КОД БЕЗОПАСНОСТИ

Средство защиты информации

Secret Net Studio

Руководство администратора

Настройка и эксплуатация. Антивирус и средство обнаружения вторжений

RU.88338853.501400.001 91 7

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

БД	База данных
БРП	База решающих правил
ПО	Программное обеспечение

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio" RU.88338853.501400.001 (далее — Secret Net Studio, система защиты, изделие). В нем содержатся сведения, необходимые администраторам для настройки и управления антивирусом и механизмом обнаружения вторжений. Перед изучением данного руководства необходимо ознакомиться с документами [**1**], [**3**].

Условные обозначения

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

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

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

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

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

- Эта пиктограмма сопровождает информацию предостерегающего характера.

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

Другие источники информации

Сайт в интернете. Вы можете посетить сайт компании "Код Безопасности" (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

Secret Net Studio содержит следующие механизмы защиты от вредоносных программ:

- антивирус;
- обнаружение и предотвращение вторжений.

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
Быстрое/полное сканирование	Проверки, запускаемые администратором из программы управления
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. Если пропущено несколько одинаковых задач, будет запущена только одна из них
Автоматическая проверка съемных носителей	В Secret Net Studio реализована возможность автоматической проверки съемных носителей при их подключении к компьютеру
Уровень антивирусной защиты	В Secret Net Studio возможен выбор уровня антивирусной защиты при сканировании в реальном времени
Проверяемые объекты	Возможен выбор проверяемых объектов (память, загрузочные секторы, диски, каталоги, файлы и ссылки на файлы)
Список исключений	Создание списка объектов (файлов, каталогов и дисков), которые не проверяются при сканировании объектов в режиме реального времени и при сканировании по расписанию. Список исключений действует глобально для всех видов сканирования и не настраивается отдельно для разных режимов (кроме сканирования по команде "Проверить на вирусы (игнорировать белый список)"

Функция	Описание
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
Управление карантином	Просмотр помещенных в карантин файлов, восстановление и удаление файлов из карантина
Отключение антивируса	В Secret Net Studio реализована возможность отключения антивируса в программе управления

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

Глава 2
Антивирус

Настройка работы антивируса осуществляется централизованно в программе управления и может выполняться на разных уровнях структуры объектов управления:

- на уровне объектов "Домен", "Сервер безопасности" и "Организационная единица" можно выполнить настройку параметров работы антивируса с помощью групповых политик. Значения параметров на уровне "Сервер безопасности" имеют приоритет перед аналогичными значениями, заданными на уровне объектов "Компьютер";
- на уровне объектов "Компьютер" можно выполнить настройку параметров работы антивируса для отдельного компьютера, а также осуществлять управление работой антивируса (запуск сканирования, работа с объектами в карантине и т.п.) на данном компьютере.

Примечание. В состав Secret Net Studio также входит компонент "Локальный центр управления". Он позволяет управлять антивирусом непосредственно на защищаемом компьютере.

Настройка групповых политик

Параметры работы антивируса разделены на следующие группы:

- профили режимов сканирования. Профиль сканирования — это набор заранее заданных параметров сканирования, которые будут применены при проверке системы в соответствующем режиме;
- расписание сканирования — определяет время и периодичность проведения проверок в соответствии с заданным профилем сканирования;
- исключения — определяют перечень файлов и каталогов, которые нужно исключить из проверки.

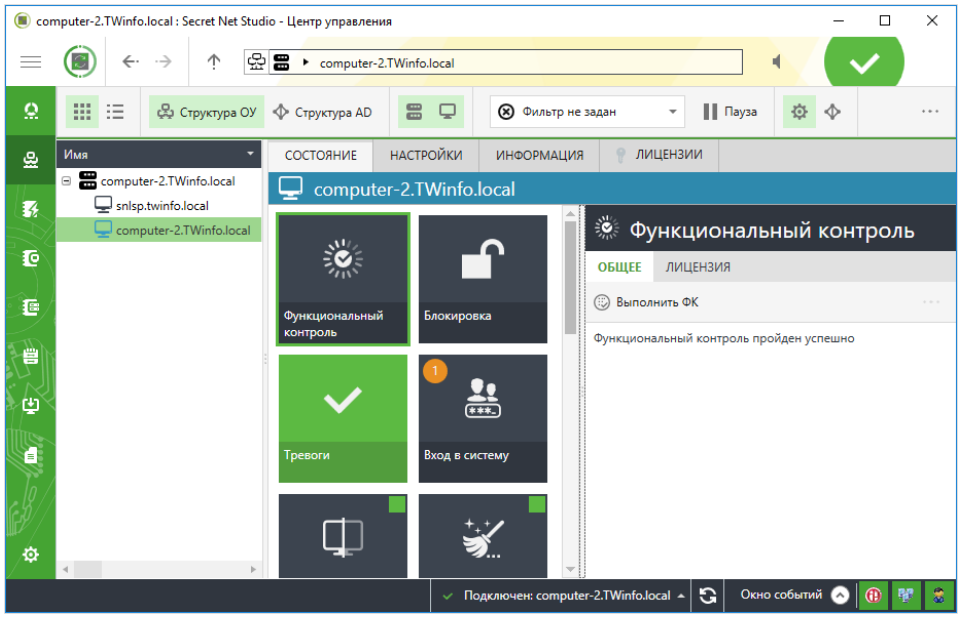
Для настройки параметров:

1. Вызовите программу управления Secret Net Studio.

   Совет. Для настройки параметров антивируса непосредственно на защищаемом компьютере вызовите программу "Локальный центр управления", в представлении "Компьютер" перейдите на вкладку "Настройки" и в разделе "Политики" выберите элемент "Антивирус". Далее настройка этого механизма выполняется так же, как и в случае централизованного управления.

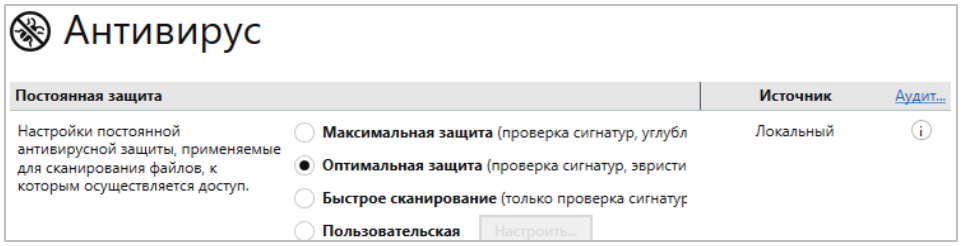
   На экране появится основное окно программы.
2. Откройте представление "Компьютеры", в левой части экрана в списке объектов управления найдите нужный компьютер (домен, сервер безопасности), вызовите для него контекстное меню и выберите в нем команду "Свойства".

   В правой части экрана появится информация о состоянии данного объекта.



3. Перейдите на вкладку "Настройки" и нажмите при необходимости кнопку "Загрузить настройки", затем в разделе "Политики" выберите элемент "Антивирус".

   В правой части экрана появится область настройки выбранных параметров.



Совет. Если выполняется настройка групповой политики, переведите выключатель в верхнем левом углу нужного раздела параметров в положение "Вкл".

4. Настройте нужные параметры и для сохранения новых значений нажмите кнопку "Применить" внизу вкладки "Настройки".

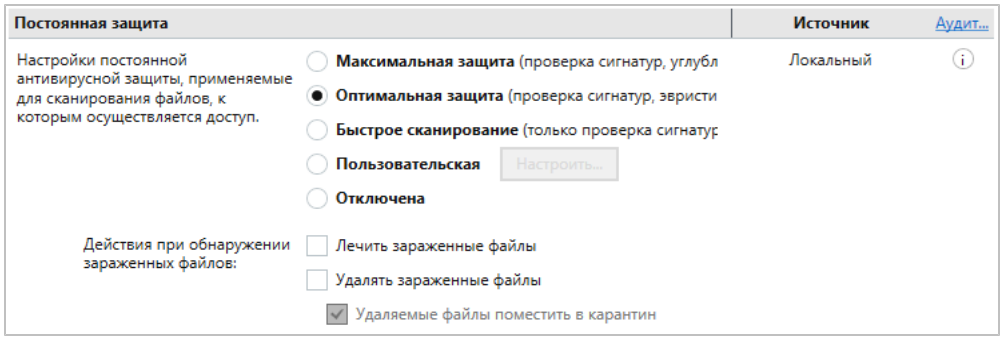
Настройка профилей сканирования

В системе имеются следующие профили режимов сканирования.

