КОД БЕЗОПАСНОСТИ

Средство защиты информации

Secret Net Studio

Руководство администратора

Принципы построения

RU.88338853.501400.001 91 1

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

Оглавление

Список сокращений

AD	Active Directory
API	Application Programming Interface
BIOS	Basic Input/Output System
FAT	File Allocation Table
GPT	GUID Partition Table
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IMAPI	Image Mastering Application Programming Interface
MBR	Master Boot Record
MS	Microsoft
MSDN	Microsoft Developers Network
NTFS	New Technology File System
PCMCIA	Personal Computer Memory Card International Association
PKI	Public Key Infrastructure
ReFS	Resilient File System
SSL	Secure Socket Layer
TLS	Transport Layer Security
UDF	Universal Disk Format
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VPN	Virtual Private Network
XML	Extensible Markup Language
XPS	XML Paper Specification
АПКШ	Аппаратно-программный комплекс шифрования
АС	Автоматизированная система
БД	База данных
ЗПС	Замкнутая программная среда
ИС	Информационная система
КЦ	Контроль целостности
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 Studio" RU.88338853.501400.001 (далее — Secret Net Studio, система защиты, изделие). В нем содержатся сведения, необходимые администраторам для ознакомления с принципами работы и возможностями применения Secret Net Studio.

Условные обозначения

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

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

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

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

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

- Эта пиктограмма сопровождает информацию предостерегающего характера.

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

Другие источники информации

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

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

Глава 1
Общие сведения

Назначение системы

Система Secret Net Studio предназначена для обеспечения безопасности информационных систем на компьютерах, функционирующих под управлением операционных систем MS Windows 10/8/7 и Windows Server 2012/2008.

При использовании соответствующих подсистем изделие обеспечивает:

- защиту от несанкционированного доступа к информационным ресурсам компьютеров;
- контроль устройств, подключаемых к компьютерам;
- обнаружение вторжений в информационную систему;
- антивирусную защиту;
- межсетевое экранирование сетевого трафика;
- авторизацию сетевых соединений;

Управление функционированием системы Secret Net Studio может осуществляться централизованно или локально.

Основные функции

Система Secret Net Studio реализует следующие основные функции:

- Контроль входа пользователей в систему (идентификация и аутентификация пользователей).
- Дискреционное разграничение доступа к файловым ресурсам, устройствам, принтерам.
- Мандатное (полномочное) разграничение доступа к файловым ресурсам, устройствам, принтерам, сетевым интерфейсам, включая:
  - контроль потоков конфиденциальной информации в системе;
  - контроль вывода информации на съемные носители.
- Контроль состояния устройств компьютера с возможностями:
  - блокирования компьютера при изменении состояния заданных устройств;
  - блокирования подключения запрещенного устройства (устройства из запрещенной группы).
- Теневое копирование информации, выводимой на внешние носители и на печать.
- Автоматическая маркировка документов, выводимых на печать.
- Контроль целостности файловых объектов и реестра.
- Создание замкнутой программной среды для пользователей (контроль запуска исполняемых модулей, загрузки динамических библиотек, исполнения скриптов по технологии Active Scripts).
- Очистка оперативной и внешней памяти при ее перераспределении.
- Изоляция процессов (выполняемых программ) в оперативной памяти.
- Защита содержимого локальных жестких дисков при несанкционированной загрузке операционной системы.
- Антивирусная защита компьютеров.
- Обнаружение вторжений.
- Межсетевое экранирование сетевого трафика.
- Авторизация сетевых соединений.

- Управление ПАК "Соболь" (управление пользователями, контролем целостности, получение событий безопасности).
- Функциональный контроль ключевых защитных подсистем.
- Регистрация событий безопасности.
- Централизованное и локальное управление параметрами работы механизмов защиты.
- Централизованное и локальное управление параметрами работы пользователей.
- Мониторинг и оперативное управление защищаемыми компьютерами.
- Централизованный сбор, хранение и архивирование журналов.

Состав устанавливаемых компонентов

Система Secret Net Studio состоит из следующих программных пакетов, устанавливаемых на компьютерах:

1. "Secret Net Studio" (далее — клиент).
2. "Secret Net Studio — Сервер безопасности" (далее — сервер безопасности или СБ).
3. "Secret Net Studio — Центр управления" (далее — программа управления).

Назначение компонентов

Клиент

Клиент системы Secret Net Studio предназначен для реализации защиты компьютера, на котором установлен данный компонент. Защита реализуется путем применения защитных механизмов, расширяющих и дополняющих средства безопасности ОС Windows. Защитные механизмы — это совокупность настраиваемых программных средств, входящих в состав клиента и обеспечивающих безопасное использование ресурсов.

Клиент 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.

Режим функционирования определяется при установке клиентского ПО.

Сервер безопасности

Сервер безопасности реализует возможности централизованного управления клиентами в сетевом режиме функционирования. Данный компонент обеспечивает:

- хранение данных централизованного управления;
- координацию работы других компонентов в процессе централизованного управления системой;
- получение от клиентов и обработку информации о состоянии защищаемых компьютеров;
- управление пользователями и авторизацией сетевых соединений;
- централизованный сбор, хранение и архивирование журналов.

Программа управления

Программа управления используется для централизованного управления серверами безопасности и клиентами в сетевом режиме функционирования. Данный компонент обеспечивает:

- управление параметрами объектов;

- отображение информации о состоянии защищаемых компьютеров и произошедших событиях тревоги;
- загрузку журналов событий;
- оперативное управление компьютерами.

Лицензии на использование подсистем

Механизмы защиты системы Secret Net Studio доступны для использования при наличии соответствующих зарегистрированных лицензий. Лицензируются следующие механизмы:

- механизмы, входящие в базовую защиту (обязательная лицензия);
- дискреционное управление доступом;
- контроль устройств;
- затирание данных;
- замкнутая программная среда;
- полномочное управление доступом;
- контроль печати;
- защита дисков и шифрование данных;
- межсетевой экран;
- авторизация сетевых соединений;
- обнаружение и предотвращение вторжений;
- антивирус;
- шифрование трафика с использованием VPN клиента.

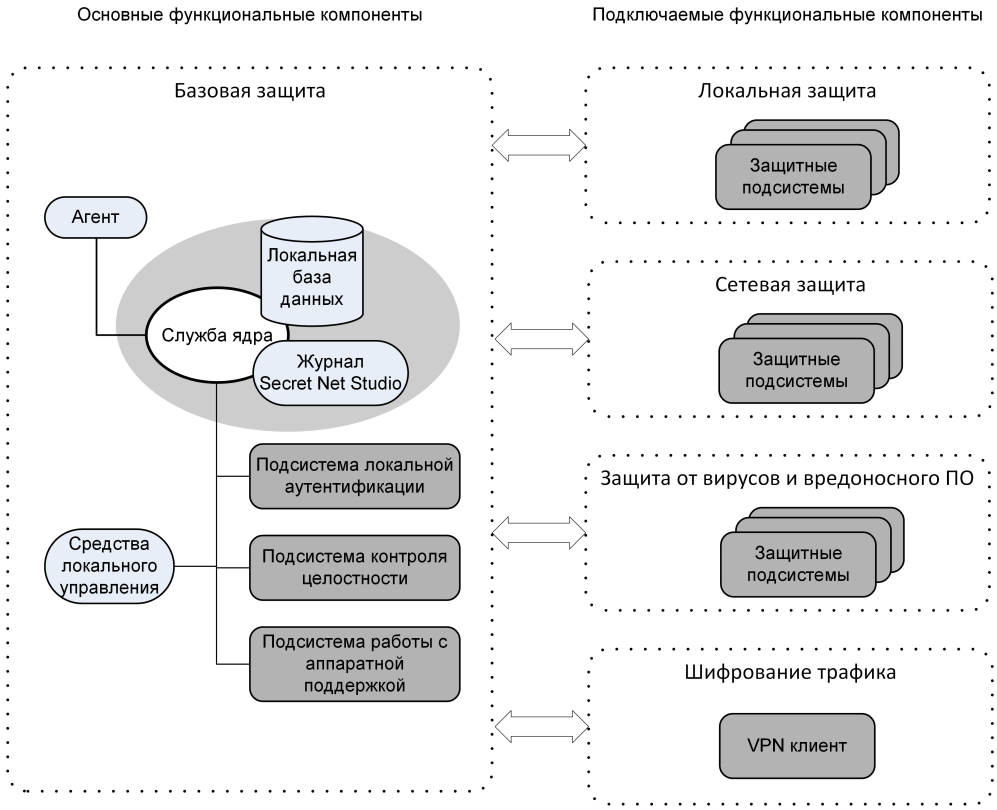
Глава 2
Составные части клиента Secret Net Studio

Группы функциональных компонентов клиента

В состав клиента системы Secret Net Studio входят следующие функциональные компоненты:

- основные программные службы, модули и защитные подсистемы (базовая защита);
- дополнительно подключаемые функциональные компоненты, условно разделенные на следующие группы:
  - локальная защита;
  - сетевая защита;
  - защита от вирусов и вредоносного ПО;
  - шифрование трафика.

Обобщенная структурная схема клиента представлена на следующем рисунке.



Базовая защита

В базовую защиту входят следующие программные службы, модули и защитные подсистемы:

- ядро;
- агент;
- средства локального управления;
- подсистема локальной аутентификации;
- 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 обеспечивает их взаимодействие.

Ядро выполняет следующие функции:

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

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

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

Агент

Агентом является программный модуль в составе клиента, обеспечивающий взаимодействие с сервером безопасности. Агент принимает команды от сервера безопасности и отправляет ему данные о состоянии компьютера.

Агент используется только в сетевом режиме функционирования клиента.

Средства локального управления

Средства локального управления обеспечивают:

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

Подсистема локальной аутентификации

Подсистема используется в механизме защиты входа в систему. Совместно с ОС Windows подсистема обеспечивает:

- проверку возможности входа пользователя в систему;
- оповещение остальных модулей о начале или завершении работы пользователя;
- блокировку работы пользователя;
- 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. Дополнительно с помощью модуля входа в систему реализуется функциональный контроль работоспособности системы Secret Net Studio.

Подсистема контроля целостности

Подсистема контроля целостности обеспечивает проверку неизменности ресурсов компьютера: каталогов, файлов, ключей и значений реестра. В составе механизма контроля целостности подсистема реализует защиту от подмены

ресурсов, сравнивая их с определенными эталонными значениями. Данная подсистема выполняет контролирующие функции не при обращении пользователя к ресурсам, а при наступлении определенных событий в системе (загрузка, вход пользователя, контроль по расписанию).

Подсистема аппаратной поддержки

Подсистема используется в механизме защиты входа в систему для работы с устройствами аппаратной поддержки. Она обеспечивает взаимодействие системы Secret Net Studio с определенным набором устройств и состоит из следующих модулей:

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

Подключаемые функциональные компоненты клиента

Локальная защита

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

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

Сетевая защита

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

- межсетевой экран;
- авторизация сетевых соединений.

Защита от вирусов и вредоносного ПО

К группе защиты от вирусов и вредоносного ПО относятся подсистемы, реализующие применение следующих механизмов защиты:

- обнаружение и предотвращение вторжений;
- антивирус.

Шифрование трафика (VPN клиент)

Подсистема шифрования трафика обеспечивает безопасную передачу данных через общедоступные незащищенные сети. Для организации передачи данных используется технология "виртуальной частной сети" (Virtual Private Network — VPN), реализуемая аппаратно-программным комплексом шифрования (АПКШ) "Континент". При установлении соединения с сервером доступа АПКШ "Континент" подсистема шифрования трафика выступает в роли VPN клиента.

Глава 3
Механизмы защиты, реализуемые клиентом

Защита 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 Studio идентификация пользователей может выполняться в следующих режимах:

- "По имени" — для входа в систему пользователь может ввести свои учетные данные (имя и пароль) или использовать аппаратные средства, поддерживаемые ОС;
- "Смешанный" — для входа в систему пользователь может ввести свои учетные данные (имя и пароль) или использовать персональный идентификатор, поддерживаемый системой Secret Net Studio;
- "Только по идентификатору" — каждый пользователь для входа в систему должен обязательно использовать персональный идентификатор, поддерживаемый системой Secret Net Studio.

