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:	**http://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" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

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

Глава 1
Общие сведения

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

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". С помощью данного компонента возможно управление 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", перейдите на вкладку "Настройки" и в разделе "Политики" выберите элемент "Антивирус". Далее настройка этого механизма выполняется так же, как и в случае централизованного управления.

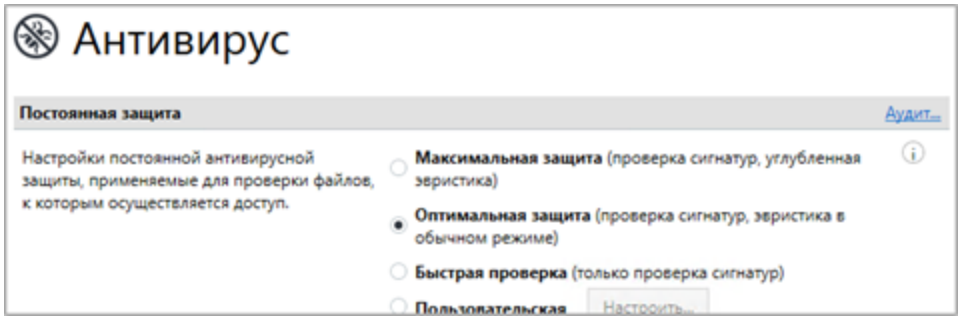
   На экране появится основное окно программы.

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

   В правой части экрана появится информация о состоянии данного компьютера.

3. Перейдите на вкладку "Настройки", затем в разделе "Политики" выберите элемент "Антивирус".

   В средней части экрана появится область настройки выбранных параметров.



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

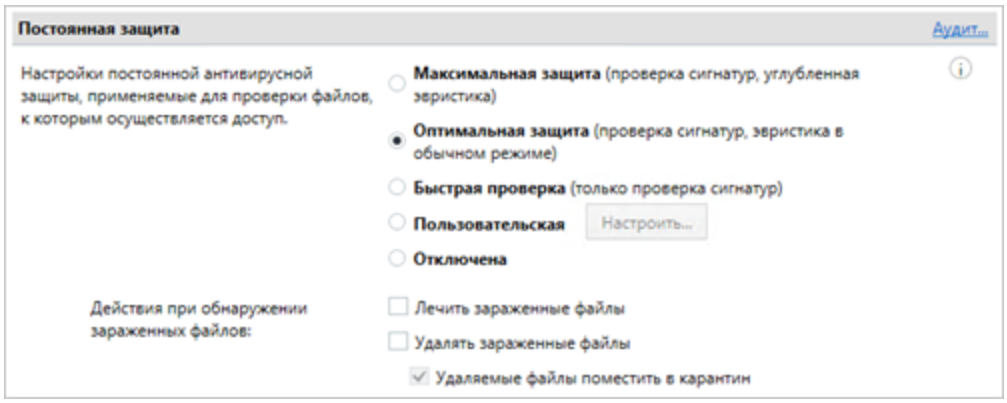
Настройка профилей сканирования

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
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	Выполняется поиск файлов, зараженных известными вредоносными программами. Проверяются все постоянные и съемные диски. При сканировании используется глубокий уровень эвристического анализа новых угроз (см. стр.**12**). Файлы и архивы размером более 100 Мб пропускаются
Оптимальная защита	Проверяются файлы при любой попытке доступа, проверяются все постоянные и съемные диски. При сканировании используется эвристический анализ в обычном режиме (см. стр.**12**). Файлы размером более 100 Мб и архивы размером более 50 Мб пропускаются
Быстрая проверка	Выполняется поиск файлов, зараженных известными вредоносными программами, проверяются только постоянные диски. Файлы размером более 50 Мб пропускаются
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.**11**).
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
Удалять зараженные файлы	Зараженные файлы будут удалены
Удаляемые файлы поместить в карантин	Удаляемые файлы будут перемещены в карантин. Перемещенные в карантин файлы в дальнейшем можно восстановить в случае необходимости

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.

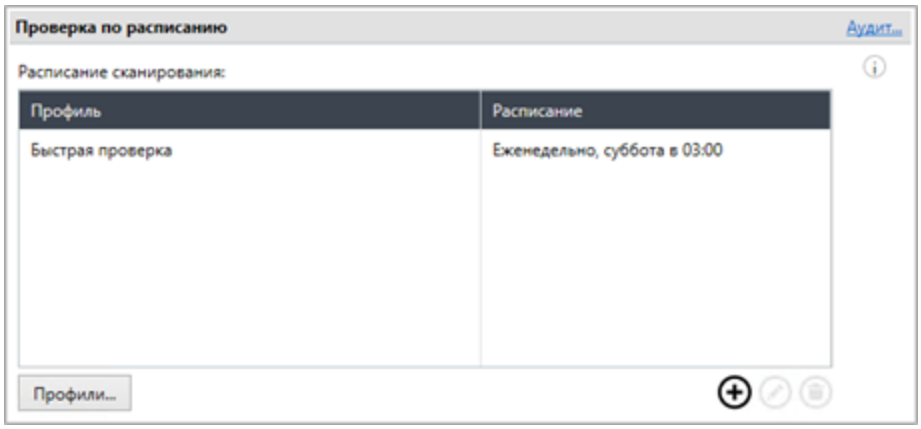
4. Нажмите кнопку-ссылку "Аудит" и настройте параметры регистрации событий антивируса.

