КОД безопасности

Средство защиты информации

Secret Net Studio

Руководство администратора

Настройка и эксплуатация. Доверенная среда

RU.88338853.501400.001 91 8

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

Оглавление

Список сокращений

BIOS	Basic Input/Output System
BSOD	Blue Screen Of Death
MBR	Master Boot Record
SLAT	Second Level Address Translation
SMEP	Supervisor Mode Execution Prevention
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
АРМ	Автоматизированное рабочее место
ДС	Доверенная среда
КС	Контрольная сумма
КЦ	Контроль целостности
ОС	Операционная система

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 для установки, настройки механизма доверенной среды (далее — ДС) и эксплуатации компьютера с функционирующей ДС.

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" (https://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 https://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 ДС

Доверенная среда Secret Net Studio является механизмом защиты, обеспечивающим внешний по отношению к операционной системе (ОС) контроль работы ОС и системы защиты, установленных на компьютере. Контроль достигается выполнением следующих функций безопасности:

- Контроль целостности (КЦ) файлов. Выполняется до загрузки ОС компьютера.
- Контроль запуска и функционирования модулей Secret Net Studio (драйверов, служб, приложений) и других драйверов. Выполняется на протяжении всего сеанса работы на компьютере.
- Блокировка от записи страниц памяти, в которых размещаются модули Secret Net Studio и другие драйверы. Обеспечивается на протяжении всего сеанса работы на компьютере.
- Обнаружение компьютерных атак, их предотвращение или аварийное завершение работы ОС компьютера при невозможности предотвращения атаки. Выполняется на протяжении всего сеанса работы на компьютере.
- Регистрация событий в журнале ДС.

Основное назначение ДС — защита информационной системы от внешнего нарушителя.

Примечание. ДС доступна в Secret Net Studio версии 8.5 и выше.

При функционирующей ДС загрузка ОС компьютера возможна только с использованием загрузочного носителя, подготовленного заранее средствами Secret Net Studio. Загрузочный носитель содержит:

- ОС ДС — специализированная ОС на базе ОС Linux, которая взаимодействует с памятью, файловой системой и ОС компьютера для реализации функций безопасности ДС;
- гипервизор ДС, обеспечивающий загрузку ОС ДС и выполнение функций безопасности ДС;
- загрузчик ДС (MBR или UEFI), предназначенный для считывания ОС ДС, гипервизора ДС и размещения их в оперативной памяти компьютера;
- настройки ДС.

Внимание! Загрузочный носитель ДС следует использовать только на доверенных АРМ.

Доверенная среда является защитным механизмом Secret Net Studio с отдельной лицензией.

Примечание. ДС является новым защитным механизмом Secret Net Studio, который находится в стадии активной разработки. Особенности настройки механизма и экранные формы могут отличаться от приведенных в данном руководстве. При возникновении вопросов по работе с ДС рекомендуется обратиться в департамент сервиса компании "Код Безопасности".

Системные требования

Требования для установки ДС Secret Net Studio приведены в таблице ниже.

Элемент	Требование
Процессор	2 ядра и более (поддерживается работа с технологией Hyper-threading). Поддержка технологии виртуализации. Для процессоров AMD Family 10h, Intel Core i3, i5, i7 и более поздних – поддержка SLAT
ОС	Windows 7 SP1 (x64) и выше
Жесткий диск (системный)	Свободное пространство — не менее 2 МБ
Системная плата	Наличие свободного USB-разъема
UEFI/BIOS	USB-флеш-накопитель должен являться первым загрузочным устройством
USB-флеш-накопитель	Объем памяти не менее 32 МБ
Лицензия	Требуется лицензия Secret Net Studio на механизм "Доверенная среда"

Примечание. Ознакомьтесь с ограничениями и рекомендациями по использованию ДС в текущей реализации (см. стр.26).

Глава 2
Включение доверенной среды

Для функционирования ДС необходимо выполнить следующие действия:

- зарегистрировать лицензию на механизм ДС в Secret Net Studio;
- подготовить загрузочный носитель ДС;
- включить механизм ДС.

Регистрация лицензии на механизм ДС

Процедура регистрации лицензии на механизм ДС аналогична процедурам регистрации лицензий на другие механизмы защиты Secret Net Studio.

Лицензия может быть зарегистрирована централизованно и локально:

- при установке Secret Net Studio;
- при функционирующем Secret Net Studio.

Пояснение. После регистрации лицензии ДС по умолчанию выключена.

Регистрация при установке Secret Net Studio

Лицензия на механизм ДС может быть зарегистрирована совместно с лицензиями на другие механизмы защиты при установке Secret Net Studio. Инструкции по установке приведены в документе [**2**]:

- локальная установка — глава "Локальная установка компонентов", раздел "Установка клиента";
- централизованная установка — глава "Настройка централизованной установки клиента".

Регистрация при функционирующем Secret Net Studio

Лицензию на механизм ДС можно зарегистрировать отдельно при функционирующем Secret Net Studio. Инструкции по регистрации лицензий приведены в документах:

- локальная регистрация — документ [**3**], глава "Дополнительные возможности локального администрирования", раздел "Локальная регистрация лицензий";
- централизованная регистрация — документ [**4**], глава "Настройка и контроль централизованного развертывания ПО", раздел "Управление лицензиями на использование механизмов защиты".

Создание загрузочного носителя ДС

Загрузочный носитель ДС можно создать на любом компьютере с ДС Secret Net Studio (централизованно и локально).

Совет.

- Рекомендуется создавать загрузочный носитель ДС на компьютере с типовой конфигурацией Secret Net Studio, на которой планируется использование ДС. Это связано с тем, что при создании загрузочного носителя ДС формируется список модулей Secret Net Studio, целостность которых будет контролироваться.
- Рекомендуется создавать загрузочный носитель на доверенном АРМ администратора ДС.

Создание загрузочного носителя ДС доступно и при включенной, и при выключенной ДС.

Для создания загрузочного носителя ДС необходим отдельный USB-флеш-накопитель.

Перед выполнением процедуры создания загрузочного носителя ДС подключите USB-флеш-накопитель к компьютеру.

Внимание! При создании загрузочного носителя ДС все данные на USB-флеш-накопителе уничтожаются. Создается раздел небольшого объема для служебной информации ДС; память USB-флеш-накопителя используется лишь частично. Для дальнейшего использования устройства в качестве обычного USB-флеш-накопителя и задействования всего объема памяти выполните полную очистку по инструкции со стр.28.

Ниже приведена процедура создания загрузочного носителя ДС в программе управления в локальном режиме работы. В централизованном режиме процедура выполняется аналогично.

Для создания загрузочного носителя ДС:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Локальный центр управления".

   Запустится программа управления Secret Net Studio в локальном режиме.

2. В панели "Компьютер" на вкладке "Состояние" выберите элемент "Доверенная среда".

   В правой части окна отобразятся сведения о подсистеме "Доверенная среда", подобные представленным на рисунке ниже.