Название	Назначение
Постоянная защита	Этот профиль определяет параметры сканирования объектов системы в режиме реального времени
Сканирование подключаемых носителей	Этот профиль определяет параметры автоматической проверки всех подключаемых к компьютеру съемных носителей. Работает только совместно с профилем "Постоянная защита"
Контекстное сканирование	Этот профиль определяет параметры проверки, запускаемой пользователем из контекстного меню проводника Windows
Полное сканирование	Профиль определяет параметры проверки, запускаемой администратором из программы управления или по расписанию. В этом режиме выполняется проверка запущенных процессов, параметров автозапуска и загрузочных секторов
Быстрое сканирование	Профиль определяет параметры быстрой проверки, запускаемой администратором из программы управления или по расписанию. В этом режиме выполняется быстрое сканирование системы для проверки ее уязвимых мест. К ним относятся запущенные в памяти процессы, уязвимые файлы и папки, съемные носители

В области настройки параметров антивируса перейдите к разделу, параметры которого нужно настроить.

Постоянная защита



Для настройки параметров постоянной защиты:

1. Установите уровень антивирусной защиты при сканировании в реальном времени.

Параметр	Описание
Максимальная защита	Сканирование выполняется при любой попытке доступа к файлам. Проверяются все без исключения файлы любого размера, находящиеся на всех постоянных и съемных дисках. При сканировании используется глубокий уровень эвристического анализа новых угроз (см. стр.**12**)
Оптимальная защита	Сканирование выполняется при любой попытке доступа к файлам. Проверяются только файлы с расширениями zip, xl*, ws*, vxe, vxd, vb*, tsp, tmp, th*, ta*, sys, swf, sl*, sh*, scr, sc*, rtf, reg, ra*, prg, prf, pp*, png, pif, ph*, pdf, otm, osx, om, ms*, md*, lnk, js*, jp*, isp, ins, inf, ico, ht*, hlp, gif, exe, drv, do*, dll, crt, cpl, com, cmd, cla, chm, cab, bin, bdx, bat, asx, asp*, ar*, ad*, находящиеся на всех постоянных и съемных дисках. Файлы (включая архивы) размером более 100 Мб пропускаются. При сканировании используется эвристический анализ в обычном режиме (см. стр.**12**)
Быстрое сканирование	Сканирование выполняется при любой попытке доступа к файлам. Проверяются только файлы с расширениями zip, xl*, ws*, vxe, vxd, vb*, tsp, tmp, th*, ta*, sys, swf, sl*, sh*, scr, sc*, rtf, reg, ra*, prg, prf, pp*, png, pif, ph*, pdf, otm, osx, om, ms*, md*, lnk, js*, jp*, isp, ins, inf, ico, ht*, hlp, gif, exe, drv, do*, dll, crt, cpl, com, cmd, cla, chm, cab, bin, bdx, bat, asx, asp*, ar*, ad*, находящиеся на всех постоянных и съемных дисках. Файлы (включая архивы) размером более 50 Мб пропускаются. Эвристический анализ не используется, проверяются только сигнатуры
Пользовательская	Проверка, выполняемая в соответствии с индивидуальными параметрами уровня постоянной защиты
Отключена	Сканирование объектов в реальном времени не выполняется

2. Для настройки пользовательского профиля сканирования нажмите кнопку "Настроить" (см. стр.**12**).
3. Выберите действия, которые необходимо выполнять при обнаружении зараженных файлов.

Параметр	Описание
Лечить зараженные файлы	Если отмечен данный пункт, будет произведена попытка лечения зараженных файлов

Параметр	Описание
Удалять зараженные файлы	Зараженные файлы будут удалены
Удаляемые файлы поместить в карантин	Удаляемые файлы будут перемещены в карантин. Файлы остаются на прежнем месте, но их атрибут меняется на "Скрытый", а к имени файла добавляется ".quarantine". Перемещенные в карантин файлы в дальнейшем можно восстановить в случае необходимости (см. стр.**15**)

Примечание. Если одновременно отмечены пункты "Лечить зараженные файлы" и "Удалять зараженные файлы", то при обнаружении зараженных объектов будет выполнена попытка их лечения, а при неудаче файлы будут удалены.

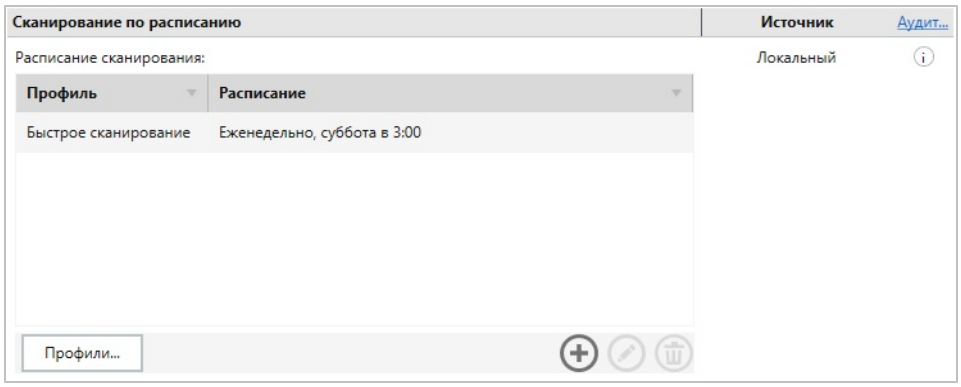
4. Нажмите кнопку-ссылку "Аудит" и настройте параметры регистрации событий антивируса.
5. Нажмите кнопку "Применить" внизу вкладки "Настройки".

Настройка остальных профилей сканирования выполняется аналогично настройке профиля "Постоянная защита".

Сканирование по расписанию

Для настройки сканирования по расписанию:

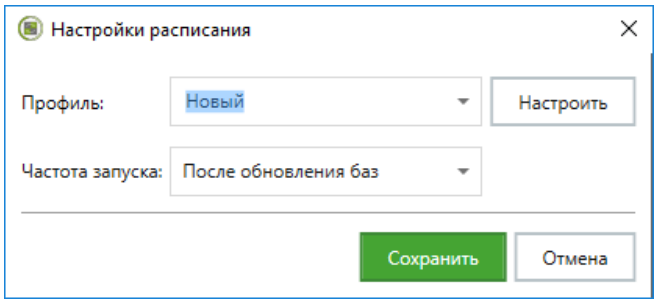
1. В области настройки параметров антивируса перейдите к разделу "Сканирование по расписанию".



Совет. Для изменения расписания используйте кнопки, расположенные внизу списка.

2. Для добавления в расписание новой проверки нажмите кнопку "Добавить".

Появится следующий диалог.



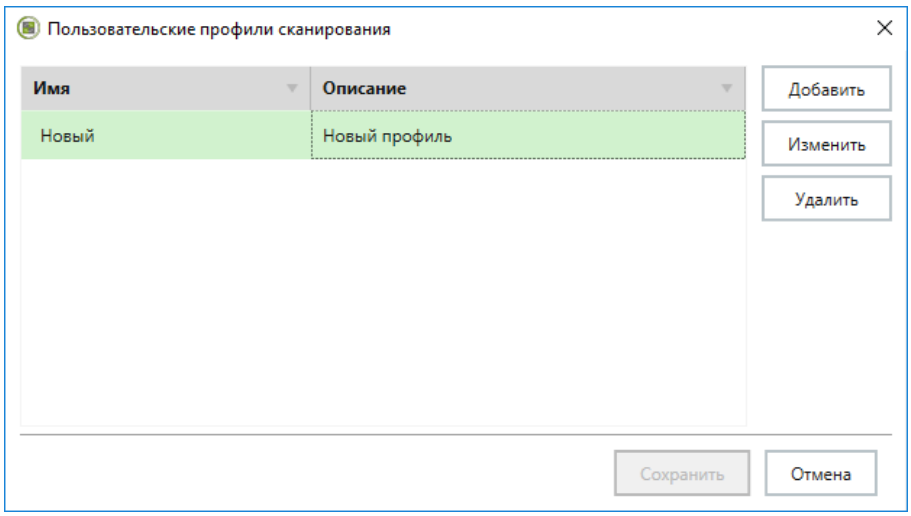
3. Выберите профиль сканирования, частоту запуска проверки и нажмите кнопку "Сохранить".