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

Проверка по расписанию

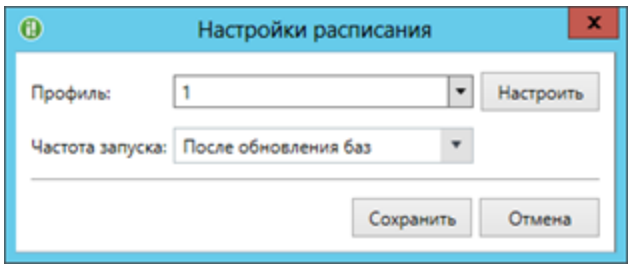
Для настройки сканирования по расписанию:

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



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

   Откроется диалог:



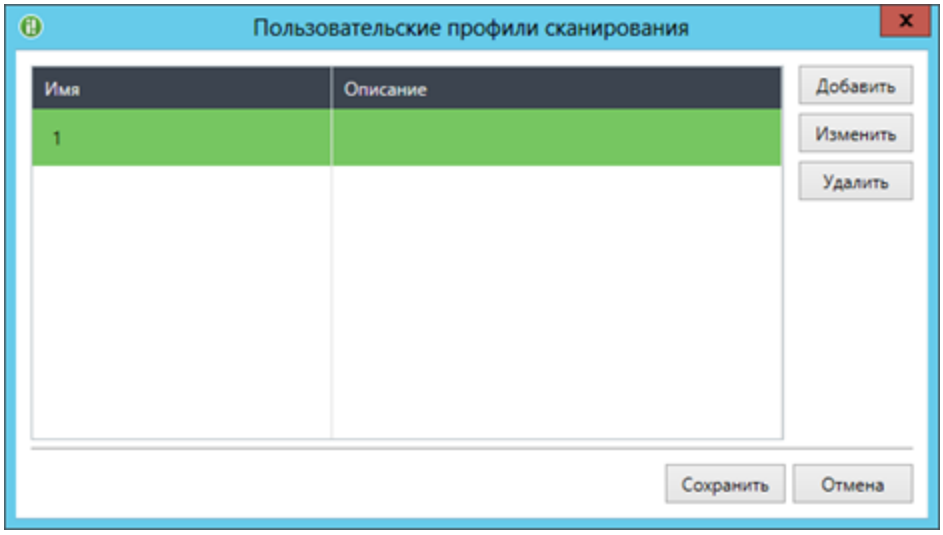
3. Выберите профиль сканирования и частоту запуска проверки и нажмите кнопку "Сохранить".

Примечание. Чтобы настроить пользовательский профиль сканирования, нажмите кнопку "Настроить".

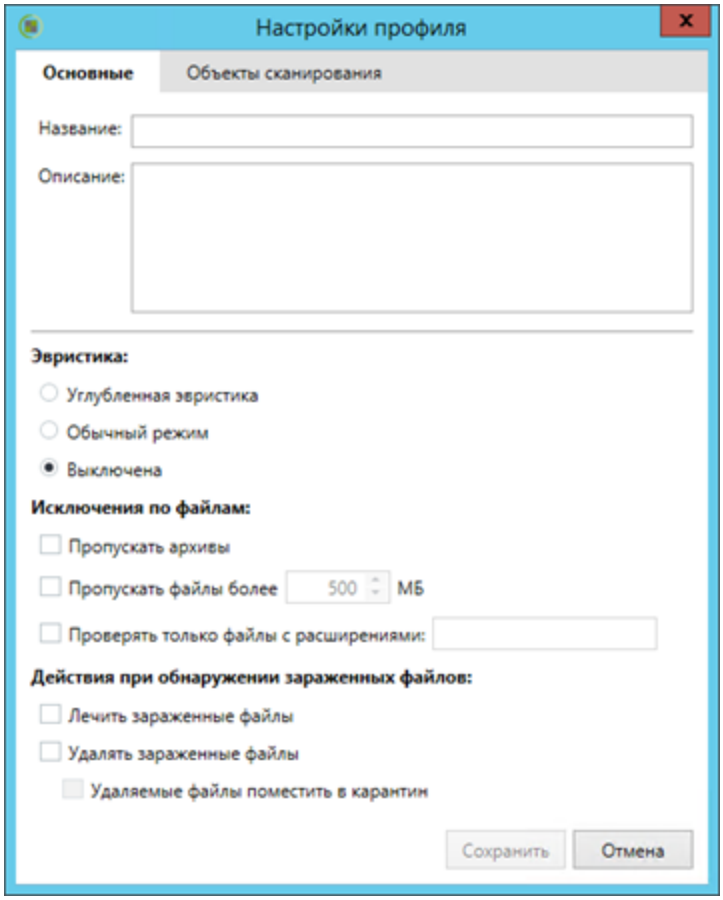
Для создания нового профиля сканирования:

1. Нажмите кнопку "Профили...".