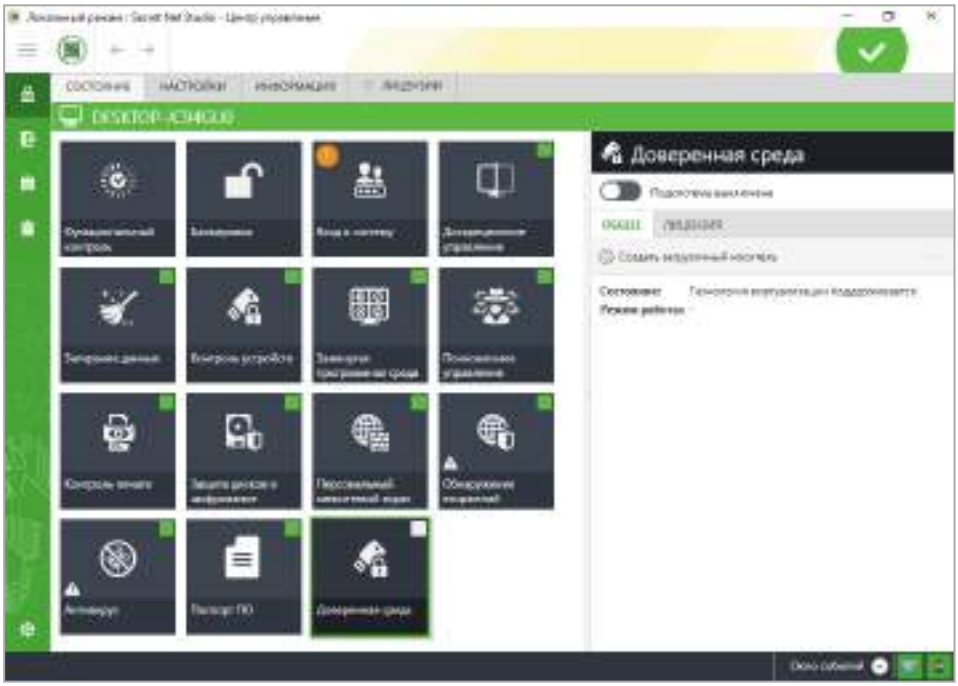
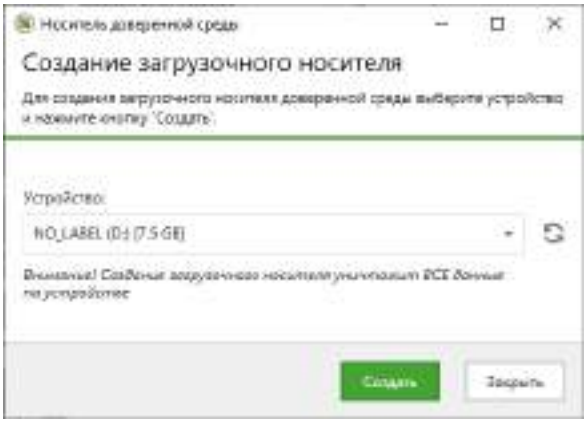


Рис.1 Сведения о подсистеме "Доверенная среда"

3. Нажмите кнопку "Создать загрузочный носитель".

   На экране появится окно создания загрузочного носителя ДС, подобное представленному на рисунке ниже.



4. Выберите подключенный USB-флеш-накопитель в раскрывающемся списке устройств.
5. Нажмите кнопку "Создать".

   Начнется процедура записи данных на USB-флеш-накопитель. По окончании процедуры в окне создания загрузочного носителя ДС появится сообщение об успешном завершении записи.
6. Нажмите кнопку "Закрыть".

   Загрузочный носитель ДС подготовлен к работе.

Включение механизма ДС

Включение механизма ДС выполняется локально на компьютере, на котором планируется использование ДС.

Внимание! Перед включением ДС Secret Net Studio убедитесь, что:

- Компьютер соответствует системным требованиям, приведенным на стр.7. Информация о соответствии/несоответствии отображается в программе управления в централизованном и локальном режимах работы (окно со сведениями о подсистеме "Доверенная среда" (см. Рис.1 на стр. 9), параметр "Состояние"). Перечень возможных значений данного параметра при несоответствии компьютера системным требованиям приведен на стр.25.
- Подготовлен загрузочный носитель ДС (см. стр.8). Без него невозможно войти в ОС компьютера.

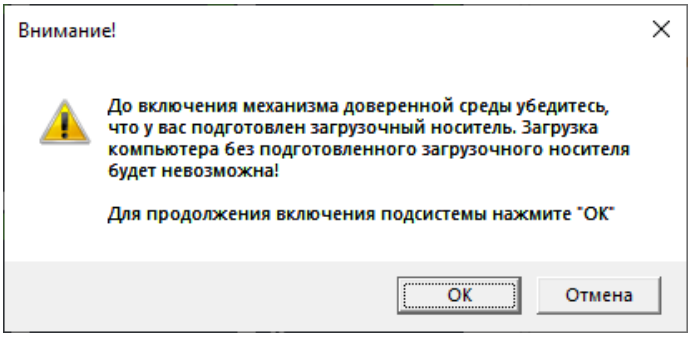
Для включения ДС:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Локальный центр управления".

   Запустится программа управления Secret Net Studio в локальном режиме.
2. В панели "Компьютер" на вкладке "Состояние" выберите элемент "Доверенная среда".

   В правой части окна отобразятся сведения о подсистеме "Доверенная среда".
3. Переключите тумблер "Подсистема выключена" в положение "Вкл".

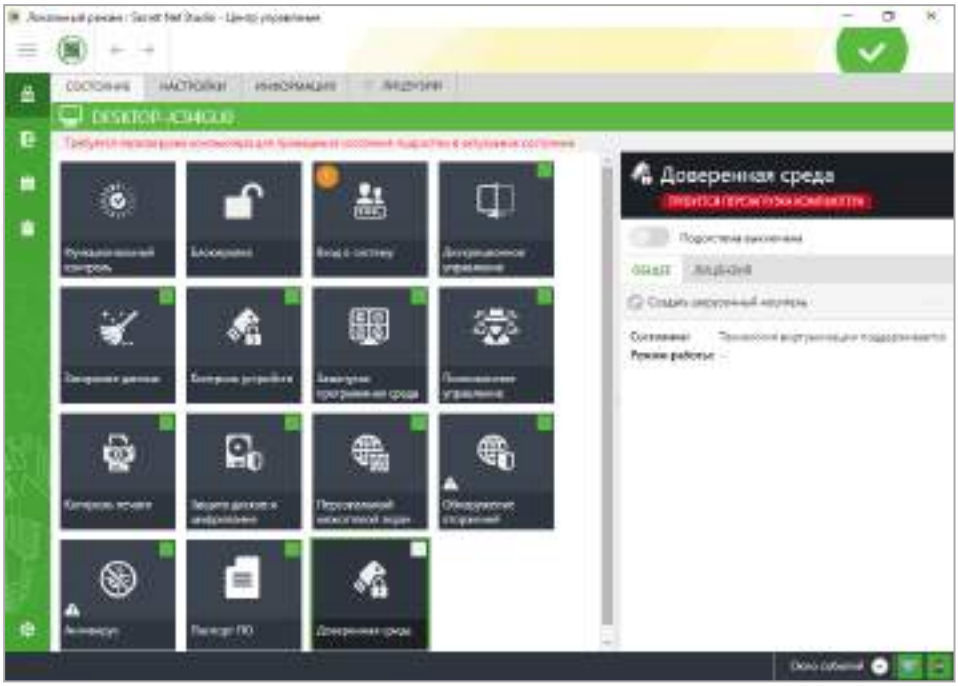
   Появится предупреждение:



4. Если загрузочный носитель ДС подготовлен, нажмите кнопку "ОК".