В качестве персональных идентификаторов в Secret Net Studio применяются средства идентификации и аутентификации на базе идентификаторов eToken, Rutoken, JaCarta, ESMART или iButton. Чтобы использовать эти устройства, необходимо зарегистрировать их в системе защиты (присвоить пользователям).

Аутентификация пользователей может выполняться в усиленном режиме с дополнительной проверкой пароля пользователя системой Secret Net Studio. В режиме усиленной аутентификации пароли пользователей проверяются на соответствие требованиям политики паролей как в операционной системе, так и в Secret Net Studio.

Дополнительно для защиты компьютеров в Secret Net Studio предусмотрены следующие режимы:

- разрешение интерактивного входа только для доменных пользователей — в этом режиме блокируется вход в систему локальных пользователей (под локальными учетными записями);
- запрет 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).

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 Studio может контролировать неудачные попытки входа в систему при включенном режиме усиленной аутентификации по паролю. Если пользователь определенное количество раз вводит пароль, который не был сохранен в БД Secret Net Studio, — 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 политиках с помощью программы управления. Блокировка при изъятии идентификатора выполняется при условии, что 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 Studio;
- 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 управления.

Аппаратные средства защиты

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

Аппаратные средства	Основные решаемые задачи
Средства идентификации и аутентификации на базе идентификаторов eToken, Rutoken, JaCarta и ESMART	• 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

Аппаратные средства	Основные решаемые задачи
Устройство Secret Net Card	• 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
Программно-аппаратный комплекс (ПАК) "Соболь" версии 3.0	• 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" или Secret Net Card;
- USB-ключи eToken PRO, eToken PRO (Java), Rutoken, Rutoken S, Rutoken ЭЦП, Rutoken Lite, JaCarta PKI, JaCarta PKI Flash, JaCarta ГОСТ, JaCarta ГОСТ Flash, JaCarta-2 PKI/ГОСТ, ESMART Token, ESMART Token ГОСТ;
- контактные смарт- карты eToken PRO, eToken PRO (Java), Rutoken ЭЦП, Rutoken Lite, JaCarta PKI, JaCarta ГОСТ, ESMART Token, ESMART Token ГОСТ с любыми совместимыми USB-считывателями.

Общие сведения об интеграции Secret Net Studio и комплексов "Соболь"

ПАК "Соболь" обеспечивает дополнительную защиту от несанкционированного доступа к информационным ресурсам компьютера, на котором установлена система Secret Net Studio. ПАК "Соболь" может функционировать как автономно, так и совместно с Secret Net Studio.

В автономном режиме работы ПАК "Соболь" реализует свои основные функции до старта операционной системы независимо от Secret Net Studio. 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 Studio, разрешается доступ к энергонезависимой памяти комплекса. В этом случае значительная часть функций управления комплексом осуществляется с помощью средств администрирования Secret Net Studio. Перечень функций представлен в следующей таблице.

Функция	Описание
Управление входом пользователя Secret Net Studio в комплекс "Соболь" с помощью идентификатора, инициализированного и присвоенного пользователю в системе Secret Net Studio	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 и объектов реестра формируются средствами администрирования Secret Net Studio
Автоматическая передача записей журнала регистрации событий ПАК "Соболь" в журнал Secret Net Studio	Передача записей и их преобразование осуществляются автоматически при загрузке подсистемы аппаратной поддержки Secret Net Studio

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

Внимание!
В режиме интеграции системы Secret Net Studio 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 Studio реализован ряд криптографических преобразований на основе ГОСТ 28147– 89, ГОСТ Р34.10– 2001. Перечень используемых ключей шифрования представлен в следующей таблице.

Наименование ключа	Назначение	Место хранения
Симметричный ключ ЦУ	Шифрование аутентификаторов[1] в хранилище объектов централизованного управления Secret Net Studio. 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"

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

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 защитные подсистемы загружены и функционируют.

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

При неуспешном завершении функционального контроля в журнале Secret Net Studio регистрируется событие с указанием причин (это возможно при условии работоспособности ядра Secret Net Studio). 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 Studio, 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.

Регистрация событий

В процессе работы системы Secret Net Studio события, происходящие на компьютере и связанные с безопасностью системы, регистрируются в журнале Secret Net Studio. 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. Например, файлы могут контролироваться на их существование, целостность содержимого, неизменность прав доступа, атрибутов.

В системе предусмотрена возможность настройки периодичности контроля по определенным дням и времени в течение дня. Запуск процесса контроля может выполняться при загрузке ОС, при входе пользователя в систему или после входа.

При проверке целостности могут применяться различные варианты реакции системы на выполнение заданий контроля. Можно настраивать регистрацию определенных типов событий (успех или ошибка проверки отдельного объекта, либо всего задания контроля) и действия в случае нарушения целостности (игнорировать ошибку, заблокировать компьютер или принять новое значение как эталон).

Вся информация об объектах, методах, расписаниях контроля сосредоточена в специальной структуре, которая называется **модель данных**. Модель данных хранится в локальной базе данных системы Secret Net Studio и представляет собой иерархический список объектов с описанием связей между ними.

Используются следующие категории объектов в порядке от низшего уровня иерархии к высшему:

- ресурсы;
- группы ресурсов;
- задачи;
- задания;
- субъекты управления (компьютеры, пользователи, группы компьютеров и пользователей).

Модель данных является общей для механизмов контроля целостности и замкнутой программной среды.

Управление локальными моделями данных на защищаемых компьютерах можно осуществлять централизованно (для клиентов в сетевом режиме функционирования). Для централизованного управления в глобальном каталоге 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 выполняется локальная синхронизация этих изменений на защищаемом компьютере. Новые параметры из централизованного хранилища передаются на компьютер, помещаются в локальную модель данных и затем используются защитными механизмами.

Синхронизация может выполняться в следующие моменты:

- при загрузке компьютера;
- при входе пользователя в систему;
- после входа (в фоновом режиме во время работы пользователя);
- периодически через определенные интервалы времени;
- принудительно по команде администратора;
- непосредственно после внесения изменений в ЦБД КЦ-ЗПС.

Редактирование централизованных моделей данных осуществляется со следующими особенностями: для изменения 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.

Дискреционное управление доступом к ресурсам файловой системы

В состав системы Secret Net Studio 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 при локальных или сетевых обращениях, включая обращения от имени системной учетной записи;
- невозможность доступа к объектам в обход установленных прав доступа (если используются стандартные средства ОС или прикладные программы без собственных драйверов для работы с файловой системой);

- независимость действия от встроенного механизма избирательного разграничения доступа ОС Windows. То есть установленные права доступа к файловым объектам в системе Secret Net Studio не влияют на аналогичные права доступа в ОС Windows и наоборот.

Аналогично реализации в ОС Windows матрица доступа в системе Secret Net Studio представляет собой списки файловых объектов, в которых определены учетные записи с правами доступа. Права устанавливают разрешения или запреты 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 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). Эти права наследуются от корневых каталогов логических 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.

Перемещение файлового объекта в пределах своего логического раздела осуществляется с сохранением явно заданных прав доступа для этого объекта. Если для объекта включен режим наследования — после перемещения вступают в действие права того каталога, в который перемещен объект. При перемещении объекта в другой логический раздел принудительно включается режим наследования прав.

Аудит операций с файловыми объектами

При работе механизма дискреционного управления доступом в журнале Secret Net Studio 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 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 его удаления. Включение и отключение аудита операций может выполнять администратор ресурса при настройке дополнительных параметров прав доступа к файловому объекту.

Затирание удаляемой информации

Затирание удаляемой информации обеспечивает невозможность восстановления и повторного использования данных после удаления. Гарантированное уничтожение достигается путем записи случайных последовательностей чисел на место удаленной информации в освобождаемой области памяти. Для большей надежности может быть выполнено несколько циклов (проходов) затирания.

При настройке механизма можно установить различное количество циклов затирания для локальных и сменных дисков, оперативной памяти, а также для файловых объектов, удаляемых с помощью специальной команды.

Внимание!

Затирание файла подкачки виртуальной памяти выполняется стандартными средствами ОС Windows при выключении компьютера. Если в Secret Net Studio включен режим затирания оперативной памяти, рекомендуется дополнительно в политиках Windows включить действие стандартного параметра "Завершение работы: очистка файла подкачки виртуальной памяти" (размещается в разделе Конфигурация компьютера\Параметры Windows\Параметры безопасности\Локальные политики\Параметры безопасности).

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

Контроль подключения и изменения устройств компьютера

Механизм контроля подключения и изменения устройств компьютера обеспечивает:

- своевременное обнаружение изменений 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.

Разграничение доступа к устройствам

Разграничение доступа пользователей к устройствам выполняется на основании списков устройств, которые формируются механизмом контроля подключения и изменения устройств (см. стр.**20**).

Система Secret Net Studio 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 — чтобы разграничить доступ с помощью механизма полномочного управления доступом.

Возможности по разграничению доступа зависят от типов устройств. Разграничение 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, ограничены 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 Studio выставляются права доступа 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. Далее администратор безопасности разграничивает доступ пользователей к устройствам в соответствии с требованиями политики безопасности. Для этого можно выполнить 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. При подключении новое устройство включается в соответствующую группу, класс и модель (если есть). Доступ пользователей к этому устройству будет разграничен автоматически — в соответствии с правилами, которые установлены для группы, класса или модели.

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

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.

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

Попытки запуска неразрешенных ресурсов регистрируются в журнале как события тревоги.

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 (журнал безопасности или журнал Secret Net Studio), содержащих сведения о запусках программ, библиотек и сценариев.

Для файлов, входящих в список, можно включить проверку целостности с использованием механизма контроля целостности (см. стр.**17**). 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.

Изоляция процессов

В системе Secret Net Studio может применяться режим изоляции процессов для предотвращения стороннего доступа к данным определенных исполняемых модулей. При действующем режиме контролируются следующие операции с данными, которыми обмениваются различные процессы:

- чтение данных из буфера обмена;
- чтение данных в окне другого процесса;
- запись данных в окно другого процесса;
- перетаскивание данных между процессами методом drag-and-drop.

Процесс считается изолированным, если в модели данных включена изоляция для ресурса, соответствующего исполняемому файлу этого процесса. Для изолированного процеса обмен данными с другими процессами невозможен. Разрешается использование буфера обмена только при записи и чтении данных одного и того же процесса. Неизолированные процессы обмениваются данными без ограничений.

Изоляция процессов реализуется при включенном механизме замкнутой программной среды (должен функционировать драйвер механизма). Режим работы механизма ЗПС может быть любым. При этом для исключения возможностей

запуска копий исполняемых файлов в неизолированной среде рекомендуется настроить механизм ЗПС и включить жесткий режим работы механизма.

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.

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. Это необходимо для того, чтобы исключить возможность сохранения конфиденциальных данных в файлах с меньшей категорией конфиденциальности.

Полномочное разграничение доступа на уровне устройств осуществляется следующим образом. Если устройство подключается во время сеанса работы пользователя с уровнем допуска ниже, чем категория 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 категориям всех подключенных устройств.

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

Доступ к содержимому конфиденциального файла предоставляется пользователю, если категория файла не превышает уровень допуска пользователя. При этом категория конфиденциальности 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 режиме контроля потоков сохранение информации разрешено только с категорией, равной уровню конфиденциальности сессии. Полностью запрещается доступ к данным, категория 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.

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 сетевого интерфейса можно выбрать уровни конфиденциальности сессий, в которых этот интерфейс будет доступен пользователю. Если открыта сессия с другим уровнем конфиденциальности, 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 внешние носители. Внешними носителями в системе Secret Net Studio считаются сменные диски, для которых включен режим доступа "без учета категории конфиденциальности". При копировании или перемещении конфиденциального ресурса на таком носителе может не сохраниться исходная категория конфиденциальности ресурса. Поэтому чтобы осуществлять вывод конфиденциальной информации на внешие носители в режиме контроля потоков, пользователь должен обладать соответствующей привилегией.