   На экране появится окно:



2. В правой части окна нажмите кнопку "Добавить.
Откроется окно настройки профиля.

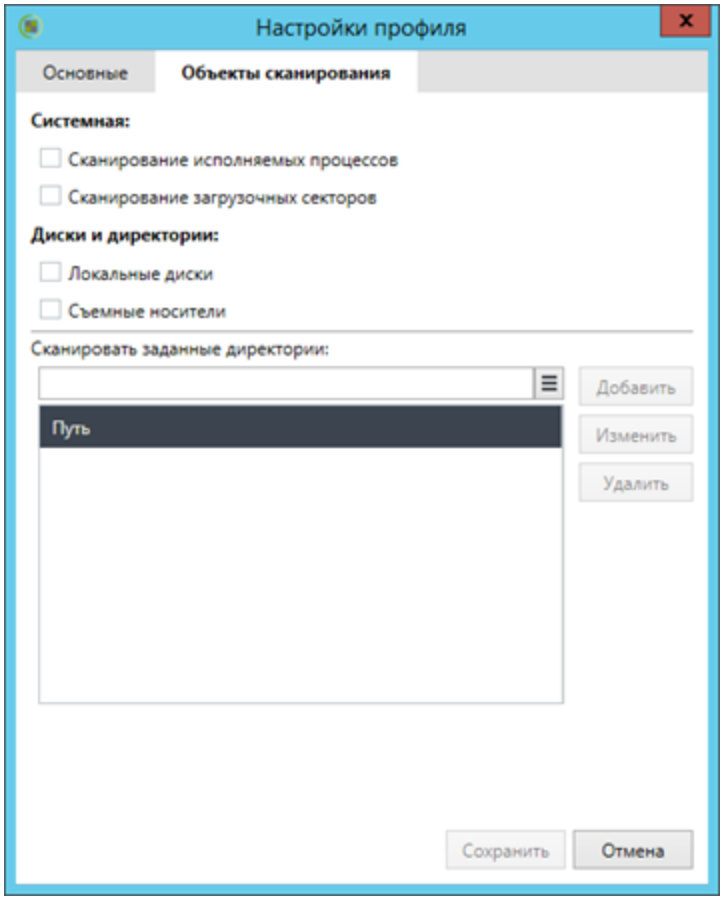


3. На вкладке "Основные" укажите следующие параметры.

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 раширениями" — 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".
   Откроется окно.



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

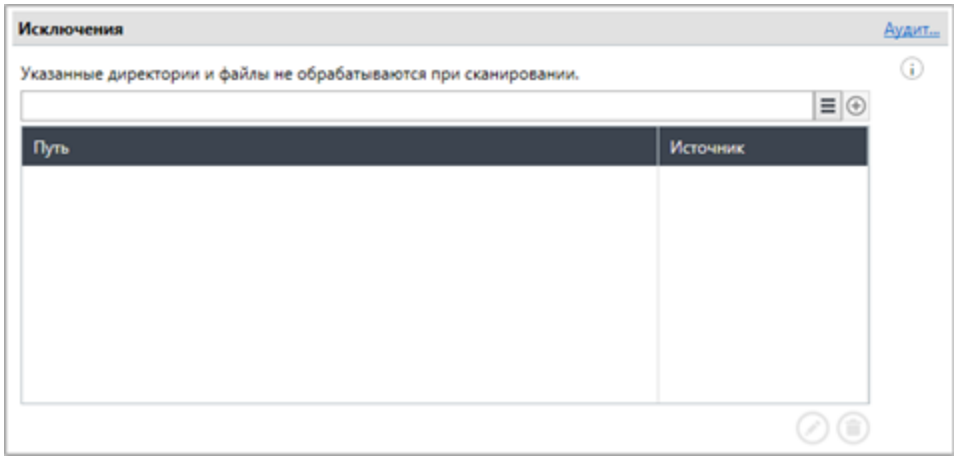
5. Настройте параметры.

Параметр	Описание
Системная	Выберите объекты, проверку которых нужно произвести
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"

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.

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

Регистрация событий

Для настройки регистрации событий:

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

   На экране появится окно:

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.

