Код безопасности
ГК «Информзащита»

Средство защиты информации

SECRET NET 6

Руководство администратора

Принципы построения

RU.88338853.501410.007 91 1

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

Версия: 6.5 Последнее обновление: 14-09-10

Оглавление

Список сокращений

AD	Active Directory
API	Application Programming Interface
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
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
USB	Universal Serial Bus
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 6" RU.88338853.501410.007 (далее — система Secret Net 6 или Secret Net 6). В нем содержатся сведения, необходимые администраторам для ознакомления с принципами работы и возможностями применения системы Secret Net 6.

Условные обозначения

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

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы выглядят так: [1].

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

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

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

Другие источники информации

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

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

Глава 1
Общие сведения

Назначение системы

Система Secret Net 6 предназначена для защиты от несанкционированного доступа к информационным ресурсам компьютеров, функционирующих под управлением операционных систем MS Windows 2000/XP/2003/Vista/2008/7.

Основные функции

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

Система Secret Net 6 может функционировать в следующих режимах:

- автономный режим — предусматривает только локальное управление защитными функциями;
- сетевой режим — предусматривает локальное и централизованное управление защитными функциями, а также централизованное получение информации и управление защищаемыми компьютерами.

Основные защитные функции, реализуемые системой Secret Net 6:

- контроль входа пользователей в систему;
- разграничение доступа пользователей к 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 Secret Net 6;
- контроль вывода конфиденциальных данных на печать;
- контроль целостности защищаемых ресурсов;
- контроль аппаратной конфигурации компьютера;
- функциональный контроль ключевых компонентов Secret Net 6;
- уничтожение (затирание) содержимого файлов при их удалении;
- 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);
- защита доступа к Active Directory при сетевых обращениях компонентов системы Secret Net 6 (только в сетевом режиме функционирования).

Состав системы

Система Secret Net 6 состоит из следующих отдельно устанавливаемых программных средств:

1. Компонент "Secret Net 6" (далее — клиент).
2. Компонент "Модификатор схемы Active Directory" (далее — модификатор AD). Используется только в сетевом режиме функционирования.
3. Компонент "Secret Net 6 — Сервер безопасности" (далее — сервер безопасности или СБ). Используется только в сетевом режиме функционирования.
4. Компонент "Secret Net 6 — Средства управления" (далее — средства управления). Используется только в сетевом режиме функционирования.

Лицензирование

Имеется ряд ограничений на использование системы Secret Net 6, связанных с политикой лицензирования данного продукта. Лицензируются следующие параметры:

- режим функционирования системы Secret Net 6;
- разрешенные для использования версии программного обеспечения;
- количество клиентов в глобальном каталоге (в сетевом режиме функционирования);
- количество подчиненных клиентов 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 6 определяются приобретенными лицензиями.

Глава 2
Архитектура и компоненты

Общая структура взаимодействия компонентов

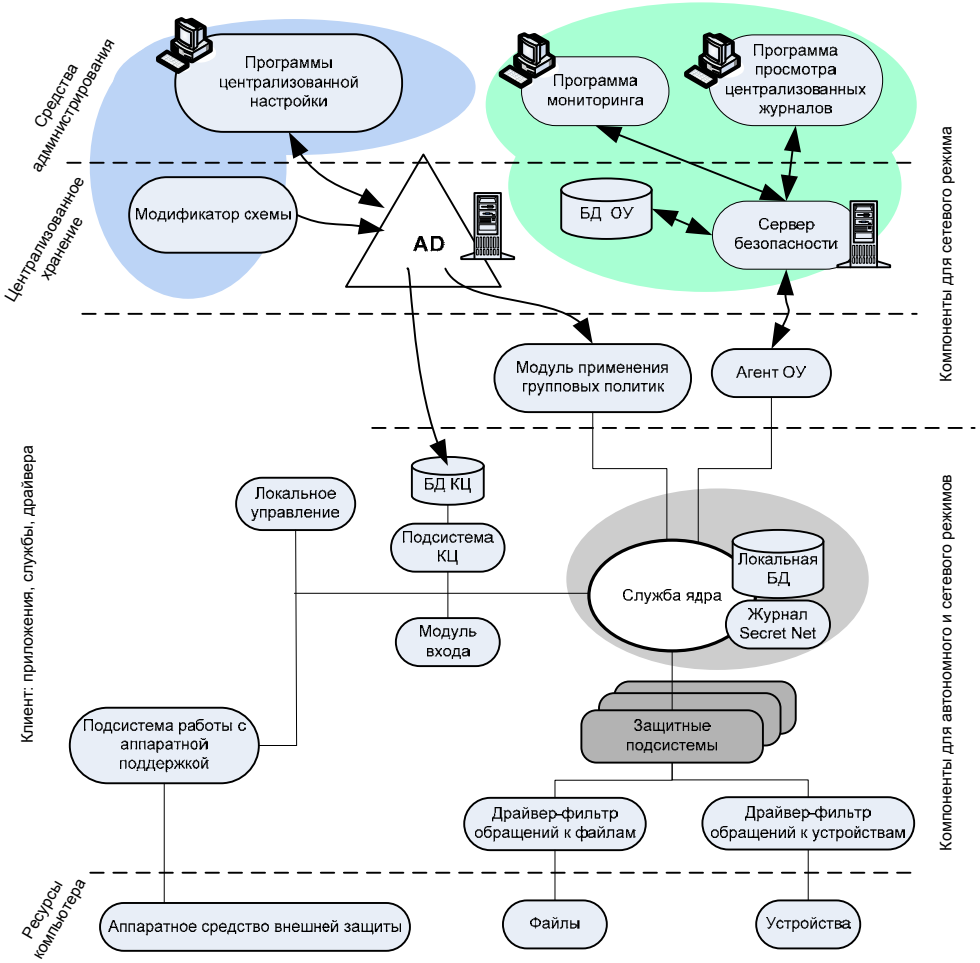


Рис. 1. Архитектура системы Secret Net 6

На рисунке приведена обобщенная структура системы Secret Net 6, представлены основные компоненты и взаимосвязи между ними.

Составные части клиента

Клиент системы Secret Net 6 включает следующие основные компоненты и подсистемы:

- Служба ядра.
- Локальная база данных системы защиты.
- Подсистема регистрации и журнал Secret Net.
- 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 6;
- 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 6, которые следят за происходящими событиями. Перечень событий Secret Net 6, подлежащих регистрации, устанавливается администратором безопасности.

В локальной БД Secret Net 6 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 6, обеспечивается службой ядра.

Подсистема локального управления

Подсистема локального управления обеспечивает:

- управление объектами защиты (устройствами, файлами, каталогами);
- управление параметрами пользователей и защитных механизмов;
- сохранение и получение информации в локальной БД Secret Net 6;
- 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.
- **Разграничение доступа к устройствам** — обеспечивает разграничение доступа к заданным устройствам компьютера (портам, USB-устройствам, локальным логическим дискам и др.).
- **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).

При обращении пользователя к ресурсам компьютера (файлам или устройствам) драйверы-фильтры 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 ресур-

су. 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 6 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).

Компоненты централизованного управления

Возможность централизованного управления доступна в сетевом режиме функционирования системы Secret Net 6.

