователи, входящие в локальную группу администраторов. При этом для всех пользователей действуют разрешающие права доступа к любым ресурсам на чтение, запись, выполнение и удаление (RWXD), наследуемые от корневых каталогов логическоих разделов. Во избежание непреднамеренной блокировки работы ОС, которая может произойти из-за некорректно установленных прав доступа к ресурсам, отсутствует возможность изменения прав доступа для корневого каталога системного диска (%SystemDrive%) и всего системного каталога (%SystemRoot%).

Копирование и перемещение файловых объектов

При копировании файлового объекта для его копии принудительно включается режим наследования прав доступа, даже если оригинальный объект обладает явно заданными правами.

Если файловый объект перемещается в пределах своего логического раздела, явно заданные права доступа сохраняются для этого объекта, а при включенном режиме наследования вступают в действие права того каталога, в который перемещен объект. При перемещении в другой логический раздел — принудительно включается режим наследования прав.

Аудит операций с файловыми объектами

При работе механизма дискреционного управления доступом в журнале Secret Net могут регистрироваться события успешного доступа к объектам, запрета доступа или изменения прав. По умолчанию регистрация событий успешного доступа не осуществляется, а события запрета доступа и изменения прав регистрируются для всех файловых объектов. Включение и отключение общей регистрации указанных событий осуществляется администратором безопасности при настройке параметров групповых политик.

Для файловых объектов можно детализировать аудит по выполняемым операциям, которые требуют определенных прав доступа. Например, включить аудит успешного доступа при выполнении операций записи в файл или удаления. Включение и отключение аудита операций может выполнять администратор ресурса при настройке дополнительных параметров прав доступа к файловому объекту.

Разграничение доступа к устройствам

Разграничение доступа пользователей к устройствам выполняется на основании списков устройств, формируемых и поддерживаемых в актуальном состоянии механизмом контроля подключения и изменения устройств (см. стр.40).

Система Secret Net предоставляет следующие возможности для разграничения доступа пользователей к устройствам:

- установка стандартных разрешений и запретов на выполнение операций с устройствами;
- назначение устройствам категорий конфиденциальности или допустимых уровней конфиденциальности сессий пользователей для разграничения доступа с использованием механизма полномочного управления доступом.

Возможности по разграничению доступа зависят от типов устройств. Разграничение доступа пользователей не осуществляется полностью или частично для устройств, имеющих особую специфику использования или необходимых для функционирования компьютера. Например, не ограничивается доступ к процессору и оперативной памяти, отсутствуют некоторые возможности разграничения доступа для портов ввода/вывода.

Для устройств с отключенным режимом контроля или запрещенных для подключения не действует разграничение доступа по установленным разрешениям и запретам на выполнение операций. Права доступа пользователей к таким устройствам не контролируются.

При установке клиентского ПО системы Secret Net устанавливаются права доступа (разрешения и запреты на выполнение операций) для всех обнаруженных устройств, поддерживающих такое разграничение доступа. По умолчанию предоставляется полный доступ трем стандартным группам пользователей: "Система", "Администраторы" и "Все" — то есть всем пользователям разрешен доступ без ограничений ко всем устройствам, обнаруженным на компьютере при установке системы Secret Net. Далее администратор безопасности разграничивает доступ пользователей к устройствам, выполняя настройку прав доступа непосредственно для устройств или для классов и групп, к которым относятся устройства.

Настройка прав доступа для классов и групп позволяет подготовить систему защиты к возможным подключениям новых устройств. Если в системе появляется новое устройство, оно включается в соответствующую группу, класс и модель (если есть). Доступ пользователей к этому устройству будет разграничен автоматически, в соответствии с правилами, действующими для группы, класса или модели устройств.

Разграничение доступа пользователей к устройствам с назначенными категориями конфиденциальности или уровнями конфиденциальности сессий осуществляется механизмом полномочного управления доступом.

Полномочное управление доступом

Механизм полномочного управления доступом обеспечивает:

- разграничение доступа пользователей к информации, которой назначена категория конфиденциальности (конфиденциальная информация);
- контроль подключения и использования устройств с назначенными категориями конфиденциальности;
- контроль потоков конфиденциальной информации в системе;
- контроль использования сетевых интерфейсов, для которых указаны допустимые уровни конфиденциальности сессий пользователей;
- контроль печати конфиденциальных документов.

По умолчанию в системе предусмотрены следующие категории конфиденциальности: "неконфиденциально" (для общедоступной информации), "конфиденциально" и "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.

Категорию конфиденциальности можно назначить для следующих ресурсов:

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

Доступ пользователя к конфиденциальной информации осуществляется в соответствии с его уровнем допуска. Если уровень допуска пользователя ниже, чем категория конфиденциальности ресурса, система блокирует доступ к этому ресурсу. После получения доступа к конфиденциальной информации уровень конфиденциальности программы (процесса) повышается до категории конфиденциальности ресурса, чтобы все сохраняемые данные имели эту категорию конфиденциальности.

Полномочное разграничение доступа на уровне устройств осуществляется следующим образом. Если устройство подключается во время сеанса работы пользователя, уровень допуска которого ниже, чем категория конфиденциальности устройства, система блокирует подключение устройства. При подключении такого устройства до начала сеанса работы пользователя — запрещается вход пользователя в систему. В режиме контроля потоков уровень конфиденциальности сессии пользователя должен соответствовать заданным категориям конфиденциальности всех подключенных устройств.

Функционирование устройства разрешено независимо от уровня допуска пользователя, если для этого устройства включен режим доступа "Устройство доступно без учета категории конфиденциальности" (включен по умолчанию).

Доступ к содержимому конфиденциального файла предоставляется пользователю, если категория конфиденциальности файла не превышает уровень допуска пользователя. При этом категория конфиденциальности, заданная для устройства, на котором располагается файл, также анализируется и имеет более высокий приоритет по сравнению с категорией конфиденциальности файла. Если категория файла ниже категории конфиденциальности устройства — система считает категорию файла равной категории устройства. При обратной ситуации, когда категория файла превышает категорию конфиденциальности устройства, такое состояние расценивается как некорректное и доступ к файлу запрещается.

Режим контроля потоков

При использовании механизма в режиме контроля потоков конфиденциальной информации всем процессам обработки данных в системе присваивается единый уровень конфиденциальности. Нужный уровень конфиденциальности из числа

доступных пользователю выбирается перед началом сессии работы на компьютере. Этот уровень нельзя изменить до окончания сессии.

В этом режиме сохранение информации разрешено только с категорией, равной уровню конфиденциальности сессии. Полностью запрещается доступ к данным, категория конфиденциальности которых превышает уровень конфиденциальности сессии (даже если уровень допуска пользователя позволяет доступ к таким данным). Таким образом, режим контроля потоков обеспечивает строгое соблюдение принципов полномочного разграничения доступа и предотвращает несанкционированное копирование или перемещение конфиденциальной информации.

Реализация режима контроля потоков накладывает дополнительные ограничения на работу пользователей в системе. Уровень конфиденциальности сессии, отличный от неконфиденциального, следует выбирать только при необходимости обработки конфиденциальных данных. Для корректной настройки системы первый вход пользователя на компьютер должен осуществляться в неконфиденциальной сессии (конфигурационный вход).

В режиме контроля потоков запрещается использование устройств, которым назначена категория конфиденциальности, отличающаяся от выбранного уровня сессии. Если на момент входа пользователя к компьютеру подключены устройства с различными категориями конфиденциальности, вход запрещается по причине конфликта подключенных устройств. Использование устройств, которым назначена категория конфиденциальности выше, чем уровень допуска пользователя, ограничивается так же, как и при отключенном режиме контроля потоков.