Управление работой антивируса на защищаемых компьютерах

Программа управления Secret Net Studio позволяет осуществлять для отдельного компьютера:

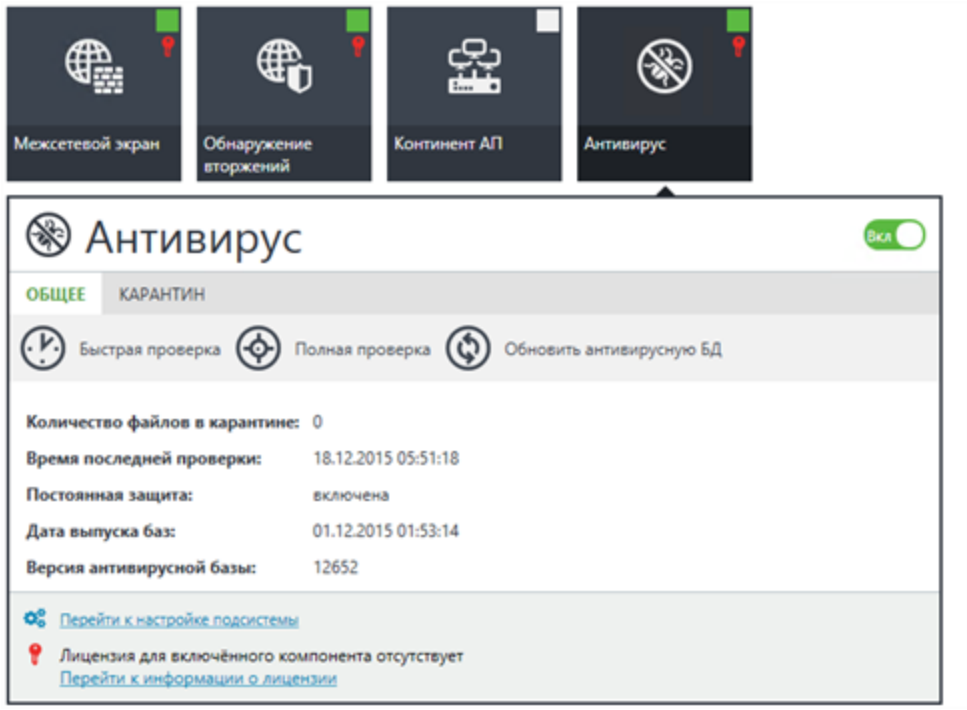
- запуск процедуры сканирования;
- просмотр и управление содержимым карантина;
- запуск процедуры обновления антивирусных баз.

Для управления работой антивируса:

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

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

   Откроется панель управления работой антивируса.



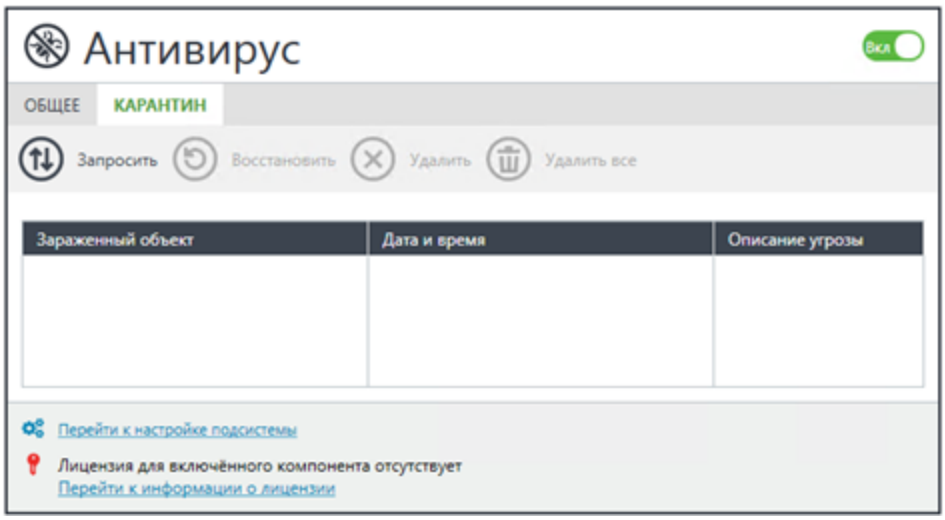
3. Выполните нужные действия с помощью кнопок "Быстрая проверка", "Полная проверка" и "Обновить антивирусную БД" (см. стр. **24**). Настройка параметров сканирования производится с помощью политик (см. стр. **8**).

Примечание. Нажмите кнопку-ссылку "Перейти к настройке подсистемы", чтобы перейти к настройке локальных политик антивируса.
Нажмите кнопку-ссылку "Перейти к информации о лицензии", чтобы просмотреть сведения о действующей лицензии.