Для предотвращения несанкционированного вывода конфиденциальных документов на локальные и сетевые принтеры используется механизм контроля печати. Механизм обеспечивает вывод конфиденциальных документов на печать только при наличии соответствующей привилегии. Также в распечатываемые документы может автоматически добавляться специальный маркер (гриф), в котором указывается категория конфиденциальности документа. События печати регистрируются в журнале Secret Net Studio.

Контроль печати

Механизм контроля печати обеспечивает:

- разграничение доступа пользователей к принтерам;
- регистрацию событий вывода документов на печать в журнале Secret Net Studio;
- 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 и 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.

Теневое копирование выводимых данных

Механизм теневого копирования обеспечивает создание в системе дубликатов данных, выводимых на съемные 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) 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).

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.**24**). 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 Studio. Доступ к дубликатам в хранилище теневого копирования осуществляется с помощью программы управления Secret Net Studio в локальном режиме работы.

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

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 Studio. 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. При этом часть служебных данных для механизма защиты дисков сохраняется в системном реестре.

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.

Механизм защиты дисков может использоваться при условии, если физический диск, с которого выполняется загрузка ОС, относится к одному из следующих типов:

- диск с таблицей разделов на идентификаторах GUID (GUID Partition Table — GPT) на компьютере с интерфейсом UEFI (Unified Extensible Firmware Interface). При включении механизма на диск записывается специальный загрузчик Secret Net Studio в скрытом системном UEFI-разделе, после чего загрузчик регистрируется в UEFI;
- диск с основной загрузочной записью (Master Boot Record — MBR). При включении механизма на этом диске модифицируется MBR и часть остального пространства нулевой дорожки диска.

Внимание!
При использовании диска с основной загрузочной записью в настройках BIOS компьютера должна быть отключена функция проверки загрузочных вирусов. Для отключения функции установите значение "Disabled" для параметра "Boot Virus Detection" (наличие данной функции и название параметра зависит от используемой версии BIOS).

При работе механизма обеспечивается защита до 128 логических разделов при общем количестве физических дисков до 32. Логические разделы, для которых устанавливается режим защиты, должны иметь файловую систему FAT, NTFS или ReFS. Разделы могут быть на физических дисках с основной загрузочной записью (MBR) или с таблицей разделов на идентификаторах GUID (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.

Шифрование данных в криптоконтейнерах

Система Secret Net Studio предоставляет возможность шифрования содержимого объектов файловой системы (файлов и папок). Для операций зашифрования и расшифрования используются специальные хранилища — криптографические контейнеры или криптоконтейнеры.

Физически криптоконтейнер представляет собой файл, который можно подключить к системе в качестве дополнительного диска. Криптоконтейнер является образом диска, но все действия с ним выполняются через драйвер механизма шифрования. Драйвер обеспечивает работу с пользовательскими данными в контейнере в режиме "прозрачного шифрования". То есть пользователь, после подключения криптоконтейнера в качестве диска, выполняет операции с файлами на этом диске так же, как и на любом другом носителе. Дополнительных действий для зашифрования или расшифрования файлов не требуется. Все криптографические операции с файлами выполняются автоматически.

Криптоконтейнеры можно подключать к системе с локальных дисков, сменных носителей или с сетевых ресурсов. Доступный объем для записи данных указывается при создании криптоконтейнера. Предельное ограничение объема определяется исходя из свободного пространства на ресурсе и типа файловой системы. Минимальный размер контейнера — 1 МБ.

Для разграничения доступа пользователей к криптоконтейнерам в системе Secret Net Studio предусмотрены следующие права:

- чтение данных — предоставляет только возможности чтения файлов в криптоконтейнере;
- полный доступ к данным — предоставляет возможности чтения и записи файлов в криптоконтейнере;
- управление криптоконтейнером — предоставляет возможности управления списком пользователей, имеющих доступ к криптоконтейнеру, а также чтения и записи файлов.

Создание криптоконтейнеров доступно пользователям с соответствующей привилегией. По умолчанию эта привилегия предоставлена всем учетным записям, которые входят в локальные группы администраторов или пользователей.

Пользователь, создавший криптоконтейнер, получает право на управление им и в дальнейшем может делегировать (предоставить) это право доступа другому пользователю. При необходимости создатель криптоконтейнера может быть удален из списка пользователей с правами доступа с тем условием, что в списке будет присутствовать хотя бы один пользователь с правами на управление криптоконтейнером.

Для работы с шифрованными ресурсами пользователи должны иметь ключи шифрования. Процедуры генерации и выдачи ключей выполняются администратором безопасности. Для пользователей создаются ключевые пары, каждая из которых состоит из открытого и закрытого ключей. Открытые ключи хранятся в общем хранилище (для ключей локальных пользователей используется локальная БД Secret Net Studio, для доменных — хранилище глобального каталога). Закрытые ключи хранятся в ключевых носителях, присвоенных пользователям. Носителями для хранения закрытых ключей (ключевой информации) могут являться идентификаторы или сменные носители, такие как флеш-карты, флеш-накопители и т. п.

Общие сведения о ключевой схеме

Реализация ключевой схемы шифрования криптоконтейнеров базируется на алгоритмах ГОСТ Р34.10-2012, ГОСТ Р34.11-2012 и ГОСТ 28147–89. Во время криптографических операций генерируются и вычисляются определенные наборы ключей и дополнительных значений, используемых для доступа к криптоконтейнеру.

Криптоконтейнер содержит следующие группы данных:

- управляющая информация криптоконтейнера — представляет собой структуру зашифрованных ключей и значений для доступа к криптоконтейнеру;
- зашифрованные данные пользователей — криптографически преобразованные файлы, помещенные в криптоконтейнер пользователями.

Управляющая информация криптоконтейнера формируется при его создании. Изначально в этой структуре совместно с другими сведениями сохраняется открытый ключ пользователя, создавшего криптоконтейнер. Далее в процессе формирования списка пользователей, имеющих доступ к контейнеру, открытые ключи этих пользователей также помещаются в структуру. С использованием открытых ключей шифруются соответствующие части структуры.

Файлы, помещаемые пользователями в криптоконтейнер, шифруются с использованием ключей шифрования, рассчитанных на основе базового ключа шифрования — общего для всех пользователей криптоконтейнера. Базовый ключ шифрования генерируется при создании криптоконтейнера. Вычисление ключа осуществляется при доступе к криптоконтейнеру с помощью закрытого ключа пользователя.

Для дополнительной защиты базового ключа шифрования может использоваться специальный "корпоративный ключ". Данный ключ генерируется при создании криптоконтейнера, если включен параметр "использовать корпоративный ключ". Ключ сохраняется в системном реестре компьютера и применяется для зашифрования и расшифрования базового ключа.

При использовании корпоративного ключа доступ к криптоконтейнеру возможен при условии, если ключ хранится в системном реестре (в зашифрованном виде). Поэтому для доступа к криптоконтейнеру на другом компьютере корпоративный ключ необходимо импортировать в реестр этого компьютера.

Смена ключей

В процессе эксплуатации системы следует регулярно выполнять смену ключей пользователей и базовых ключей шифрования криптоконтейнеров.

Смена ключей пользователя выполняется самим пользователем или администратором безопасности. Периодичность смены ключей пользователей контролируется системой и может настраиваться путем ограничения максимального и минимального сроков действия ключей. При смене ключей пользователя в системе сохраняются две ключевые пары — текущая и предыдущая. Предыдущая ключевая пара необходима для перешифрования на новом ключе соответствующей части управляющей информации в криптоконтейнерах пользователя. Процесс перешифрования управляющей информации запускается автоматически после смены ключей.

Внимание!

Автоматическое перешифрование управляющей информации возможно при условии доступности криптоконтейнера. Например, если криптоконтейнер недоступен по сети или находится на сменном носителе, который не подключен в данный момент, — перешифрование не происходит. В этом случае после смены ключей для перешифрования управляющей информации пользователю необходимо выполнить какую-либо операцию с таким криптоконтейнером (например, подключить криптоконтейнер) до следующей смены ключей. Иначе во время следующей смены будет заменена предыдущая ключевая пара, и пользователь не сможет получить доступ к криптоконтейнеру из-за несовпадения ключей. Для возобновления доступа потребуется удалить пользователя из списка имеющих доступ к криптоконтейнеру и затем снова добавить в этот список.

Смена базового ключа шифрования криптоконтейнера выполняется пользователем с правами на управление криптоконтейнером. Для смены базового ключа пользователь инициирует процедуру перешифрования криптоконтейнера, в результате чего все зашифрованные данные криптоконтейнера будут перешифрованы на новом базовом ключе. При использовании корпоративного ключа его смена происходит автоматически при смене базового ключа.

Межсетевой экран

Система Secret Net Studio обеспечивает контроль сетевого трафика на сетевом, транспортном и прикладном уровнях на основе формируемых правил фильтрации.

Подсистема межсетевого экранирования Secret Net Studio реализует следующие основные функции:

- фильтрация на сетевом уровне с независимым принятием решений по каждому пакету;
- фильтрация пакетов служебных протоколов (ICMP, IGMP и т.д.), необходимых для диагностики и управления работой сетевых устройств;
- фильтрация с учетом входного и выходного сетевого интерфейса для проверки подлинности сетевых адресов;
- фильтрация на транспортном уровне запросов на установление виртуальных соединений (TCP-сессий);
- фильтрация на прикладном уровне запросов к прикладным сервисам (фильтрация по символьной последовательности в пакетах);
- фильтрация с учетом полей сетевых пакетов;
- фильтрация с учетом даты/времени суток.

Фильтрация сетевого трафика осуществляется на интерфейсах Ethernet (IEEE 802.3) и Wi-Fi (IEEE 802.11b/g/n). События, связанные с работой межсетевого экрана, регистрируются в журнале Secret Net Studio.

Авторизация сетевых соединений

При действующем механизме авторизации сетевых соединений осуществляется добавление специальной служебной информации к сетевым пакетам, с помощью которой обеспечивается аутентичность и целостность передаваемых данных и защита от атак типа Man in the Middle.

Подсистема авторизации сетевых соединений обеспечивает:

- получение с сервера авторизации, входящего в состав компонента "Secret Net Studio — Сервер безопасности", правил авторизации соединений (список параметров соединений, в которые будет добавляться служебная информация);
- получение с сервера авторизации сессионных данных для добавления служебной информации;
- добавление в сетевой трафик специальной служебной информации для пакетов, удовлетворяющих правилам авторизации;
- разбор специальной служебной информации во входящих пакетах и передачу информации о контексте удаленного пользователя в подсистему межсетевого экранирования для фильтрации по правилам.

Авторизация сетевых соединений осуществляется на интерфейсах Ethernet (IEEE 802.3) и Wi-Fi (IEEE 802.11b/g/n).

Обнаружение и предотвращение вторжений

Secret Net Studio реализует обнаружение и блокирование внешних и внутренних вторжений, направленных на защищаемый компьютер.

Настройка параметров механизма осуществляется администратором безопасности с помощью групповых и локальных политик в программе управления Secret Net Studio.

Вся информация об активности механизма обнаружения и предотвращения вторжений регистрируется в журнале Secret Net Studio.

Функция	Описание
Детекторы сетевых атак	Фильтрация входящего трафика, используемая для блокировки внешних атак. Детекторы атак функционируют на прикладном уровне модели OSI. Анализ входящих данных производится с помощью изучения поведения
Сигнатурный анализ	Контроль входящего и исходящего сетевого трафика на наличие элементов, зарегистрированных в базе решающих правил (БРП). Атакующие компьютеры могут блокироваться на заданный промежуток времени

Антивирус

Secret Net Studio позволяет осуществлять эвристический анализ данных и автоматическую проверку на наличие вредоносных программ, зарегистрированных в базе сигнатур. При проверке компьютера осуществляется сканирование жестких дисков, сетевых папок, внешних запоминающих устройств и др. Это позволяет обнаружить и заблокировать внешние и внутренние сетевые атаки, направленные на защищаемый компьютер.