В централизованном управлении задействованы компоненты, которые можно разделить на следующие группы:

- **Средства централизованной настройки и управления** — обеспечивают централизованное управление параметрами защитных подсистем клиентов.
- **Средства оперативного управления** — предоставляют возможности мониторинга защищаемых компьютеров и оперативного управления ими с рабочего места администратора, а также осуществляют централизованный сбор, хранение и архивирование системных журналов.

Такое разделение дает возможность распределить функции и полномочия между пользователями — сотрудниками службы безопасности и сотрудниками технических подразделений — для решения следующих задач:

- **Настройка системы и управление работой защитных механизмов**.
- **Мониторинг и оперативное управление** — получение актуальной информации о состоянии системы и управление состоянием защищаемых компьютеров в режиме реального времени.
- **Аудит** — отслеживание действий пользователей на основании сведений, хранящихся в журналах регистрации событий.

Средства централизованной настройки и управления

В состав средств централизованной настройки входят следующие компоненты:

- **Модификатор схемы AD**;
- **Программы централизованной настройки**;
- **Модуль применения групповых политик**.

Модификатор схемы AD

Модификатор схемы Active Directory (AD) представляет собой программное средство автоматического добавления в схему AD классов и атрибутов, необходимых для функционирования системы Secret Net 6. Компонент применяется однократно перед развертыванием системы в домене.

Схема Active Directory содержит правила создания объектов в домене (лесе доменов). Эти правила определяют информацию, которая может быть сохранена с каждым объектом, и тип данных, соответствующий этой информации. Таким образом, в домене нельзя создать объект, если он не описан в схеме AD.

При развертывании домена в нем создается схема AD по умолчанию, которая содержит большинство постоянно используемых классов и атрибутов. Они имеют универсальный характер и являются **основными объектами схемы**. Такая схема AD именуется "базовой схемой AD".

Для некоторых задач набор объектов классов и атрибутов, имеющийся в базовой схеме AD, может оказаться недостаточным. Процесс расширения схемы называется **модификацией схемы AD** и является стандартным. Модификация схемы AD для установки системы Secret Net 6 — это процедура описания в схеме AD объектов Secret Net 6, выполняемая Модификатором AD. Без выполнения этой процедуры невозможна установка и эксплуатация системы Secret Net 6 в сетевом режиме функционирования.

Программы централизованной настройки

Централизованная настройка защитных механизмов и изменение параметров пользователей осуществляются следующими средствами:

- **Редактор свойств пользователей и редактор объектов групповой политики** — представляют собой расширения стандартных средств централизованного управления ОС Windows и доступны в соответствующих стандартных оснастках. Данные средства могут использоваться после установки клиентского ПО в сетевом режиме функционирования на контроллерах домена или на компьютерах с установленными средствами централизованного управления Microsoft Administration Tools Pack (AdminPack).
- **Программа "Контроль программ и данных" в централизованном режиме работы** — устанавливается на защищаемых компьютерах при установке клиентского ПО в сетевом режиме функционирования. В этой программе можно централизованно выполнять настройку механизмов контроля целостности и замкнутой программной среды.

В качестве хранилища централизованно заданных параметров используется Active Directory.

Модуль применения групповых политик

Модуль применения групповых политик включается в состав клиентского ПО при установке в сетевом режиме функционирования. Он обеспечивает запрос централизованно заданных параметров для применения их на защищаемом компьютере.

Средства оперативного управления

Средства оперативного управления обеспечивают решение следующих задач:

- оперативный контроль состояния автоматизированной системы (получение информации о состоянии рабочих станций и о действиях пользователей);
- оповещение о событиях НСД;

- выдача оперативных команд управления — выключение, перезагрузка, блокировка компьютеров, запуск процесса применения групповых политик, утверждение изменений аппаратной конфигурации компьютеров;
- централизованный сбор, хранение и архивирование журналов;
- загрузка записей журналов для просмотра и анализа зарегистрированных событий.

В состав средств оперативного управления входят следующие программные компоненты:

- **Сервер безопасности (СБ)**;
- **Агент оперативного управления (Агент ОУ)**;
- **База данных оперативного управления (БД ОУ)**;
- **Программа мониторинга**;
- **Программа просмотра централизованных журналов**;
- **Программа конфигурирования**;
- **Программа "Сертификаты"**.

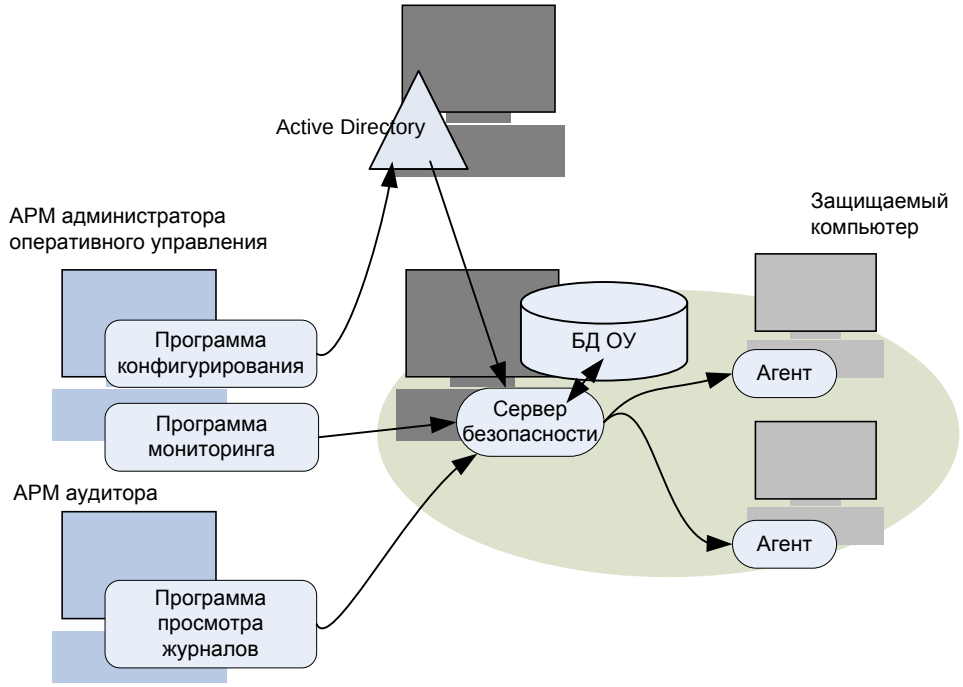
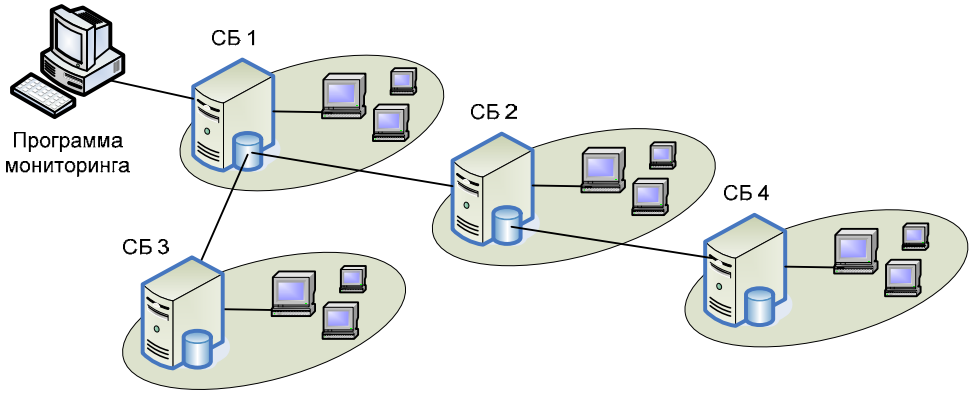


Рис. 2. Основные компоненты контура оперативного управления

Контур оперативного управления имеет архитектуру клиент–сервер. Клиентами по отношению к серверу безопасности являются агенты, установленные на защищаемых компьютерах, и программы мониторинга и просмотра журналов, установленные соответственно на рабочих местах администратора, ответственного за оперативное управление, и аудитора. 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.