Пояснение. Если загрузочный носитель ДС не подготовлен, нажмите кнопку "Отмена" и создайте его по инструкции, приведенной на стр.8.

В программе управления появится предупреждение о необходимости перезагрузки компьютера, подобное представленному на рисунке ниже.



5. Подключите загрузочный носитель ДС к компьютеру.

Внимание!

- Убедитесь, что в UEFI/BIOS первым загрузочным устройством является USB-флеш-накопитель.
- В некоторых UEFI/BIOS порядок загрузки сбивается после каждого включения компьютера. В таком случае при каждом включении компьютера нужно указывать порядок загрузки в UEFI/BIOS Setup (меню Boot).

Внимание! При включении компьютера без загрузочного носителя ДС на экране блокировки ОС компьютера появится сообщение "Ошибка выполнения функционального контроля. Причины: доверенная среда не функционирует". Вход в ОС будет невозможен.

6. Перезагрузите компьютер.

Начнется процесс загрузки ОС ДС с загрузочного носителя ДС. При успешной загрузке на экране появится меню ОС ДС (см. Рис.2 на стр.**13**).

Механизм ДС будет функционировать в мягком режиме (см. стр.**15**).

Пояснение. При невыполнении системных требований после перезагрузки могут возникнуть ошибки. В этом случае следуйте инструкциям из сообщений об ошибках.

При возникновении системной ошибки BSOD ознакомьтесь с причиной ее возникновения по коду, отображенном на экране. Возможные коды ошибок, связанных с функционированием ДС, и их описание приведены на стр.**25**.

Глава 3
Настройка доверенной среды

Настройка механизма ДС выполняется локально в административном режиме ДС администратором ДС.

Инструкция по входу в административный режим ДС приведена на стр.**12**.

Администратору ДС доступны следующие операции:

- выбор режима работы ДС (см. стр.**15**);
- настройка контроля целостности (см. стр.**17**);
- работа с журналом событий (см. стр.**21**);
- смена пароля администратора ДС (см. стр.**14**);
- снятие блокировки компьютера (см. стр.**20**).

Перед настройкой механизма ДС ознакомьтесь с описанием интерфейса ОС ДС и инструкциями по выполнению типовых действий (см. ниже).

Интерфейс ОС ДС

ОС ДС имеет текстовый интерфейс (см. Рис.2 на стр.**13**). Язык интерфейса — английский.

Управление осуществляется с помощью клавиатуры. Ниже приведен перечень типовых команд, знание которых упростит пользование данным руководством.

- Для навигации по пунктам меню используйте клавиши < ↑ > и < ↓ >.
- Для навигации по кнопкам в интерфейсе используйте клавиши <→> и <←>.
- Для выбора пункта меню, нажатия кнопки, выбора записи журнала и т. п. используйте клавишу <Enter>.
- Для установки отметки " * " в перечне вариантов (например, при выборе режима работы ДС) используйте клавишу <Пробел>.
- Для выхода или отмены используйте клавишу <Esc> или кнопки "Exit", "Cancel" в интерфейсе.

Вход в административный режим ДС

Внимание! Перед включением компьютера убедитесь, что:
- подключен загрузочный носитель ДС;
- в UEFI/BIOS первым загрузочным устройством является USB-флеш-накопитель.

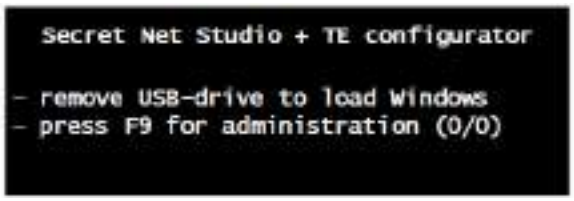
Внимание! При включении компьютера без загрузочного носителя ДС на экране блокировки ОС компьютера появится сообщение "Ошибка выполнения функционального контроля. Причины: доверенная среда не функционирует". Вход в ОС будет невозможен.

Для входа в административный режим ДС:

1. Включите компьютер.

   Начнется процесс загрузки ОС ДС с загрузочного носителя ДС.

   При успешной загрузке на экране появится меню ОС ДС:



Пояснение.
- При невыполнении системных требований могут возникнуть ошибки. В этом случае следуйте инструкциям из сообщений об ошибках.
- При возникновении системной ошибки BSOD ознакомьтесь с причиной ее возникновения по коду, отображенному на экране. Возможные коды ошибок, связанных с функционированием ДС, и их описание приведены на стр.**25**.
- При функционировании ДС в жестком режиме и возникновении событий, приводящих к остановке работы ОС (см. Табл.1 на стр.**15**), на экране появится окно с сообщением о наличии новых событий в журнале (см. Рис.5 на стр.**20**). В этом случае следуйте инструкции по снятию блокировки компьютера, приведенной на стр.**20**.

2. Нажмите клавишу <F9>.

Пояснение. Для загрузки ОС компьютера без входа в административный режим ДС извлеките загрузочный носитель ДС.

3. Введите пароль администратора ДС.

Внимание!
- При первой загрузке ОС ДС пароль администратора ДС — "12345678".
- В целях безопасности настоятельно рекомендуется сменить пароль администратора ДС после первой загрузки ОС ДС (см. стр.**14**).

На экране появится меню администратора ДС:

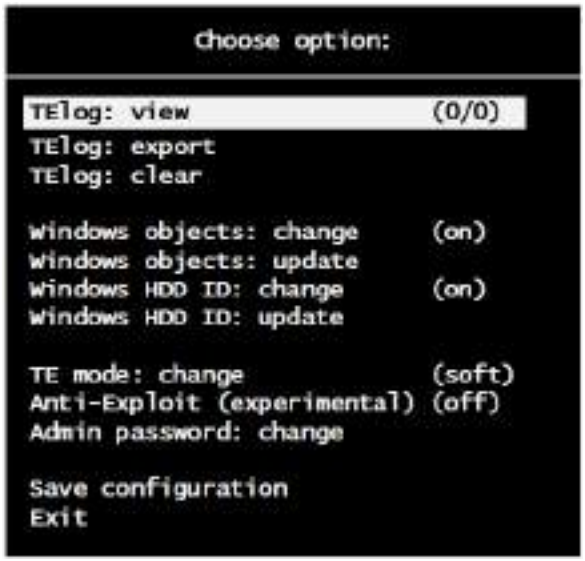


Рис.2 Меню администратора ДС

Внимание! При первом входе в административный режим ДС определяется расположение файла журнала ДС, которое необходимо сохранить. Для этого выберите в меню администратора ДС пункт "Save configuration".