Настройка параметров установленного антивируса осуществляется администратором безопасности с помощью групповых и локальных политик в программе управления Secret Net Studio.

Вся информация об активности механизма регистрируется в журнале Secret Net Studio.

Для обеспечения антивирусной защиты предусмотрены следующие функции.

Функция	Описание
Постоянная защита	Проверка файлов в режиме реального времени. Обнаружение компьютерных вирусов сигнатурными и эвристическими методами при попытках получения доступа к исполняемым файлам, файлам документов, изображений, архивов, скриптов и другим типам потенциально опасных файлов
Контекстное сканирование	Проверка, запускаемая пользователем из контекстного меню в проводнике Windows
Сканирование по расписанию	Проверка, запускаемая по расписанию. Параметры проверки настраиваются администратором в программе управления. Пропущенное сканирование по расписанию (например, компьютер выключен) принудительно запускается после восстановления работы компьютера
Автоматическая проверка съемных носителей	В Secret Net Studio реализована возможность автоматической проверки съемных носителей при их подключении к компьютеру
Список исключений	Создание списка файлов, которые не проверяются при проверке файлов в режиме реального времени и при сканировании по расписанию. Список исключений действует глобально для всех видов сканирования и не настраивается отдельно для разных режимов
Выполнение действий с обнаруженными вирусами	Возможно выполнение следующих действий с зараженными объектами: удаление, изолирование (перемещение в карантин), блокировка доступа (только в режиме постоянной защиты), лечение. Выбор реакции на обнаруженные вредоносные программы осуществляется в настройках параметров антивируса
Обновление антивирусных баз	Автоматическое обновление базы с сервера обновлений, запускаемое в фоновом режиме, или ручное обновление базы из выбранной директории
Контроль целостности сигнатур	Проверка неизменности базы сигнатур при загрузке службы и при обновлении. При несанкционированном изменении базы создается запись в журнале Secret Net Studio

Шифрование трафика с использованием VPN клиента

В состав клиентского ПО системы Secret Net Studio включен VPN клиент, предназначенный для организации доступа удаленных пользователей к ресурсам, защищаемым средствами АПКШ "Континент". VPN клиент обеспечивает криптографическую защиту трафика, циркулирующего по каналу связи. На стороне сервера доступа АПКШ "Континент" VPN клиент системы Secret Net Studio рассматривается как отдельный абонентский пункт (АП).

При подключении абонентского пункта к серверу доступа выполняется процедура установки соединения, в ходе которой осуществляется взаимная аутентификация абонентского пункта и сервера доступа. Завершается процедура установки соединения генерацией сеансового ключа, который используется для шифрования трафика между абонентским пунктом и сервером доступа.

При аутентификации используются сертификаты X.509v3. Расчет хэш-функции выполняется по алгоритму ГОСТ Р 34.11—1994 или ГОСТ Р 34.11—2012, формирование и проверка электронной подписи — по алгоритму ГОСТ Р 34.10—2001 или ГОСТ Р 34.10—2012.

Генерация закрытого ключа и формирование на его основе открытого при создании запроса на получение сертификата удостоверяющего центра выполняется средствами встроенного криптопровайдера "Код Безопасности CSP". Поддерживается работа с внешним криптопровайдером "КриптоПро CSP".

Для VPN клиента можно создать и настроить несколько подключений. Например, если защищаемая сеть АПКШ "Континент" имеет в составе несколько серверов доступа. В этом случае для соединения с каждым из них можно использовать отдельное подключение. При установленном соединении с сервером доступа другие подключения запрещаются. Поэтому перед активацией другого подключения необходимо разорвать текущее соединение.

Глава 4
Организация централизованного управления системой

Взаимодействующие компоненты

Клиент в сетевом режиме функционирования

Для реализации централизованного управления на всех защищаемых компьютерах должно быть установлено ПО клиента в сетевом режиме функционирования. Эти компьютеры необходимо подчинить серверам безопасности.

Сервер безопасности

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 тревоги, 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 управления системы Secret Net Studio;
- контроль действительности лицензий на использование компонентов системы Secret Net Studio;
- 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.

Сервер безопасности реализует функции контроля и управления защищаемыми компьютерами при условии их подчинения. Серверу могут быть подчинены компьютеры с установленным клиентом Secret Net Studio.

Для функционирования сервера безопасности требуется наличие системы управления базами данных (СУБД), реализуемой сервером СУБД MS SQL. Сервер безопасности и сервер СУБД могут быть установлены на разных компьютерах (рекомендуется) или на одном компьютере.

Сервер авторизации

В состав ПО сервера безопасности входит отдельное приложение — сервер авторизации. Данное приложение обеспечивает работу механизмов межсетевого экрана и авторизации сетевых соединений. Сервер авторизации устанавливается и удаляется вместе с ПО сервера безопасности.

Программа управления

Программа управления устанавливается на рабочих местах администраторов и используется для централизованного управления защищаемыми компьютерами. Программа осуществляет взаимодействие с сервером безопасности, через который выполняются необходимые действия.

Домены безопасности

В системе Secret Net Studio реализация централизованного управления компьютерами и синхронизации параметров защиты базируется на концепции доменов безопасности. Домены безопасности 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.

Сервер безопасности использует базу данных служб облегченного доступа к каталогам Active Directory (Active Directory Lightweight Directory Services, AD LDS). Контроль получения и применения параметров на защищаемых компьютерах осуществляется самим сервером безопасности.

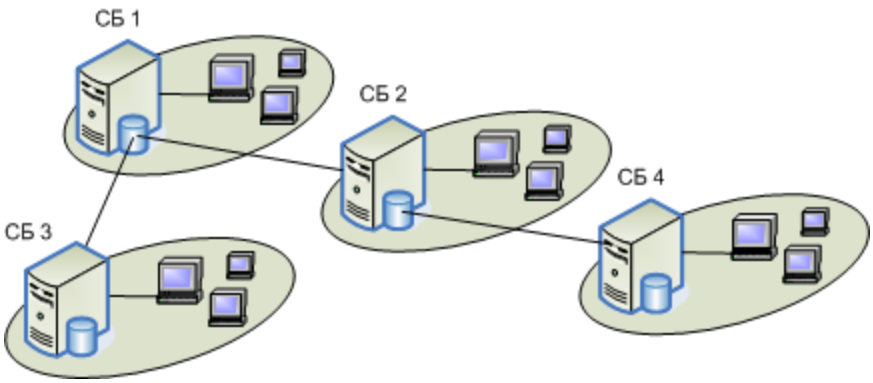
Домен безопасности создается как часть структуры леса доменов безопасности. Для леса назначается группа пользователей, которым будут предоставлены права на создание новых доменов безопасности. Эта группа будет являться группой администраторов леса доменов безопасности. При создании домена безопасности назначается группа пользователей, которым будут предоставлены права администрирования домена безопасности, — группа администраторов домена безопасности.

Внимание!
Чтобы обеспечить бесперебойное функционирование защищаемых компьютеров, следует предусмотреть наличие в домене безопасности постоянно работающего резервного сервера безопасности.

Сетевая структура системы Secret Net Studio

Сетевая структура системы Secret Net Studio 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 Studio 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 Studio, является вопрос наделения полномочиями администраторов безопасности. При необходимости разделить полномочия администраторов следует 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.

Управление доменными пользователями

Настройка параметров доменных пользователей для работы в системе Secret Net Studio осуществляется в программе управления пользователями. Программа входит в состав средств управления Secret Net Studio и дополнительно предоставляет возможности создания и удаления учетных записей, а также позволяет настраивать основные параметры пользователей и групп.

Штатные средства ОС (оснастки для управления пользователями) рекомендуется использовать только для настройки параметров, отсутствующих в программе управления пользователями. При создании или удалении учетных записей с использованием штатных средств некоторые функции управления и контроля могут быть недоступны до синхронизации изменений в системе Secret Net Studio.

Централизованное хранение данных

Компоненты системы Secret Net Studio используют следующие структуры централизованного хранения данных:

- база данных сервера безопасности на сервере СУБД — содержит централизованные журналы и оперативную информацию для мониторинга системы;
- база данных служб AD LDS — содержит параметры системы Secret Net Studio, относящиеся к учетным записям, 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.

Приложение

Необходимые права для установки и управления

Система Secret Net Studio 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 Studio и управления работой системы пользователи дополнительно должны обладать определенными административными полномочиями. Состав необходимых прав и привилегий для администрирования зависит от выполняемых операций.

Для автономного режима функционирования установка ПО клиента Secret Net Studio и все функции управления доступны пользователям, входящим в локальную группу администраторов компьютера. Некоторые функции (например, управление журналом Secret Net Studio) могут быть переданы другим пользователям путем предоставления соответствующих привилегий.

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

- **Администраторы леса доменов безопасности** — пользователи, включенные в группу администраторов леса доменов безопасности Secret Net Studio (группа указывается при установке сервера безопасности, 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 Studio (группа указывается при установке сервера безопасности, 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);
- **привилегия *<название_привилегии>*** — пользователи, которым назначена указанная привилегия.

Установка и удаление компонентов

Основные операции при установке или удалении компонентов системы Secret Net Studio представлены в следующих таблицах.

Табл.1 Установка и удаление сервера безопасности

Операция	Учетные записи с правами на выполнение
Создание групп пользователей для администраторов леса домена безопасности и администраторов домена безопасности	Пользователи с правами для создания групп в домене AD и для включения пользователей в группы
Установка с созданием домена в новом лесу доменов безопасности	Administrators (доменный пользователь) + Администраторы домена безопасности
Установка с созданием нового домена безопасности в существующем лесу	Administrators + Администраторы леса доменов безопасности + Администраторы домена безопасности
Установка с добавлением сервера в существующий домен безопасности	Administrators + Администраторы леса доменов безопасности + Администраторы домена безопасности

Операция	Учетные записи с правами на выполнение
Удаление в штатном режиме: с одновременным удалением сервера из структуры ОУ	Administrators + Администраторы домена безопасности
Удаление в нештатном режиме: без корректировки структуры ОУ[1]	Administrators

[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 управления (см. стр.**37**). Данный вариант возможен, если в системе присутствует хотя бы один сервер безопасности, доступный для подключения программы. При нештатном удалении последнего сервера леса доменов данные леса доменов безопасности уничтожаются при удалении ПО сервера.

Табл.2 Установка и удаление клиента

Операция	Учетные записи с правами на выполнение
Установка с подключением к серверу безопасности	Administrators + Администраторы домена безопасности
Установка без подключения к серверу безопасности[1]	Administrators
Удаление с одновременным удалением клиента из структуры ОУ	Administrators + Администраторы домена безопасности
Удаление без корректировки структуры ОУ[2]	Administrators

[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 управления (см. стр.**37**).

[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 управления (см. стр.**37**).

Табл.3 Установка и удаление программы управления

Операция	Учетные записи с правами на выполнение
Установка	Administrators
Удаление	Administrators

Настройка механизмов и управление параметрами объектов

Основные операции при настройке механизмов защиты системы Secret Net Studio и изменении параметров объектов (пользователей, компьютеров) представлены в следующей таблице.

Табл.4 Настройка механизмов и управление параметрами объектов

Операция	Учетные записи с правами на выполнение
Создание и удаление групп пользователей	Пользователи с правами для создания и удаления учетных записей в домене AD + Administrators
Создание и удаление пользователей	Пользователи с правами для создания и удаления учетных записей в домене AD + Администраторы домена безопасности + Administrators

Операция	Учетные записи с правами на выполнение
Управление параметрами пользователей, присвоение и настройка идентификаторов	Администраторы домена безопасности + Administrators
Формирование списка компьютеров для входа в ПАК "Соболь"	Администраторы домена безопасности
Управление ключами ЦУ ПАК "Соболь"	Администраторы домена безопасности + Administrators
Локальное управление параметрами компьютера: редактирование учетной информации, подключение ПАК "Соболь"	Администраторы домена безопасности + Administrators
Управление параметрами КЦ-ЗПС	Администраторы домена безопасности + Administrators

Работа с программой управления в централизованном режиме

Основные операции в программе управления системы Secret Net Studio представлены в следующей таблице.