Совет. Если выбран пользовательский профиль сканирования, нажмите кнопку "Настроить" для изменения его параметров.

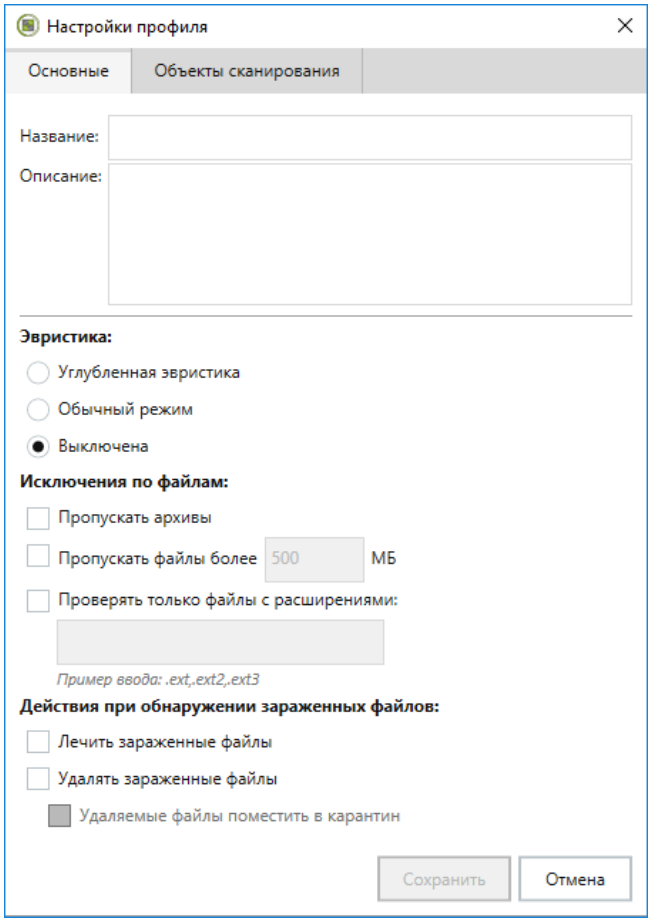
4. Нажмите кнопку "Применить" внизу вкладки "Настройки".

Для создания и настройки пользовательского профиля сканирования:

1. Нажмите кнопку "Профили...".
   Появится следующий диалог.



2. В правой части диалога нажмите кнопку "Добавить".
   Появится следующий диалог.

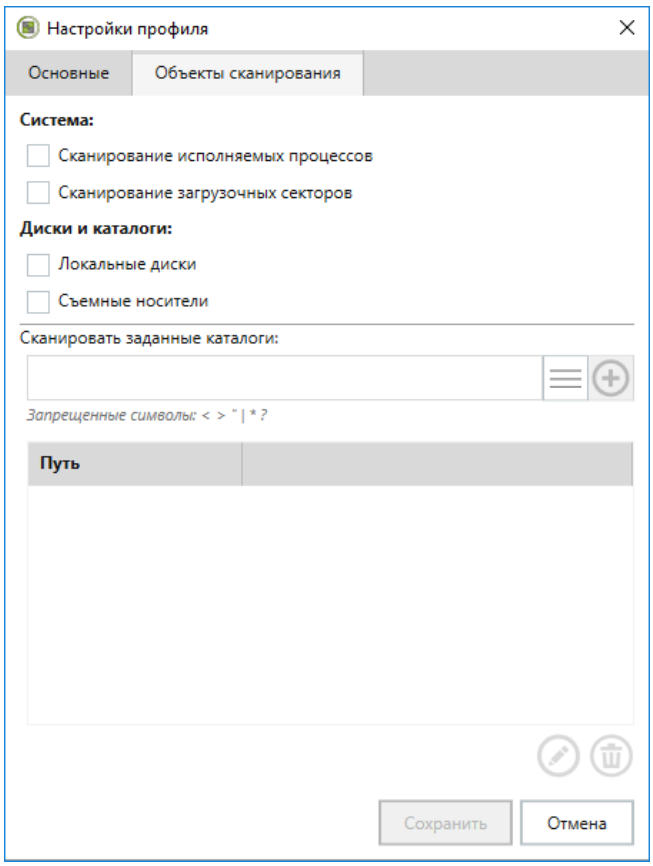


3. На вкладке "Основные" укажите следующие параметры.

Параметр	Описание
Название	Название профиля сканирования
Описание	Описание профиля

Параметр	Описание
Эвристика	• "Углубленная эвристика" — высокая вероятность обнаружения неизвестных вирусов, высокая вероятность ложных срабатываний. Скорость сканирования при углубленной эвристике более низкая, чем при эвристике в обычном режиме; • "Обычный режим" — глубина эвристики ограничена: низкая вероятность обнаружения неизвестных вирусов, низкая вероятность ложных срабатываний; • "Выключена" — эвристическое сканирование будет выключено
Исключения по файлам	Настройте параметры исключаемых из проверок файлов. • "Пропускать архивы" — при выборе данного пункта файлы архивов будут исключены из проверок антивируса; • "Пропускать файлы более" — при выборе параметра укажите размер пропускаемых при сканировании файлов; • "Проверять только файлы с расширениями" — будут проверяться только файлы с указанным расширением. Укажите расширения файлов, используя запятую в качестве разделителя
Действия при обнаружении зараженных файлов	Действия, которые нужно выполнять при обнаружении зараженных файлов (см. стр.**9**)

4. Перейдите на вкладку "Объекты сканирования".



Примечание. При настройке сканирования в режиме реального времени (профиль "Постоянная защита") вкладка "Объекты сканирования" недоступна.

5. Настройте нужные параметры и нажмите кнопку "Сохранить".

Параметр	Описание
Системная	Выберите объекты, проверку которых нужно провести

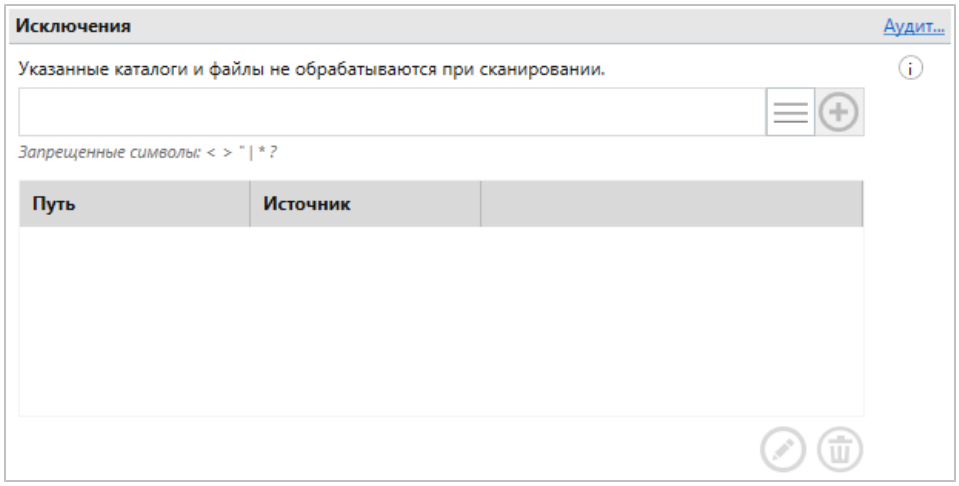
Параметр	Описание
Диски и директории	• Выберите диски и директории, которые необходимо проверять при запуске данного профиля сканирования. • Укажите путь к директории, которую нужно включить в проверку, и нажмите кнопку "Добавить". При необходимости используйте переменные среды окружения из раскрывающегося списка. Чтобы отредактировать путь, нажмите кнопку "Изменить". Для удаления директории из списка нажмите "Удалить"

6. Нажмите кнопку "Применить" внизу вкладки "Настройки".

Список исключений

Для настройки списка исключений:

1. В области настройки параметров антивируса перейдите к разделу "Исключения".



2. Чтобы внести в список директорию или файл, укажите путь к объекту и нажмите кнопку "Добавить". При необходимости используйте переменные среды окружения из раскрывающегося списка. Объекты из списка исключений пропускаются при любом профиле сканирования.

