



**КОД**  
безопасности

Средство защиты информации

# Secret Net Studio

## Руководство администратора

Настройка и эксплуатация. Антивирус и средство обнаружения вторжений



© Компания "Код Безопасности", 2020. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

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

# Оглавление

<b>Список сокращений</b> .....	<b>4</b>
<b>Введение</b> .....	<b>5</b>
<b>Общие сведения</b> .....	<b>6</b>
Антивирус .....	6
Обнаружение и предотвращение вторжений .....	7
<b>Антивирус</b> .....	<b>8</b>
Настройка групповых политик .....	8
Настройка профилей сканирования .....	9
Сканирование по расписанию .....	15
Список исключений .....	17
Регистрация событий .....	18
Управление работой антивируса на защищаемых компьютерах .....	19
Просмотр лицензии .....	19
Управление карантинном .....	20
Утилита управления антивирусом .....	20
Устранение неисправностей .....	21
<b>Обнаружение и предотвращение вторжений</b> .....	<b>22</b>
Настройка групповых политик .....	22
Детекторы сетевых атак .....	23
Сигнатурные анализаторы .....	30
Блокировка телеметрии Windows .....	31
Контроль сетевых адаптеров .....	31
Управление работой механизма обнаружения вторжений .....	32
Просмотр лицензии .....	33
<b>Обновление</b> .....	<b>34</b>
Настройка обновления .....	34
Загрузка обновлений с сетевого ресурса .....	36
Утилита обновления .....	36
<b>Документация</b> .....	<b>38</b>

## Список сокращений

<b>БД</b>	База данных
<b>БРП</b>	База решающих правил
<b>ПО</b>	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.

# Глава 1

## Общие сведения

Secret Net Studio содержит следующие механизмы защиты от вредоносных программ:

- Антивирус;
- Обнаружение вторжений.

### Антивирус

Антивирус Secret Net Studio позволяет осуществлять проверку файловых объектов на наличие вредоносных программ по данным в базе сигнатур и на основе эвристического анализа. При проверке компьютера осуществляется сканирование жестких дисков, сетевых папок, внешних запоминающих устройств и др. Это позволяет обнаружить и заблокировать внешние и внутренние атаки, направленные на защищаемый компьютер.

Для антивирусной защиты возможно использование одного из следующих вариантов антивируса:

- Антивирус;
- Антивирус (технология ESET);
- Антивирус (технология Kaspersky).

Используемый вариант антивируса определяется лицензией Secret Net Studio (см. стр. [19](#)).

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
<b>Постоянная защита</b>	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
<b>Контекстное сканирование</b>	Проверка, запускаемая пользователем из контекстного меню в проводнике Windows
<b>Быстрое/полное сканирование</b>	Проверки, запускаемые администратором из программы управления или пользователем (только быстрое сканирование) на защищаемом компьютере
<b>Почтовый антивирус</b>	Проверка входящих и исходящих сообщений электронной почты на наличие вредоносных программ
<b>Сканирование по расписанию</b>	Проверка, запускаемая по расписанию. Пропущенное сканирование по расписанию принудительно запускается после восстановления работы компьютера. Если пропущено несколько одинаковых задач, будет запущена только одна из них
<b>Сканирование подключаемых носителей</b>	Автоматическая проверка съемных носителей при их подключении к компьютеру
<b>Выбор уровня антивирусной защиты</b>	Выбор уровня антивирусной защиты при сканировании