4. Выберите нужный параметр для настройки:
   - TElog: view — просмотр журнала событий;
   - TElog: export — экспорт журнала событий;
   - TElog: clear — очистка журнала событий;
   - Windows objects: change — изменение перечня объектов КЦ;
   - Windows objects: update — обновление эталонных КС объектов КЦ;
   - TE mode: change — изменение режима работы ДС;
   - Admin password: change — смена пароля администратора ДС.

Пояснение. Параметры "Windows HDD ID: change" и "Windows HDD ID: update" имеются в ранних версиях Secret Net Studio с ДС. Они предназначены для оптимизации загрузки ДС при наличии нескольких разделов на жестких дисках компьютера. При установке параметра "Windows HDD ID: change" в значение "On" в конфигурации ДС сохраняется номер раздела, на котором хранится журнал ДС, и в дальнейшем загрузка выполняется сразу с нужного раздела. Параметр "Windows HDD ID: update" предназначен для обновления сведений о загрузочном разделе.
После установки пакетов обновлений указанные параметры могут отсутствовать.

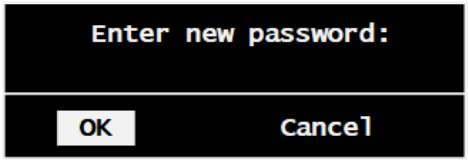
Смена пароля администратора ДС

Внимание! В целях безопасности настоятельно рекомендуется сменить пароль администратора ДС после первой загрузки ОС ДС.
Дальнейшая смена пароля администратора ДС выполняется с частотой, установленной политикой безопасности организации.

Для смены пароля администратора ДС:

1. В меню администратора ДС (см. Рис.2 на стр.**13**) выберите команду "Admin password: change".

   Появится окно для ввода нового пароля:



2. Введите новый пароль.

   Пояснение.
   - Пароль может содержать только следующие символы:
     - 1234567890 — цифры;
     - abcdefghijklmnopqrstuvwxyz — латинские буквы нижнего регистра (строчные);
     - ABCDEFGHIJKLMNOPQRSTUVWXYZ — латинские буквы верхнего регистра (заглавные);
     - _$!@#;%^:&?*)(-+=/|.,<>`~"\ — специальные символы.
   - Для установки стойкого пароля рекомендуется соблюдать следующие требования:
     - длина пароля должна быть не менее 6 символов;
     - пароль должен содержать хотя бы одну цифру;
     - пароль должен содержать хотя бы одну букву верхнего регистра (заглавная буква);
     - пароль должен содержать хотя бы одну букву нижнего регистра (строчная буква);
     - пароль должен содержать хотя бы один специальный символ;
     - пароль не должен содержать двух или более рядом стоящих одинаковых символов;
     - пароль не должен содержать двух или более рядом стоящих цифр, образующих возрастающую последовательность вида 123... или убывающую 987...;
     - при смене пароля новый пароль не должен совпадать с текущим.

3. Нажмите кнопку "OK".

   Появится окно для подтверждения пароля:

4. Повторно введите новый пароль.
5. Нажмите кнопку "OK".

   При успешном подтверждении пароля появится сообщение о смене пароля.

Пояснение. При возникновении ошибки появится сообщение "Passwords not matched". В этом случае нажмите кнопку "ОК" и повторите процедуру смены пароля.

6. Нажмите кнопку "ОК".
7. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном сохранении конфигурации.
8. Нажмите кнопку "ОК".

Выбор режима работы ДС

ДС Secret Net Studio может функционировать в мягком и жестком режимах.

В мягком режиме ДС обеспечивает обнаружение и, если это возможно, предотвращение компьютерных атак, а также регистрацию событий безопасности в журнал событий ДС.

В жестком режиме ДС дополнительно обеспечивает остановку работы ОС компьютера при невозможности предотвращения атаки.

Особенности реакции ДС на разные типы компьютерных атак в мягком и жестком режимах работы ДС представлены в таблице ниже.

Табл.1 Особенности режимов работы ДС

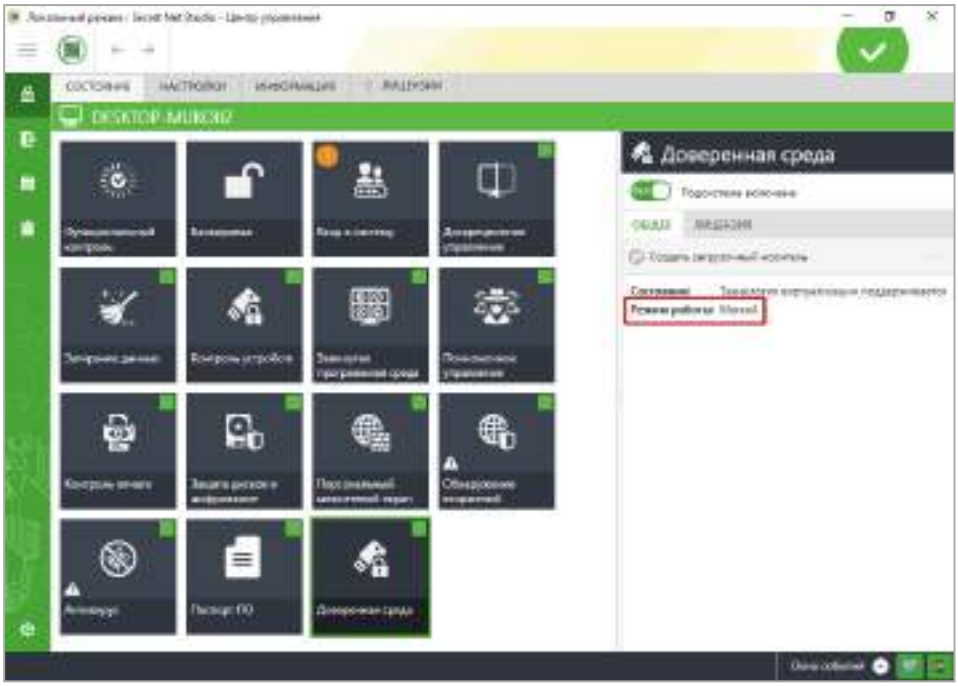
Тип атаки	Реакция ДС	
	Мягкий режим	Жесткий режим
Изменение драйверов СЗИ[1] (установка пакетов обновлений)	Обнаружение Предотвращение	Обнаружение Предотвращение
Остановка драйверов СЗИ	Обнаружение	Обнаружение Остановка ОС
Остановка процессов СЗИ[2]	Обнаружение Предотвращение	Обнаружение Предотвращение
Обнаружение вредоносного ПО[3]	Обнаружение Предотвращение	Обнаружение Предотвращение
Нарушение КС объектов КЦ	Обнаружение	Обнаружение Остановка ОС

[1] Драйвер СЗИ – драйвер Secret Net Studio, поставленный на контроль в ДС.
[2] Процесс СЗИ – процесс Secret Net Studio, который использует API ДС для защиты.
[3] Вредоносное ПО, найденное при обнаружении компьютерных атак (см. стр.**19**).