Для управления карантином:

1. Откройте панель управления работой антивируса и 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	Выбранный файл будет восстановлен из карантина
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
```

Примечание. Утилита av_cli.exe и утилита управления сервером обновлений avus.exe (см. раздел "Настройка сервера обновлений" в документе "Настройка и эксплуатация. Антивирус и средство обнаружения вторжений") используют одинаковые параметры для управления обновлениями.

Глава 3
Обнаружение и предотвращение вторжений

Управление работой механизма обнаружения и предотвращения вторжений осуществляется централизованно в программе управления и может выполняется 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". С помощью данного компонента возможно управление механизмом обнаружения и предотвращения вторжений 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", 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.

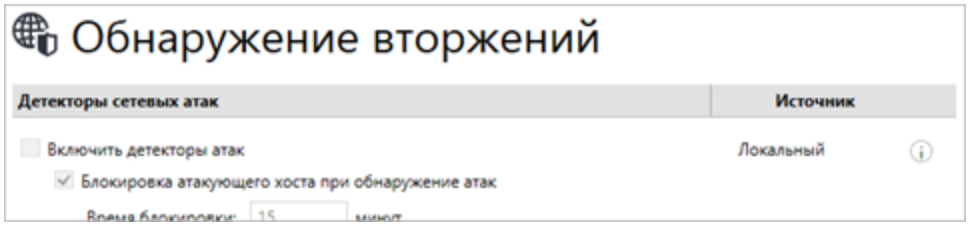
   На экране появится основное окно программы.

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

   В правой части экрана появится информация о состоянии компьютера.

3. Перейдите на вкладку "Настройки", затем в разделе "Политики" выберите элемент "Обнаружение вторжений".

   В средней части экрана появится область настройки выбранных параметров.

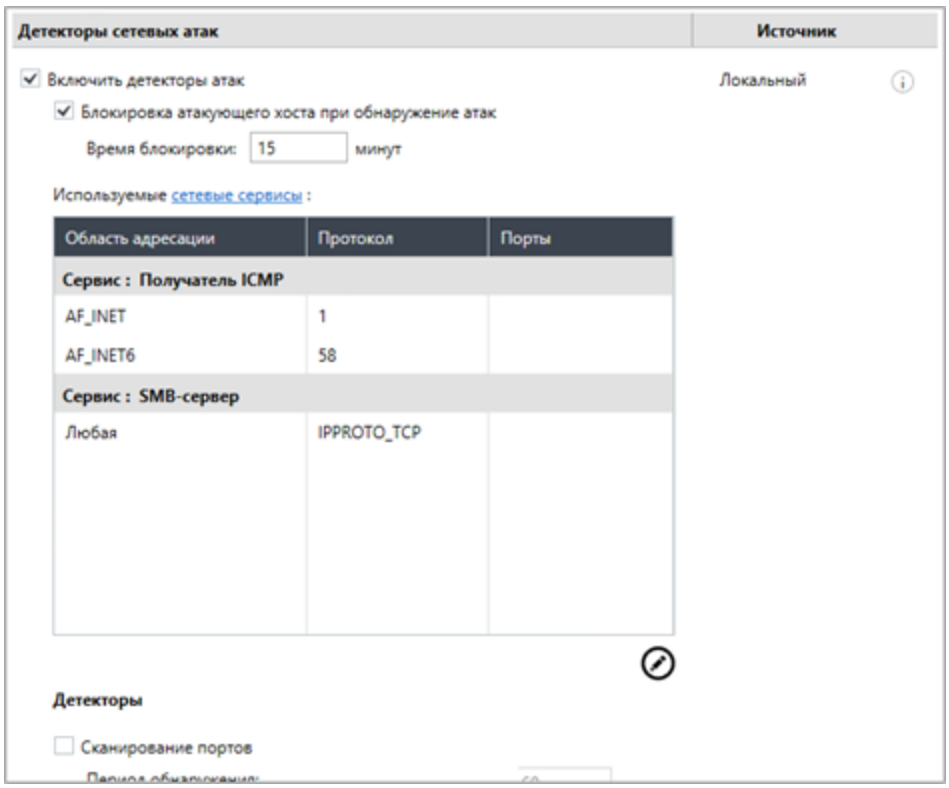


4. Настройте нужные параметры и для сохранения новых значений нажмите кнопку "Применить" в верхней части вкладки "Настройки".

Детектор сетевых атак

Для включения детекторов атак:

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



2. Настройте параметры детекторов.

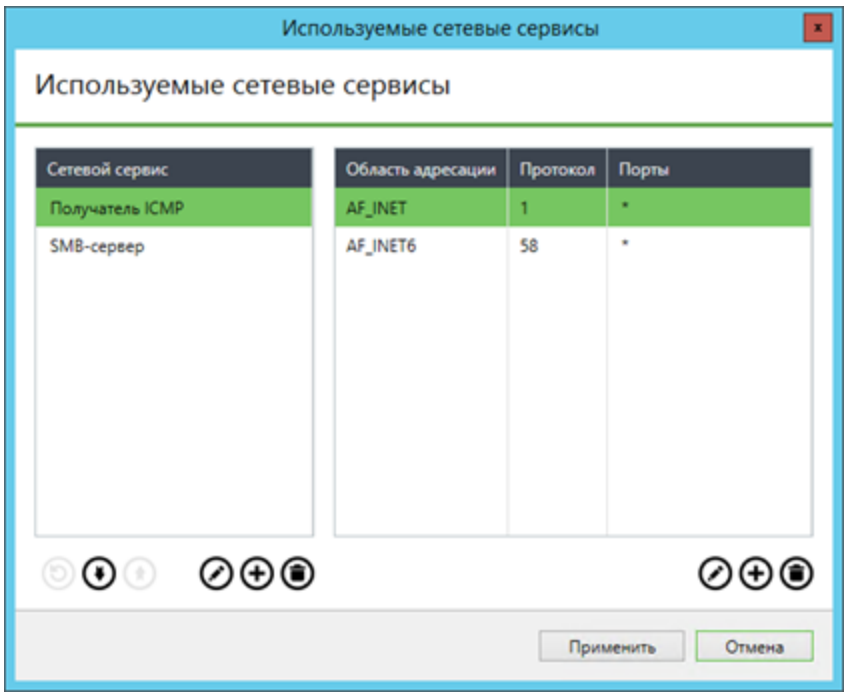
Параметр	Описание
Включить детекторы атак	Отметьте данный пункт, чтобы запустить детектор сетевых атак
Блокировка атакующего хоста при обнаружении атак	Если данный пункт отмечен, IP-адрес атакующего хоста будет заблокирован

Параметр	Описание
Время блокировки (минуты)	Длительность блокировки хоста

Примечание. 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, нажмите кнопку "Редактировать".

   На экране появится следующий диалог.



Примечание. Чтобы отредактировать список сетевых сервисов, используйте кнопки в левой части окна:

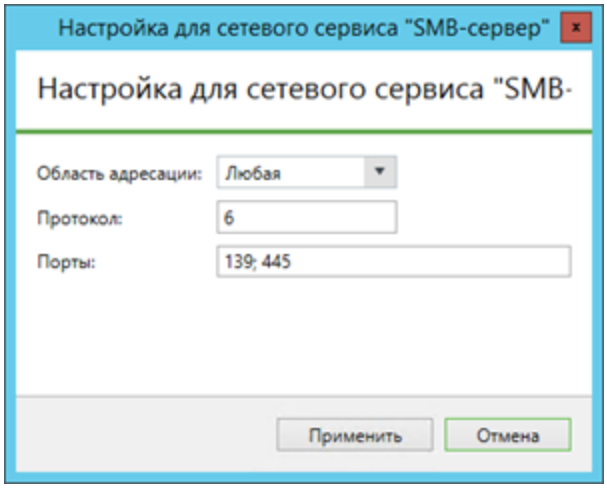
- Используйете кнопки "Вниз" и "Вверх" для управления приоритетом используемых сетевых сервисов;
- Нажмите кнопку "Редактировать", чтобы заменить шаблон сетевого сервиса;