Табл.5 Использование программы управления

Операция	Учетные записи с правами на выполнение
Подключение к серверу безопасности и просмотр информации	Привилегия "Просмотр информации" для сервера подключения
Конфигурирование агентов (добавление в структуру ОУ, удаление, подчинение и настройка параметров в режиме конфигурирования)	Администраторы домена безопасности
Конфигурирование серверов безопасности (добавление в структуру ОУ, удаление, подчинение и настройка параметров в режиме конфигурирования)	Администраторы домена безопасности
Корректировка структуры ОУ после нештатного удаления сервера безопасности: удаление сервера при подключении к СБ в другом домене в том же лесу[1]	Администраторы домена безопасности (в домене сервера подключения) + Администраторы домена безопасности (в домене удаленного сервера)
Настройка параметров групповых политик доменов и организационных подразделений	Администраторы домена безопасности + Привилегия "Редактирование политик" для сервера подключения
Удаленная настройка локальных параметров Secret Net Studio: параметры локальной политики безопасности, аппаратная конфигурация, состояние защитных механизмов	Привилегии "Редактирование политик" + "Выполнение оперативных команд" для сервера подключения
Выполнение команд оперативного управления компьютерами: блокировка, перезагрузка, обновление политик	Привилегия "Выполнение оперативных команд" для сервера подключения
Запуск процесса внеочередного сбора журналов с защищаемых компьютеров	Привилегия "Сбор журналов по команде" для сервера подключения
Запуск процесса внеочередного архивирования журналов в БД сервера безопасности	Привилегия "Архивирование/восстановление журналов" для сервера подключения
Квитирование событий тревоги (подтверждение приема информации)	Привилегия "Квитирование сообщений о тревогах" для сервера подключения

[1] Операция выполняется, если ПО сервера безопасности было удалено в нештатном режиме без корректировки структуры ОУ (см. стр. **35**) и при этом для подключения программы доступен СБ в другом домене того же леса. Если можно выполнить подключение к серверу в том же домене, для удаления объекта из структуры достаточно полномочий, требуемых при конфигурировании серверов безопасности (см. выше).

Оценка размера БД для сервера безопасности

Для установки и функционирования сервера безопасности в системе должен быть установлен сервер СУБД. Чтобы обеспечить производительность и необходимое время хранения накопленных данных, предварительно следует оценить размер будущей базы данных и нужный объем диского пространства на компьютере сервера СУБД. Исходя из результатов оценки принимается решение о выборе редакции СУБД (свободно распространяемые редакции имеют ограничение на размер базы данных) и аппаратной конфигурации компьютера.

Основные критерии для оценки:

- Поток событий — количество регистрируемых событий в течение определенного периода времени. Базовое значение — поток событий в секунду (Events Per Second, EPS). Суммируются события, регистрируемые в штатных журналах ОС и в журнале Secret Net Studio. Нужно учитывать, что на поток событий существенно влияют роль компьютера в системе (сервер, рабочая станция), а также заданные параметры функционирования и регистрации в подсистемах.
- Размер записей о событиях — объем сохраняемой информации о событиях в записях журналов. Зависит от заполнения полей в записях различными данными: описания событий, сведения об источниках и объектах, другие данные. Размер записи о событии может варьироваться в широких пределах, поэтому целесообразно оценивать среднее значение.
- Срок хранения журналов — определяет время хранения журналов в базе данных и в архивах. Журналы должны быть доступны для оперативного получения сведений об инцидентах и нарушениях политики безопасности, для проведения аудита и определения потенциальных угроз. Срок хранения журналов должен быть достаточным, чтобы осуществлять ретроспективный анализ состояния системы.

> **Примечание.**
> Для обеспечения работоспособности сервера СУБД и минимизации издержек на поддержку инфраструктуры необходимо регулярно выполнять архивацию журналов. По умолчанию архивы сохраняются в подкаталоге \Archive каталога установки сервера безопасности. При необходимости архив можно загрузить в базу данных для анализа содержимого хранящихся в нем журналов.

Ниже рассматривается пример расчета для типовой АС класса защищенности 1Г, состоящей из одного сервера безопасности и 100 клиентских компьютеров. Для сервера безопасности используется компьютер под управлением ОС Windows Server 2012, для клиентов — ОС Windows 8.

Табл.6 Поток событий и средний размер записей на сервере безопасности

Журналы	Среднее количество событий в секунду (EPS)	Средний размер записи (байт)
Штатные журналы ОС	3	1000
Журнал Secret Net Studio	0,05	800

Табл.7 Поток событий и средний размер записей на клиенте

Журналы	Среднее количество событий в секунду (EPS)	Средний размер записи (байт)
Штатные журналы ОС	1	1000
Журнал Secret Net Studio	0,05	800

Табл.8 Объем журналов

Журналы	Количество событий в день	Заполнение БД за день (МБ)[1]	Объем журналов в БД за 7 дней (МБ)[2]	Объем журналов в архиве за 1 год (МБ)[3]
Сервер безопасности, 1 компьютер				
Штатные журналы ОС	259 200	259,2	1 814,4	2 365
Журнал Secret Net Studio	4 320	3,5	24,2	31,5
Клиент Secret Net Studio, 100 компьютеров				
Штатные журналы ОС	8 640 000	8 640	60 480	78 840
Журнал Secret Net Studio	432 000	345,6	2 419,2	3 153
Всего для сервера безопасности и клиентов				
		9 248,3	**64 737,8**	**84 390**

[1] Указан размер таблиц, содержащих журналы событий. Общий размер базы данных зависит также от размеров журнала транзакций и проводимых операциях по оптимизации/сжатию базы.

[2] При использовании СУБД MS SQL Express 2012 (в данной редакции действует ограничение на размер базы в 10 ГБ) следует уменьшить число источников данных. Для этого можно сократить количество подчиненных компьютеров до 10, либо в параметрах передачи локальных журналов отключить сбор штатных журналов ОС.

[3] С учетом сжатия архива с коэффициентом 40:1.

Внимание!

Чтобы не увеличивался общий объем базы и сохранялась производительность, регулярно выполняйте операции по архивированию логов СУБД и оптимизации структуры базы для удаления пустых страниц и дефрагментации записей в базе. В случае переполнения базы (при использовании свободно распространяемых СУБД, имеющих ограничения по размеру базы) необходимо выполнить действия по очистке базы данных, описанные в документе с комментариями к выпущенной версии (Release Notes).

Рекомендации по настройке для соответствия требованиям о защите информации

Автоматизированные системы

При определенных вариантах настройки система Secret Net Studio 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":

- АС первой группы:
  - 1Б;
  - 1В;
  - 1Г;
  - 1Д.
- АС второй группы:
  - 2А;
  - 2Б.
- АС третьей группы:
  - 3А;
  - 3Б.

Использование 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";
- изделие Secret Net Card.

При функционировании системы Secret Net Studio 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 Studio.

Параметры политик Secret Net Studio

Для соответствия классам защищенности АС должны быть настроены параметры политик, перечисленные в следующей таблице. Настройка параметров осуществляется в программе управления на вкладке "Настройки", раздел "Политики".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.9 Параметры политик

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	**2А, 2Б**	**3А, 3Б**
Группа "Вход в систему"			
Максимальный период неактивности до блокировки экрана	все: Не более 10 (реком.)	все: Не более 10 (реком.)	все: Не более 10 (реком.)
Запрет вторичного входа в систему	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Режим идентификации пользователя	все: Смешанный (реком.)	все: Смешанный (реком.)	все: Смешанный (реком.)
Режим аутентификации пользователя	все: Усиленная по паролю (обяз.)	все: Усиленная по паролю (обяз.)	все: Усиленная по паролю (обяз.)
Режим аутентификации пользователя: Регистрировать неверные аутентификационные данные	1Б,1В,1Г: Да (обяз.) 1Д: –	все: Да (обяз.)	3А: Да (обяз.) 3Б: –
Парольная политика	все: Заданы значения (обяз.)	все: Заданы значения (обяз.)	все: Заданы значения (обяз.)
Минимальная длина пароля	1Б: Не менее 8 символов (обяз.) 1В,1Г,1Д: Не менее 6 символов (обяз.)	все: Не менее 6 символов (обяз.)	все: Не менее 6 символов (обяз.)
Срок действия пароля	1Б: Не более 90 дней (обяз.) 1В,1Г,1Д: Не более 180 дней (обяз.)	все: Не более 180 дней (обяз.)	все: Не более 180 дней (обяз.)
Группа "Журнал"			
Максимальный размер журнала защиты	1Б,1В: Не менее 4096 (реком.) 1Г,1Д: Не менее 2048 (реком.)	2А: Не менее 4096 (реком.) 2Б: Не менее 2048 (реком.)	все: Не менее 2048 (реком.)
Политика перезаписи событий	все: Затирать по мере необходимости (реком.)	все: Затирать по мере необходимости (реком.)	все: Затирать по мере необходимости (реком.)
Учетные записи с привилегией просмотра журнала	все: Локальная группа администраторов (реком.)	все: Локальная группа администраторов (реком.)	все: Локальная группа администраторов (реком.)
Учетные записи с привилегией управления журналом	все: Локальная группа администраторов (реком.)	все: Локальная группа администраторов (реком.)	все: Локальная группа администраторов (реком.)
Группа "Ключи пользователя"			
Максимальный срок действия ключа	все: Не более 360 (реком.)	все: Не более 360 (реком.)	все: Не более 360 (реком.)
Предупреждение об истечении срока действия ключа	все: Не менее 14 (реком.)	все: Не менее 14 (реком.)	все: Не менее 14 (реком.)
Группа "Оповещение о тревогах"			
Локальное оповещение о тревогах	1Б: Включено (обяз.) 1В,1Г,1Д: Включено (реком.)	все: Включено (реком.)	все: Включено (реком.)