Внимание! Необходимо указывать полный путь к файлу или директории. Например, D:\Work.

При добавлении в список исключений директории — все объекты этой директории будут пропускаться при сканировании.

Совет. Для изменения пути к объекту выберите его в списке и нажмите кнопку "Редактировать". Для удаления объекта из списка исключаемых при проверках нажмите кнопку "Удалить".

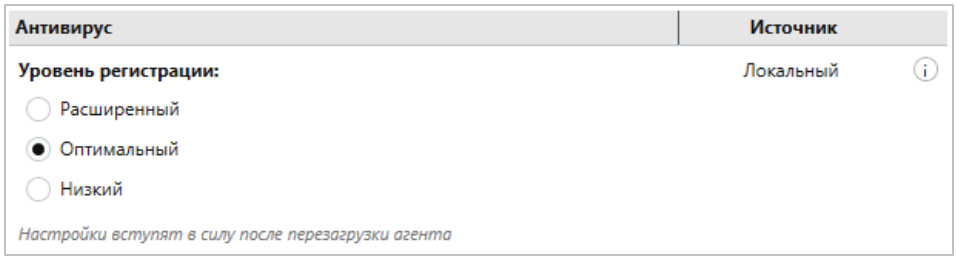
3. Нажмите кнопку "Применить" внизу вкладки "Настройки".

Регистрация событий

Для настройки регистрации событий:

1. В списке параметров и политик перейдите к разделу "Регистрация событий", затем выберите элемент "Антивирус".

   В правой части экрана появится область настройки данных параметров.



2. Укажите уровень регистрации событий.
   - Расширенный.

     Регистрируются все происходящие события.

     Внимание! Количество регистрируемых событий может быть очень большим.
   - Оптимальный.

     Регистрируются все важные и некоторые информационные события.
   - Низкий.

     Регистрируются только важные события.
3. Нажмите кнопку "Применить" внизу вкладки "Настройки".

Управление работой антивируса на защищаемых компьютерах

Программа управления Secret Net Studio позволяет осуществлять для отдельного компьютера:

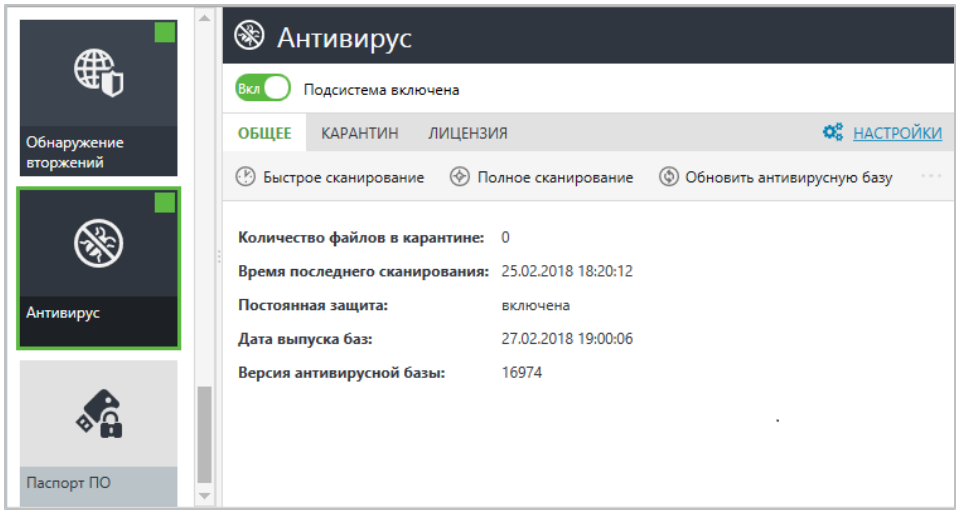
- запуск процедуры сканирования;
- просмотр и управление содержимым карантина;
- запуск процедуры обновления антивирусных баз.

Для управления работой антивируса:

1. В списке объектов управления выберите нужный компьютер, вызовите для него контекстное меню и выберите в нем команду "Свойства".

   На экране появится информация о состоянии данного компьютера.
2. На вкладке "Состояние" найдите и выберите объект "Антивирус".

   В правой части экрана появится панель управления работой антивируса.



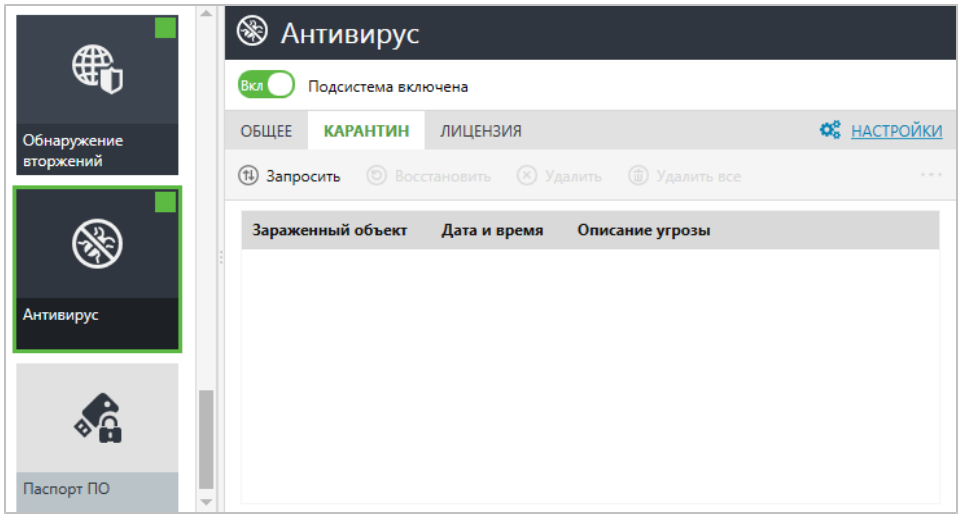
3. Для включения или отключения антивируса переведите в нужное положение переключатель в левом верхнем углу панели.
4. Выполните нужные действия с помощью кнопок "Быстрое сканирование", "Полное сканирование" и "Обновить антивирусную базу" (см. стр.**25**).

Примечание. Настройка параметров сканирования выполняется при настройке политик (см. стр.8). Нажмите кнопку-ссылку "НАСТРОЙКИ", чтобы перейти к настройке политики антивируса. Перейдите на вкладку "Лицензия" и нажмите кнопку-ссылку "Перейти к информации о лицензии", чтобы просмотреть сведения о действующей лицензии.

Для управления карантином:

1. В панели управления работой антивируса перейдите на вкладку "Карантин".

   На вкладке "Карантин" можно просмотреть список файлов и каталогов, помещенных в карантин на данном компьютере. Также здесь находятся кнопки управления элементами этого списка.



2. Выполните нужные действия.

Параметр	Описание
Запросить	Будет загружен список файлов, помещенных в карантин на данном компьютере
Восстановить	Выбранные файлы будут восстановлены из карантина. Чтобы восстановить сразу несколько файлов, выделите их в списке объектов и нажмите кнопку "Восстановить"
Удалить	Выбранный файл будет удален из каталога карантина
Удалить все	Карантин будет очищен

Внимание! Восстановленные из карантина объекты добавляются в список исключений для всех профилей сканирования. Это необходимо для того, чтобы при сканировании данный объект не попал в карантин повторно.

Файлы, находящиеся в карантине более 30 дней, будут автоматически удалены. Для настройки данного параметра используйте утилиту управления антивирусом av_cli.exe, входящую в состав продукта.

Утилита управления антивирусом

Внимание! Утилита управления антивирусом предназначена для специалистов технической поддержки. НЕ РЕКОМЕНДУЕТСЯ использовать данную утилиту для обычной настройки антивируса.

В состав Secret Net Studio входит утилита управления антивирусом av_cli.exe.

Для вызова подробной информации о программе откройте командную строку и введите следующую команду:

```
av_cli.exe
```

Управление карантином

Для утилиты av_cli.exe доступны следующие команды управления карантином:

- Отобразить объекты в карантине:

  ```
  av_cli.exe -c:-list_quarantine_objects
  ```

  В результате работы команды на экран будет выведен список объектов в карантине и их идентификационные номера.