Режим контроля потоков позволяет установить ограничения на использование сетевых интерфейсов. Для каждого устройства, присутствующего в списке устройств в качестве сетевого интерфейса, можно выбрать 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, функционирование этого интерфейса блокируется системой защиты. Это позволяет организовать работу пользователя в различных сетях в зависимости от выбранного уровня конфиденциальности сессии.

Для сетевых интерфейсов предусмотрен режим доступности "Адаптер доступен всегда" (включен по умолчанию). В этом режиме функционирование сетевого интерфейса разрешено независимо от уровня конфиденциальности сессии.

Вывод конфиденциальной информации

Механизм полномочного управления доступом осуществляет контроль вывода конфиденциальной информации на другие носители с потерей категории конфиденциальности (так называемые внешние носители). Устройство считается внешним носителем, если для него включен режим доступа "Устройство доступно без учета категории конфиденциальности" и файловая система для хранения данных отличается от NTFS. Чтобы осуществлять вывод конфиденциальной информации на такие носители в режиме контроля потоков, пользователь должен обладать соответствующей привилегией.

Для предотвращения несанкционированного вывода конфиденциальных документов на локальные и сетевые принтеры предусмотрен режим контроля печати конфиденциальных документов. В этом режиме вывод конфиденциальных документов на печать возможен только при наличии соответствующей привилегии. В распечатываемые конфиденциальные документы автоматически добавляется гриф конфиденциальности. Гриф может быть выбран из готового набора или создан администратором. События печати регистрируются в журнале Secret Net.

Замкнутая программная среда

Механизм замкнутой программной среды позволяет определить для любого пользователя компьютера индивидуальный перечень программного обес-

печения, разрешенного для использования. Система защиты контролирует и обеспечивает запрет использования следующих ресурсов:

- файлы запуска программ и библиотек, не входящие в перечень разрешенных для запуска и не удовлетворяющие определенным условиям;
- сценарии, не входящие в перечень разрешенных для запуска и не зарегистрированные в базе данных.

Примечание.
Сценарий (называемый также скрипт) представляет собой последовательность исполняемых команд и/или действий в текстовом виде. Система Secret Net контролирует выполнение сценариев, созданных по технологии Active Scripts.

Попытки запуска неразрешенных ресурсов фиксируются как события НСД в журнале Secret Net.

На этапе настройки механизма составляется список ресурсов, разрешенных для запуска и выполнения. Список может быть сформирован автоматически на основании сведений об установленных на компьютере программах или по записям журналов, содержащих сведения о запусках программ, библиотек и сценариев. Также предусмотрена возможность ручного формирования списка. Для файлов, входящих в список, можно включить режим контроля целостности (см. стр. 39). По этой причине механизм замкнутой программной среды и механизм контроля целостности используют единую модель данных.

Механизм замкнутой программной среды не осуществляет блокировку запускаемых программ, библиотек и сценариев в следующих случаях:

- при наличии у пользователя привилегии "Замкнутая программная среда: Не действует" (по умолчанию привилегия предоставлена администраторам компьютера) — контроль запускаемых пользователем ресурсов не осуществляется;
- при включенном мягком режиме работы подсистемы замкнутой программной среды — в этом режиме контролируются попытки запуска программ, библиотек и сценариев, но разрешается использование любого ПО. Этот режим обычно используется на этапе настройки механизма.

Защита информации на локальных дисках

Механизм защиты информации на локальных дисках компьютера (механизм защиты дисков) предназначен для блокирования доступа к жестким дискам при несанкционированной загрузке компьютера. Загрузка считается санкционированной, если она выполнена средствами операционной системы с установленным клиентским ПО Secret Net. Все другие способы загрузки ОС считаются несанкционированными (например, загрузка с внешнего носителя или загрузка другой ОС, установленной на компьютере).

Механизм обеспечивает защиту информации при попытках доступа, осуществляемых с помощью штатных средств операционной системы.

Действие механизма защиты дисков основано на модификации загрузочных секторов (boot-секторов) логических разделов на жестких дисках компьютера. Содержимое загрузочных секторов модифицируется путем кодирования с использованием специального ключа, который автоматически генерируется при включении механизма. Модификация позволяет скрыть информацию о логических разделах при несанкционированной загрузке компьютера — разделы с модифицированными загрузочными секторами будут восприниматься системой как неформатированные или поврежденные.

При санкционированной загрузке компьютера осуществляется автоматическое раскодирование содержимого boot-секторов защищенных логических разделов при обращении к ним.

Выбор логических разделов, для которых устанавливается режим защиты (то есть модифицируются boot-секторы), осуществляет администратор.

Для реализации защитных функций механизма физический диск, с которого выполняется загрузка ОС, должен быть с основной загрузочной записью (Master Boot Record — MBR). При включении механизма на этом диске модифицируется MBR и часть остального пространства нулевой дорожки диска. Кроме того, часть служебных данных Secret Net сохраняется в системном реестре.

Механизм обеспечивает защиту до 128 логических разделов при общем количестве физических дисков до 32. Логические разделы, для которых устанавливается режим защиты, должны иметь файловую систему NTFS, FAT32 или FAT16. Разделы могут быть на физических дисках с основной загрузочной записью (MBR) или с таблицей разделов на идентификаторах GUID (GUID Partition Table — GPT). Диски с другими типами разбиения на логические разделы не поддерживаются (например, динамические диски).

При использовании механизма защиты дисков на компьютере должна быть установлена только одна операционная система. Если установлено несколько ОС, после включения механизма в одной из них не гарантируется устойчивая работа остальных ОС.

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

Затирание информации, удаляемой с дисков

Затирание информации на дисках необходимо для предотвращения восстановления и повторного использования удаляемой информации. Гарантированное уничтожение достигается путем записи последовательности случайных чисел на место удаленной информации в освобождаемую область диска. Для большей надежности может быть выполнено несколько циклов (проходов) затирания.

При настройке механизма можно установить различное количество циклов затирания для локальных и сменных дисков, а также для файлов, имеющих категорию конфиденциальности.

Затирание данных выполняется автоматически при удалении файла с диска.

Внимание!
Затирание файла подкачки страниц выполняется стандартными средствами ОС Windows при выключении компьютера.
Не осуществляется затирание файлов, помещаемых в "Корзину", — так как во время нахождения в этой папке файлы не удаляются с диска. Затирание таких файлов происходит после очистки содержимого "Корзины".

Регистрация событий

В процессе работы системы Secret Net события, происходящие на компьютере и связанные с безопасностью системы, регистрируются в журнале Secret Net. Все записи журнала хранятся в файле на системном диске. Формат данных идентичен формату журнала безопасности ОС Windows.

Предоставляются возможности для настройки перечня регистрируемых событий и параметров хранения журнала. Это позволяет обеспечить оптимальный объем сохраняемых сведений с учетом размера журнала и нагрузки на систему.

Контроль целостности

Механизм контроля целостности осуществляет слежение за неизменностью контролируемых объектов. Контроль проводится в автоматическом режиме в соответствии с заданным расписанием.

Объектами контроля могут быть файлы, каталоги, элементы системного реестра и секторы дисков (последние только при использовании ПАК "Соболь"). Каждый тип объектов имеет свой набор контролируемых параметров. Так, файлы могут контролироваться на целостность содержимого, прав доступа, атрибутов, а также на их существование, т. е. на наличие файлов по заданному пути.

В системе предусмотрена возможность выбора времени контроля. В частности, контроль может быть выполнен при загрузке ОС, при входе пользователя в систему, по заранее составленному расписанию.