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	**2А, 2Б**	**3А, 3Б**
Группа "Дискреционное управление доступом"			
Учетные записи с привилегией управления правами доступа	1Б,1В,1Г: Локальная группа администраторов (обяз.) 1Д: Локальная группа администраторов (реком.)	все: –	все: –
Группа "Затирание данных"			
Количество циклов затирания на локальных дисках	1Б,1В: Не менее 2 (обяз.) 1Г: Не менее 1 (обяз.) 1Д: –	2А: Не менее 2 (обяз.) 2Б: –	3А: Не менее 2 (обяз.) 3Б: –
Количество циклов затирания на сменных носителях	1Б,1В: Не менее 2 (обяз.) 1Г: Не менее 1 (обяз.) 1Д: –	2А: Не менее 2 (обяз.) 2Б: –	3А: Не менее 2 (обяз.) 3Б: –
Количество циклов затирания оперативной памяти	1Б,1В: Не менее 2 (обяз.) 1Г: Не менее 1 (обяз.) 1Д: –	2А: Не менее 2 (обяз.) 2Б: –	3А: Не менее 2 (обяз.) 3Б: –
Группа "Полномочное управление доступом"			
Названия уровней конфиденциальности	1Б,1В: Настроено (обяз.) 1Г,1Д: –	2А: Настроено (обяз.) 2Б: –	все: –
Режим работы	1Б,1В: Контроль потоков включен (обяз.) 1Г,1Д: –	2А: Контроль потоков включен (обяз.) 2Б: –	все: –
Режим работы: Строгий контроль терминальных подключений	1Б,1В: Да (реком.) 1Г,1Д: –	2А: Да (реком.) 2Б: –	все: –
Группа "Замкнутая программная среда"			
Учетные записи, на которые не действуют правила замкнутой программной среды	1Б,1В: Локальная группа администраторов (реком.) 1Г,1Д: –	2А: Локальная группа администраторов (реком.) 2Б: –	все: –
Группа "Контроль приложений"			
Перенаправление буфера обмена в RDP-подключениях	1Б,1В: Запрет для всех типов подключений (реком.) 1Г,1Д: –	2А: Запрет для всех типов подключений (реком.) 2Б: –	3А: Запрет для всех типов подключений (реком.) 3Б: –
Группа "Межсетевой экран"			
Протоколы	все: Включен доступ только для протокола IPv4 (обяз.)	все: Включен доступ только для протокола IPv4 (обяз.)	все: Включен доступ только для протокола IPv4 (обяз.)
Включить ICMP-защиту	1Б,1В: Да (реком.) 1Г,1Д: –	2А: Да (реком.) 2Б: –	3А: Да (реком.) 3Б: –
ICMP-сообщения: Эхо-ответ	1Б,1В: Получение (реком.) 1Г,1Д: –	2А: Получение (реком.) 2Б: –	3А: Получение (реком.) 3Б: –
ICMP-сообщения: Адресат недоступен	1Б,1В: Получение, Отправка (реком.) 1Г,1Д: –	2А: Получение, Отправка (реком.) 2Б: –	3А: Получение, Отправка (реком.) 3Б: –

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	**2А, 2Б**	**3А, 3Б**
ICMP-сообщения: Эхо-запрос	1Б,1В: Отправка (реком.) 1Г,1Д: –	2А: Отправка (реком.) 2Б: –	3А: Отправка (реком.) 3Б: –
ICMP-сообщения: Ходатайство маршрутизатора	1Б,1В: Получение, Отправка (реком.) 1Г,1Д: –	2А: Получение, Отправка (реком.) 2Б: –	3А: Получение, Отправка (реком.) 3Б: –
ICMP-сообщения: Превышение временного интервала	1Б,1В: Получение (реком.) 1Г,1Д: –	2А: Получение (реком.) 2Б: –	3А: Получение (реком.) 3Б: –
ICMP-сообщения: Заблокировать остальные типы	1Б,1В: Да (реком.) 1Г,1Д: –	2А: Да (реком.) 2Б: –	3А: Да (реком.) 3Б: –
Режим обучения	все: Выключен (реком.)	все: Выключен (реком.)	все: Выключен (реком.)
Группа "Авторизация сетевых соединений"			
Защита соединений для группы everyone	1Б,1В,1Г: Да (реком.) 1Д: –	2А: Да (реком.) 2Б: –	все: –
Обработка сетевых пакетов: Параметры обработки сетевых пакетов	1Б,1В,1Г: Подпись, Пакет целиком (обяз.) 1Д: –	2А: Подпись, Пакет целиком (обяз.) 2Б: –	все: –
Обработка сетевых пакетов: Защита от replay-атак	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Группа "Контроль устройств"			
Перенаправление устройств в RDP-подключениях	1Б,1В: Запрет для всех типов устройств и подключений (реком.) 1Г: Запрет для всех типов устройств для подключения удаленных устройств к компьютеру (реком.) 1Д: –	2А: Запрет для всех типов устройств и подключений (реком.) 2Б: –	3А: Запрет для всех типов устройств и подключений (реком.) 3Б: –
Список устройств: Параметры контроля	1Б,1В,1Г: Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.) 1Д: –	2А: Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.) 2Б: –	все: –
Список устройств: Разрешения	1Б,1В,1Г: Заданы (обяз.) 1Д: –	2А: Заданы (обяз.) 2Б: –	все: –
Группа "Контроль печати"			
Маркировка документов	1Б,1В: Да (обяз.) 1Г,1Д: –	2А: Да (обяз.) 2Б: –	3А: Да (обяз.) 3Б: –

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	**2А, 2Б**	**3А, 3Б**
Перенаправление принтеров в RDP-подключениях	1Б,1В: Запрет для всех типов подключений (реком.) 1Г: Запрет для подключения удаленных принтеров к компьютеру (реком.) 1Д: –	2А: Запрет для всех типов подключений (реком.) 2Б: –	3А: Запрет для всех типов подключений (реком.) 3Б: –
Список принтеров: Разрешения	1Б,1В,1Г: Заданы (обяз.) 1Д: –	2А: Заданы (обяз.) 2Б: –	все: –
Группа "Антивирус"			
Постоянная защита	все: Оптимальная защита (реком.)	все: Оптимальная защита (реком.)	все: Оптимальная защита (реком.)
Сканирование подключаемых носителей	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Проверка по расписанию	все: Профиль "Быстрая проверка", расписание: "Еженедельно, суббота в 03:00" (реком.)	все: Профиль "Быстрая проверка", расписание: "Еженедельно, суббота в 03:00" (реком.)	все: Профиль "Быстрая проверка", расписание: "Еженедельно, суббота в 03:00" (реком.)
Группа "Обнаружение вторжений"			
Включить детекторы атак	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Блокировка атакующего хоста при обнаружении атак	все: Да, время блокировки — 15 мин. (реком.)	все: Да, время блокировки — 15 мин. (реком.)	все: Да, время блокировки — 15 мин. (реком.)
Сканирование портов	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
ARP-spoofing	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
SYN-FLOOD	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Аномальный трафик	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
DDoS	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
DoS	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Включить сигнатурные анализаторы	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Анализатор HTTP	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Анализатор HTTP: Контроль входящего трафика	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Анализатор HTTP: Контроль исходящего трафика	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)

Параметры пользователей

Для соответствия классам защищенности АС должны быть настроены параметры пользователей, перечисленные в следующей таблице. Настройка параметров осуществляется в программе управления пользователями в диалоговом окне настройки свойств пользователя.

Условные обозначения:

- "Да" — включить параметр;

- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.10 Параметры пользователей

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	**2А, 2Б**	**3А, 3Б**
Группа параметров "Доступ" в диалоге "Параметры безопасности"			
Уровень допуска	1Б,1В: Назначен уполномоченным пользователям (обяз.) 1Г,1Д: –	2А: Назначен уполномоченным пользователям (обяз.) 2Б: –	все: –
Привилегия: Печать конфиденциальных документов	1Б,1В: Назначена уполномоченным пользователям (обяз.) 1Г,1Д: –	2А: Назначена уполномоченным пользователям (обяз.) 2Б: –	все: –
Привилегия: Управление категориями конфиденциальности	1Б,1В: Назначена уполномоченным пользователям (обяз.) 1Г,1Д: –	2А: Назначена уполномоченным пользователям (обяз.) 2Б: –	все: –
Привилегия: Вывод конфиденциальной информации	1Б,1В: Назначена уполномоченным пользователям (обяз.) 1Г,1Д: –	2А: Назначена уполномоченным пользователям (обяз.) 2Б: –	все: –

Параметры механизмов КЦ и ЗПС

Для соответствия классам защищенности АС должны быть настроены параметры механизмов КЦ и ЗПС, перечисленные в следующей таблице. Настройка параметров осуществляется в программе "Контроль программ и данных".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.11 Параметры механизмов КЦ и ЗПС

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	**2А, 2Б**	**3А, 3Б**
Диалог "Режимы" в диалоговом окне настройки свойств компьютера			
Режим ЗПС включен	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Мягкий режим	1Б,1В: Нет (реком.) 1Г,1Д: –	2А: Нет (реком.) 2Б: –	все: –
Проверять целостность модулей перед запуском	1Б,1В: Да (обяз.) 1Г,1Д: –	2А: Да (обяз.) 2Б: –	все: –
Проверять заголовки модулей перед запуском	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Контролировать исполняемые скрипты	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Диалоговое окно настройки параметров задания контроля СЗИ			

Параметр	Классы защищенности АС		
	1Б, 1В, 1Г, 1Д	**2А, 2Б**	**3А, 3Б**
Метод контроля ресурсов	все: Содержимое (обяз.)	все: –	все: –
Алгоритм	1Б: Имитовставка (реком.) 1В,1Г,1Д: CRC32 (реком.)	все: –	все: –
Регистрация событий: Успех завершения	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Регистрация событий: Ошибка завершения	все: Да (обяз.)	все: Да (обяз.)	все: Да (обяз.)
Регистрация событий: Успех проверки	все: Нет (реком.)	все: Нет (реком.)	все: Нет (реком.)
Регистрация событий: Ошибка проверки	все: Да (обяз.)	все: Да (обяз.)	все: Да (обяз.)
Реакция на отказ: Действия	все: Заблокировать компьютер (реком.)	все: Заблокировать компьютер (реком.)	все: Заблокировать компьютер (реком.)
Расписание	1Б: При загрузке ОС и по расписанию(обяз.) 1В,1Г,1Д: При загрузке ОС или чаще (обяз.)	все: При загрузке ОС или чаще (обяз.)	все: При загрузке ОС или чаще (обяз.)
Диалоговое окно настройки параметров заданий контроля ОС (файлы и реестр)			
Метод контроля ресурсов	все: Содержимое (реком.)	все: –	все: –
Алгоритм	1Б: Имитовставка (реком.) 1В,1Г,1Д: CRC32 для реестра и встроенная ЭЦП для файлов (реком.)	все: –	все: –
Регистрация событий: Успех завершения	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Регистрация событий: Ошибка завершения	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Регистрация событий: Успех проверки	все: Нет (реком.)	все: Нет (реком.)	все: Нет (реком.)
Регистрация событий: Ошибка проверки	все: Да (реком.)	все: Да (реком.)	все: Да (реком.)
Реакция на отказ: Действия	все: Заблокировать компьютер (реком.)	все: Заблокировать компьютер (реком.)	все: Заблокировать компьютер (реком.)
Расписание	1Б: При загрузке ОС и по расписанию (реком.) 1В,1Г,1Д: При загрузке ОС или чаще (реком.)	все: При загрузке ОС или чаще (реком.)	все: При загрузке ОС или чаще (реком.)

Государственные информационные системы

При определенных вариантах настройки система Secret Net Studio обеспечивает соответствие требованиям для государственных информационных систем (ГИС), изложенным в следующих нормативно-методических документах:

- Меры защиты информации в государственных информационных системах. (документ утвержден ФСТЭК России 11 февраля 2014 г.).
- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17).

Для классов защищенности ГИС К1, К2, К3 и К4 определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- целостность информационной системы и информации;
- доступность информации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных.