В зависимости от особенностей построения сети и ее топологии, в домене можно установить не один, а несколько серверов безопасности с подчинением по иерархическому принципу. На рисунке представлен пример использования нескольких серверов (СБ1 – СБ4) в рамках одного домена.



Каждый сервер контролирует работу своей группы защищаемых компьютеров и работает со своей базой данных. Как видно из рисунка, серверы безопасности СБ2 и СБ3 являются подчиненными по отношению к СБ1, а СБ4 – подчиненным по отношению к СБ2.

Программа мониторинга, как и программа просмотра централизованных журналов, может подключаться к различным серверам безопасности. Выбор сервера осуществляется при запуске программы.

Администратор может использовать программу для просмотра сведений только о тех компьютерах, которые относятся к выбранному серверу и к его подчиненным серверам. Сведения о других компьютерах, которые относятся к вышестоящим серверам безопасности или к серверам других ветвей подчинения, не загружаются в программу. Выполнение ряда действий с компьютерами (например, применение команд оперативного управления) доступно только для компьютеров, находящихся в непосредственном подчинении выбранному серверу безопасности.

В представленном на рисунке примере программа мониторинга подключена к серверу СБ1, что дает возможность просмотра сведений о компьютерах, относящихся ко всем серверам СБ1–СБ4. Но команды оперативного управления могут применяться только к компьютерам, подчиненным серверу СБ.

Сервер безопасности

Сервер безопасности обеспечивает взаимодействие компонентов оперативного управления и выполняет следующие основные функции:

1. Работа с базой данных оперативного управления.
2. Работа с журналами:
   - передает агентам команды на сбор и передачу журналов;
   - получает от агентов локальные журналы и помещает их в БД оперативного управления для хранения;
   - передает журналы из БД оперативного управления программе просмотра журналов;
   - архивирует или восстанавливает журналы по командам, поступающим от программы просмотра журналов;
   - протоколирует действия, связанные с сессиями, и хранит их в БД оперативного управления.
3. Работа с агентами оперативного управления:
   - ведет учет агентов оперативного управления;
   - обеспечивает соединение агентов с использованием сертификатов;
   - управляет сессиями обмена информацией с агентами;
   - получает от агентов информацию о смене состояния компьютера и передает ее программе мониторинга;
   - принимает от агентов уведомления о НСД и передает их программе мониторинга для оповещения оператора;
   - принимает от программы мониторинга команды оперативного управления и передает их агентам для выполнения.

Агент оперативного управления

Агент устанавливается на защищаемых компьютерах при установке клиента в сетевом режиме функционирования. Агент обеспечивает передачу данных серверу безопасности и прием от него оперативных команд.

В процессе работы системы защиты агент выполняет следующие функции:

- устанавливает соединение с сервером безопасности и восстанавливает соединение после перезапуска рабочей станции или сервера безопасности;
- получает от ядра системы защиты уведомление о НСД и передает его серверу безопасности для оповещения оператора средствами программы мониторинга;
- передает локальные журналы серверу безопасности;
- получает от ядра системы защиты информацию об изменении состояния компьютера и передает ее серверу безопасности для отображения в программе мониторинга;
- выполняет оперативные команды, поступающие от сервера безопасности.

База данных оперативного управления

База данных оперативного управления предназначена для хранения журналов, поступающих с рабочих станций, и другой информации для работы компонентов контура. Взаимодействие с базой данных осуществляет сервер безопасности.

Для организации базы данных используется СУБД Oracle.

Программа мониторинга

Программа мониторинга выполняет следующие функции:

- получение от сервера безопасности информации об изменении состояния компьютера и отображение сведений о текущем состоянии;
- информирование оператора о получении уведомления о НСД;
- передача команд оператора на утверждение изменений аппаратной конфигурации, на перезагрузку компьютера или принудительный выход пользователя и пр.

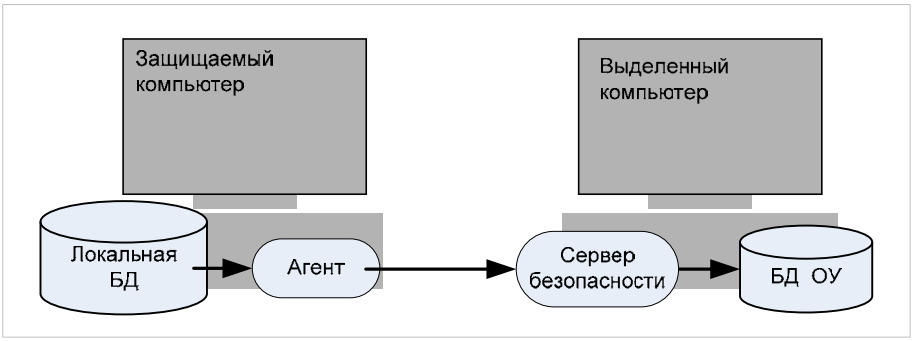
В процессе работы программа мониторинга взаимодействует с сервером безопасности, по отношению к которому она является клиентом.

При изменении состояния какого-либо компьютера установленный на нем агент передает эти сведения серверу безопасности, а сервер в свою очередь — программе мониторинга. Аналогичным образом в программу мониторинга поступают сведения о НСД.

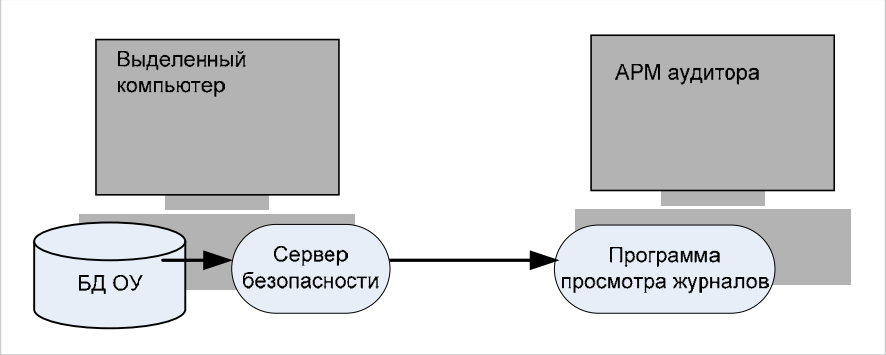
Программа просмотра централизованных журналов

Программа устанавливается на рабочем месте сотрудника, уполномоченного проводить аудит системы защиты.