При обнаружении несоответствия могут применяться различные варианты реакции на возникающие ситуации нарушения целостности, например, регистрация события в журнале Secret Net, блокировка компьютера.

Вся информация об объектах, методах, расписаниях контроля сосредоточена в **модели данных**. Модель данных хранится в локальной базе данных системы Secret Net и представляет собой иерархический список объектов и описание связей между ними. В модели используются следующие категории объектов в порядке от низшего уровня иерархии к высшему: ресурсы, группы ресурсов, задачи, задания и субъекты активности (компьютеры, пользователи, группы компьютеров и пользователей). Модель, включающая в себя объекты всех категорий, между которыми установлены связи, — это подробная инструкция системе Secret Net, определяющая, что и как должно контролироваться. Модель данных является общей для механизмов контроля целостности и замкнутой программной среды.

В сетевом режиме функционирования системы Secret Net управление локальными моделями данных на защищаемых компьютерах можно осуществлять централизованно. Для организации централизованного управления в AD создаются две модели данных — для компьютеров под управлением 32-разрядных версий ОС Windows и для компьютеров с 64-разрядными версиями операционных систем. Такое разделение позволяет учитывать специфику используемого ПО на защищаемых компьютерах с различными платформами.

Каждая из централизованных моделей данных является общей для всех защищаемых компьютеров под управлением версий ОС Windows соответствующей разрядности (32- или 64- разрядные версии). При изменении параметров централизованной модели, которая должна применяться на защищаемом компьютере, выполняется локальная синхронизация этих изменений. Новые параметры из централизованного хранилища передаются на компьютер, помещаются в локальную модель данных и затем используются защитными механизмами.

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.

Контроль подключения и изменения устройств компьютера

Механизм контроля подключения и изменения устройств компьютера обеспечивает:

- своевременное обнаружение изменений в аппаратной конфигурации компьютера и реагирование на эти изменения;
- поддержание в актуальном состоянии списка устройств компьютера, который используется механизмом разграничения доступа к устройствам.

Изменения аппаратной конфигурации отслеживаются системой защиты для устройств с включенным режимом контроля "Устройство постоянно подключено к компьютеру".

Начальная аппаратная конфигурация компьютера определяется на этапе установки системы, при этом значения параметров контроля задаются по умолчанию. Настройку политики контроля можно выполнить индивидуально для каждого устройства или применять к устройствам наследуемые параметры от моделей, классов и групп, к которым относятся устройства.

Используются следующие методы контроля конфигурации:

- Статический контроль конфигурации. Каждый раз при загрузке компьютера подсистема получает информацию об актуальной аппаратной конфигурации и сравнивает ее с эталонной.
- Динамический контроль конфигурации. Во время работы компьютера (а также при выходе из спящего режима) драйвер-фильтр устройств отслеживает факты подключения, отключения или изменения параметров устройств. Если произошло изменение конфигурации, драйвер-фильтр выдает оповещение об этом, и система выполняет определенные действия.

При обнаружении изменений аппаратной конфигурации система ожидает утверждения этих изменений администратором безопасности. Процедура утверждения аппаратной конфигурации необходима для санкционирования обнаруженных изменений и принятия текущей аппаратной конфигурации в качестве эталонной.

Теневое копирование выводимых данных

Механизм теневого копирования обеспечивает создание в системе дубликатов данных, выводимых на отчуждаемые носители информации. Дубликаты (копии) сохраняются в специальном хранилище, доступ к которому имеют только уполномоченные пользователи. Действие механизма распространяется на те устройства, для которых включен режим сохранения копий при записи информации.

При включенном режиме сохранения копий вывод данных на внешнее устройство возможен только при условии создания копии этих данных в хранилище теневого копирования. Если по каким-либо причинам создать дубликат невозможно, операция вывода данных блокируется.

Теневое копирование поддерживается для устройств следующих видов:

- подключаемые сменные диски;
- дисководы гибких дисков;
- дисководы оптических дисков с функцией записи;
- принтеры.

При выводе данных на подключаемый сменный диск (например, USB-флеш-накопитель) или дискету в хранилище теневого копирования создаются копии файлов, записанных на носитель в ходе операции вывода. Если файл открыт для редактирования непосредственно со сменного носителя, при сохранении новой версии файла в хранилище будет создан его отдельный дубликат.

Для устройства записи оптических дисков механизм теневого копирования создает в хранилище образ диска, если для записи используется интерфейс Image Mastering API (IMAPI), или копии файлов, если запись осуществляется в формате файловой системы Universal Disk Format (UDF). Другие интерфейсы записи запрещаются для использования.

Внимание!

Некоторые программные пакеты, имеющие функцию записи оптических дисков, используют собственные драйверы управления устройствами. Такие драйверы могут осуществлять доступ к устройству в обход механизма теневого копирования. Для обеспечения гарантированного контроля запись дисков необходимо осуществлять только с использованием штатных средств ОС Windows.

Теневое копирование распечатываемых документов осуществляется с использованием механизма контроля печати (см. стр.**42**). В качестве копии выводимой на печать информации сохраняется образ печатаемого документа в формате XPS (сокр. от XML Paper Specification) — открытый графический формат

фиксированной разметки на базе языка XML, разработанный компанией Microsoft.

Контроль вывода данных с помощью механизма теневого копирования является одной из задач аудита. События вывода данных регистрируются в журнале Secret Net. Доступ к дубликатам в хранилище теневого копирования осуществляется в программе просмотра журналов. Программа предоставляет средства для поиска по содержимому хранилища и для выполнения файловых операций с данными (открытие файлов, копирование и др.).

Администратор настраивает функционирование механизма теневого копирования в групповых политиках. При настройке определяются параметры хранилища теневого копирования, а также включается или отключается действие механизма для всех устройств или принтеров.

Функциональный контроль подсистем

Функциональный контроль предназначен для обеспечения гарантии того, что к моменту входа пользователя в ОС (т. е. к моменту начала работы пользователя) все ключевые компоненты Secret Net загружены и функционируют.

При функциональном контроле проверяется наличие в системе и работоспособность следующих компонентов:

- ядро Secret Net;
- модуль входа в систему;
- криптоядро;
- модуль репликации;
- подсистема контроля целостности;
- фильтр устройств;
- подсистема аппаратной поддержки.

Запуск функционального контроля инициирует модуль входа в систему. Если нарушен и сам модуль входа в систему, то функциональный контроль проводит модуль репликации.

В случае успешного завершения функционального контроля этот факт регистрируется в журнале Secret Net.

При неуспешном завершении функционального контроля в журнале Secret Net регистрируется событие с указанием причин (это возможно при условии работоспособности ядра Secret Net). Вход в систему разрешается только пользователям, входящим в локальную группу администраторов компьютера.

Одной из важных задач функционального контроля является обеспечение защиты ресурсов компьютера при запуске ОС в безопасном режиме (Safe mode). Безопасный режим запуска не является штатным режимом функционирования для системы Secret Net, однако при необходимости администратор может его использовать для устранения неполадок. Поскольку в безопасном режиме не действуют некоторые функции системы защиты, функциональный контроль в этих условиях завершается с ошибкой. В результате блокируется вход любых пользователей кроме администраторов. Поэтому при надлежащем соблюдении правил политики безопасности, когда никто из обычных пользователей не обладает полномочиями администратора, доступ к ресурсам компьютера в обход механизмов защиты невозможен.

Контроль печати

Механизм контроля печати обеспечивает:

- разграничение доступа пользователей к принтерам;
- регистрацию событий вывода документов на печать в журнале Secret Net;
- вывод на печать документов с определенной категорией конфиденциальности;

- автоматическое добавление грифа в распечатываемые документы (маркировка документов);
- теневое копирование распечатываемых документов.