Использование средств доверенной загрузки

В системах ГИС классов К1 и К2 должны применяться средства доверенной загрузки операционной системы. В качестве средства доверенной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net Studio в ГИС всех классов защищенности рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net Studio

Для соответствия классам защищенности ГИС должны быть настроены параметры политик, перечисленные в следующей таблице. Настройка параметров осуществляется в программе управления на вкладке "Настройки", раздел "Политики".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.12 Параметры политик

Параметр	Классы защищенности ГИС			
	К1	К2	К3	К4
Группа "Вход в систему"				
Максимальный период неактивности до блокировки экрана	Не более 5 (обяз.)	Не более 15 (реком.)	Не более 15 (реком.)	–

Параметр	Классы защищенности ГИС			
	К1	К2	К3	К4
Запрет вторичного входа в систему	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Количество неудачных попыток аутентификации	От 3 до 4 (обяз.)	От 3 до 8 (обяз.)	От 3 до 10 (обяз.)	От 3 до 10 (обяз.)
Режим идентификации пользователя	Только по идентификатору (обяз.)	Только по идентификатору (реком.)	Смешанный (реком.)	Смешанный (реком.)
Режим аутентификации пользователя	Усиленная по паролю (обяз.)	Усиленная по паролю (обяз.)	Усиленная по паролю (обяз.)	Усиленная по паролю (обяз.)
Парольная политика	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Минимальная длина пароля	Не менее 8 символов (обяз.)	Не менее 6 символов (обяз.)	Не менее 6 символов (обяз.)	Не менее 6 символов (обяз.)
Срок действия пароля	Не более 60 дней (обяз.)	Не более 90 дней (обяз.)	Не более 120 дней (обяз.)	Не более 180 дней (обяз.)
Сложность пароля	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Группа "Журнал"				
Максимальный размер журнала защиты	Не менее 4096 (реком.)	Не менее 4096 (реком.)	Не менее 4096 (реком.)	Не менее 4096 (реком.)
Политика перезаписи событий	Затирать по мере необходимости (реком.)	Затирать по мере необходимости (реком.)	Затирать по мере необходимости (реком.)	Затирать по мере необходимости (реком.)
Учетные записи с привилегией просмотра журнала	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Учетные записи с привилегией управления журналом	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Ключи пользователя"				
Максимальный срок действия ключа	Не более 360 (реком.)	Не более 360 (реком.)	Не более 360 (реком.)	Не более 360 (реком.)
Предупреждение об истечении срока действия ключа	Не менее 14 (реком.)	Не менее 14 (реком.)	Не менее 14 (реком.)	Не менее 14 (реком.)
Группа "Оповещение о тревогах"				
Локальное оповещение о тревогах	Включено (реком.)	Включено (реком.)	Включено (реком.)	Включено (реком.)
Группа "Дискреционное управление доступом"				
Учетные записи с привилегией управления правами доступа	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Затирание данных"				

Параметр	Классы защищенности ГИС			
	К1	**К2**	**К3**	**К4**
Количество циклов затирания на локальных дисках	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)	–
Количество циклов затирания на сменных носителях	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)	–
Количество циклов затирания оперативной памяти	Не менее 2 (обяз.)	–	–	–
Группа "Полномочное управление доступом"				
Названия уровней конфиден-циальности	Настроено (обяз.)*	–	–	–
Режим работы	Контроль потоков включен (обяз.)*	–	–	–
Режим работы: Строгий контроль терминальных подключений	Да (обяз.)*	–	–	–
Группа "Замкнутая программная среда"				
Учетные записи, на которые не действуют правила замкнутой программной среды	Локальная группа администраторов (реком.)	–	–	–
Группа "Межсетевой экран"				
Протоколы	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)
Включить ICMP-защиту	Да (реком.)	Да (реком.)	–	–
ICMP-сообщения: Эхо-ответ	Получение (реком.)	Получение (реком.)	–	–
ICMP-сообщения: Адресат недоступен	Получение, Отправка (реком.)	Получение, Отправка (реком.)	–	–
ICMP-сообщения: Эхо-запрос	Отправка (реком.)	Отправка (реком.)	–	–
ICMP-сообщения: Ходатайство маршрутизатора	Получение, Отправка (реком.)	Получение, Отправка (реком.)	–	–
ICMP-сообщения: Превышение временного интервала	Получение (реком.)	Получение (реком.)	–	–
ICMP-сообщения: Заблокировать остальные типы	Да (реком.)	Да (реком.)	–	–
Режим обучения	Выключен (реком.)	Выключен (реком.)	Выключен (реком.)	Выключен (реком.)
Группа "Авторизация сетевых соединений"				

Параметр	Классы защищенности ГИС			
	К1	К2	К3	К4
Защита соединений для группы everyone	Да (реком.)	Да (реком.)	–	–
Обработка сетевых пакетов: Параметры обработки сетевых пакетов	Подпись, Пакет целиком (обяз.)	Подпись, Пакет целиком (обяз.)	–	–
Обработка сетевых пакетов: Защита от replay-атак	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Группа "Контроль устройств"				
Перенаправление устройств в RDP-подключениях	Запрет для всех типов устройств и подключений (реком.)	Запрет для всех типов устройств и подключений (реком.)	Запрет для всех типов устройств и подключений (реком.)	Запрет для всех типов устройств и подключений (реком.)
Список устройств: Параметры контроля	Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.)
Список устройств: Разрешения	Заданы (обяз.)	Заданы (обяз.)	Заданы (обяз.)	Заданы (обяз.)
Группа "Контроль печати"				
Список принтеров: Разрешения	Заданы (обяз.)	Заданы (обяз.)	Заданы (обяз.)	Заданы (обяз.)
Группа "Антивирус"				
Постоянная защита	Оптимальная защита (реком.)	Оптимальная защита (реком.)	Оптимальная защита (реком.)	Оптимальная защита (реком.)
Сканирование подключаемых носителей	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Проверка по расписанию	Профиль "Быстрая проверка", расписание: "Еженедельно, суббота в 03:00" (реком.)	Профиль "Быстрая проверка", расписание: "Еженедельно, суббота в 03:00" (реком.)	Профиль "Быстрая проверка", расписание: "Еженедельно, суббота в 03:00" (реком.)	Профиль "Быстрая проверка", расписание: "Еженедельно, суббота в 03:00" (реком.)
Группа "Обнаружение вторжений"				
Включить детекторы атак	Да (обяз.)	Да (обяз.)	Да (реком.)	Да (реком.)
Блокировка атакующего хоста при обнаружении атак	Да, время блокировки — 15 мин. (обяз.)	Да, время блокировки — 15 мин. (обяз.)	Да, время блокировки — 15 мин. (реком.)	Да, время блокировки — 15 мин. (реком.)
Сканирование портов	Да (обяз.)	Да (обяз.)	Да (реком.)	Да (реком.)
ARP-spoofing	Да (обяз.)	Да (обяз.)	Да (реком.)	Да (реком.)
SYN-FLOOD	Да (обяз.)	Да (обяз.)	Да (реком.)	Да (реком.)

Параметр	Классы защищенности ГИС			
	К1	К2	К3	К4
Аномальный трафик	Да (обяз.)	Да (обяз.)	Да (реком.)	Да (реком.)
DDoS	Да (обяз.)	Да (обяз.)	Да (реком.)	Да (реком.)
DoS	Да (обяз.)	Да (обяз.)	Да (реком.)	Да (реком.)
Включить сигнатурные анализаторы	Да (обяз.)	Да (обяз.)	Да (реком.)	Да (реком.)
Анализатор HTTP	Да (обяз.)	Да (обяз.)	Да (реком.)	Да (реком.)
Анализатор HTTP: Контроль входящего трафика	Да (обяз.)	Да (обяз.)	Да (реком.)	Да (реком.)
Анализатор HTTP: Контроль исходящего трафика	Да (обяз.)	Да (обяз.)	Да (реком.)	Да (реком.)

*Действие является обязательным, если для реализации меры ОЦЛ.6 (ограничение прав пользователей по вводу информации в систему) будет применяться механизм полномочного управления доступом системы Secret Net Studio. Если для реализации указанной меры защиты применяются другие решения, действие не обязательно для выполнения.

Параметры пользователей

Для соответствия классам защищенности ГИС должны быть настроены параметры пользователей, перечисленные в следующей таблице. Настройка параметров осуществляется в программе управления пользователями в диалоговом окне настройки свойств пользователя.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.13 Параметры пользователей

Параметр	Классы защищенности ГИС			
	К1	К2	К3	К4
Группа параметров "Идентификатор" в диалоге "Параметры безопасности"				
Электронный идентификатор пользователя	Присвоен (обяз.)	Присвоен (реком.)	–	–
Интеграция с ПАК "Соболь"	Да (реком.)	Да (реком.)	–	–
Группа параметров "Доступ" в диалоге "Параметры безопасности"				
Уровень допуска	Назначен уполномоченным пользователям (обяз.)*	–	–	–
Привилегия: Управление категориями конфиденциальности	Назначена уполномоченным пользователям (обяз.)*	–	–	–

*Действие является обязательным, если для реализации меры ОЦЛ.6 (ограничение прав пользователей по вводу информации в систему) будет применяться механизм

полномочного управления доступом системы Secret Net Studio. Если для реализации указанной меры защиты применяются другие решения, действие не обязательно для выполнения.

Параметры механизмов КЦ и ЗПС

Для соответствия классам защищенности ГИС должны быть настроены параметры механизмов КЦ и ЗПС, перечисленные в следующей таблице. Настройка параметров осуществляется в программе "Контроль программ и данных".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.14 Параметры механизмов КЦ и ЗПС

Параметр	Классы защищенности ГИС			
	К1	К2	К3	К4
Диалог "Режимы" в диалоговом окне настройки свойств компьютера				
Режим ЗПС включен	Да (обяз.)	–	–	–
Мягкий режим	Нет (обяз.)	–	–	–
Проверять целостность модулей перед запуском	Да (обяз.)	–	–	–
Проверять заголовки модулей перед запуском	Да (реком.)	–	–	–
Контролировать исполняемые скрипты	Да (реком.)	–	–	–
Диалоговое окно настройки параметров задания контроля СЗИ				
Метод контроля ресурсов	Содержимое (обяз.)	Содержимое (обяз.)	–	–
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–	–
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	–	–
Регистрация событий: Ошибка завершения	Да (обяз.)	Да (обяз.)	–	–
Регистрация событий: Ошибка проверки	Да (обяз.)	Да (обяз.)	–	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–	–
Расписание	При загрузке ОС и по расписанию (обяз.)	При загрузке ОС и по расписанию (обяз.)	–	–
Диалоговое окно настройки параметров задания контроля ОС (файлы и реестр)				
Метод контроля ресурсов	Содержимое (реком.)	Содержимое (реком.)	–	–
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–	–
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	–	–
Регистрация событий: Ошибка завершения	Да (реком.)	Да (реком.)	–	–

Параметр	Классы защищенности ГИС			
	К1	К2	К3	К4
Регистрация событий: Успех проверки	Нет (реком.)	Нет (реком.)	–	–
Регистрация событий: Ошибка проверки	Да (реком.)	Да (реком.)	–	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–	–
Расписание	При загрузке ОС и по расписанию (реком.)	При загрузке ОС и по расписанию (реком.)	–	–

Информационные системы персональных данных

При определенных вариантах настройки система Secret Net Studio обеспечивает соответствие требованиям для информационных систем персональных данных (ИСПДн), изложенным в документе "Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (утвержден приказом ФСТЭК России от 18 февраля 2013 г. № 21).

Для уровней защищенности ИСПДн 1, 2, 3 и 4 определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- целостность информационной системы и информации;
- доступность информации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных.

Использование средств доверенной загрузки

В системах ИСПДн уровней 1 и 2 должны применяться средства доверенной загрузки операционной системы. В качестве средства доверенной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net Studio в ИСПДн всех уровней защищенности рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net Studio

Для соответствия уровням защищенности ИСПДн должны быть настроены параметры политик, перечисленные в следующей таблице. Настройка параметров осуществляется в программе управления на вкладке "Настройки", раздел "Политики".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;

- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.15 Параметры политик

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Группа "Вход в систему"				
Максимальный период неактивности до блокировки экрана	Не более 5 (обяз.)	Не более 15 (реком.)	Не более 15 (реком.)	–
Запрет вторичного входа в систему	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Количество неудачных попыток аутентификации	От 3 до 4 (обяз.)	От 3 до 8 (обяз.)	От 3 до 10 (обяз.)	От 3 до 10 (обяз.)
Режим идентификации пользователя	Только по идентификатору (обяз.)	Только по идентификатору (реком.)	Смешанный (реком.)	Смешанный (реком.)
Режим аутентификации пользователя	Усиленная по паролю (обяз.)	Усиленная по паролю (обяз.)	Усиленная по паролю (обяз.)	Усиленная по паролю (обяз.)
Парольная политика	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Минимальная длина пароля	Не менее 8 символов (обяз.)	Не менее 6 символов (обяз.)	Не менее 6 символов (обяз.)	Не менее 6 символов (обяз.)
Срок действия пароля	Не более 60 дней (обяз.)	Не более 90 дней (обяз.)	Не более 120 дней (обяз.)	Не более 180 дней (обяз.)
Сложность пароля	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Группа "Журнал"				
Максимальный размер журнала защиты	Не менее 4096 (реком.)	Не менее 4096 (реком.)	Не менее 4096 (реком.)	Не менее 4096 (реком.)
Политика перезаписи событий	Затирать по мере необходимости (реком.)	Затирать по мере необходимости (реком.)	Затирать по мере необходимости (реком.)	Затирать по мере необходимости (реком.)
Учетные записи с привилегией просмотра журнала	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Учетные записи с привилегией управления журналом	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Ключи пользователя"				
Максимальный срок действия ключа	Не более 360 (реком.)	Не более 360 (реком.)	Не более 360 (реком.)	Не более 360 (реком.)
Предупреждение об истечении срока действия ключа	Не менее 14 (реком.)	Не менее 14 (реком.)	Не менее 14 (реком.)	Не менее 14 (реком.)
Группа "Оповещение о тревогах"				