По умолчанию ДС функционирует в мягком режиме.

Текущий режим работы ДС можно посмотреть:

- в программе управления Secret Net Studio в локальном и централизованном режимах — сведения о механизме "Доверенная среда", параметр "Режим работы" (пример из программы управления в локальном режиме приведен на рисунке ниже);



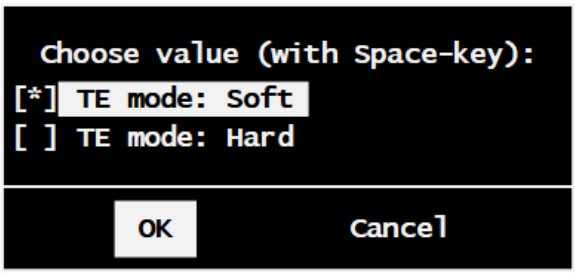
- в меню администратора ДС (см. Рис.2 на стр.**13**) — пункт "TE mode: change" (см. рисунок ниже).

Внимание! Операции обновления, исправления, удаления компонентов Secret Net Studio (в том числе пакетов обновлений) возможны только в мягком режиме работы ДС или при выключенной ДС. При попытке выполнения указанных действий в жестком режиме работы ДС появится сообщение "Для изменения или удаления программы, ее компонентов или пакетов исправлений необходимо переключить доверенную среду в мягкий режим работы".

Для смены режима работы ДС:

1. В меню администратора ДС (см. Рис.2 на стр.**13**) выберите команду "TE mode: change".

   Появится окно выбора режима работы ДС:



2. Выберите нужный режим работы, установив отметку клавишей <Пробел>:
   - TE mode: Soft — для установки мягкого режима работы ДС;
   - TE mode: Hard — для установки жесткого режима работы ДС.
3. Нажмите кнопку "OK".

   Пояснение. Для отмены нажмите кнопку "Cancel".
4. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном сохранении изменений.
5. Нажмите кнопку "OK".

Настройка контроля целостности в ДС

Функция контроля целостности в ДС обеспечивает:

- блокировку модификации кода драйверов Secret Net Studio в памяти (в том числе с возможностью блокировки модификации кода сторонних драйверов);
- защиту от несанкционированной остановки драйверов Secret Net Studio;
- защиту от несанкционированного терминирования ключевых процессов Secret Net Studio.

При создании загрузочного носителя ДС на контроль по умолчанию ставятся критические службы и драйверы Secret Net Studio и рассчитываются их эталонные контрольные суммы (КС). Список объектов КЦ ДС по умолчанию приведен на стр.**26**.

При эксплуатации ДС можно ставить на контроль другие драйверы и файлы.

Процедуры КЦ разных объектов различаются:

- Целостность драйвера контролируется посредством проверки запуска драйвера на этапе загрузки ОС, проверки КС драйвера в памяти до исполнения его кода, блокировки памяти драйвера от записи;
- Целостность файла контролируется посредством проверки КС файла до загрузки ОС.

При нарушении целостности объектов КЦ в жестком режиме работы ДС обеспечивается остановка работы ОС компьютера. Появляется окно системной ошибки BSOD с кодом "0x5ECCODE0" (см. стр. **25**). Информация о нарушении фиксируется в журнале событий ДС.

Список объектов КЦ, созданный по умолчанию, можно редактировать:

- изменять путь к объекту КЦ (см. ниже);
- ставить на контроль/снимать с контроля выбранный объект КЦ (см. стр.**18**);
- добавлять объекты в список (см. стр.**19**);
- исключать объекты из списка (см. стр.**19**).

Внимание! После изменения списка необходимо выполнить перерасчет эталонных КС объектов КЦ (см. стр.**19**).

Для изменения пути к объекту КЦ:

1. В меню администратора ДС (см. Рис.2 на стр.**13**) выберите команду "Windows objects: change".

   Появится окно с таблицей объектов КЦ, подобное представленному на рисунке ниже.

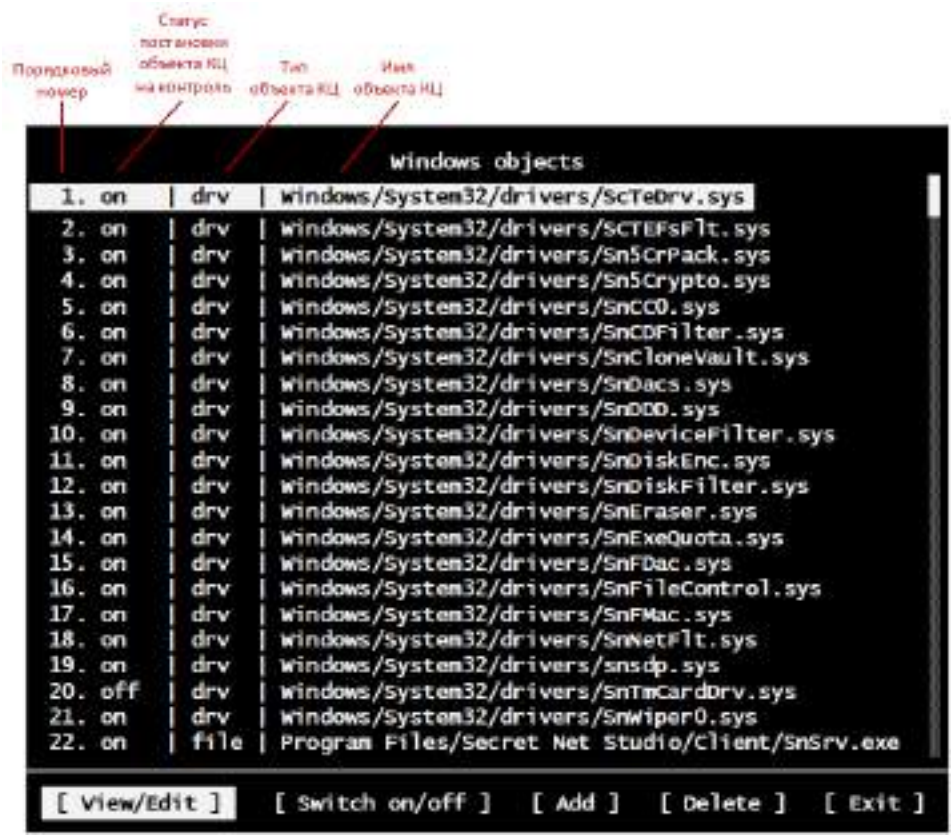


Рис.3 Окно с таблицей объектов КЦ

2. Выберите нужный объект в таблице и нажмите кнопку "[View/Edit]".