Для реализации функций маркировки и/или теневого копирования распечатываемых документов в систему добавляются драйверы "виртуальных принтеров". Виртуальные принтеры соответствуют реальным принтерам, установленным на компьютере. Список виртуальных принтеров автоматически формируется при включении контроля печати или режима теневого копирования. Печать в этом случае разрешается только на виртуальные принтеры.

При печати на виртуальный принтер выполняются дополнительные преобразования для получения образа распечатываемого документа в формате XML Paper Specification (XPS). Далее XPS-документ копируется в хранилище теневого копирования (если для принтера включена функция теневого копирования), модифицируется нужным образом и после этого передается для печати в соответствующее печатающее устройство.

Приложение

Необходимые права для установки и управления

Система Secret Net обеспечивает возможности входа и выполнения операций для любых зарегистрированных пользователей в рамках полномочий, которыми они обладают в ОС и механизмах защиты. Для установки компонентов Secret Net и управления работой системы пользователи дополнительно должны обладать определенными административными полномочиями. Состав необходимых прав и привилегий для администрирования зависит от выполняемых операций.

В автономном режиме функционирования системы Secret Net установка ПО и все функции управления доступны пользователям, входящим в локальную группу администраторов компьютера. Некоторые функции (например, управление журналом Secret Net) могут быть переданы другим пользователям путем предоставления соответствующих привилегий.

Ниже в данном разделе приводится список основных операций при использовании системы Secret Net в сетевом режиме функционирования. Для каждой операции указаны учетные записи, для которых доступно выполнение действий. Используются следующие условные обозначения учетных записей:

- **Enterprise Admins** — пользователи, включенные в стандартную группу "Администраторы предприятия" (Enterprise Admins);
- **Schema Admins** — пользователи, включенные в стандартную группу "Администраторы схемы" (Schema Admins);
- **Domain Admins** — пользователи, включенные в стандартную доменную группу администраторов (Domain Admins);
- **Group Policy Creator Owners** — пользователи, включенные в стандартную группу владельцев-создателей групповой политики (Group Policy Creator Owners);
- **Администраторы леса доменов безопасности** — пользователи, включенные в группу администраторов леса доменов безопасности Secret Net (группа указывается при установке сервера безопасности с размещением хранилища объектов ЦУ вне Active Directory, если выбран вариант создания домена в новом лесу доменов безопасности — то есть устанавливается первый СБ в лесу доменов безопасности);
- **Администраторы домена безопасности** — пользователи, включенные в группу администраторов домена безопасности Secret Net (группа указывается при установке сервера безопасности с размещением хранилища объектов ЦУ вне Active Directory, если выбран вариант создания нового домена безопасности — то есть устанавливается первый СБ в домене безопасности);
- **Administrators** — пользователи, включенные в стандартную локальную группу администраторов компьютера (Administrators);
- **SecretNetAdmins** — пользователи, включенные в группу SecretNetAdmins (специальная группа, создаваемая в домене Windows при установке системы Secret Net и применяемая для делегирования административных полномочий на управление объектами выделенного организационного подразделения);
- **доступ к объекту <*тип_объекта*>** — пользователи, которым предоставлен доступ к объекту и его параметрам на чтение и запись стандартными средствами Windows;
- **привилегия <*название_ привилегии*>** — пользователи, которым назначена указанная привилегия.

Установка и удаление компонентов

Основные операции при установке или удалении компонентов системы Secret Net представлены в следующих таблицах. Сведения о выполнении процедур см.

в документе [**2**].

Табл.1 Предварительные действия перед развертыванием системы Secret Net

Операция	Учетные записи с правами на выполнение	
	Хранилище объектов ЦУ в БД Active Directory	**Хранилище объектов ЦУ вне Active Directory**
Модификация схемы AD	Enterprise Admins + Schema Admins	Операция не требуется
Регистрация конфигурационных данных в разделе конфигурации каталога AD с помощью командного файла	Операция не требуется (выполняется при модификации схемы AD)	Enterprise Admins[1)]
Создание групп пользователей для администраторов леса домена безопасности и администраторов домена безопасности	Операция не требуется	Пользователи с правами для создания групп в домене AD и для включения пользователей в группы

Примечание:

1) Операция не требуется, если настройка параметров пользователей будет осуществляться только в программе управления пользователями из состава ПО клиента системы Secret Net (параметры Secret Net будут отсутствовать в стандартной оснастке "Active Directory — пользователи и компьютеры"). Кроме того, регистрацию данных можно осуществить позже при установке сервера безопасности — для этого необходимо однократно выполнить установку сервера пользователем с правами на изменение конфигурации каталога AD.

Табл.2 Установка и удаление сервера безопасности

Операция	Учетные записи с правами на выполнение	
	Хранилище объектов ЦУ в БД Active Directory	**Хранилище объектов ЦУ вне Active Directory**
Установка с размещением хранилища объектов ЦУ в AD	Administrators + Domain Admins	–
Установка с созданием домена в новом лесу доменов безопасности	–	Administrators (доменный пользователь)
Установка с созданием нового домена безопасности в существующем лесу	–	Administrators + Администраторы леса доменов безопасности
Установка с добавлением сервера в существующий домен безопасности	–	Administrators + Администраторы леса доменов безопасности + Администраторы домена безопасности
Удаление в штатном режиме: с одновременным удалением сервера из структуры ОУ	Administrators + Domain Admins	Administrators + Администраторы домена безопасности
Удаление в нештатном режиме: без корректировки структуры ОУ[1)]	Administrators	Administrators

Примечание:

1) Операция, в результате которой на компьютере будет удалено ПО сервера безопасности, но информация о сервере останется в структуре ОУ. Для удаления сервера из структуры можно использовать программу оперативного управления (см. стр. 47). Данный вариант возможен, если в системе присутствует хотя бы один сервер безопасности, доступный для подключения программы. При нештатном удалении последнего сервера леса доменов происходит следующее: если хранилище объектов ЦУ размещается в AD — сведения о сервере остаются в AD, но никак не влияют на работу службы каталогов (при необходимости администратор домена может их удалить в оснастке ADSIEdit); если хранилище объектов ЦУ размещается вне AD — данные леса доменов безопасности уничтожаются при удалении ПО сервера.

Табл.3 Установка и удаление клиента

Операция	Учетные записи с правами на выполнение	
	Хранилище объектов ЦУ в БД Active Directory	**Хранилище объектов ЦУ вне Active Directory**
Установка с подключением к серверу безопасности	Administrators + Domain Admins ИЛИ Administrators + SecretNetAdmins + доступ к объекту "Компьютер"	Administrators + Администраторы домена безопасности
Установка без подключения к серверу безопасности[1)]	Administrators	Administrators
Удаление с одновременным удалением клиента из структуры ОУ	Administrators + Domain Admins ИЛИ Administrators + SecretNetAdmins + доступ к объекту "Компьютер"	Administrators + Администраторы домена безопасности
Удаление без корректировки структуры ОУ[2)]	Administrators	Administrators

Примечания:

1) Операция, в результате которой на компьютере будет установлено ПО клиента, но клиент не будет связан с сервером безопасности в структуре ОУ. Для добавления сопоставленного клиенту агента в структуру и подчинения его серверу безопасности можно использовать программу оперативного управления (см. стр.47).
2) Операция, в результате которой на компьютере будет удалено ПО клиента, но информация о клиенте останется в структуре ОУ. Для удаления сопоставленного клиенту агента из структуры ОУ можно использовать программу оперативного управления (см. стр.47).