- Удалить файлы из карантина:

  ```
  av_cli.exe -c:-remove_file_from_quarantine -quarantine_
  file_id:<идентификатор файла>
  ```

Например:

```
av_cli -c:remove_file_from_quarantine -quarantine_file_
id:1
```

- Удалить старые файлы из карантина:

```
av_cli.exe -c:-remove_files_from_quarantine_older_than
-days:<количество дней>
```

Например:

```
av_cli -c:remove_files_from_quarantine_older_than -days:2
```

- Восстановить файл из карантина (доступно только для администратора):

```
av_cli.exe -c:-restore_file -p:"<путь к файлу>"
```

Например:

```
av_cli -c:restore_file -p:"c:\checkAV\test heuristic\heur\
!ITW#460.vxe.quarantine"
```

```
av_cli -c:restore_file -p:"\\computer\open_share\!test for
localize\!ITW#460.vxe.quarantine"
```

С помощью утилиты av_cli.exe можно восстановить файл из карантина, даже если компьютер не подключен к сети и нет возможности восстановить файл в программе управления Secret Net Studio.

Восстановить файл, помещенный в карантин с подключаемого носителя, можно на любом компьютере. Для этого необходимо установить антивирус Secret Net Studio и с помощью утилиты av_cli.exe выполнить команду восстановления файла из карантина, указав путь к файлу с расширением .quarantine.

Глава 3
Обнаружение и предотвращение вторжений

Управление работой механизма обнаружения и предотвращения вторжений осуществляется централизованно в программе управления и может выполняться на разных уровнях структуры объектов управления:

- на уровне объектов "Домен", "Сервер безопасности" и "Организационная единица" можно выполнить настройку параметров работы этого механизма с помощью групповых политик. Значения параметров на уровне "Сервер безопасности" имеют приоритет перед аналогичными значениями, заданными на уровне объектов "Компьютер";
- на уровне объектов "Компьютер" можно выполнить настройку параметров работы этого механизма для отдельного компьютера, а также осуществлять управление работой механизма на данном компьютере.

Примечание. В состав Secret Net Studio также входит компонент "Локальный центр управления". Он позволяет управлять антивирусом непосредственно на защищаемом компьютере.

Настройка групповых политик

Механизм обнаружения и предотвращения вторжений позволяет выполнять следующие функции:

- применение детектора сетевых атак для блокирования атак и обнаружения попыток сканирования портов;
- применение сигнатурного анализатора, проверяющего входящий и исходящий трафик на наличие зарегистрированных сигнатур.

Для настройки и управления работой механизма:

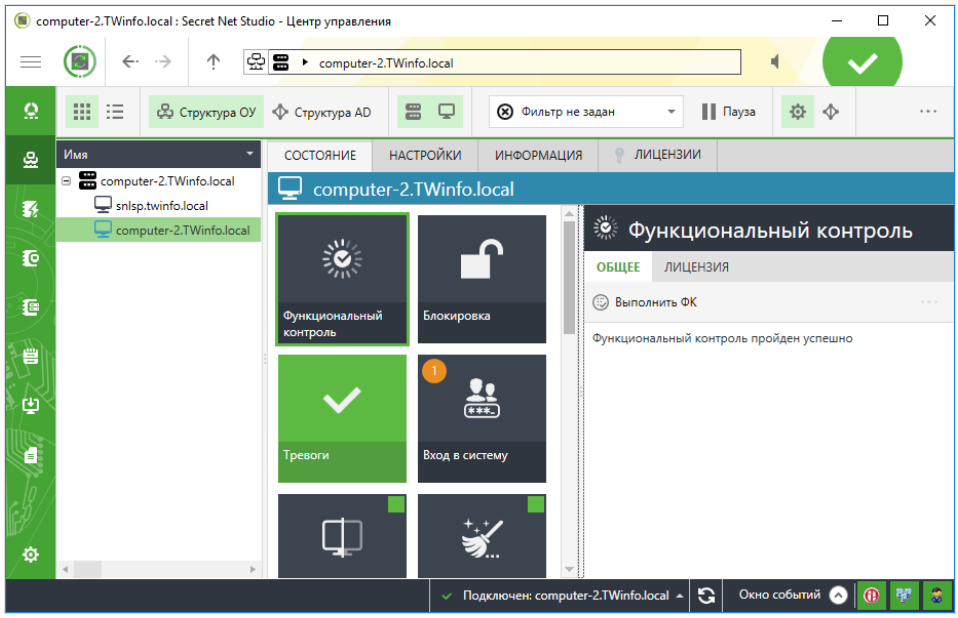
1. Вызовите программу управления Secret Net Studio.

   Совет. Для настройки параметров механизма обнаружения и предотвращения вторжений непосредственно на защищаемом компьютере вызовите программу "Локальный центр управления", в представлении "Компьютер" перейдите на вкладку "Настройки" и в разделе "Политики" выберите элемент "Обнаружение вторжений". Далее настройка этого механизма выполняется так же, как и в случае централизованного управления.

   На экране появится основное окно программы.

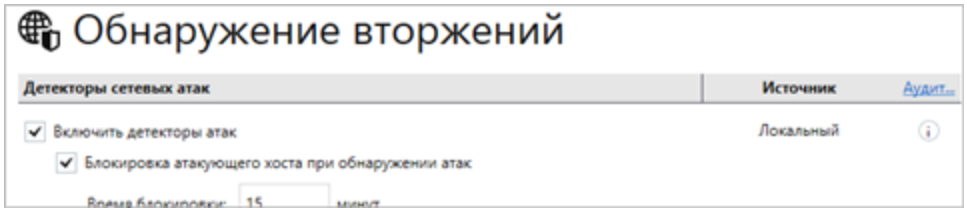
2. Откройте представление "Компьютеры", в левой части экрана в списке объектов управления найдите нужный компьютер (домен, сервер безопасности), вызовите для него контекстное меню и выберите в нем команду "Свойства".

   В правой части экрана появится информация о состоянии данного объекта.



3. Перейдите на вкладку "Настройки" и нажмите при необходимости кнопку "Загрузить настройки", затем в разделе "Политики" выберите элемент "Обнаружение вторжений".

   В правой части экрана появится область настройки выбранных параметров.

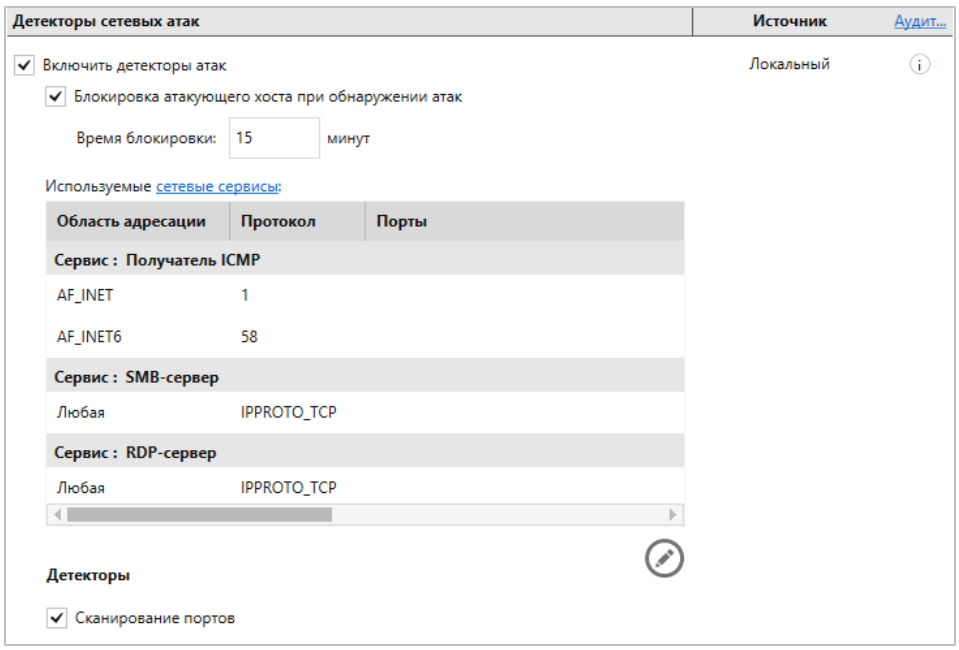


4. Настройте нужные параметры и для сохранения новых значений нажмите кнопку "Применить" внизу вкладки "Настройки".