Функция	Описание
<b>Выбор объектов для сканирования</b>	Выбор проверяемых объектов (исполняемые процессы, загрузочные секторы, локальные диски, съемные носители, папки и файлы)
<b>Настройка списка исключений</b>	Создание списка объектов (файлов, папок и дисков), которые не проверяются при сканировании. 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)")
<b>Выполнение действий с обнаруженными вирусами</b>	Возможно выполнение следующих действий с зараженными объектами: удаление, изолирование (перемещение в карантин), блокировка доступа (только в режиме постоянной защиты). Выбор реакции на обнаруженные вредоносные программы осуществляется при настройке параметров антивируса
<b>Обновление антивирусных баз</b>	Автоматическое обновление баз с сервера обновлений, запускаемое в фоновом режиме, обновление баз вручную в панели управления работой антивируса (см. стр. 19) или из выбранной папки
<b>Контроль целостности сигнатур</b>	Проверка неизменности базы сигнатур при загрузке службы и при обновлении. Если обнаружено несанкционированное изменение базы, создается запись в журнале Secret Net Studio
<b>Управление карантином</b>	Просмотр помещенных в карантин файлов, восстановление и удаление файлов из карантина
<b>Отключение антивируса</b>	Возможность отключения антивируса в программе управления 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
<b>Детекторы сетевых атак</b>	Фильтрация входящего трафика, используемая для блокировки внешних атак. Детекторы атак функционируют на канальном, сетевом и транспортном уровнях модели OSI. Анализ входящих данных производится методом изучения поведения
<b>Сигнатурный анализ</b>	Контроль входящего и исходящего сетевого трафика на наличие элементов, зарегистрированных в базе решающих правил (БРП) и базах опасных веб-ресурсов. Атакующие компьютеры могут блокироваться на заданный промежуток времени
<b>Блокировка телеметрии Windows</b>	Блокировка сбора данных о системе средствами ОС Windows
<b>Контроль сетевых адаптеров</b>	Контроль включения неразборчивого режима

## Глава 2

# Антивирус

Настройка работы антивируса осуществляется централизованно в программе управления Secret Net Studio 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 на данном компьютере (запуск сканирования, работа с объектами в карантине и т.п.).

**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 представлены в следующих группах:

- профили сканирования — представляют собой наборы 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 папок, которые нужно исключить из проверки.

#### Для настройки параметров:

1. Вызовите программу управления Secret Net Studio.

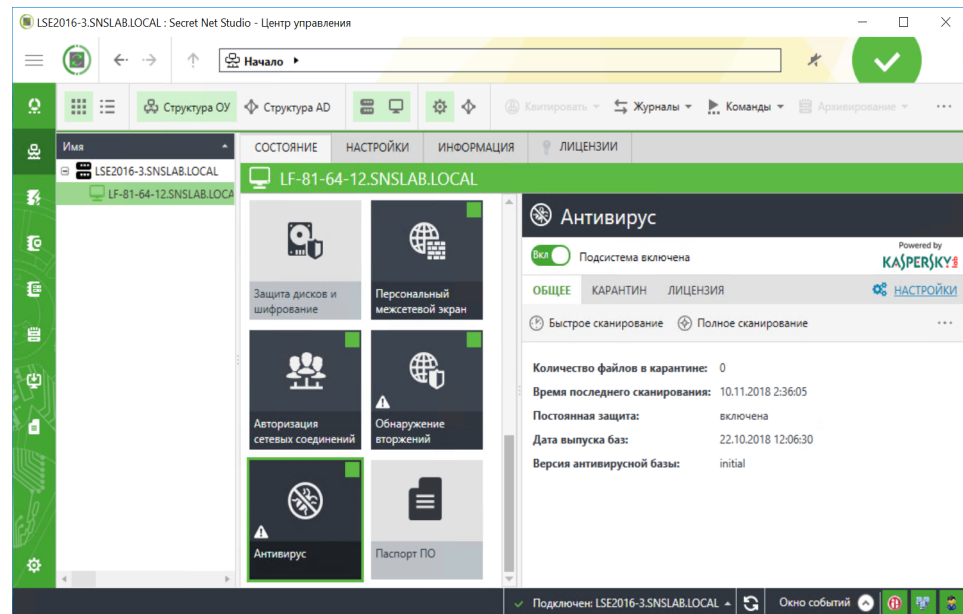
**Совет.** Для настройки параметров антивируса непосредственно на защищаемом компьютере вызовите программу "Локальный центр управления", в представлении "Компьютер" перейдите на вкладку "Настройки" и в разделе "Политики" выберите элемент "Антивирус". Далее настройка этого механизма выполняется так же,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