Табл.4 Установка и удаление программы оперативного управления

Операция	Учетные записи с правами на выполнение	
	Хранилище объектов ЦУ в БД Active Directory	**Хранилище объектов ЦУ вне Active Directory**
Установка	Administrators	Administrators
Удаление	Administrators	Administrators

Настройка механизмов и управление параметрами объектов

Основные операции при настройке механизмов защиты системы Secret Net и изменении параметров объектов (пользователей, компьютеров) представлены в следующей таблице. Сведения о выполнении процедур см. в документе [**3**].

Табл.5 Настройка механизмов и управление параметрами объектов

Операция	Учетные записи с правами на выполнение	
	Хранилище объектов ЦУ в БД Active Directory	**Хранилище объектов ЦУ вне Active Directory**
Создание и удаление пользователей	Пользователи с правами для создания и удаления учетных записей в домене AD	Пользователи с правами для создания и удаления учетных записей в домене AD
Управление параметрами пользователей, в том числе присвоение и настройка идентификаторов пользователей	Domain Admins + Administrators ИЛИ SecretNetAdmins + Administrators + доступ к объекту "Пользователь"	Администраторы домена безопасности + Administrators

Операция	Учетные записи с правами на выполнение	
	Хранилище объектов ЦУ в БД Active Directory	**Хранилище объектов ЦУ вне Active Directory**
Управление параметрами пользователей, в том числе формирование списка компьютеров для входа в ПАК "Соболь"	Domain Admins ИЛИ SecretNetAdmins + доступ к объектам "Пользователь" и "Компьютер"	Администраторы домена безопасности
Управление параметрами пользователей, в том числе ключами ЦУ ПАК "Соболь"	Domain Admins + Administrators	Администраторы домена безопасности + Administrators
Управление параметрами пользователей, в том числе параметрами интеграции с СЗИ TrustAccess	Domain Admins	Администраторы домена безопасности
Локальное управление параметрами компьютера: редактирование учетной информации, подключение ПАК "Соболь"	Domain Admins + Administrators ИЛИ SecretNetAdmins + Administrators + доступ к объекту "Компьютер"	Администраторы домена безопасности + Administrators
Настройка параметров групповых политик доменов и организационных подразделений в оснастках ОС Windows	Domain Admins ИЛИ SecretNetAdmins + Group Policy Creator Owners + доступ к объекту групповой политики	Администраторы домена безопасности + Group Policy Creator Owners + доступ к объекту групповой политики
Управление параметрами КЦ-ЗПС	Domain Admins + Administrators ИЛИ SecretNetAdmins + Administrators	Администраторы домена безопасности + Administrators

Использование программы оперативного управления

Основные операции в программе оперативного управления системы Secret Net представлены в следующей таблице. Сведения о выполнении процедур см. в документе [**4**].

Табл.6 Использование программы оперативного управления

Операция	Учетные записи с правами на выполнение	
	Хранилище объектов ЦУ в БД Active Directory	**Хранилище объектов ЦУ вне Active Directory**
Подключение к серверу безопасности и просмотр информации	Привилегия "Читать/просматривать данные" для сервера подключения	Привилегия "Читать/просматривать данные" для сервера подключения
Конфигурирование агентов (добавление в структуру ОУ, удаление, подчинение и настройка параметров в режиме конфигурирования)	Domain Admins ИЛИ SecretNetAdmins + доступ к объекту "Компьютер"	Администраторы домена безопасности
Конфигурирование серверов безопасности (добавление в структуру ОУ, удаление, подчинение и настройка параметров в режиме конфигурирования)	Domain Admins	Администраторы домена безопасности

Операция	Учетные записи с правами на выполнение	
	Хранилище объектов ЦУ в БД Active Directory	**Хранилище объектов ЦУ вне Active Directory**
Корректировка структуры ОУ после нештатного удаления сервера безопасности: удаление сервера при подключении к СБ в другом домене в том же лесу[1)]	Domain Admins (в домене сервера подключения) + Enterprise Admins	Администраторы домена безопасности (в домене сервера подключения) + Администраторы домена безопасности (в домене удаленного сервера)
Настройка параметров групповых политик доменов и организационных подразделений	Domain Admins + Привилегия "Управлять настройками Secret Net" для сервера подключения	Администраторы домена безопасности + Привилегия "Управлять настройками Secret Net" для сервера подключения
Удаленная настройка локальных параметров Secret Net: параметры локальной политики безопасности, аппаратная конфигурация, состояние защитных механизмов	Привилегия "Управлять настройками Secret Net" для сервера подключения	Привилегия "Управлять настройками Secret Net" для сервера подключения
Выполнение команд оперативного управления компьютерами: блокировка, перезагрузка, обновление политик, сбор журналов	Привилегия "Выполнять оперативные команды" для сервера подключения	Привилегия "Выполнять оперативные команды" для сервера подключения
Запуск процесса внеочередного архивирования журналов в БД сервера безопасности	Привилегия "Архивировать/ восстанавливать журналы" для сервера подключения	Привилегия "Архивировать/ восстанавливать журналы" для сервера подключения
Квитирование событий НСД (подтверждение приема информации)	Привилегия "Квитировать события НСД" для сервера подключения	Привилегия "Квитировать события НСД" для сервера подключения

Примечание:

1) Операция выполняется, если ПО сервера безопасности было удалено в нештатном режиме без корректировки структуры ОУ (см. стр. 45) и при этом для подключения программы доступен СБ в другом домене того же леса. Если подключение можно выполнить к серверу в том же домене, для удаления объекта из структуры достаточно полномочий, требуемых при конфигурировании серверов безопасности (см. выше).

Рекомендации по настройке для соответствия требованиям к автоматизированным системам

При определенных вариантах настройки система Secret Net обеспечивает соответствие требованиям для следующих классов защищенности автоматизированных систем (АС) согласно классификации документа "Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации":

- 1Д;
- 1Г;
- 1В;
- 1Б.

Общие сведения о настройке для соответствия классам защищенности

Класс 1Д

Для соответствия классу 1Д необходимо:

- настроить механизм защиты входа в систему — включить режим усиленной аутентификации пользователей (по паролю или по ключу);
- настроить механизм контроля целостности — построить модель данных по умолчанию, добавить новое задание "Контроль СЗИ" для контроля файлов и параметров реестра системы защиты. В созданном задании включить режим проведения проверки "При входе" и установить связь задания с задачей "Secret Net 7".

Если применяется режим усиленной аутентификации пользователей по паролю, в операционной системе необходимо настроить следующие параметры в политике паролей:

- установить минимальную длину пароля 6 символов;
- установить максимальный срок действия пароля не более 180 дней.

Класс 1Г

Для соответствия классу 1Г необходимо выполнить действия по настройке, указанные для систем класса 1Д, а также:

- настроить механизм затирания информации — установить не менее одного цикла затирания на локальных и сменных дисках компьютера;
- настроить механизмы разграничения доступа к устройствам и контроля подключения и изменения устройств. Рекомендуемый порядок настройки при параметрах по умолчанию: подключить к компьютеру все необходимые устройства, утвердить аппаратную конфигурацию и затем для групп устройств USB, PCMCIA и IEEE1394 включить режим контроля "Подключение устройства запрещено";
- не отключать механизм контроля печати (включен по умолчанию для рабочих станций);
- настроить механизм дискреционного управления доступом — реализовать разграничение доступа к каталогам и файлам на основе матрицы доступа субъектов (пользователей, групп) к объектам.

Для усиления защиты рекомендуется:

- использовать механизм полномочного управления доступом в режиме без контроля потоков конфиденциальной информации (это позволит разграничить доступ пользователей к файлам на основе категорий конфиденциальности);
- настроить разграничение доступа к принтерам.