- Нажмите кнопку "Удалить" для удаления сетевого сервиса;
- Нажмите кнопку "Обновить", чтобы обновить список сетевых сервисов.

Примечание. Чтобы отредактировать настройки сетевого сервиса, используйте кнопки в правой части окна:

- Нажмите кнопку "Добавить", чтобы добавить новую настройку сетевого сервиса;
- Нажмите кнопку "Удалить" для удаления настройки сервиса.

4. Для добавления нового сетевого сервиса, нажмите кнопку "Добавить" в левой части окна и выберите шаблон сетевого сервиса. Чтобы настроить параметры сетевого сервиса, выберите его название в левой части окна, затем выберите нужный набор параметров в правой части окна и нажмите кнопку "Редактировать".

   На экране появится следующий диалог.



5. Настройте парамеры сетевого сервиса 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 сетевого сервиса
Протокол	Выберите протокол, для которого действует сервис
Порты	Укажите номер порта, для которого действует сетевой сервис

6. Включите необходимые детекторы и настройте параметры их работы.

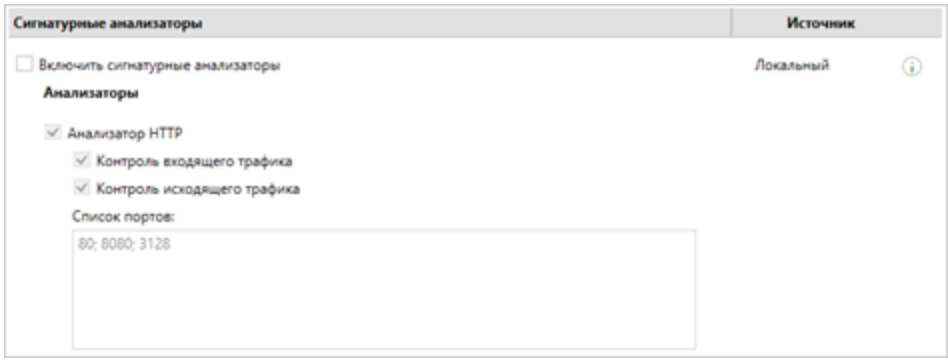
Детектор	Описание
Сканирование портов	Отметьте данный пункт, чтобы включить детектирование сканирования портов
Период обнаружения	Период, в течение которого выполняется подсчет обращений к портам защищаемых компьютеров
Максимальное количество обращений к портам за указанный период	По достижении указанного 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
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

Детектор	Описание
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	Отметьте данный пункт, чтобы блокировать пакеты при срабатывании детектора атак. В этом случае, если за указанный период времени было создано больше указанного количества полуоткрытых соединений, то новые соединения создаваться не будут
Аномальный трафик	Отметьте данный пункт, чтобы включить детектирование аномального трафика
Блокировать пакет, если детектор сработал	Отметьте данный пункт, чтобы блокировать пакеты аномального трафика 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
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

Сигнатурный анализатор

Для настройки анализатора:

1. В области настройки параметров механизма обнаружения вторжений перейдите к разделу "Сигнатурный анализатор".



2. Настройте параметры.

Параметр	Описание
Включить сигнатурный анализатор	Отметьте данный пункт, чтобы запустить сигнатурный анализатор