Детектор сетевых атак

Для включения и настройки детекторов атак:

1. В области настройки параметров механизма обнаружения вторжений перейдите к разделу "Детекторы сетевых атак".



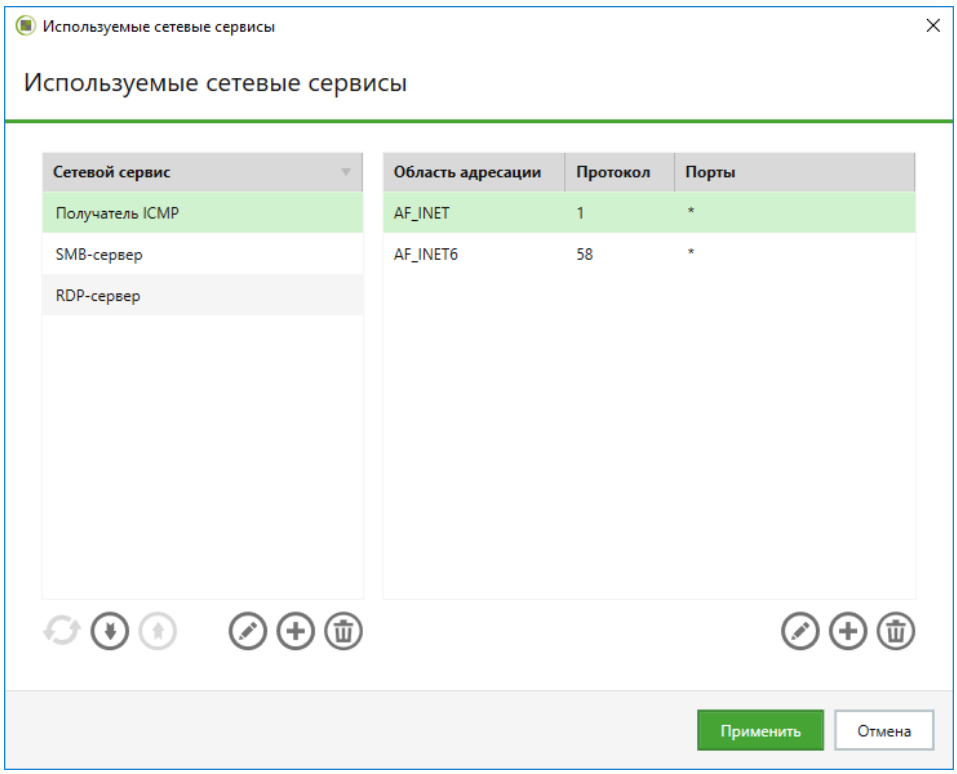
2. Настройте параметры детекторов.

Параметр	Описание
Включить детекторы атак	Отметьте данный пункт, чтобы активировать детекторы сетевых атак
Блокировка атакующего хоста при обнаружении атак	При включении детекторов атак данная функция активируется по умолчанию для всех детекторов. В этом случае IP-адрес атакующего хоста будет заблокирован
Время блокировки ... минут	Длительность блокировки хоста

Совет. Для настройки шаблонов сетевых сервисов нажмите кнопку-ссылку "сетевые сервисы".

3. Чтобы можно было указывать индивидуальные параметры срабатывания DoS-детектора для разных протоколов и портов, настройте список сетевых сервисов. Для этого нажмите кнопку "Редактировать".

На экране появится следующий диалог.



Совет. Для изменения списка сетевых сервисов используйте кнопки в левой части диалога.

- Используйте кнопки "Вниз" и "Вверх" для управления приоритетом используемых сетевых сервисов.
- Нажмите кнопку "Редактировать", чтобы заменить шаблон сетевого сервиса.
- Нажмите кнопку "Удалить" для удаления выбранного сетевого сервиса.
- Нажмите кнопку "Обновить", чтобы обновить список сетевых сервисов.

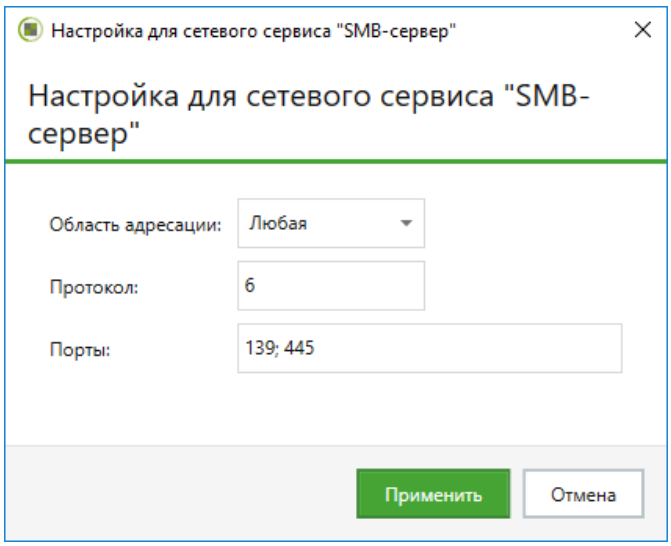
Совет. Для настройки сетевого сервиса используйте кнопки в правой части диалога:

- Нажмите кнопку "Добавить", чтобы добавить новую настройку сетевого сервиса.
- Нажмите кнопку "Редактировать", чтобы изменить выбранную настройку сетевого сервиса.
- Нажмите кнопку "Удалить" для удаления выбранной настройки сервиса.

4. Для добавления нового сетевого сервиса нажмите кнопку "Добавить" в левой части диалога, в появившемся диалоге укажите или выберите из списка имеющихся шаблонов имя сервиса и нажмите кнопку "Добавить". Чтобы настроить сетевой сервис, выберите его название в левой части диалога и

выполните нужные действия, используя кнопки в правой части диалога. Например, для изменения имеющейся настройки выберите ее в правом списке и нажмите кнопку "Редактировать".

На экране появится следующий диалог.



5. Внесите нужные изменения в параметры настройки и нажмите кнопку "Применить". Для сохранения параметров всех сетевых сервисов нажмите кнопку "Применить" в диалоге со списком сетевых сервисов.

Параметр	Описание
Область адресации	Выберите область адресации для сетевого сервиса
Протокол	Укажите номер протокола, для которого действует сервис
Порты	Укажите номера портов, для которых действует сетевой сервис, отделяя один от другого символом ";" (точка с запятой). Или укажите символ "*" (звездочка), если сетевой сервис должен действовать для всех портов

6. Включите необходимые детекторы и настройте параметры их работы.

Детектор, Параметр	Описание
Сканирование портов	Отметьте данный пункт, чтобы включить детектирование сканирования портов
Период обнаружения	Период, в течение которого выполняется подсчет обращений к портам защищаемых компьютеров
Максимальное количество обращений к портам за указанный период	По достижении указанного количества обращений сервер считается атакующим
ARP-spoofing	Отметьте данный пункт, чтобы включить детектирование атак типа "Man in the middle", применяемых в сетях с использованием протокола ARP
Время после ARP-запроса, в течение которого ожидается ARP-ответ	Укажите время, в течение которого детектор должен ожидать ответ на ARP-запрос. Если за указанный период времени получено более одного ответа на запрос, сработает детектор атаки