В операционной системе рекомендуется настроить следующие параметры:

- включить очистку страничного файла виртуальной памяти при завершении работы системы;
- включить режим уничтожения файлов сразу после удаления, не помещая их в корзину;
- включить аудит отслеживания процессов;
- установить размер журнала безопасности не менее 2048 Кб и включить политику перезаписи событий по необходимости.

Класс 1В

Для соответствия классу 1В необходимо выполнить обязательные и рекомендуемые действия по настройке, указанные для систем класса 1Г (включение аудита отслеживания процессов остается в качестве рекомендуемого действия), а также:

- в механизме полномочного управления доступом включить режим контроля потоков конфиденциальной информации;
- в механизме контроля печати включить режим маркировки документов (стандартная или расширенная обработка) для добавления грифов при выводе на печать;
- настроить механизм замкнутой программной среды и включить жесткий режим работы механизма.

Класс 1Б

Для соответствия классу 1Б необходимо выполнить действия по настройке, указанные для систем класса 1В, а также:

- в механизме замкнутой программной среды включить режим контроля целостности модулей перед запуском;
- настроить механизм контроля целостности — в задании "Контроль СЗИ" (создается для контроля файлов и параметров реестра системы защиты) включить режим проведения проверки не только при входе пользователя в систему, а также и по расписанию.

Если применяется режим усиленной аутентификации пользователей по паролю, в операционной системе необходимо настроить следующие параметры в политике паролей:

- установить минимальную длину пароля 8 символов;
- установить максимальный срок действия пароля не более 90 дней.

Использование дополнительных средств защиты загрузки

В АС должны применяться средства, исключающие доступ пользователя к ресурсам компьютера в обход механизмов системы защиты. Для систем любого класса до 1Б включительно в качестве таких средств могут использоваться:

- изделие "Программно-аппаратный комплекс "Соболь";
- изделия Secret Net Card и Secret Net Touch Memory Card;
- механизм защиты дисков системы Secret Net.

При функционировании системы Secret Net на виртуальных машинах в виртуальной инфраструктуре на базе продуктов VMware Infrastructure или VMware vSphere в качестве средства доверенной загрузки виртуальных машин может применяться изделие "Средство защиты информации vGate R2" или "Средство защиты информации vGate-S R2", совместимое с версией используемого продукта.

Вместо вышеперечисленных средств или совместно с любым из них может быть разработан и внедрен комплекс организационно-технических мероприятий, обеспечивающих невозможность доступа пользователей к информации на дисках компьютера в обход механизмов системы Secret Net.

Настраиваемые параметры системы Secret Net

Состав действующих механизмов защиты

Для соответствия классам защищенности АС в системе Secret Net должны быть включены механизмы защиты, перечисленные в следующей таблице ("Да" — механизм включен, "Нет" — механизм отключен, "–" — значение параметра на усмотрение администратора безопасности). Описание процедур включения и отключения механизмов см. в документе [**3**].

Табл.7 Механизмы защиты системы Secret Net

Параметр	Класс защищенности			
	1Б	**1В**	**1Г**	**1Д**
Затирание данных	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Контроль устройств	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Контроль печати	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Дискреционное управление доступом	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Полномочное управление доступом	Да (обязательно)	Да (обязательно)	Да (рекомендуется)	–
Замкнутая программная среда	Да (обязательно)	Да (обязательно)	–	–
Шифровать управляющий сетевой трафик	–	–	–	–

Параметры политики безопасности

Для соответствия классам защищенности АС должны быть настроены параметры групповой политики, перечисленные в следующей таблице (приведены минимально допустимые значения или "Да" — параметр включен, "Нет" — параметр отключен, "–" — значение параметра на усмотрение администратора безопасности). Описание процедур настройки параметров см. в документе [**3**].

Табл.8 Параметры политики безопасности

Параметр	Класс защищенности			
	1Б	**1В**	**1Г**	**1Д**
Группа "Настройки подсистем"				
Администрирование: Локальное оповещение о НСД	–	–	–	–
Вход в систему: Максимальный период неактивности до блокировки экрана	10 (рекомендуется)	10 (рекомендуется)	10 (рекомендуется)	10 (рекомендуется)
Вход в систему: Разрешить интерактивный вход только доменным пользователям	–	–	–	–
Вход в систему: Реакция на изъятие идентификатора	–	–	–	–

Параметр	Класс защищенности			
	1Б	1В	1Г	1Д
Вход в систему: Режим аутентификации пользователя	Усиленная по паролю ИЛИ по ключу (обязательно)	Усиленная по паролю ИЛИ по ключу (обязательно)	Усиленная по паролю ИЛИ по ключу (обязательно)	Усиленная по паролю ИЛИ по ключу (обязательно)
Вход в систему: Режим аутентификации пользователя (с использованием КриптоПро)	–	–	–	–
Вход в систему: Режим аутентификации пользователя: регистрировать неверные аутентификационные данные	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Вход в систему: Режим идентификации пользователя	Смешанный (рекомендуется)	Смешанный (рекомендуется)	Смешанный (рекомендуется)	Смешанный (рекомендуется)
Вход в систему: Количество неудачных попыток аутентификации	–	–	–	–
Вход в систему: Запрет вторичного входа в систему	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Журнал: Максимальный размер журнала защиты	4096 (рекомендуется)	4096 (рекомендуется)	2048 (рекомендуется)	2048 (рекомендуется)
Журнал: Политика перезаписи событий	Затирать по мере необходимости (рекомендуется)	Затирать по мере необходимости (рекомендуется)	Затирать по мере необходимости (рекомендуется)	Затирать по мере необходимости (рекомендуется)
Затирание данных: Количество циклов затирания конфиденциальной информации	–	–	–	–
Затирание данных: Количество циклов затирания на локальных дисках	2 (обязательно)	2 (обязательно)	1 (обязательно)	–
Затирание данных: Количество циклов затирания на сменных носителях	2 (обязательно)	2 (обязательно)	1 (обязательно)	–
Контроль печати: Маркировка документов	Да (обязательно)	Да (обязательно)	Да (рекомендуется)	–
Контроль печати: Теневое копирование	–	–	–	–
Контроль устройств: Перенаправление устройств в RDP-подключениях	Включен запрет для всех типов (рекомендуется)	Включен запрет для всех типов (рекомендуется)	Включен запрет для всех типов (рекомендуется)	–
Контроль устройств: Теневое копирование	–	–	–	–
Полномочное управление доступом: Названия уровней конфиденциальности	Настроено (обязательно)	Настроено (обязательно)	Настроено (рекомендуется)	–

Параметр	Класс защищенности			
	1Б	**1В**	**1Г**	**1Д**
Полномочное управление доступом: Режим работы	Контроль потоков включен (обязательно)	Контроль потоков включен (обязательно)	Контроль потоков отключен (рекомендуется)	–
Полномочное управление доступом: Режим работы: строгий контроль терминальных подключений	Да (рекомендуется)	Да (рекомендуется)	–	–
Полномочное управление доступом: Режим работы: автоматический выбор максимального уровня сессии	–	–	–	–
Теневое копирование: Размер хранилища	–	–	–	–
Группа "Ключи пользователя"				
Максимальный срок действия ключа	Не более 360 (рекомендуется)	Не более 360 (рекомендуется)	Не более 360 (рекомендуется)	Не более 360 (рекомендуется)
Минимальный срок действия ключа	–	–	–	–
Предупреждение об истечении срока действия ключа	Не менее 14 (рекомендуется)	Не менее 14 (рекомендуется)	Не менее 14 (рекомендуется)	Не менее 14 (рекомендуется)
Группа "Привилегии"				
Дискреционное управление доступом: Управление правами доступа	Administrators (обязательно)	Administrators (обязательно)	Administrators (обязательно)	Administrators (рекомендуется)
Журнал: Просмотр журнала системы защиты	Administrators (рекомендуется)	Administrators (рекомендуется)	Administrators (рекомендуется)	Administrators (рекомендуется)
Журнал: Управление журналом системы защиты	Administrators (рекомендуется)	Administrators (рекомендуется)	Administrators (рекомендуется)	Administrators (рекомендуется)
Замкнутая программная среда: Не действует	Administrators (рекомендуется)	Administrators (рекомендуется)	–	–
Группа "Регистрация событий"				
TrustAccess: Ошибка синхронизации учетной информации с TrustAccess	–	–	–	–
TrustAccess: Синхронизация учетной информации с TrustAccess	–	–	–	–
Администрирование: Добавлен пользователь	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Удален пользователь	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Изменены параметры пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Изменены параметры действующей политики безопасности	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)