По запросу сервера безопасности агенты передают ему локальные журналы защищаемых компьютеров, и сервер загружает их в свою базу данных оперативного управления. После передачи локальные журналы очищаются. Сбор журналов осуществляется сервером по команде аудитора или по расписанию, составленному администратором ОУ.



Программа просмотра централизованных журналов позволяет аудитору просматривать записи журналов из БД ОУ. По запросу аудитора сервер выбирает из базы данных запрашиваемые журналы и передает их программе.



С помощью программы просмотра журналов аудитор может выдавать команды серверу на архивацию журналов, а также на восстановление журналов из архива. В программе предусмотрена возможность экспорта содержимого журнала в файл.

Программа конфигурирования

Программа конфигурирования позволяет редактировать схему взаимодействия серверов безопасности и агентов, изменять их настройки. Информация о конфигурации системы сохраняется в Active Directory.

Программа "Сертификаты"

Программа предназначена для выполнения действий с доверенными сертификатами сервера безопасности.

Программа "Сертификаты" устанавливается в составе программного обеспечения сервера безопасности.

Глава 3
Защитные механизмы

Защитные механизмы — это программные и аппаратные средства в составе клиента системы Secret Net 6, предназначенные для реализации защитных функций системы. В зависимости от назначения защитные механизмы условно распределены по следующим группам:

1. Механизм защиты входа в систему.
2. Механизмы разграничения доступа и защиты ресурсов:
   - механизм полномочного разграничения доступа к объектам файловой системы;
   - механизм замкнутой программной среды;
   - механизм разграничения доступа к устройствам компьютера;
   - механизм затирания информации, удаляемой с дисков компьютера.
3. Механизмы контроля и регистрации:
   - механизм функционального контроля подсистем;
   - механизм регистрации событий безопасности;
   - механизм контроля целостности;
   - механизм контроля аппаратной конфигурации компьютера;
   - механизм контроля печати.

Управление защитными механизмами

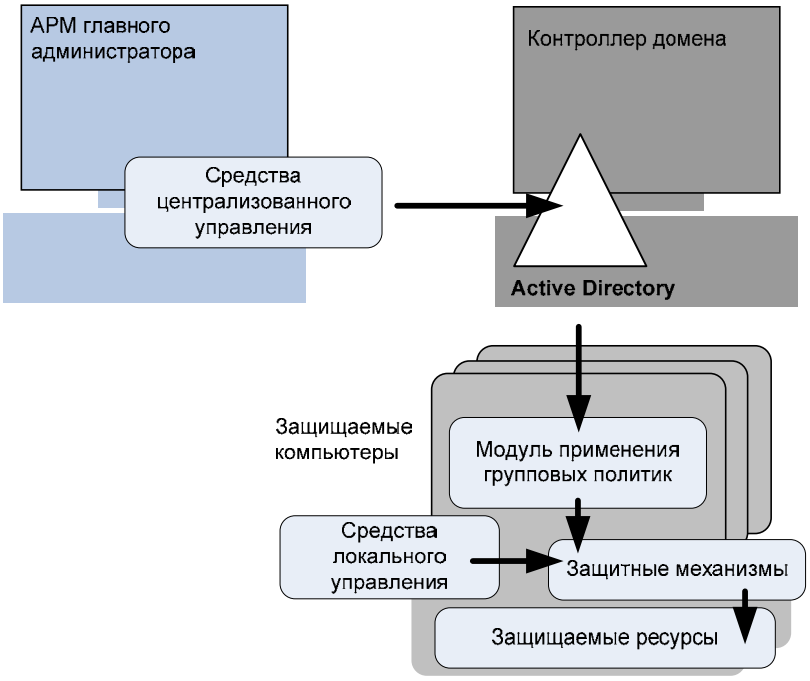
Настройка защитных механизмов может выполняться средствами локального управления, а в сетевом режиме функционирования системы — также и средствами централизованной настройки и управления.

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 Active Directory 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 применения групповых политик 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) до политики организационного подразделения, в которое входит рабочая станция. 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 AD

В сетевом режиме функционирования системы Secret Net 6 предусмотрен режим усиленной защиты доступа к Active Directory. В этом режиме сетевые обращения к AD, выполняемые компонентами системы Secret Net 6, осуществляются с использованием протоколов Secure Socket Layer/Transport Layer Security (SSL/TLS). Данные протоколы предусматривают проверку подлинности контроллера домена и реализуют функции установки безопасного соединения с использованием сертификатов.

Для использования режима защиты доступа к AD 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.

Механизм защиты входа в систему

Защита от несанкционированного входа предназначена для предотвращения доступа посторонних лиц к защищенному компьютеру. К этой группе средств относятся:

- средства идентификации и аутентификации пользователей;
- функции 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.

Для обеспечения дополнительной защиты входа в Secret Net 6 могут применяться средства идентификации и аутентификации на базе USB-ключей eToken, iKey, Rutoken или идентификаторов iButton. Такие устройства должны быть зарегистрированы (присвоены пользователям) средствами системы защиты. Кроме того, предусмотрен режим усиленной аутентификации, основанный на дополнительной проверке подлинности предъявленной ключевой информации пользователя. Носителями ключевой информации могут являться USB-ключи, идентификаторы или сменные носители, такие как дискеты, Flash-карты, Flash-

накопители и т. п. Генерация ключевой информации выполняется средствами системы Secret Net 6.

В системе Secret Net 6 идентификация и аутентификация пользователей могут выполняться в следующих режимах:

- "Стандартный" — 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 может использовать персональный идентификатор, поддерживаемый системой Secret Net 6;
- "Только по идентификатору" — каждый пользователь для входа в систему должен обязательно использовать персональный идентификатор, поддерживаемый системой Secret Net 6.

Для повышения степени защищенности компьютеров от несанкционированного использования предусмотрены следующие возможности:

- включение режима разрешения интерактивного входа только для доменных пользователей — в этом режиме блокируется вход в систему локальных учетных записей (не зарегистрированных в домене);
- включение режима запрета вторичного входа в систему — в этом режиме блокируется запуск команд и сетевых подсоединений с вводом учетных данных другого пользователя (не выполнившего интерактивный вход в систему).

Блокировка компьютера

Механизм блокировки компьютера предназначен 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 6 контролирует неудачные попытки аутентификации пользователя по ключевой информации. Если в режиме усиленной аутентификации пользователь определенное количество раз предъявляет неверную ключевую информацию, 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 может быть включен самим пользователем или системой после некоторого периода простоя компьютера. Длительность интервала неактивности (простоя компьютера), после которого автоматически включается режим блокировки, устанавливается настройкой параметров и распространяется на всех пользователей. Для снятия блокировки необходимо указать пароль текущего пользователя.

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 6;
- при нарушении 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 мониторинга.