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Локальное оповещение о тревогах	Включено (реком.)	Включено (реком.)	Включено (реком.)	Включено (реком.)
Группа "Дискреционное управление доступом"				
Учетные записи с привилегией управления правами доступа	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)	Локальная группа администраторов (реком.)
Группа "Затирание данных"				
Количество циклов затирания на локальных дисках	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)	–
Количество циклов затирания на сменных носителях	Не менее 2 (обяз.)	Не менее 1 (обяз.)	Не менее 1 (обяз.)	–
Группа "Полномочное управление доступом"				
Названия уровней конфиден-циальности	Настроено (обяз.)*	–	–	–
Режим работы	Контроль потоков включен (обяз.)*	–	–	–
Режим работы: Строгий контроль терминальных подключений	Да (обяз.)*	–	–	–
Группа "Межсетевой экран"				
Протоколы	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)	Включен доступ только для протокола IPv4 (обяз.)
Включить ICMP-защиту	Да (реком.)	Да (реком.)	–	–
ICMP-сообщения: Эхо-ответ	Получение (реком.)	Получение (реком.)	–	–
ICMP-сообщения: Адресат недоступен	Получение, Отправка (реком.)	Получение, Отправка (реком.)	–	–
ICMP-сообщения: Эхо-запрос	Отправка (реком.)	Отправка (реком.)	–	–
ICMP-сообщения: Ходатайство маршрутизатора	Получение, Отправка (реком.)	Получение, Отправка (реком.)	–	–
ICMP-сообщения: Превышение временного интервала	Получение (реком.)	Получение (реком.)	–	–
ICMP-сообщения: Заблокировать остальные типы	Да (реком.)	Да (реком.)	–	–
Режим обучения	Выключен (реком.)	Выключен (реком.)	Выключен (реком.)	Выключен (реком.)
Группа "Авторизация сетевых соединений"				

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Защита соединений для группы everyone	Да (реком.)	Да (реком.)	–	–
Обработка сетевых пакетов: Параметры обработки сетевых пакетов	Подпись, Пакет целиком (обяз.)	Подпись, Пакет целиком (обяз.)	–	–
Обработка сетевых пакетов: Защита от replay-атак	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Группа "Контроль устройств"				
Перенаправление устройств в RDP-подключениях	Запрет для всех типов устройств и подключений (реком.)	Запрет для всех типов устройств и подключений (реком.)	Запрет для всех типов устройств и подключений (реком.)	Запрет для всех типов устройств и подключений (реком.)
Список устройств: Параметры контроля	Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для групп "Устройства USB", "Устройства PCMCIA" и "Устройства IEEE1394" включен режим "Подключение устройства запрещено" (обяз.)	–	–
Список устройств: Разрешения	Заданы (обяз.)	Заданы (обяз.)	–	–
Группа "Контроль печати"				
Список принтеров: Разрешения	Заданы (обяз.)	Заданы (обяз.)	–	–
Группа "Антивирус"				
Постоянная защита	Оптимальная защита (реком.)	Оптимальная защита (реком.)	Оптимальная защита (реком.)	Оптимальная защита (реком.)
Сканирование подключаемых носителей	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Проверка по расписанию	Профиль "Быстрая проверка", расписание: "Ежедельно, суббота в 03:00" (реком.)	Профиль "Быстрая проверка", расписание: "Ежедельно, суббота в 03:00" (реком.)	Профиль "Быстрая проверка", расписание: "Ежедельно, суббота в 03:00" (реком.)	Профиль "Быстрая проверка", расписание: "Ежедельно, суббота в 03:00" (реком.)
Группа "Обнаружение вторжений"				
Включить детекторы атак	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Блокировка атакующего хоста при обнаружении атак	Да, время блокировки — 15 мин. (реком.)	Да, время блокировки — 15 мин. (реком.)	Да, время блокировки — 15 мин. (реком.)	Да, время блокировки — 15 мин. (реком.)
Сканирование портов	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
ARP-spoofing	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
SYN-FLOOD	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Аномальный трафик	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
DDoS	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
DoS	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Включить сигнатурные анализаторы	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Анализатор HTTP	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Анализатор HTTP: Контроль входящего трафика	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Анализатор HTTP: Контроль исходящего трафика	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)

*Действие является обязательным, если для реализации меры ОЦЛ.6 (ограничение прав пользователей по вводу информации в систему) будет применяться механизм полномочного управления доступом системы Secret Net Studio. Если для реализации указанной меры защиты применяются другие решения, действие не обязательно для выполнения.

Параметры пользователей

Для соответствия уровням защищенности ИСПДн должны быть настроены параметры пользователей, перечисленные в следующей таблице. Настройка параметров осуществляется в программе управления пользователями в диалоговом окне настройки свойств пользователя.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.16 Параметры пользователей

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Группа параметров "Идентификатор" в диалоге "Параметры безопасности"				
Электронный идентификатор пользователя	Присвоен (обяз.)	Присвоен (реком.)	–	–
Интеграция с ПАК "Соболь"	Да (реком.)	Да (реком.)	–	–
Группа параметров "Доступ" в диалоге "Параметры безопасности"				
Уровень допуска	Назначен уполномоченным пользователям (обяз.)*	–	–	–
Привилегия: Управление категориями конфиденциальности	Назначена уполномоченным пользователям (обяз.)*	–	–	–

*Действие является обязательным, если для реализации меры ОЦЛ.6 (ограничение прав пользователей по вводу информации в систему) будет применяться механизм

полномочного управления доступом системы Secret Net Studio. Если для реализации указанной меры защиты применяются другие решения, действие не обязательно для выполнения.

Параметры механизмов КЦ и ЗПС

Для соответствия уровням защищенности ИСПДн должны быть настроены параметры механизмов КЦ и ЗПС, перечисленные в следующей таблице. Настройка параметров осуществляется в программе "Контроль программ и данных".

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности.

Табл.17 Параметры механизмов КЦ и ЗПС

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Диалоговое окно настройки параметров задания контроля СЗИ				
Метод контроля ресурсов	Содержимое (обяз.)	Содержимое (обяз.)	–	–
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–	–
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	–	–
Регистрация событий: Ошибка завершения	Да (обяз.)	Да (обяз.)	–	–
Регистрация событий: Ошибка проверки	Да (обяз.)	Да (обяз.)	–	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–	–
Расписание	При загрузке ОС и по расписанию (обяз.)	При загрузке ОС и по расписанию (обяз.)	–	–
Диалоговое окно настройки параметров задания контроля ОС (файлы и реестр)				
Метод контроля ресурсов	Содержимое (реком.)	Содержимое (реком.)	–	–
Алгоритм	CRC32 (реком.)	CRC32 (реком.)	–	–
Регистрация событий: Успех завершения	Да (реком.)	Да (реком.)	–	–
Регистрация событий: Ошибка завершения	Да (реком.)	Да (реком.)	–	–
Регистрация событий: Успех проверки	Нет (реком.)	Нет (реком.)	–	–
Регистрация событий: Ошибка проверки	Да (реком.)	Да (реком.)	–	–
Реакция на отказ: Действия	Заблокировать компьютер (реком.)	Заблокировать компьютер (реком.)	–	–
Расписание	При загрузке ОС и по расписанию (реком.)	При загрузке ОС и по расписанию (реком.)	–	–

Применение параметров после настройки

При изменении параметров объектов и защитных механизмов Secret Net Studio не все значения могут вступать в силу сразу после сохранения изменений. Некоторые параметры применяются на защищаемых компьютерах в определенные моменты времени.

Ниже перечислены параметры, вступающие в силу после перезагрузки компьютера или при следующем входе пользователя в систему. Остальные параметры применяются сразу после сохранения измененных значений.

Табл.18 Параметры в программе управления

Параметр	Момент применения
Вкладка "Состояние" для компьютера — средства включения и отключения механизмов	
Дискреционное управление	После перезагрузки
Затирание данных	После перезагрузки
Контроль устройств	После перезагрузки
Замкнутая программная среда	После перезагрузки
Полномочное управление	После перезагрузки
Контроль печати	После перезагрузки
Защита дисков и шифрование	После перезагрузки
Вкладка "Настройки", раздел "Политики" — параметры группы "Вход в систему"	
Максимальный период неактивности до блокировки экрана	При следующем входе в систему
Запрет вторичного входа в систему	После перезагрузки
Реакция на изъятие идентификатора	При следующем входе в систему
Количество неудачных попыток аутентификации	При следующем входе в систему
Разрешить интерактивный вход только доменным пользователям	При следующем входе в систему
Режим идентификации пользователя	При следующем входе в систему
Режим аутентификации пользователя	При следующем входе в систему
Парольная политика	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Журнал"	
Максимальный размер журнала системы защиты	При увеличении — сразу. При уменьшении — после очистки журнала
Учетные записи с привилегией просмотра журнала системы защиты	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Ключи пользователя"	
Все настраиваемые параметры группы	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Дискреционное управление доступом"	
Учетные записи с привилегией управления правами доступа	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Полномочное управление доступом"	
Режим работы: Контроль потоков отключен	После перезагрузки
Режим работы: Контроль потоков включен	После перезагрузки
Режим работы: Строгий контроль терминальных подключений	При следующем входе в систему

Параметр	Момент применения
Режим работы: Автоматический выбор максимального уровня сессии	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Замкнутая программная среда"	
Учетные записи, на которые не действуют правила замкнутой программной среды	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Защита диска и шифрование данных"	
Учетные записи с привилегией на создание криптоконтейнера	При следующем входе в систему
Вкладка "Настройки", раздел "Политики" — параметры группы "Контроль приложений"	
Перенаправление буфера обмена в RDP-подключениях	При следующем терминальном входе
Вкладка "Настройки", раздел "Политики" — параметры группы "Контроль устройств"	
Перенаправление устройств в RDP-подключениях	При следующем терминальном входе
Вкладка "Настройки", раздел "Политики" — параметры группы "Контроль печати"	
Маркировка документов	При следующем входе в систему
Теневое копирование	При следующем входе в систему
Перенаправление принтеров в RDP-подключениях	При следующем терминальном входе
Вкладка "Настройки", раздел "Политики" — параметры группы "Шифрование трафика"	
Учетные записи с привилегией управления настройками подключений к серверу доступа	При следующем входе в систему
Вкладка "Настройки", раздел "Параметры" — параметры группы "Управление трассировкой"	
Все настраиваемые параметры группы	После перезагрузки

Табл.19 Параметры в программе "Контроль программ и данных"

Параметр	Момент применения
Список ресурсов в задании ЗПС	При следующем входе в систему*
Диалоговое окно настройки параметров субъекта управления, диалог "Режимы"	
Режим ЗПС включен	При следующем входе в систему*
Изоляция процесса включена	При следующем входе в систему*

*При централизованной настройке возможно принудительное применение изменений по команде "Перезагрузка параметров работы пользователей" в контекстном меню субъектов управления.

Табл.20 Параметры в программе управления пользователями

Параметр	Момент применения
Операции с учетными записями: удаление, блокировка, смена пароля	При следующем входе в систему
Окно настройки свойств пользователя, диалог "Параметры безопасности" — параметры группы "Идентификатор"	
Список электронных идентификаторов пользователя	При следующем входе в систему
Окно настройки свойств пользователя, диалог "Параметры безопасности" — параметры группы "Доступ"	
Все параметры полномочного управления доступом	При следующем входе в систему

Документация

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