Параметр	Класс защищенности			
	1Б	1В	1Г	1Д
Администрирование: Изменен ключ пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Удален ключ пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Изменен пароль пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Включена защитная подсистема	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Отключена защитная подсистема	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Установлена защита для диска	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Отключена защита для диска	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Завершение работы пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Идентификатор не зарегистрирован	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Пользователь приостановил сеанс работы на компьютере	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Пользователь возобновил сеанс работы на компьютере	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Пароль пользователя не соответствует требованиям безопасности	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Система защиты инициировала блокировку сессии пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Компьютер заблокирован системой защиты	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Компьютер разблокирован	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Ошибка выполнения функционального контроля	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Успешное завершение функционального контроля	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Вход пользователя в систему	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Запрет входа пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)

Параметр	Класс защищенности			
	1Б	**1В**	**1Г**	**1Д**
Дискреционное управление доступом: Доступ к файлу или каталогу	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Дискреционное управление доступом: Запрет доступа к файлу или каталогу	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Дискреционное управление доступом: Изменение прав доступа	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Замкнутая программная среда: Запрет запуска программы	Да (обязательно)	Да (обязательно)	–	–
Замкнутая программная среда: Запуск программы	Да (обязательно)	Да (обязательно)	–	–
Замкнутая программная среда: Запрет загрузки библиотеки	Да (обязательно)	Да (обязательно)	–	–
Замкнутая программная среда: Загрузка библиотеки	Нет (рекомендуется)	Нет (рекомендуется)	–	–
Замкнутая программная среда: Запрет исполнения неизвестного скрипта	Да (обязательно)	Да (обязательно)	–	–
Замкнутая программная среда: Исполнение скрипта	Да (обязательно)	Да (обязательно)	–	–
Контроль конфигурации: Успешное завершение контроля аппаратной конфигурации	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	–
Контроль конфигурации: Обнаружены изменения в процессе контроля аппаратной конфигурации	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Контроль конфигурации: Обнаружено новое устройство	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Контроль конфигурации: Устройство удалено из системы	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Контроль конфигурации: Изменены параметры устройства	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Контроль конфигурации: Утверждение аппаратной конфигурации компьютера	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	–
Контроль конфигурации: Выход из спящего режима	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	–
Контроль конфигурации: Переход в спящий режим	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	–
Контроль печати: Печать документа	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Контроль печати: Начало печати документа	Да (обязательно)	Да (обязательно)	–	–

Параметр	Класс защищенности			
	1Б	1В	1Г	1Д
Контроль печати: Успешное завершение печати документа	Да (рекомендуется)	Да (рекомендуется)	–	–
Контроль печати: Запрет прямого обращения к принтеру	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	–
Контроль печати: Ошибка при печати документа	Да (обязательно)	Да (обязательно)	–	–
Контроль печати: Начало печати экземпляра документа	Да (обязательно)	Да (обязательно)	–	–
Контроль печати: Успешное завершение печати экземпляра документа	Да (рекомендуется)	Да (рекомендуется)	–	–
Контроль печати: Ошибка при печати экземпляра документа	Да (обязательно)	Да (обязательно)	–	–
Контроль печати: Запрет печати документа	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Контроль печати: Сохранение копии напечатанного документа	–	–	–	–
Контроль приложений: Завершение процесса	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Контроль приложений: Запуск процесса	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Контроль целостности: Начало обработки задания на контроль целостности	–	–	–	–
Контроль целостности: Успешное завершение задания на контроль целостности	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Обнаружено нарушение целостности при обработке задания	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Успешная проверка целостности ресурса	–	–	–	–
Контроль целостности: Нарушение целостности ресурса	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Для ресурса отсутствует эталонное значение	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Удаление устаревших эталонных значений	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Текущее значение ресурса принято в качестве эталонного	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)

Параметр	Класс защищенности			
	1Б	1В	1Г	1Д
Контроль целостности: Ресурс восстановлен по эталонному значению	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Ошибка при восстановлении ресурса по эталонному значению	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Ошибка при открытии базы данных контроля целостности	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Ошибка при принятии текущего значения ресурса в качестве эталонного	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Ошибка при расчете эталона	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Исправление ошибок в базе данных	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Установка задания КЦ на контроль	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Снятие задания КЦ с контроля	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Добавление учетной записи к заданию ЗПС	Да (обязательно)	Да (обязательно)	–	–
Контроль целостности: Удаление учетной записи из задания ЗПС	Да (обязательно)	Да (обязательно)	–	–
Контроль целостности: Создание задания	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Удаление задания	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Изменение задания	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Создание задачи	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Удаление задачи	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Изменение задачи	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Создание группы ресурсов	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Удаление группы ресурсов	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Изменение группы ресурсов	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Синхронизация локальной базы данных с центральной	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)

Параметр	Класс защищенности			
	1Б	1В	1Г	1Д
Контроль целостности: Ошибка синхронизации локальной базы данных с центральной	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Общие события: Событие	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Общие события: Несанкционированное действие	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Общие события: Ошибка	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Общие события: Предупреждение	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Общие события: Информационное событие	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Полномочное управление доступом: Изменение параметров конфиденциальности ресурса	Да (обязательно)	Да (обязательно)	Да (рекомендуется)	–
Полномочное управление доступом: Запрет изменения параметров конфиденциальности ресурса	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	–
Полномочное управление доступом: Доступ к конфиденциальному ресурсу	Да (обязательно)	Да (обязательно)	Да (рекомендуется)	–
Полномочное управление доступом: Запрет доступа к конфиденциальному ресурсу	Да (обязательно)	Да (обязательно)	Да (рекомендуется)	–
Полномочное управление доступом: Вывод конфиденциальной информации на внешний носитель	Да (обязательно)	Да (обязательно)	–	–
Полномочное управление доступом: Запрет вывода конфиденциальной информации на внешний носитель	Да (обязательно)	Да (обязательно)	–	–
Полномочное управление доступом: Перемещение конфиденциального ресурса	Да (обязательно)	Да (обязательно)	Да (рекомендуется)	–
Полномочное управление доступом: Запрет перемещения конфиденциального ресурса	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	–
Полномочное управление доступом: Удаление конфиденциального ресурса	Да (обязательно)	Да (обязательно)	Да (рекомендуется)	–