Аппаратные средства защиты

В Secret Net 6 поддерживается работа со следующими аппаратными средствами:

- средства идентификации и аутентификации на базе USB-ключей eToken, iKey и Rutoken;
- устройства Secret Net Card и Secret Net Touch Memory Card PCI;
- программно-аппаратные комплексы (ПАК) "Соболь" версий 3.0 и 2.1.

В таблице (см. ниже) приведены сведения о каждой из названных групп аппаратных средств. Более подробная информация о средствах аппаратной поддержки Secret Net 6 содержится в документе [8].

Аппаратные средства	Основные функции
Средства идентификации и аутентификации на базе USB-ключей	1. Хранение данных для идентификации и аутентификации. 2. Хранение ключевой информации для усиленной аутентификации.
Устройства Secret Net Card и Secret Net Touch Memory Card PCI	1. Чтение данных для идентификации и аутентификации. 2. Чтение ключевой информации для усиленной аутентификации. 3. Блокировка несанкционированной загрузки ОС со съемных носителей.
ПАК "Соболь"	1. Регистрация пользователей и назначение им персональных идентификаторов и паролей для входа в систему. 2. Идентификация и аутентификация пользователей до загрузки ОС Windows. 3. Чтение ключевой информации для усиленной аутентификации. 4. Управление параметрами процедуры идентификации и аутентификации пользователя (защита от подбора пароля). 5. Контроль целостности файлов на жестком диске и секторов жесткого диска до загрузки ОС. 6. Блокировка несанкционированной загрузки ОС со съемных носителей. 7. Регистрация событий безопасности. 8. Возможность интеграции с системой Secret Net 6.

Для более тесного взаимодействия Secret Net 6 с ПАК "Соболь" предусмотрен режим интеграции. В этом режиме средствами администрирования Secret Net 6 можно управлять следующими функциями ПАК "Соболь":

Функция	Описание
Управление входом пользователя Secret Net 6 в комплекс "Соболь" с помощью идентификатора, инициализированного и присвоенного пользователю в системе Secret Net 6	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 6
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 6

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

Механизмы разграничения доступа и защиты ресурсов

Система Secret Net 6 включает в свой состав несколько механизмов разграничения доступа пользователей к ресурсам компьютера:

- механизм избирательного разграничения доступа;
- механизм полномочного разграничения доступа;
- механизм замкнутой программной среды.

Ресурсы компьютера делятся на 3 типа:

Ресурсы файловой системы	Локальные и подключенные к компьютеру сетевые диски и размещающиеся на них каталоги и файлы
Аппаратные ресурсы	Локальные и сетевые принтеры, коммуникационные порты, физические диски, дисководы, приводы оптических дисков, устройства, подключаемые к шинам USB и PCMCIA, IEEE 1394, Secure Digital
Ресурсы операционной системы	Системные файлы, ключи системного реестра и т. д.

Механизм полномочного разграничения доступа и механизм замкнутой программной среды применяются только к ресурсам файловой системы.

Избирательное управление доступом

Избирательное разграничение доступа к локальным ресурсам компьютера осуществляется на основании предоставления прав и привилегий пользователям компьютера.

Для разграничения доступа к ресурсам файловой системы, системному реестру и системным средствам управления используются стандартные механизмы ОС Windows. Для разграничения доступа к дискам, портам и другим устройствам используются средства Secret Net 6 — механизм разграничения доступа к устройствам.

Примечание. Подробные сведения о механизме избирательного разграничения доступа в ОС Windows можно найти в документации к этой ОС, MSDN, а также на интернет-сайте компании Microsoft.

Разграничение доступа к устройствам

Разграничение доступа пользователей к устройствам выполняется на основании списков устройств, формируемых (и поддерживаемых в актуальном состоянии) механизмом контроля аппаратной конфигурации (см. стр. 24).

При установке Secret Net 6 на компьютер устанавливаются и права доступа к устройствам по умолчанию. Они предоставляют полный доступ трем стандартным группам пользователей ("Система", "Администраторы" и "Все") к устройствам компьютера — т. е. всем пользователям разрешен доступ без ограничений ко всем устройствам, подключенным к компьютеру на момент установки Secret Net 6.

Права доступа складываются из разрешений и запретов на выполнение определенных операций. Набор операций зависит от типа устройства. Если в процессе работы в системе появляется новое устройство, система защиты определяет его и относит к соответствующей группе. Доступ пользователей к этому устройству устанавливается автоматически в соответствии с правилами, действующими для группы или класса устройств.

Подсистема РДУ может функционировать в следующих режимах:

- "Жесткий" режим. При превышении пользователями прав доступа к устройствам доступ блокируется, попытки доступа регистрируются в журнале Secret Net.
- "Мягкий" режим. Права доступа пользователей к устройствам контролируются, но не ограничиваются, попытки доступа регистрируются в журнале Secret Net.
- Подсистема отключена. Права доступа пользователей к устройствам не контролируются.

Полномочное разграничение доступа

Механизм полномочного разграничения доступа (называемый также "механизм полномочного управления доступом") обеспечивает:

- разграничение доступа пользователей к конфиденциальным документам;
- контроль потоков конфиденциальной информации в системе;
- контроль вывода конфиденциальной информации на внешние устройства;
- контроль печати конфиденциальных документов.

Механизм полномочного разграничения доступа обеспечивает управление доступом пользователей к конфиденциальной информации, хранящейся в файлах на локальных и подключенных сетевых дисках с файловой системой NTFS. Доступ осуществляется в соответствии с категорией конфиденциальности, присвоенной информации, и уровнем допуска пользователя к конфиденциальной информации.

Для каждого пользователя компьютера устанавливается некоторый уровень допуска к конфиденциальной информации. Файлам и каталогам назначается категория конфиденциальности, которая определяется расширенным атрибутом файла или каталога. По умолчанию используются 3 категории конфиденциальности информации: "неконфиденциально" (для общедоступной информации), "конфиденциально" и "строго конфиденциально". Названия категорий, предлагаемые по умолчанию, могут быть заменены другими.

Полномочные правила разграничения доступа действуют совместно со стандартными правилами избирательного разграничения доступа в ОС Windows. Поэтому доступ к объекту разрешен только в том случае, если он разрешен и по полномочным, и по избирательным правилам доступа.

Доступ к конфиденциальным файлам осуществляется следующим образом. Когда пользователь (программа, запущенная пользователем) осуществляет попытку доступа к конфиденциальному файлу, драйвер подсистемы полномочного разграничения доступа определяет категорию конфиденциальности данного файла. Затем категория конфиденциальности файла сопоставляется с уровнем допуска пользователя к конфиденциальной информации. И если уровень конфиденциальности файла не превышает уровень допуска пользователя, то ему предоставляется доступ к этому файлу.

Кроме того, механизм полномочного управления доступом обеспечивает контроль потоков конфиденциальной информации. При использовании контроля потоков предотвращаются следующие несанкционированные действия:

- копирование или перемещение конфиденциальных файлов в другие, неконфиденциальные каталоги;
- запись конфиденциальной информации в файлы, не имеющие соответствующей категории конфиденциальности;
- запись конфиденциальных файлов на любые носители информации (постоянные и сменные).