   Появится окно для изменения пути к файлу и пути к драйверу:

Рис.4 Окно изменения путей к файлу и драйверу

3. Выберите дальнейшее действие:
   - для изменения пути к файлу нажмите кнопку "[Set file path]" и внесите необходимые правки;
   - для изменения пути к драйверу нажмите кнопку "[Set driver path]" и внесите необходимые правки;
   - для возврата к таблице объектов КЦ нажмите кнопку "[OK]".
4. Нажмите кнопку "[Exit]" или клавишу <Esc>.
5. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном сохранении конфигурации.
6. Нажмите кнопку "OK".

Для постановки на контроль/снятия с контроля объекта КЦ:

1. В меню администратора ДС (см. Рис.2 на стр.**13**) выберите команду "Windows objects: change".

   Появится окно с таблицей объектов КЦ (см. Рис.3 на стр.**18**).
2. Выберите нужный объект в таблице и нажмите кнопку "[Switch on/off]".

   Выбранный объект КЦ будет поставлен на контроль/снят с контроля (изменится статус "on/off" во второй колонке таблицы объектов КЦ).
3. Нажмите кнопку "[Exit]" или клавишу <Esc>.

4. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном сохранении конфигурации.

5. Нажмите кнопку "OK".

Для добавления объекта в список объектов КЦ:

1. В меню администратора ДС (см. Рис.2 на стр.**13**) выберите команду "Windows objects: change".

   Появится окно с таблицей объектов КЦ (см. Рис.3 на стр.**18**).

2. Нажмите кнопку "[Add]".

   На экране появится окно выбора объектов.

3. Выберите объект, который хотите добавить в список контролируемых.

   Пояснение. Для корректного добавления драйвера необходимо знать его внутреннее имя. Например, у драйвера SnDacs.sys внутреннее имя \Driver\SnDacs, у драйвера SnWiper0.sys – \Driver\SnWiper.

4. Нажмите клавишу <Enter>.

   Появится окно для изменения пути к файлу и пути к драйверу (см. Рис.4 на стр.**18**).

5. При необходимости измените путь к файлу/драйверу и нажмите кнопку "[OK]".

   Объект будет добавлен в список объектов КЦ ДС.

6. Нажмите кнопку "[Exit]" или клавишу <Esc>.
7. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном сохранении конфигурации.

8. Нажмите кнопку "OK".

Для удаления объекта из списка объектов КЦ:

1. В меню администратора ДС (см. Рис.2 на стр.**13**) выберите команду "Windows objects: change".

   Появится окно с таблицей объектов КЦ (см. Рис.3 на стр.**18**).

2. Выберите нужный объект в таблице и нажмите кнопку "[Delete]".

   Объект будет удален из списка.

3. Нажмите кнопку "[Exit]" или клавишу <Esc>.
4. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном сохранении конфигурации.

5. Нажмите кнопку "OK".

Для перерасчета эталонных КС объектов КЦ:

1. В меню администратора ДС (см. Рис.2 на стр.**13**) выберите команду "Windows objects: update".

   Появится сообщение об успешном выполнении операции.

2. Нажмите кнопку "OK".
3. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном сохранении конфигурации.

4. Нажмите кнопку "OK".

Настройка обнаружения компьютерных атак

Примечание. Функция обнаружения компьютерных атак в ДС Secret Net Studio (Anti-Exploit) на данном этапе является экспериментальной. По умолчанию данная функция отключена.

ДС Secret Net Studio обеспечивает обнаружение следующих видов компьютерных атак:

- сброс SMEP;

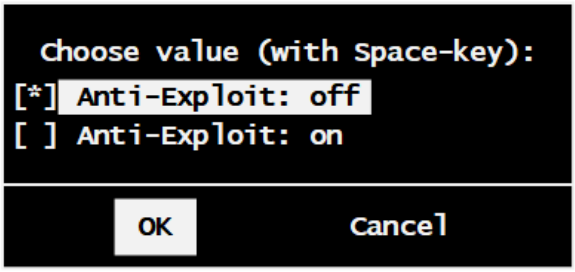
- выполнение команд в стеке;
- эксплуатация уязвимости EternalBlue;
- запись данных в защищаемую область памяти.

При обнаружении атаки ДС обеспечивает их предотвращение или остановку работы ОС компьютера в зависимости от типа атаки (см. Табл.1 на стр.**15**). Информация об атаке фиксируется в журнале событий ДС.

Для включения/выключения функции обнаружения атак:

1. В меню администратора ДС (см. Рис.2 на стр.**13**) выберите команду "Anti-Exploit (experimental)".

   Появится окно настройки функции обнаружения атак:



2. Выберите нужный вариант, установив отметку клавишей <Пробел>:
   - Anti-Exploit: off — для выключения функции обнаружения атак;
   - Anti-Exploit: on — для включения функции обнаружения атак.
3. Нажмите кнопку "OK".

   Пояснение. Для отмены нажмите кнопку "Cancel".
4. В меню администратора ДС выберите пункт "Save configuration".

   Появится сообщение об успешном выполнении операции.
5. Нажмите кнопку "OK".

Снятие блокировки компьютера

В жестком режиме работы ДС при возникновении определенных событий (см. Табл.1 на стр.**15**) останавливается работа ОС и компьютер блокируется. В этом случае при включении компьютера появляется сообщение о наличии в журнале новых событий, подобное представленному на рисунке ниже.

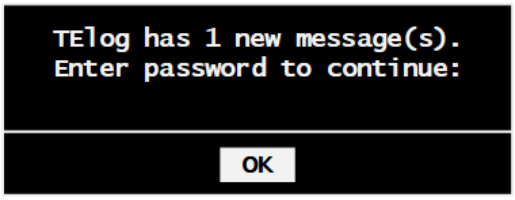


Рис.5 Сообщение о наличии новых событий (жесткий режим работы ДС)

Без просмотра администратором ДС журнала событий невозможно загрузить ОС компьютера.

Для снятия блокировки компьютера:

1. В окне с сообщением о наличии новых событий введите пароль администратора ДС и нажмите кнопку "OK".

   На экране появится окно журнала событий ДС (см. Рис.6 на стр.**22**).
2. Просмотрите подробную информацию о событии, которое привело к блокировке компьютера. Данное событие имеет статус "New".

Пояснение. Может быть несколько событий, которые привели к блокировке компьютера. Для снятия блокировки просмотрите информацию обо всех новых событиях.

Внимание! По факту произошедшего события произведите административные действия, установленные политикой безопасности организации для событий такого типа.

3. Закройте журнал событий, нажав кнопку "[Exit]" или клавишу <Esc>.