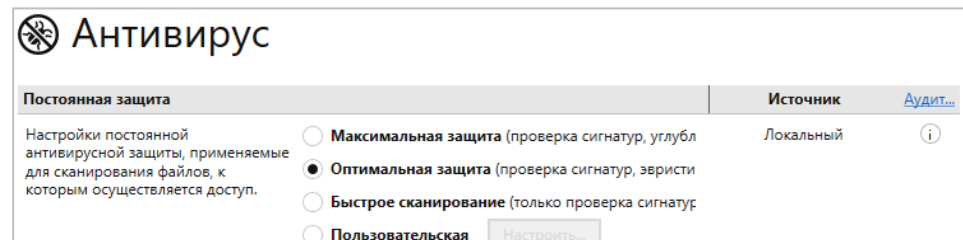


В правой части экрана появится информация о состоянии данного объекта.



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 левом верхнем 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
<b>Постоянная защита</b>	Этот профиль определяет параметры сканирования объектов системы в режиме реального времени
<b>Сканирование подключаемых носителей</b>	Этот профиль определяет параметры автоматической проверки всех подключаемых к компьютеру съемных носителей. Работает только совместно с профилем "Постоянная защита"
<b>Контекстное сканирование</b>	Этот профиль определяет параметры проверки, запускаемой пользователем из контекстного меню проводника Windows
<b>Полное сканирование</b>	Профиль определяет параметры проверки, запускаемой администратором из программы управления или по расписанию. В этом режиме выполняется проверка запущенных процессов, параметров автозапуска и загрузочных секторов

Название	Назначение
<b>Быстрое сканирование</b>	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
<b>Почтовый антивирус</b>	Профиль определяет параметры сканирования вложений сообщений электронной почты в Microsoft Outlook

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

Ниже подробно рассматривается порядок настройки профилей "Постоянная защита", "Сканирование подключаемых носителей" и "Почтовый антивирус". Настройка профилей "Контекстное сканирование", "Полное сканирование" и "Быстрое сканирование" выполняется аналогичным образом.

**Совет.** При настройке профилей "Полное сканирование" и "Быстрое сканирование" используйте кнопку "Дополнительная настройка", чтобы выполнить настройку всех имеющихся параметров сканирования (см. стр. 15).

## Постоянная защита

Постоянная защита	Источник	Аудит...
Настройки постоянной антивирусной защиты, применяемые для сканирования файлов, к которым осуществляется доступ.	<input type="radio"/> Максимальная защита (проверка сигнатур, углубл <input checked="" type="radio"/> <b>Оптимальная защита</b> (проверка сигнатур, эвристи <input type="radio"/> Быстрое сканирование (только проверка сигнатур <input type="radio"/> Пользовательская <input type="button" value="Настроить..."/> <input type="radio"/> Отключена	Локальный <input type="button" value="i"/>
Действия при обнаружении зараженных файлов:	<input type="checkbox"/> Лечить зараженные файлы <input type="checkbox"/> Удалять зараженные файлы <input checked="" type="checkbox"/> Удаляемые файлы поместить в карантин	

### Для настройки параметров постоянной защиты:

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

Параметр	Описание
<b>Максимальная защита</b>	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)
<b>Оптимальная защита</b>	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)

Параметр	Описание
<b>Быстрое сканирование</b>	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
<b>Пользовательская</b>	Проверка, выполняемая в соответствии с индивидуальными параметрами уровня постоянной защиты
<b>Отключена</b>	Сканирование объектов в реальном времени не выполняется

- Для настройки пользовательского профиля сканирования нажмите кнопку "Настроить" (см. стр. **15**).
- Выберите действия, которые необходимо выполнять при обнаружении зараженных файлов.

Параметр	Описание
<b>Удалять зараженные файлы</b>	Зараженные файлы будут удалены
<b>Удаляемые файлы поместить в карантин</b>	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. <b>19</b> )

**Примечание.** Настройка параметра "Лечить зараженные файлы" не влияет на работу антивируса.

- Нажмите кнопку-ссылку "Аудит" и настройте параметры регистрации событий антивируса (см. стр. **18**).
- Нажмите кнопку "Применить" внизу вкладки "Настройки".