Этой же цели служит процедура назначения пользовательским сессиям уровня конфиденциальности. В тех случаях, когда при определенном типе входа пользователя не может быть установлен его уровень допуска, система присваивает этой сессии самый низший уровень и запрещает работу с конфиденциальными документами. Если уровень допуска пользователя может быть установлен, то пользователю самому предоставляется возможность выбрать (но не выше уровня допуска) уровень конфиденциальности сессии, заявив тем самым о категории конфиденциальности документов, с которыми он собирается работать. В этом случае при доступе пользователя к файлу рассматривается уже не уровень допуска пользователя, а уровень конфиденциальности текущей сессии. При этом вся информация, которую вводит пользователь, имеет категорию конфиденциальности, равную уровню сессии.

Механизм полномочного управления доступом может контролировать и вывод конфиденциальной информации на внешние устройства, которыми являются:

- любые носители информации (постоянные и сменные), имеющие файловую систему, отличную от NTFS (в том числе и серверы Novell Netware);
- любые устройства, являющиеся сменными носителями информации, вне зависимости от типа их файловой системы;
- печатающие устройства.

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 из программ MS Word и MS Excel. 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 обеспечения, 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.

Сценарий (называемый также "скрипт") представляет собой последовательность исполняемых команд и/или действий в текстовом виде. Система Secret Net 6 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. 23). 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.

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.

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".

Механизмы контроля и регистрации

Система Secret Net 6 включает в свой состав следующие средства, позволяющие контролировать ее работу:

- механизм регистрации событий;
- механизм контроля целостности;
- механизм контроля аппаратной конфигурации компьютера;
- механизм функционального контроля подсистем;
- механизм контроля печати.

Регистрация событий

В процессе работы системы Secret Net 6 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 6 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 6, 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 6 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, которые должны 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 аппаратной конфигурации компьютера

Механизм контроля аппаратной конфигурации компьютера обеспечивает:

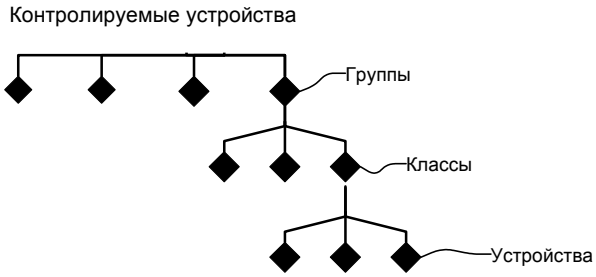
- своевременное обнаружение изменений в аппаратной конфигурации компьютера и реагирование на эти изменения;
- поддержание в актуальном состоянии списка устройств компьютера, который используется механизмом разграничения доступа к устройствам.

Изменения аппаратной конфигурации компьютера могут быть вызваны подключением к компьютеру или отключением от него различных устройств, выходом устройств из строя и добавлением или заменой отдельных устройств.

Контролируются следующие группы устройств:

- локальные устройства (диски, порты и т. п.);
- устройства, подключаемые к шине USB;
- устройства, подключаемые к шине IEEE1394;
- устройства, подключаемые к шине PCMCIA;
- устройства, подключаемые к шине Secure Digital.

Каждая группа разделена на **классы**, в которые входят устройства.



Для объектов каждого уровня определен свой набор параметров.

Аппаратная конфигурация компьютера определяется на этапе установки системы, а значения параметров контроля задаются по умолчанию. Настройку политики контроля можно выполнить индивидуально для каждого устройства, класса или группы с использованием принципа наследования параметров.

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. Драйвер-фильтр устройств отслеживает факт подключения или изъятия устройства. При изменении конфигурации определяется тип устройства и выбирается реакция на изменение конфигурации.

Предусмотрена возможность работы подсистемы в нескольких режимах. Механизм может функционировать в "мягком" или "жестком" режимах работы, а также без отслеживания изменений аппаратной конфигурации (так называемый "прозрачный режим" для обеспечения работы механизма разграничения доступа к устройствам). В "жестком" режиме при обнаружении изменений в конфигурации компьютера подсистема регистрирует соответствующие события в журнале Secret Net и выполняет блокировку компьютера. Если в процессе контроля изменений не обнаружено — регистрируется событие успешного завершения контроля. Работа в "мягком" режиме отличается тем, что при нарушении конфигурации не выполняется блокировка компьютера.

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 6 загружены и функционируют.

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

- ядро Secret Net 6;
- 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 6). Вход в систему разрешается только пользователям, входящим в локальную группу администраторов компьютера.

Контроль печати

Механизм контроля печати обеспечивает:

- регистрацию событий вывода документов на печать в журнале Secret Net;
- предотвращение несанкционированного вывода на печать конфиденциальных документов (при включенном режиме контроля печати конфиденциальных документов в механизме полномочного управления доступом);
- автоматическое добавление грифа конфиденциальности в распечатываемые конфиденциальные документы (при включенном режиме контроля печати конфиденциальных документов в механизме полномочного управления доступом).

Приложение

Рекомендации по настройке системы для соответствия требованиям нормативно-методических документов

Автоматизированные системы (АС), подлежащие защите от НСД к информации, должны соответствовать требованиям, изложенным в следующих нормативно-методических документах:

- Положение о методах и способах защиты информации в информационных системах персональных данных. Утверждено приказом ФСТЭК России от 5 февраля 2010 г. №58;
- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России, 1992.

При определенных вариантах настройки система Secret Net 6 обеспечивает соответствие требованиям для следующих классов:

- Классы информационных систем персональных данных (согласно утвержденному порядку проведения классификации информационных систем персональных данных):
  - класс 3 (К3);
  - класс 2 (К2);
  - класс 1 (К1).
- Классы защищенности 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.

Общие сведения о настройке для соответствия классам защищенности

Классы К3, К2, 1Д

Для соответствия классам К3, К2, 1Д необходимо:

- настроить механизм защиты входа в систему — включить режимы обязательного использования персональных идентификаторов и усиленной аутентификации пользователей;
- 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 6".

Классы К1, 1Г

Для соответствия классам К1, 1Г необходимо выполнить действия по настройке, указанные для систем классов К3, К2, 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 аппаратной конфигурации и включить жесткий режим работы механизмов.

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.

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 классов К1, 1Г (включение аудита отслеживания процессов не является обязательным), а также:

- в механизме полномочного управления доступом включить режим контроля потоков конфиденциальной информации;
- настроить механизм замкнутой программной среды и включить жесткий режим работы механизма.

Использование дополнительных средств защиты загрузки

В АС должны применяться средства, исключающие доступ пользователя к ресурсам компьютера в обход механизмов системы защиты. В качестве таких средств могут использоваться:

- изделие "Программно-аппаратный комплекс "Соболь";
- изделия Secret Net Card и Secret Net Touch Memory Card;
- изделие "Средство защиты информации Security Studio 6 – Trusted Boot Loader" — для систем, обрабатывающих информацию ограниченного доступа, не составляющую государственную тайну, и в которых модель нарушителя системы допускает использование только штатных средств (первый уровень нарушителя по классификации, приведенной в руководящем документе ФСТЭК "Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации" от 30 марта 1992 г.).