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 механизма обнаружения вторжений. Используйте символ ";" в качестве разделителя. По умолчанию список содержит порты 80, 8080 и 3128

Примечание. Список портов, проверяемых анализатором HTTP, не может быть пустым.

Управление работой механизма обнаружения вторжений

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

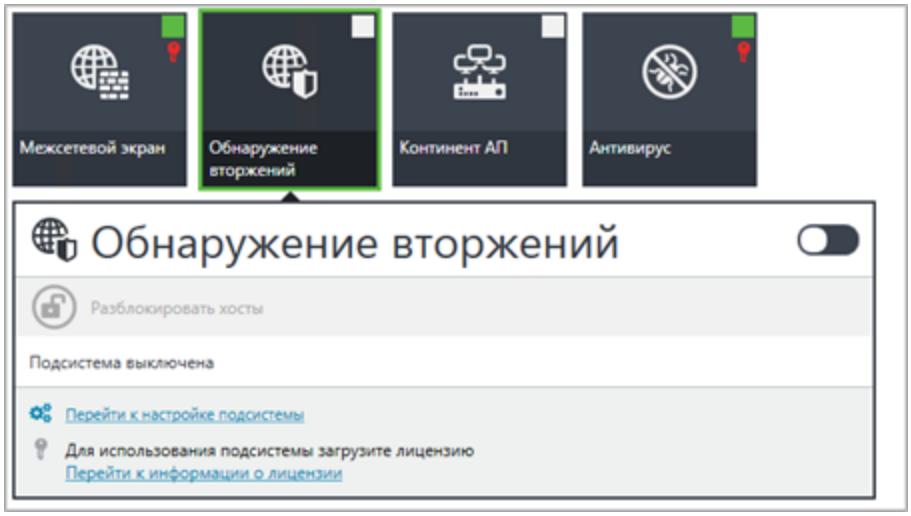
Для управления работой механизма:

1. В левой части экрана представления "Компьютеры" найдите в списке объектов управления нужный компьютер, вызовите для него контекстное меню и активируйте в нем команду "Свойства".

   В правой части экрана появится информация о состоянии данного компьютера.

2. В средней части экрана в области свойств компьютера найдите и выберите объект "Обнаружение вторжений".

   Откроется панель управления работой механизма.



3. Нажмите кнопку "Разблокировать хосты", чтобы разблокировать все хосты, заблокированные механизмом обнаружения вторжения на данном компьютере.

Примечание. Нажмите кнопку-ссылку "Перейти к настройке подсистемы", чтобы перейти к настройке групповых политик механизма обнаружения вторжений (см. стр.17).
Нажмите кнопку-ссылку "Перейти к информации о лицензии", чтобы просмотреть сведения о действующей лицензии.

Глава 4
Обновление

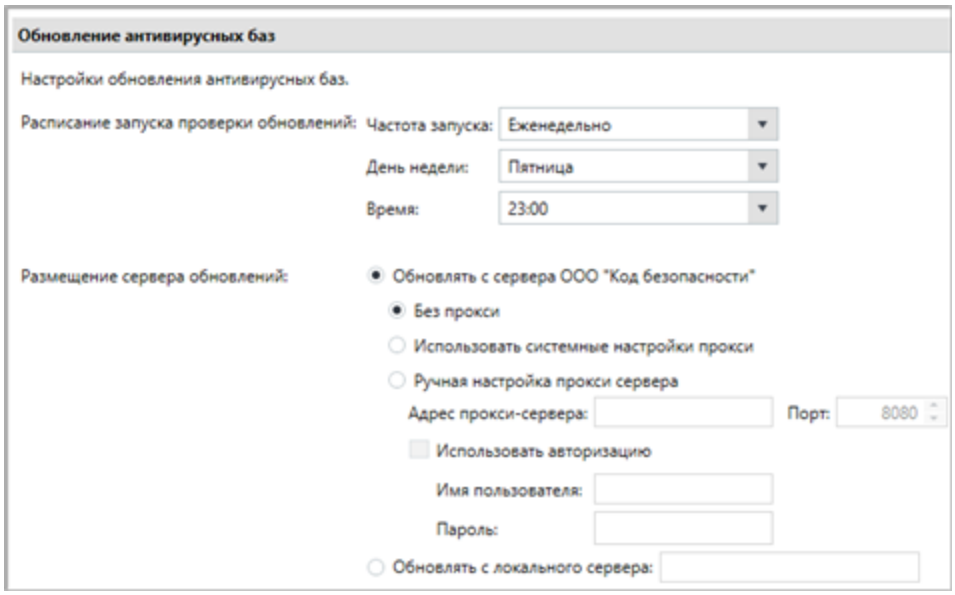
Для полноценной защиты компьютеров от вредоносных программ предусмотрена установка следующих обновлений:

- обновление антивирусных баз (см. стр.**24**);
- обновление базы решающих правил (см. стр.**25**).

Обновление антивирусных баз

Для настройки обновления:

1. В разделе "Политики" выберите элемент "Обновление".



2. 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.
3. Если в локальной сети установлен сервер обновлений антивирусных баз Secret Net Studio, отметьте пункт "Обновлять с локального сервера" и укажите адрес сервера. Иначе отметьте пункт "Обновлять с сервера ООО "Код безопасности" 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
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

Примечание.
Воможна установка обновлений из сетевой папки. В этом случае учетная запись компьютера должна иметь доступ к указанному ресурсу.
Если защищаемый компьютер не подключен к Интернету, обновление антивирусных баз можно произвести с помощью утилиты обновления (см. стр.**25**).

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 следущей ссылке:
   - https://updates.securitycode.ru:43442 для антивируса;
2. Чтобы скачать утилиту нажмите на ссылку:
   - "Текущая утилита обновления для антивируса";

   Примечание. В имени файла указана версия антивирусной базы, которая содержится в утилите.
3. 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, то откат к предыдущей версии баз произойдет автоматически. В остальных случаях откат к предыдущим версиям антивирусных баз возможен только через утилиту av_cli.exe (см. стр.**16**) или avus.exe (см. раздел "Настройка сервера обновлений" в документе "Сервер обновлений. Установка и настройка").

Обновление базы решающих правил

База решающих правил содержит сигнатуры сетевых атак. При появлении новых сетевых атак формируется обновление базы решающих правил.

Для обновления БРП:

1. Выполните загрузку доступного обновления для базы решающих правил в личном кабинете на сайте компании "Код Безопасности" (http://www.securitycode.ru/).
2. Выполните проверку целостности загруженных обновлений. Для этого сравните контрольные суммы файлов БРП с контрольными суммами, указанными на сайте компании "Код Безопасности".
3. На компьютере с установленным ПО клиента Secret Net Studio войдите в систему под именем учетной записи администратора. Откройте командную строку и выполните следующие команды:

   cd "**<путь_1>**"

   ScLocalCfg.exe NIPS Set signatures /file **<путь_2>**

   где:

- **<путь_1>** — путь к каталогу установки Secret Net Studio. По умолчанию C:\Program Files\Secret Net Studio\. В случае изменения каталога установки продукта укажите путь к новому каталогу установки;
- **<путь_2>** — путь к загруженному файлу обновления для БРП.

Чтобы выполнить централизованное обновление БРП, необходимо разместить файл обновления в папке общего доступа, а затем настроить на компьютерах клиентов Secret Net Studio обновление по расписанию из данного каталога.

Для получения списка используемых сигнатур:

- На компьютере с установленным ПО клиента Secret Net Studio войдите в систему под именем учетной записи администратора. Откройте командную строку и выполните следующие команды:

  cd "**<путь_1>**"

  ScLocalCfg.exe NIPS Get signatures /file **<путь_3>**

  где **<путь_3>** — путь к файлу БРП.

Для просмотра количества используемых сигнатур:

- На компьютере с установленным ПО клиента Secret Net Studio войдите в систему под именем учетной записи администратора. Откройте командную строку и выполните следующие команды:

  cd "**<путь_1>**"

  ScAuthModCfg.exe /s

Документация

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