## Сканирование подключаемых носителей

Сканирование подключаемых носителей
Аудит...

Настройки сканирования съемных носителей при их подключении к защищаемому компьютеру. i

Сканировать подключаемые носители

**Эвристика:**

- Углубленная эвристика
- Обычный режим
- Выключена

**Файлы:**

- Пропускать файлы более  МБ
- Максимальное время проверки файла  секунд

**Архивы:**

- Проверять архивы
- Пропускать архивы более  МБ
- Максимальное время проверки архива  секунд
- Максимальная вложенность в архиве

**Расширения файлов:**

- Сканировать все файлы
- Проверять только файлы с расширениями:
- Пример ввода: .ext,.ext2,.ext3
- Пропускать файлы с расширениями:
- Пример ввода: .ext,.ext2,.ext3

**Действия при обнаружении зараженных файлов:**

- Лечить зараженные файлы
- Удалять зараженные файлы
- Удаляемые файлы поместить в карантин

### Для настройки параметров сканирования:

1. Отметьте пункт "Сканировать подключаемые носители", чтобы включить сканирование.
2. Настройте значения параметров.

Параметр	Описание
<b>Эвристика</b>	<p>Выберите уровень эвристики.</p> <ul style="list-style-type: none"> <li>• "Углубленная эвристика" — высокая вероятность обнаружения неизвестных вирусов, высокая вероятность ложных срабатываний. Скорость сканирования при углубленной эвристике более низкая, чем при эвристике в обычном режиме;</li> <li>• "Обычный режим" — глубина эвристики ограничена: низкая вероятность обнаружения неизвестных вирусов, низкая вероятность ложных срабатываний;</li> <li>• "Выключена" — эвристическое сканирование будет выключено</li> </ul>
<b>Файлы</b>	<p>Настройте параметры исключаемых из проверок файлов.</p> <ul style="list-style-type: none"> <li>• "Пропускать файлы более" — при выборе параметра определите размер пропускаемых при сканировании файлов;</li> <li>• "Максимальное время проверки файла" — при выборе параметра время проверки каждого файла будет ограничено указанным числом секунд</li> </ul>

Параметр	Описание
<b>Архивы</b>	<p>Отметьте пункт "Проверять архивы" и настройте дополнительные параметры:</p> <ul style="list-style-type: none"> <li>"Пропускать архивы более" — при выборе параметра определите размер пропускаемых при сканировании архивов;</li> <li>"Максимальное время проверки архива" — при выборе параметра проверка архива будет прекращена по истечении указанного числа секунд;</li> <li>"Максимальная вложенность в архиве" — при выборе параметра не будут проверяться объекты, размещенные в иерархии объектов архива глубже указанного уровня вложенности.</li> </ul> <p>По умолчанию проверка архивов включена</p>
<b>Расширения файлов</b>	<p>Настройте параметры сканирования для файлов с разными расширениями.</p> <ul style="list-style-type: none"> <li>"Сканировать все файлы" — при сканировании будут проверяться все файлы на съемных носителях;</li> <li>"Проверять только файлы с расширениями" — будут проверяться только файлы с указанными расширениями. Укажите расширения файлов, используя запятую в качестве разделителя;</li> <li>"Пропускать файлы с расширениями" — файлы с указанными расширениями будут исключены из проверки. Укажите расширения файлов, используя запятую в качестве разделителя</li> </ul>
<b>Действия при обнаружении зараженных файлов</b>	<p>Выберите действия, которые нужно выполнять при обнаружении зараженных файлов (см. стр. <b>11</b>)</p>

3. Нажмите кнопку-ссылку "Аудит" и настройте параметры регистрации событий антивируса (см. стр. **18**).
4. Нажмите кнопку "Применить" внизу вкладки "Настройки".