Настраиваемые параметры системы Secret Net 6

Состав действующих механизмов защиты

Для соответствия классам защищенности АС в системе Secret Net 6 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. 1. Механизмы защиты системы Secret Net 6

Параметр	Классы защищенности		
	1В	К1, 1Г	К3, К2, 1Д
Затирание данных	Да (обязательно)	Да (обязательно)	–
Контроль устройств	Да (обязательно)	Да (обязательно)	–
Полномочное управление доступом	Да (обязательно)	Да (рекомендуется)	–
Замкнутая программная среда	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 документах [3], [4], [5].

Табл. 2. Параметры политики безопасности

Параметр	Классы защищенности		
	1В	**К1, 1Г**	**К3, К2, 1Д**
Группа "Настройки подсистем"			
Вход в систему: Запрет вторичного входа в систему	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход в систему: Количество неудачных попыток аутентификации	–	–	–
Вход в систему: Максимальный период неактивности до блокировки экрана	10 (рекомендуется)	10 (рекомендуется)	10 (рекомендуется)
Вход в систему: Разрешить интерактивный вход только доменным пользователям	–	–	–
Вход в систему: Режим аутентификации пользователя	Усиленная (обязательно)	Усиленная (обязательно)	Усиленная (обязательно)
Вход в систему: Режим входа пользователя	Смешанный (рекомендуется)	Смешанный (рекомендуется)	Смешанный (рекомендуется)
Журнал: Максимальный размер журнала защиты	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)
Сеть: Запрет использования сетевых интерфейсов		–	–
Затирание данных: Количество циклов затирания конфиденциальной информации	–	–	–
Затирание данных: Количество циклов затирания на локальных дисках	2 (обязательно)	1 (обязательно)	–
Затирание данных: Количество циклов затирания на сменных носителях	2 (обязательно)	1 (обязательно)	–
Контроль устройств: Режим работы	Жесткий (обязательно)	Жесткий (обязательно)	–
Разграничение доступа к устройствам: Режим работы	Жесткий (обязательно)	Жесткий (обязательно)	–
Полномочное управление доступом: Гриф конфиденциальности для Microsoft Excel	Настроен (обязательно)	–	–

Параметр	Классы защищенности		
	1В	К1, 1Г	К3, К2, 1Д
Полномочное управление доступом: Гриф конфиденциальности для Microsoft Word	Настроен (обязательно)	–	–
Полномочное управление доступом: Название уровней конфиденциальности	Настроен (обязательно)	Настроен (рекомендуется)	–
Полномочное управление доступом: Режим контроля печати конфиденциальных документов	Да (обязательно)	Да (рекомендуется)	–
Полномочное управление доступом: Режим работы	Контроль потоков включен (обязательно)	Контроль потоков отключен (рекомендуется)	–
Группа "Ключи пользователя"			
Максимальный срок действия ключа	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)
Группа "Привилегии"			
Журнал: Просмотр журнала системы защиты	Administrators, Users (рекомендуется)	Administrators, Users (рекомендуется)	Administrators, Users (рекомендуется)
Журнал: Управление журналом системы защиты	Administrators (рекомендуется)	Administrators (рекомендуется)	Administrators (рекомендуется)
Замкнутая программная среда: Не действует	Administrators (рекомендуется)	–	–
Группа "Регистрация событий"			
Администрирование: Добавлен пользователь	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Удален пользователь	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Изменены параметры пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Изменены параметры действующей политики безопасности	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Изменен ключ пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)
Администрирование: Удален ключ пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Завершение работы пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Идентификатор не зарегистрирован	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Пользователь приостановил сеанс работы на компьютере	Да (обязательно)	Да (обязательно)	Да (обязательно)

Параметр	Классы защищенности		
	1В	К1, 1Г	К3, К2, 1Д
Вход/выход: Пользователь возобновил сеанс работы на компьютере	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Компьютер заблокирован системой защиты	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Компьютер разблокирован	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Ошибка выполнения функционального контроля	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Успешное завершение функционального контроля	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Вход пользователя в систему	Да (обязательно)	Да (обязательно)	Да (обязательно)
Вход/выход: Запрет входа пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)
Замкнутая программная среда: Запрет запуска программы	Да (обязательно)	–	–
Замкнутая программная среда: Запуск программы	Да (обязательно)	–	–
Замкнутая программная среда: Запрет загрузки библиотеки	Да (обязательно)	–	–
Замкнутая программная среда: Загрузка библиотеки	Нет (рекомендуется)	–	–
Замкнутая программная среда: Запрет исполнения неизвестного скрипта	Да (обязательно)	–	–
Замкнутая программная среда: Запрет исполнения скрипта	Да (обязательно)	–	–
Замкнутая программная среда: Исполнение скрипта	Да (обязательно)	–	–
Контроль аппаратной конфигурации: Успешное завершение контроля аппаратной конфигурации	Да (рекомендуется)	Да (рекомендуется)	–
Контроль аппаратной конфигурации: Ошибка при контроле аппаратной конфигурации	Да (обязательно)	Да (обязательно)	–
Контроль аппаратной конфигурации: Обнаружено новое устройство	Да (обязательно)	Да (обязательно)	–
Контроль аппаратной конфигурации: Устройство удалено из системы	Да (обязательно)	Да (обязательно)	–
Контроль аппаратной конфигурации: Изменение параметров устройства	Да (обязательно)	Да (обязательно)	–

Параметр	Классы защищенности		
	1В	К1, 1Г	К3, К2, 1Д
Контроль аппаратной конфигурации: Утверждение аппаратной конфигурации	Да (рекомендуется)	Да (рекомендуется)	–
Контроль печати: Печать документа	Да (обязательно)	Да (обязательно)	–
Контроль печати: Печать конфиденциального документа	Да (обязательно)	Да (рекомендуется)	–
Контроль печати: Прямое обращение к принтеру	Да (рекомендуется)	Да (рекомендуется)	–
Контроль печати: Запрет прямого обращения к принтеру	Да (рекомендуется)	Да (рекомендуется)	–
Контроль печати: Запрет печати конфиденциального документа	Да (обязательно)	Да (рекомендуется)	–
Контроль целостности: Начало обработки задания на контроль целостности	–	–	–
Контроль целостности: Завершение обработки задания на контроль целостности	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Обнаружено нарушение целостности при обработке задания	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Завершение проверки целостности ресурса	–	–	–
Контроль целостности: Нарушение целостности ресурса	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Для ресурса отсутствует эталонное значение	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Удаление устаревших эталонных значений	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Текущее значение ресурса принято в качестве эталонного	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Восстановление ресурса	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Ошибка при восстановлении ресурса по эталонному значению	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Ошибка при открытии базы данных контроля целостности	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Ошибка принятия текущего значения ресурса в качестве эталонного	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Исправление ошибок в базе данных	Да (обязательно)	Да (обязательно)	Да (обязательно)