Параметр	Класс защищенности			
	1Б	1В	1Г	1Д
Полномочное управление доступом: Конфликт категорий конфиденциальности	Да (обязательно)	Да (обязательно)	Да (рекомендуется)	–
Полномочное управление доступом: Использование механизма исключений	Да (обязательно)	Да (обязательно)	Да (рекомендуется)	–
Разграничение доступа к устройствам: Подключение устройства	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Разграничение доступа к устройствам: Отключение устройства	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Разграничение доступа к устройствам: Запрет подключения устройства	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Разграничение доступа к устройствам: Несанкционированное отключение устройства	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Разграничение доступа к устройствам: Доступ к устройству	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Разграничение доступа к устройствам: Запрет доступа к устройству	Да (обязательно)	Да (обязательно)	Да (обязательно)	–
Расширение групповой политики: Групповые политики успешно применены	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Расширение групповой политики: Ошибка применения групповых политик	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Расширение групповой политики: Предупреждение при применении групповых политик	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Сеть: Запрет сетевого подключения под другим именем	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Служба репликации: Ошибка создания контекста пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Теневое копирование: Начата запись на сменный диск	–	–	–	–
Теневое копирование: Завершена запись на сменный диск	–	–	–	–
Теневое копирование: Ошибка записи на сменный диск	–	–	–	–

Параметр	Класс защищенности			
	1Б	1В	1Г	1Д
Теневое копирование: Запрет записи на сменный диск	–	–	–	–
Теневое копирование: Начата запись образа CD/DVD/BD	–	–	–	–
Теневое копирование: Завершена запись образа CD/DVD/BD	–	–	–	–
Теневое копирование: Ошибка записи образа CD/DVD/BD	–	–	–	–
Теневое копирование: Запрет записи образа CD/DVD/BD	–	–	–	–
ЦУ КЦ-ЗПС: Установка задания КЦ на контроль	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
ЦУ КЦ-ЗПС: Снятие задания КЦ с контроля	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
ЦУ КЦ-ЗПС: Добавление учетной записи к заданию ЗПС	Да (рекомендуется)	Да (рекомендуется)	–	–
ЦУ КЦ-ЗПС: Удаление учетной записи из задания ЗПС	Да (рекомендуется)	Да (рекомендуется)	–	–
ЦУ КЦ-ЗПС: Создание задания	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Удаление задания	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Изменение задания	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Создание задачи	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Удаление задачи	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Изменение задачи	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Создание группы ресурсов	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Удаление группы ресурсов	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Изменение группы ресурсов	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Добавление субъекта	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Удаление субъекта	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Изменение субъекта	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Группа "Устройства"				
Параметры контроля устройства	Заданы (обязательно)	Заданы (обязательно)	Заданы (обязательно)	–

Параметр	Класс защищенности			
	1Б	1В	1Г	1Д
Разрешения	Заданы (обязательно)	Заданы (обязательно)	Заданы (обязательно)	–
Теневое копирование	–	–	–	–
Категория конфиденциальности	–	–	–	–
Группа "Принтеры"				
Разрешения	Заданы (обязательно)	Заданы (обязательно)	Заданы (обязательно)	–
Категория конфиденциальности	–	–	–	–
Теневое копирование	–	–	–	–

Параметры пользователей

Для соответствия классам защищенности АС должны быть настроены параметры пользователей, перечисленные в следующей таблице (приведены минимально допустимые значения или "Да" — параметр включен, "Нет" — параметр отключен, "–" — значение параметра на усмотрение администратора безопасности). Описание процедур настройки параметров см. в документе [**3**].

Табл.9 Параметры пользователей

Параметр	Класс защищенности			
	1Б	1В	1Г	1Д
Группа параметров "Идентификатор" в диалоге "Secret Net 7"				
Ключи пользователя	Да (обязательно, если используется усиленная аутентификация по ключу)	Да (обязательно, если используется усиленная аутентификация по ключу)	Да (обязательно, если используется усиленная аутентификация по ключу)	Да (обязательно, если используется усиленная аутентификация по ключу)
Пароль пользователя	–	–	–	–
Интеграция с ПАК "Соболь"	Да (рекомендуется)	Да (рекомендуется)	–	–
Группа параметров "Доступ" в диалоге "Secret Net 7"				
Уровень допуска	Назначен уполномоченным пользователям (обязательно)	Назначен уполномоченным пользователям (обязательно)	Назначен уполномоченным пользователям (рекомендуется)	–
Привилегия: Печать конфиденциальных документов	Назначена уполномоченным пользователям (обязательно)	Назначена уполномоченным пользователям (обязательно)	Назначена уполномоченным пользователям (рекомендуется)	–
Привилегия: Управление категориями конфиденциальности	Назначена уполномоченным пользователям (обязательно)	Назначена уполномоченным пользователям (обязательно)	Назначена уполномоченным пользователям (рекомендуется)	–
Привилегия: Вывод конфиденциальной информации	Назначена уполномоченным пользователям (обязательно)	Назначена уполномоченным пользователям (обязательно)	–	–

Параметры механизмов КЦ и ЗПС

Для соответствия классам защищенности АС должны быть настроены параметры механизмов КЦ и ЗПС в программе "Контроль программ и данных", перечисленные в следующей таблице (приведены минимально допустимые значения или "Да" — параметр включен, "Нет" — параметр отключен, "–" — значение параметра на усмотрение администратора безопасности). Описание процедур настройки параметров см. в документе [**3**].

Если используется механизм замкнутой программной среды, необходимо сформировать задание ЗПС.

Контроль целостности должен выполняться как минимум для заданий, созданных при установке системы.

Табл.10 Параметры механизмов КЦ и ЗПС

Параметр	Класс защищенности			
	1Б	1В	1Г	1Д
Диалог "Режимы" в диалоговом окне настройки свойств компьютера				
Режим ЗПС включен	Да (обязательно)	Да (обязательно)	–	–
Мягкий режим	Нет (обязательно)	Нет (обязательно)	–	–
Проверять целостность модулей перед запуском	Да (обязательно)	Да (рекомендуется)	–	–
Проверять заголовки модулей перед запуском	Да (рекомендуется)	Да (рекомендуется)	–	–
Контролировать исполняемые скрипты	Да (рекомендуется)	Да (рекомендуется)	–	–
Диалоговое окно настройки параметров задания контроля СЗИ				
Метод контроля ресурсов	Содержимое (обязательно)	Содержимое (обязательно)	Содержимое (обязательно)	Содержимое (обязательно)
Алгоритм	Имитовставка (рекомендуется)	CRC-7 (рекомендуется)	CRC-7 (рекомендуется)	CRC-7 (рекомендуется)
Регистрация событий: Успех завершения	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Регистрация событий: Ошибка завершения	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Регистрация событий: Успех проверки	Нет (рекомендуется)	Нет (рекомендуется)	Нет (рекомендуется)	Нет (рекомендуется)
Регистрация событий: Ошибка проверки	Да (обязательно)	Да (обязательно)	Да (обязательно)	Да (обязательно)
Реакция на отказ: Действия	Заблокировать компьютер (рекомендуется)	Заблокировать компьютер (рекомендуется)	Заблокировать компьютер (рекомендуется)	Заблокировать компьютер (рекомендуется)
Расписание	При входе и по расписанию (обязательно)	При входе (обязательно)	При входе (обязательно)	При входе (обязательно)

Документация

1. Средство защиты информации Secret Net 7. Руководство администратора. Принципы построения	RU.88338853.501410.015 91 1
2. Средство защиты информации Secret Net 7. Руководство администратора. Установка, обновление и удаление	RU.88338853.501410.015 91 2
3. Средство защиты информации Secret Net 7. Руководство администратора. Настройка механизмов защиты	RU.88338853.501410.015 91 3
4. Средство защиты информации Secret Net 7. Руководство администратора. Работа с программой оперативного управления	RU.88338853.501410.015 91 4
5. Средство защиты информации Secret Net 7. Руководство администратора. Локальная работа с журналами регистрации	RU.88338853.501410.015 91 5
6. Средство защиты информации Secret Net 7. Руководство пользователя	RU.88338853.501410.015 92