   На экране появится меню администратора ДС (см. Рис.2 на стр.**13**).

4. Выберите пункт "Exit".

   Компьютер разблокирован и готов к загрузке штатной ОС.

Работа с журналом событий

В ДС регистрируются следующие типы событий:

- попытка несанкционированной остановки служб Secret Net Studio;
- попытка выгрузки драйверов Secret Net Studio;
- нарушение целостности объектов КЦ;
- попытка модификации кода драйверов Secret Net Studio;
- ошибка при входе в административный режим ДС.

Журнал событий ДС хранится на системном диске.

Журнал событий ДС позволяет хранить не более 4096 записей. Журнал имеет свойство перезаписи — при максимальном заполнении журнала на место устаревших событий записываются новые.

При работе с журналом администратору ДС доступны следующие операции:

- просмотр журнала, в том числе просмотр подробной информации о каждом событии;
- очистка журнала;
- экспорт журнала в файл на загрузочный носитель ДС.

Просмотр

Журнал событий ДС можно просмотреть в ОС ДС (см. инструкцию ниже) и в программе управления Secret Net Studio.

Для просмотра журнала в программе управления необходимо предварительно экспортировать журнал в файл на загрузочный носитель ДС средствами ДС (см. стр.**23**). Инструкция по загрузке экспортированного журнала в программу управления приведена в документе [**4**] (глава "Работа с централизованными журналами", раздел "Загрузка записей журналов").

Для просмотра журнала событий в ОС ДС:

1. В меню администратора ДС (см. Рис.2 на стр.**13**) выберите команду "TElog: view".

   Появится окно журнала событий, подобное представленному на рисунке.

Рис.6 Журнал событий ДС

Пояснение. Если журнал событий пуст, на экране появится сообщение "TElog is empty".

2. Выполните нужное действие:

- Для навигации по событиям используйте клавиши < ↑ > и < ↓ >.
- Для просмотра подробной информации о выбранном событии нажмите кнопку "[Select]". Появится окно, подобное представленному на рисунке ниже.

Для возврата к окну журнала событий нажмите кнопку "[OK]".

Примечание. Событие перестает быть новым (теряет статус "New") после просмотра подробной информации о нем. Это необходимо для разблокировки компьютера в жестком режиме работы ДС (см. стр.20).

- Для удаления выбранного события нажмите кнопку "[Delete]" в окне журнала событий или в окне с подробной информацией о событии.
- Для возврата в меню администратора ДС нажмите кнопку "[Exit]".

Очистка

Внимание! Прежде чем выполнить очистку журнала, ознакомьтесь с его содержимым. Имеется возможность сохранить журнал в файл (см. ниже).

Для очистки журнала событий:

1. В меню администратора ДС (см. Рис.2 на стр.**13**) выберите пункт "TElog: clear" или в окне просмотра журнала событий (см. Рис.6 на стр.**22**) нажмите кнопку "[Clear TElog]".

   Журнал будет очищен. На экране появится сообщение об успешном выполнении операции.
2. Нажмите кнопку "ОК".

Экспорт

Для экспорта журнала событий:

1. В меню администратора ДС (см. Рис.2 на стр.**13**) выберите пункт "TElog: export".

   Журнал будет сохранен в файл "te.snlog" на загрузочный носитель ДС.

   На экране появится сообщение об успешном экспорте журнала в файл.
2. Нажмите кнопку "ОК".

Глава 4
Выключение доверенной среды

Выключение ДС выполняется локально на компьютере, на котором она функционирует.

Внимание! Выключение ДС возможно только при ее функционировании в мягком режиме (см. стр.15).

Для выключения ДС:

1. В меню "Пуск" ОС Windows в группе "Код Безопасности" выберите элемент "Локальный центр управления".

   Запустится программа управления Secret Net Studio в локальном режиме.
2. В панели "Компьютер" на вкладке "Состояние" выберите элемент "Доверенная среда".

   В правой части окна отобразятся сведения о подсистеме "Доверенная среда".
3. Переключите тумблер "Подсистема включена" в положение "Выкл".

   В программе управления появится предупреждение о необходимости перезагрузки компьютера.
4. Извлеките загрузочный носитель ДС.
5. Перезагрузите компьютер.

   Доверенная среда будет выключена. Загрузка ОС выполнится в стандартном режиме.

Приложение

Ошибки и предупреждения при работе с ДС

Предупреждения в программе управления

Параметр "Состояние" в окне со сведениями о подсистеме "Доверенная среда" (см. Рис.1 на стр. **9**) отражает информацию о соответствии / несоответствии компьютера системным требованиям для установки ДС. Данную информацию можно просмотреть в локальном и централизованном режимах.

При несоответствии компьютера системным требованиям параметр может принимать значения из таблицы ниже.

Текст ошибки
Версия операционной системы ниже, чем требуется
Число процессоров ниже, чем требуется
Поддержка виртуализации отключена
Second Level Address Translation не поддерживается аппаратным обеспечением
Используемый тип диска (NVMe, VHD и т.п.) не поддерживается
Работа в виртуальном окружении не поддерживается
Обнаружено несовместимое оборудование

Ошибки при включении компьютера

При включении компьютера с ДС, функционирующей в жестком режиме, может возникнуть системная ошибка BSOD. Причиной такой ошибки может являться компьютерная атака и другие нарушения безопасности информации. При невозможности самостоятельно справиться с проблемой обратитесь в департамент сервиса компании "Код Безопасности".

Коды системных ошибок BSOD, связанных с ДС, и их краткое описание приведены в таблице ниже.

Код ошибки	Пояснение
0x5ECC0DE0	Нарушение целостности процессов Secret Net Studio
0x5ECC0DE1	Ошибка инициализации драйвера ДС
0x5ECC0DE2	Сброс регистра SMEP
0x5ECC0DE3	Ошибка КС драйвера
0x5ECC0DE4	Попытка модификации драйвера
0x5ECC0DE5	Выгрузка драйвера
0x5ECC0DE6	Несанкционированное завершение процесса
0x5ECC0DE7	Срабатывание сторожевого таймера для процесса
0x5ECC0DE8	Ошибка КС процесса
0x5ECC0DE9	Атака 0-го кольца
0x5ECC0DEA	Внутренняя ошибка драйвера ДС

Объекты КЦ ДС по умолчанию

При включении ДС автоматически ставятся на контроль драйверы, службы и приложения Secret Net Studio. Перечень этих файлов приведен в таблице ниже.