Детектор, Параметр	Описание
Действие с ARP-ответами, полученными без ARP-запросов	Укажите действие, которое должен осуществлять детектор с ARP-ответами, полученными без ARP-запросов: • Игнорировать; • Логировать — записывать событие аудита; • Логировать и посылать ARP-ответы; • Активный детектор ARP-spoofing — на каждый ARP-ответ без ARP-запроса будет выдан ARP-запрос; • Активное противодействие ARP-spoofing — на каждый ARP-ответ без ARP-запроса будет выдан ARP-запрос. Исходный ответ будет заблокирован. В этом режиме также могут отбрасываться подозрительные ARP-пакеты
SYN-FLOOD	Детектирование атак типа "Отказ в обслуживании", которые заключаются в отправке большого количества SYN-запросов в достаточно короткий срок
Время, за которое учитываются полуоткрытые соединения	Укажите время, в течение которого должны учитываться новые соединения по протоколу TCP
Количество полуоткрытых соединений, после которых хост считается атакующим	Укажите количество полуоткрытых соединений, при превышении которого должен срабатывать детектор атак
Блокировать пакет, если детектор сработал	При включении детекторов атак по умолчанию активируется функция "Блокировка атакующего хоста при обнаружении атак" для всех детекторов (см. стр.**19**). Чтобы точечно отключить блокировку для детектора "SYN-FLOOD", снимите отметку с пункта "Блокировать пакет, если детектор сработал". Если данный пункт отмечен, то в случае, если за указанный период времени было создано больше указанного количества полуоткрытых соединений, новые соединения создаваться не будут
Аномальный трафик	Отметьте данный пункт, чтобы включить детектирование аномального трафика
Блокировать пакет, если детектор сработал	При включении детекторов атак по умолчанию активируется функция "Блокировка атакующего хоста при обнаружении атак" для всех детекторов (см. стр.**19**). Чтобы точечно отключить блокировку для детектора "Аномальный трафик", удалите отметку из поля "Блокировать пакет, если детектор сработал". Если это поле отмечено, пакеты аномального трафика будут блокироваться при срабатывании детектора атак
DDoS	Детектирование атак, выполняемых одновременно с большого числа компьютеров
Максимальное количество активных удаленных хостов, при превышении которого срабатывает детектор	По достижении указанного количества удаленных адресов, с которых отправляется сетевой трафик на защищаемый компьютер, срабатывает детектор атак
DoS	Детектирование атак, выполняемых с целью довести систему до отказа
Отрезок времени, за который учитывается обращение к порту	Укажите отрезок времени, за который учитывается обращение к порту

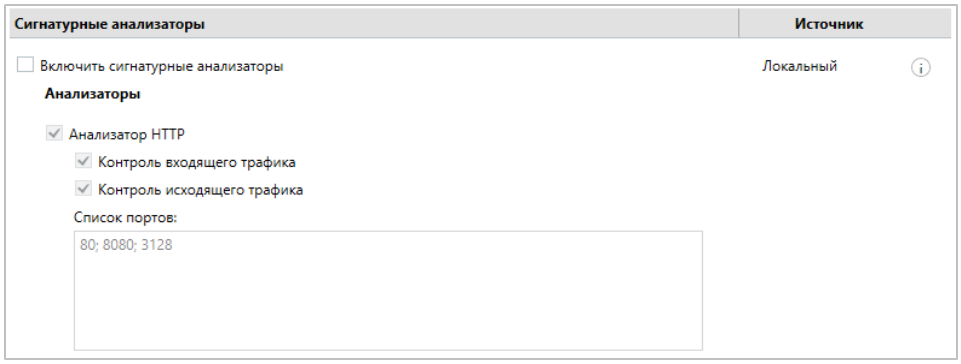
Детектор, Параметр	Описание
Максимальное количество пакетов, при превышении которого будет детектирована атака	По достижении указанного количества отправляемых с сервера пакетов за указанный отрезок времени сервер считается атакующим
Максимальный размер данных, при превышении которого будет детектирована атака	По достижении указанного размера отправляемых с сервера данных за указанный отрезок времени сервер считается атакующим
Замедлять трафик с атакующего хоста	Отметьте данный пункт, чтобы автоматически уменьшать скорость передачи данных с атакующего сервера, специально теряя часть пакетов. Замедление трафика работает, только если функция "Блокировка атакующего хоста при обнаружении атак" активна. После замедления трафика в 2 раза атакующий хост будет заблокирован

7. Нажмите кнопку "Применить" внизу вкладки "Настройки".

Сигнатурные анализаторы

Для настройки анализаторов:

1. В области настройки параметров механизма обнаружения вторжений перейдите к разделу "Сигнатурные анализаторы".



2. Настройте параметры.

Параметр	Описание
Включить сигнатурные анализаторы	Отметьте данный пункт, чтобы активировать сигнатурные анализаторы
Анализатор HTTP	Отметьте данный пункт, чтобы включить анализатор HTTP-трафика
Контроль входящего трафика	Входящий трафик будет контролироваться на наличие сигнатур, зарегистрированных в базе решающих правил
Контроль исходящего трафика	Исходящий трафик будет контролироваться на наличие сигнатур, зарегистрированных в базе решающих правил
Список портов	Укажите порты, которые необходимо проверять с помощью анализатора HTTP-трафика. Используйте символ ";" в качестве разделителя. По умолчанию список содержит порты 80, 8080 и 3128. Этот список не может быть пустым

3. Нажмите кнопку "Применить" внизу вкладки "Настройки".

Управление работой механизма обнаружения вторжений

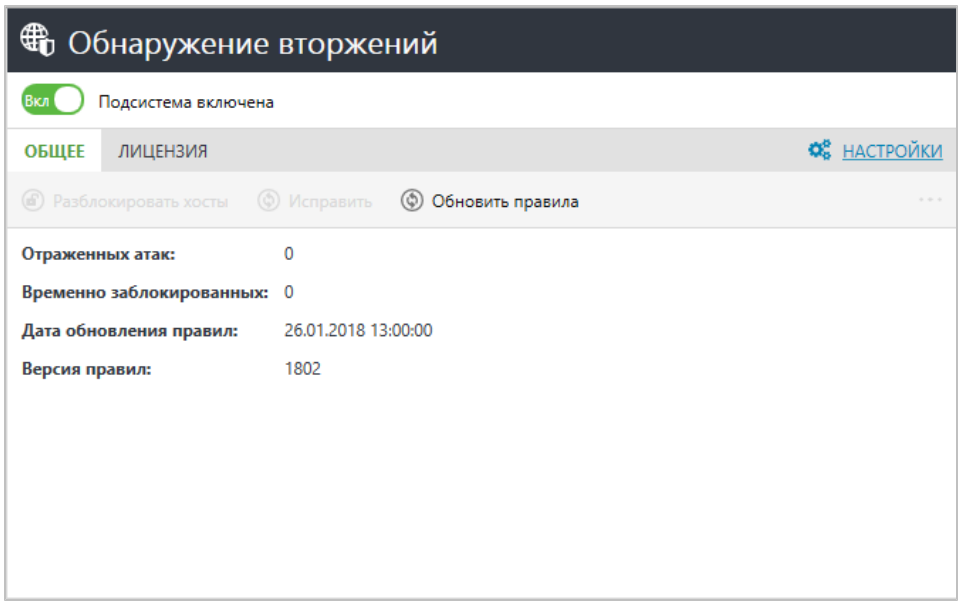
Программа управления Secret Net Studio позволяет осуществлять для отдельного компьютера отключение блокировки хостов.

Для управления работой механизма:

1. В списке объектов управления выберите нужный компьютер, вызовите для него контекстное меню и выберите в нем команду "Свойства".

   На экране появится информация о состоянии данного компьютера.
2. На вкладке "Состояние" выберите объект "Обнаружение вторжений".

   В правой части экрана появится панель управления данным механизмом.



3. Для включения или отключения механизма переведите в нужное положение переключатель в левом верхнем углу панели.
4. Выполните нужное действие с помощью следующих кнопок.

Кнопка	Описание
Разблокировать хосты	Все хосты, заблокированные механизмом обнаружения вторжений на данном компьютере, будут разблокированы
Исправить	При рассинхронизации данных сервера Secret Net Studio и компонентов сетевой защиты (например, при изменении имени компьютера) включается аварийный режим работы. Если кнопка "Исправить" активна, возможна синхронизация данных
Обновить правила	Будет выполнено обновление базы решающих правил (см. стр.**25**)

Примечание. Нажмите кнопку-ссылку "НАСТРОЙКИ", чтобы перейти к настройке политик механизма обнаружения вторжений (см. стр.**18**).
Перейдите на вкладку "Лицензия" и нажмите кнопку-ссылку "Перейти к информации о лицензии", чтобы просмотреть сведения о действующей лицензии.

Глава 4
Обновление

Для полноценной защиты от вредоносных программ в Secret Net Studio предусмотрена возможность автоматического обновления на защищаемых компьютерах антивирусных баз для антивируса и базы решающих правил для механизма обнаружения и предотвращения вторжений. Также имеется возможность выполнить автономное обновление антивирусных баз вручную средствами специальной утилиты (см. стр.27).

Настройка автоматического обновления осуществляется централизованно в программе управления и может выполняться на разных уровнях структуры объектов управления:

- на уровне объектов "Домен", "Сервер безопасности" и "Организационная единица" можно выполнить настройку параметров обновления с помощью групповых политик. Значения параметров на уровне "Сервер безопасности" имеют приоритет перед аналогичными значениями, заданными на уровне объектов "Компьютер";
- на уровне объектов "Компьютер" можно выполнить настройку параметров обновления для отдельного компьютера.