Параметр	Классы защищенности		
	1В	К1, 1Г	К3, К2, 1Д
Контроль целостности: Установка задания КЦ на контроль	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Снятие задания КЦ с контроля	Да (обязательно)	Да (обязательно)	Да (обязательно)
Контроль целостности: Добавление учетной записи к заданию ЗПС	Да (рекомендуется)	–	–
Контроль целостности: Удаление учетной записи из задания ЗПС	Да (рекомендуется)	–	–
Контроль целостности: Создание задания	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Удаление задания	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Изменение задания	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Создание задачи	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Удаление задачи	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Изменение задачи	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Создание группы ресурсов	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Удаление группы ресурсов	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Изменение группы ресурсов	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Синхронизация локальной базы данных с центральной	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Контроль целостности: Ошибка синхронизации локальной базы данных с центральной	Да (обязательно)	Да (обязательно)	Да (обязательно)
Общие события: Событие	Да (обязательно)	Да (обязательно)	Да (обязательно)
Общие события: Несанкционированное действие	Да (обязательно)	Да (обязательно)	Да (обязательно)
Общие события: Ошибка	Да (обязательно)	Да (обязательно)	Да (обязательно)
Общие события: Предупреждение	Да (обязательно)	Да (обязательно)	Да (обязательно)
Общие события: Отладочное событие	Да (обязательно)	Да (обязательно)	Да (обязательно)
Полномочное управление доступом: Изменение категории конфиденциальности	Да (обязательно)	Да (рекомендуется)	–
Полномочное управление доступом: Запрет изменения параметров конфиденциальности ресурса	Да (обязательно)	Да (рекомендуется)	–
Полномочное управление доступом: Изменение признака наследования	Да (обязательно)	Да (рекомендуется)	–

Параметр	Классы защищенности		
	1В	К1, 1Г	К3, К2, 1Д
Полномочное управление доступом: Доступ к конфиденциальному документу	Да (обязательно)	Да (рекомендуется)	–
Полномочное управление доступом: Запрет доступа к конфиденциальному документу	Да (обязательно)	Да (рекомендуется)	–
Полномочное управление доступом: Вывод конфиденциальной информации	Да (обязательно)	–	–
Полномочное управление доступом: Запрет вывода конфиденциальной информации	Да (обязательно)	–	–
Разграничение доступа к устройствам: Подключение устройства	Да (обязательно)	Да (обязательно)	–
Разграничение доступа к устройствам: Отключение устройства	Да (обязательно)	Да (обязательно)	–
Разграничение доступа к устройствам: Запрет подключения устройства	Да (обязательно)	Да (обязательно)	–
Разграничение доступа к устройствам: Несанкционированное отключение устройства	Да (обязательно)	Да (обязательно)	–
Разграничение доступа к устройствам: Доступ к устройству	Да (обязательно)	Да (обязательно)	–
Разграничение доступа к устройствам: Запрет доступа к устройству	Да (обязательно)	Да (обязательно)	–
Расширение групповой политики: Групповые политики успешно применены	Да (обязательно)	Да (обязательно)	Да (обязательно)
Расширение групповой политики: Ошибка применения групповых политик	Да (обязательно)	Да (обязательно)	Да (обязательно)
Расширение групповой политики: Предупреждение при применении групповых политик	Да (обязательно)	Да (обязательно)	Да (обязательно)
Сеть: Запрет сетевого подключения под другим именем	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Служба репликации: Ошибка создания контекста пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)
ЦУ КЦ-ЗПС: Установка задания КЦ на контроль	Да (обязательно)	Да (обязательно)	Да (обязательно)
ЦУ КЦ-ЗПС: Снятие задания КЦ с контроля	Да (обязательно)	Да (обязательно)	Да (обязательно)
ЦУ КЦ-ЗПС: Добавление учетной записи к заданию ЗПС	Да (рекомендуется)	–	–
ЦУ КЦ-ЗПС: Удаление учетной записи из задания ЗПС	Да (рекомендуется)	–	–

Параметр	Классы защищенности		
	1В	К1, 1Г	К3, К2, 1Д
ЦУ КЦ-ЗПС: Создание задания	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Удаление задания	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Изменение задания	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Создание задачи	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Удаление задачи	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Изменение задачи	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Создание группы ресурсов	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Удаление группы ресурсов	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Изменение группы ресурсов	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Добавление субъекта	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Удаление субъекта	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
ЦУ КЦ-ЗПС: Изменение субъекта	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Группа "Устройства"			
Параметры контроля аппаратной конфигурации	Заданы (обязательно)	Заданы (обязательно)	–
Параметры контроля доступа к устройствам	Заданы (обязательно)	Заданы (обязательно)	–

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 документах [3], [4].

Табл. 3. Параметры пользователей

Параметр	Классы защищенности		
	1В	К1, 1Г	К3, К2, 1Д
Режим "Идентификатор" в диалоге "Secret Net 6"			
Ключи пользователя	Да (обязательно)	Да (обязательно)	Да (обязательно)
Пароль пользователя	–	–	–
Интеграция с ПАК "Соболь"	Да (рекомендуется)	–	–
Режим "Доступ" в диалоге "Secret Net 6"			
Уровень допуска	Назначен уполномоченным пользователям (обязательно)	Назначен уполномоченным пользователям (рекомендуется)	–
Привилегия: Печать конфиденциальных документов	Назначена уполномоченным пользователям (обязательно)	Назначена уполномоченным пользователям (рекомендуется)	–
Привилегия: Управление категориями конфиденциальности	Назначена уполномоченным пользователям (обязательно)	Назначена уполномоченным пользователям (рекомендуется)	–

Параметр	Классы защищенности		
	1В	К1, 1Г	К3, К2, 1Д
Привилегия: Вывод конфиденциальной информации	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.

Для механизма контроля целостности необходимо построить модель данных по умолчанию, добавить новое задание "Контроль СЗИ" для контроля файлов и параметров реестра системы защиты и установить связь задания с задачей "Secret Net 6".

Табл. 4. Параметры механизмов КЦ и ЗПС

Параметр	Классы защищенности		
	1В	К1, 1Г	К3, К2, 1Д
Диалог "Режимы" в диалоговом окне настройки свойств компьютера			
Режим ЗПС включен	Да (обязательно)	–	–
"Мягкий" режим	Нет (обязательно)	–	–
Проверять целостность модулей перед запуском	Да (рекомендуется)	–	–
Проверять заголовки модулей перед запуском	Да (рекомендуется)	–	–
Контролировать исполняемые скрипты	Да (рекомендуется)	–	–
Диалоговое окно настройки параметров задания "Контроль СЗИ"			
Метод контроля ресурсов	Содержимое (обязательно)	Содержимое (обязательно)	Содержимое (обязательно)
Алгоритм	CRC-7 (рекомендуется)	CRC-7 (рекомендуется)	CRC-7 (рекомендуется)
Регистрация событий: Успех завершения	Да (рекомендуется)	Да (рекомендуется)	Да (рекомендуется)
Регистрация событий: Ошибка завершения	Да (обязательно)	Да (обязательно)	Да (обязательно)
Регистрация событий: Успех проверки	Нет (рекомендуется)	Нет (рекомендуется)	Нет (рекомендуется)
Регистрация событий: Ошибка проверки	Да (обязательно)	Да (обязательно)	Да (обязательно)
Реакция на отказ: Действия	Заблокировать компьютер (рекомендуется)	Заблокировать компьютер (рекомендуется)	Заблокировать компьютер (рекомендуется)
Расписание	При входе (обязательно)	При входе (обязательно)	При входе (обязательно)

Документация

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

Предметный указатель