Полное имя файла	Тип файла
SystemRoot\System32\Drivers\Sn5CrPack.sys	Драйвер
SystemRoot\System32\Drivers\Sn5Crypto.sys	Драйвер
SystemRoot\System32\Drivers\SnCC0.sys	Драйвер
SystemRoot\System32\Drivers\SnCDFilter.sys	Драйвер
SystemRoot\System32\Drivers\SnCloneVault.sys	Драйвер
SystemRoot\System32\Drivers\SnDacs.sys	Драйвер
SystemRoot\System32\Drivers\SnDDD.sys	Драйвер
SystemRoot\System32\Drivers\SnDeviceFilter.sys	Драйвер
SystemRoot\System32\Drivers\SnDiskEnc.sys	Драйвер
SystemRoot\System32\Drivers\SnDiskFilter.sys	Драйвер
SystemRoot\System32\Drivers\SnEraser.sys	Драйвер
SystemRoot\System32\Drivers\SnExeQuota.sys	Драйвер
SystemRoot\System32\Drivers\SnFDac.sys	Драйвер
SystemRoot\System32\Drivers\SnFileControl.sys	Драйвер
SystemRoot\System32\Drivers\SnFMac.sys	Драйвер
SystemRoot\System32\Drivers\SnNetFlt.sys	Драйвер
SystemRoot\System32\Drivers\snsdp.sys	Драйвер
SystemRoot\System32\Drivers\SnTmCardDrv.sys	Драйвер
SystemRoot\System32\Drivers\SnWiper0.sys	Драйвер
SystemRoot\System32\Drivers\ScTeDrv.sys	Драйвер
SystemRoot\System32\Drivers\SCTEFsFlt.sys	Драйвер
%ClientInstallDir%\SnSrv.exe	Служба
%ClientInstallDir%\SnicheckSrv.exe	Служба
%ClientInstallDir%\SnIcon.exe	Приложение

Ограничения и рекомендации

ДС является новым защитным механизмом Secret Net Studio, который находится в стадии активной разработки. В данном разделе приведены ограничения и рекомендации по использованию ДС в текущей реализации (Secret Net Studio версии 8.5).

Несовместимое оборудование и конфигурации

Ниже перечислены особенности функционирования ДС с различным оборудованием, которые актуальны даже при соответствии компьютера минимальным системным требованиям, приведенным на стр.**7**.

1. Виртуальная среда.

   ДС функционирует только при одном работающем гипервизоре, виртуальное окружение не поддерживается. Для использования ДС необходим физический компьютер.

   Примечание. Данное ограничение проверяется системой Secret Net Studio. При несоответствии конфигурации предъявляемым требованиям включение ДС будет невозможно.

2. Жесткие диски.
   - В текущей реализации ДС функционирует только с жесткими дисками SATA/AHCI.

     Работа с дисками SCSI, NVMe, а также с образами дисков VHD1 (и другими разновидностями) не поддерживается.

     Примечание. Данное ограничение проверяется системой Secret Net Studio. При несоответствии конфигурации предъявляемым требованиям включение ДС будет невозможно.
   - Рекомендуется использовать жесткий диск в режиме AHCI. Работа с жестким диском в режиме IDE нестабильна.
   - В текущей реализации не поддерживаются RAID-конфигурации и полнодисковое шифрование.
   - Не рекомендуется использовать ДС на конфигурации с несколькими ОС, так как в текущей реализации не обеспечивается запуск той ОС, в которой настроена ДС.
3. Системные платы.

   Системная плата Gigabyte H67A-UD3H-B3 с версией UEFI/BIOS F81 не поддерживается из-за некорректной работы с контроллером диска.

   Примечание. Данное ограничение проверяется системой Secret Net Studio. При несоответствии конфигурации предъявляемым требованиям включение ДС будет невозможно.
4. USB-контроллеры.
   - Наблюдается нестабильная работа с контроллером USB 3.1. Используйте контроллеры USB 3.0/2.0 при подключении загрузочного носителя ДС.
   - Подключение нескольких загрузочных USB-флеш-накопителей не поддерживается. Подключайте только загрузочный носитель ДС до включения компьютера.
5. Процессоры.

   На платформе AMD было проведено ограниченное тестирование ДС. Полное функционирование механизма не гарантируется.

Рекомендации по настройке компьютера

Ниже приведены рекомендации по настройке компьютера для обеспечения корректного функционирования ДС.

1. UEFI/BIOS.
   - Рекомендуется обновить UEFI/BIOS до последней версии.
   - В UEFI/BIOS Setup необходимо разрешить использование всех функций виртуализации. Как правило, параметры виртуализации находятся в разделе "CPU configuration".
   - В UEFI/BIOS Setup необходимо разрешить использование CSM (Compatibility Support Module). В настройках CSM рекомендуется выбрать режим "UEFI and Legacy".

     Примечание. При отсутствии в настройках CSM режима "UEFI and Legacy" необходимо выбрать режим "Legacy".
   - В UEFI/BIOS Setup в настройках USB рекомендуется активировать параметры "Full Initialization" и "USB boot first" (при наличии таких параметров).
2. Жесткий диск.
   - Не рекомендуется использовать жесткий диск с ошибками S.M.A.R.T., так как работа с таким диском нестабильна.
   - Не поддерживается работа с жестким диском с включенным аппаратным шифрованием.

Примечание. Если жесткий диск поддерживает функцию аппаратного шифрования, отключите данную функцию. Работа с диском будет осуществляться так же, как с диском без функции аппаратного шифрования.

3. ОС семейства Windows.

   Спящий режим в ОС семейства Windows приводит к нестабильной работе. Рекомендуется настроить следующие параметры с помощью powercfg.cpl:

   - отключить спящий режим;
   - для процессора установить все режимы 100%;
   - запретить отключение системного жесткого диска.

Очистка загрузочного носителя ДС

Для использования всего объема памяти USB-флеш-накопителя, применяемого ранее в качестве загрузочного носителя ДС, необходимо выполнить полную очистку USB-флеш-накопителя с помощью стандартной утилиты управления дисками ОС Windows *diskpart.exe*.

Внимание! При полной очистке все данные на USB-флеш-накопителе будут уничтожены. Чтобы снова использовать USB-флеш-накопитель для работы с ДС, выполните процедуру создания загрузочного носителя со стр.8.

Для очистки загрузочного носителя ДС:

1. Подключите загрузочный носитель ДС к компьютеру.
2. Запустите утилиту командной строки ОС Windows от имени администратора.
3. Выполните следующую команду:

   ```
   diskpart
   ```

   Запустится утилита *diskpart.exe*.
4. Выполните следующую команду:

   ```
   list disk
   ```

   Отобразится список дисков, подключенных к компьютеру.
5. Найдите в списке нужный USB-флеш-накопитель и запомните его номер.
6. Выполните следующие команды:

   ```
   select disk <номер диска>
   clean
   create partition primary
   ```

   USB-флеш-накопитель будет очищен. На носителе будет создан первичный раздел.
7. Выполните форматирование USB-флеш-накопителя в нужную файловую систему любым удобным способом.

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. Основы и базовая защита	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. Доверенная среда	RU.88338853.501400.001 91 8
9. Средство защиты информации Secret Net Studio. Руководство администратора. Сервер обновлений. Установка и настройка	
10. Средство защиты информации Secret Net Studio. Руководство пользователя	RU.88338853.501400.001 92