Примечание. В состав Secret Net Studio также входит компонент "Локальный центр управления". Он позволяет настроить параметры обновления непосредственно на защищаемом компьютере.

Настройка обновления

Для настройки обновления:

1. Вызовите программу управления Secret Net Studio.

   Совет. Для настройки параметров обновления непосредственно на защищаемом компьютере вызовите программу "Локальный центр управления", в представлении "Компьютер" перейдите на вкладку "Настройки" и в разделе "Политики" выберите элемент "Обновление". Далее настройка этих параметров выполняется так же, как и в случае централизованного управления.

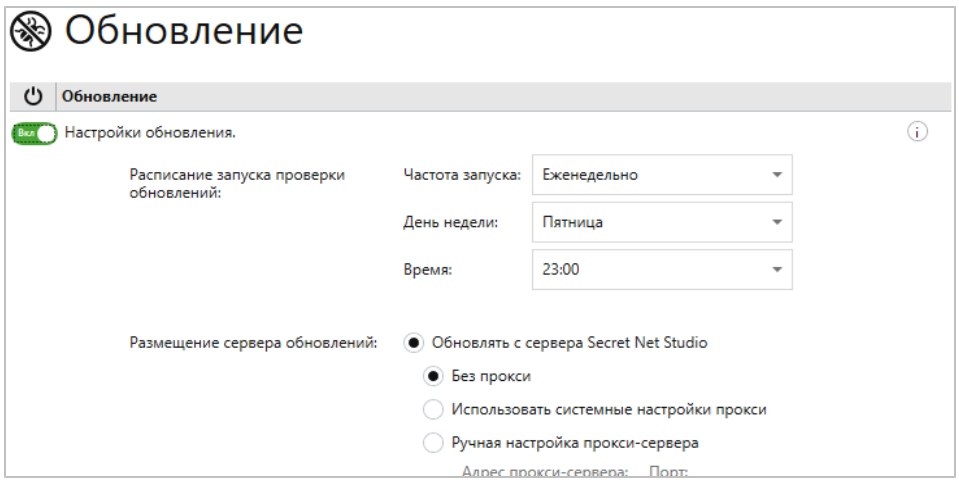
   На экране появится основное окно программы.

2. Откройте представление "Компьютеры", в левой части экрана в списке объектов управления найдите нужный компьютер (домен, сервер безопасности), вызовите для него контекстное меню и выберите в нем команду "Свойства".

   В правой части экрана появится информация о состоянии данного объекта.

3. Перейдите на вкладку "Настройки" и нажмите при необходимости кнопку "Загрузить настройки", затем в разделе "Политики" выберите элемент "Обновление".

   В правой части экрана появится область настройки выбранных параметров.



Совет. Если выполняется настройка групповой политики, переведите выключатель в левом верхнем углу раздела параметров в положение "Вкл".

4. В группе "Расписание запуска проверки обновлений" выберите частоту запуска проверки обновлений. При выборе еженедельного режима доступна возможность выбора дня и конкретного времени для выполнения программой обновлений. При ежедневном обновлении можно указать конкретное время. При выборе параметра "Планировщик отключен" обновления не будут проверяться автоматически.

Примечание. Рекомендуется выполнять обновление баз ежедневно. Если в сети большое количество рабочих станций, рекомендуется разбить их на группы и настроить для групп обновление в разное время.

5. Чтобы загружать обновления с сервера компании ООО "Код Безопасности", отметьте пункт "Обновлять с сервера Secret Net Studio" и при необходимости настройте параметры прокси-сервера.

Параметр	Описание
Без прокси	Выберите данный пункт, если соединение с сервером обновлений происходит напрямую (без прокси-сервера)
Использовать системные настройки прокси	Используется автоматическое определение прокси-сервера (не рекомендуется)
Ручная настройка прокси-сервера	Выберите данный пункт, чтобы настроить прокси-сервер вручную. Укажите адрес прокси-сервера и порт. Если на прокси-сервере используется авторизация, укажите имя пользователя и пароль

6. Если в локальной сети установлен сервер обновлений антивирусных баз Secret Net Studio или если обновления расположены в сетевой папке, отметьте пункт "Обновлять с локального сервера". Укажите:
   - IP-адрес или полное доменное имя (FQDN) локального сервера обновлений. Например, us.domain.loc;
   - путь к сетевой папке с обновлениями (см. стр. **26**). Например, \\server\sns-updates\packages.

Примечание. В случае установки обновлений из сетевой папки, учетная запись компьютера, на который загружаются обновления, должна иметь доступ к указанному ресурсу.
Если защищаемый компьютер не подключен к интернету, обновление антивирусных баз можно выполнить с помощью утилиты обновления (см. стр.**27**).

7. Нажмите кнопку "Применить" внизу вкладки "Настройки".

Загрузка обновлений с сетевого ресурса

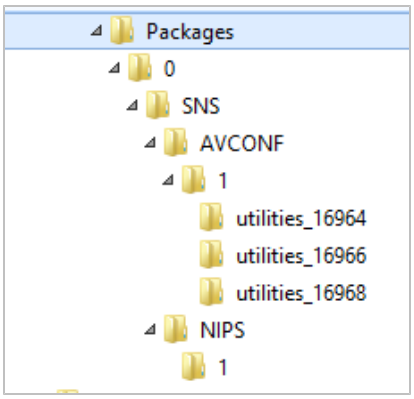
Для загрузки обновлений с сетевого ресурса:

1. Установите ПО сервера обновлений на компьютере с доступом к интернету и настройте обновление с сервера компании "Код Безопасности" (см. документ [**8**]).
2. Создайте сетевой ресурс и предоставьте к нему доступ авторизованным пользователям. Доступ к пакетам обновлений будет происходить от имени компьютеров, на которых будут работать антивирусы или каскадные серверы обновлений.
3. Настройте синхронизацию содержимого папки C:\ProgramData\Security Code\Secret Net Studio\Server\Update Server\Packages с нужным сетевым ресурсом.

Примечание. Настроить синхронизацию данных можно с помощью любой утилиты для репликации каталогов, например, Robocopy (входит в состав Windows Vista и выше).

Перенос обновлений вручную

При необходимости переноса обновлений вручную скопируйте каталог C:\ProgramData\Security Code\Secret Net Studio\Server\Update Server\Packages или синхронизируемый с ним каталог (см. выше) на съемный носитель информации и перенесите на сервер в закрытой сети.



Внимание! При переносе обновлений вручную нельзя менять структуру файлов в папке "Packages".

Утилита обновления

В состав ПО Secret Net Studio входит утилита для автономного обновления антивирусных баз. При запуске утилиты осуществляется проверка текущей версии антивирусных баз для установленного антивируса. При необходимости выполняется установка актуальных обновлений, которые содержатся в утилите.

Внимание! Утилита содержит в себе обновление только одного из антивирусов.

При установке обновлений выполняется проверка совместимости содержимого загруженного архива с версией продукта, установленного на защищаемом компьютере. Также выполняется верификация и проверка целостности архива.

Утилиту можно скачать на сайте компании "Код Безопасности" или на локальном сервере обновлений.

Для загрузки и запуска утилиты:

1. Перейдите по ссылке https://updates.securitycode.ru:43444.
2. Чтобы скачать утилиту, нажмите на ссылку:
   - "Пакет обновлений антивирусной базы антималваре";
   - "Пакет обновлений антивирусной базы".

   Примечание. В имени файла указана версия антивирусной базы, которая содержится в утилите.
3. На защищаемом компьютере запустите на исполнение загруженный файл утилиты. На экране появится сообщение о результате обновления антивирусных баз.

   Примечание. При отсутствии необходимого свободного места на диске обновления не будут установлены.

Если во время применения обновления произошел сбой, возврат к предыдущей версии баз произойдет автоматически. В остальных случаях возврат к предыдущим версиям антивирусных баз возможен только средствами утилиты av_cli.exe (см. стр. **16**) или программы управления сервером обновлений (см. документ [**8**]).

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. Сервер обновлений. Установка и настройка	
9. Средство защиты информации Secret Net Studio. Руководство пользователя	RU.88338853.501400.001 92