### Почтовый антивирус

**Почтовый антивирус** Аудит...

Настройки сканирования вложений сообщений электронной почты.

Проверять входящие сообщения i

Проверять исходящие сообщения

Эвристика:

Углубленная эвристика

Обычный режим

Выключена

Действия при обнаружении зараженных файлов:

Лечить зараженные файлы

Удалять зараженные файлы

Удаляемые файлы поместить в карантин

Дополнительная настройка...

#### Для настройки параметров почтового антивируса:

1. Отметьте пункты "Проверять входящие сообщения" и "Проверять исходящие сообщения", чтобы включить сканирование. По умолчанию включена проверка только входящих сообщений.



**Внимание!** Пользователь может остановить работу почтового антивируса, отключив настройку SNS.AVMailAddin в Microsoft Outlook. В этом случае в панели управления работой антивируса (см. стр. **19**) появится соответствующее сообщение. При перезапуске приложения работа почтового антивируса будет восстановлена.

2. Настройте значения параметров эвристики (см. стр.12) и выберите действия, которые нужно выполнять при обнаружении зараженных файлов (см. стр.11).

**Примечание.** Исходящие сообщения электронной почты не будут отправлены при обнаружении в них угроз.

3. Для настройки параметров сканирования нажмите кнопку "Дополнительная настройка" и перейдите на вкладку "Файлы".

На экране появится следующий диалог.

4. Настройте значения параметров и нажмите кнопку "Сохранить".

Параметр	Описание
<b>Пропускать файлы более</b>	При выборе параметра определите размер пропускаемых при сканировании файлов
<b>Максимальное время проверки файла</b>	При выборе параметра время проверки каждого файла будет ограничено указанным числом секунд
<b>Проверять архивы</b>	Отметьте данный пункт для проверки архивов, вложенных в сообщения электронной почты, и настройте дополнительные параметры: <ul style="list-style-type: none"> <li>"Пропускать архивы более" — при выборе параметра определите размер пропускаемых при сканировании архивов;</li> <li>"Максимальное время проверки архива" — при выборе параметра проверка архива будет прекращена по истечении указанного числа секунд;</li> <li>"Максимальная вложенность в архиве" — при выборе параметра не будут проверяться объекты, размещенные в иерархии объектов архива глубже указанного уровня вложенности.</li> </ul> По умолчанию проверка архивов включена
<b>Автоматически помещать в карантин файлы с расширениями</b>	Отметьте данный пункт, чтобы помещать в карантин файлы с указанными расширениями. Укажите расширения файлов, используя запятую в качестве разделителя. Карантин почтового антивируса представляет собой отдельную папку на компьютере пользователя

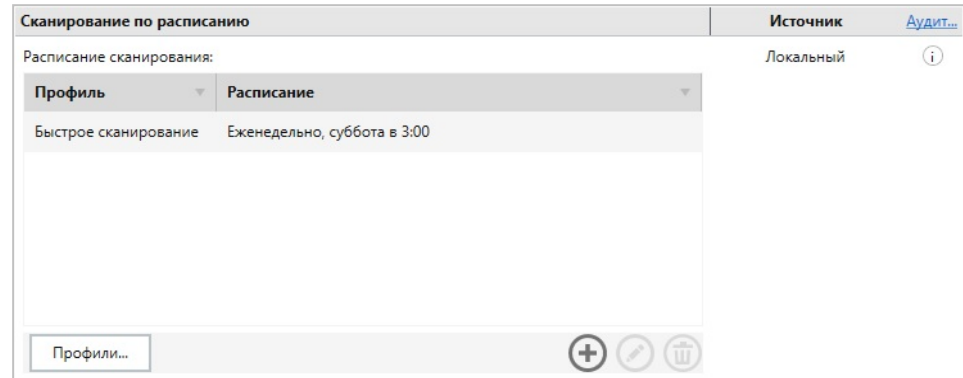
**Примечание.** На вкладках "Основные" и "Объекты сканирования" можно изменить параметры, описанные в пп. 1 и 2 данной процедуры.

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

## Сканирование по расписанию

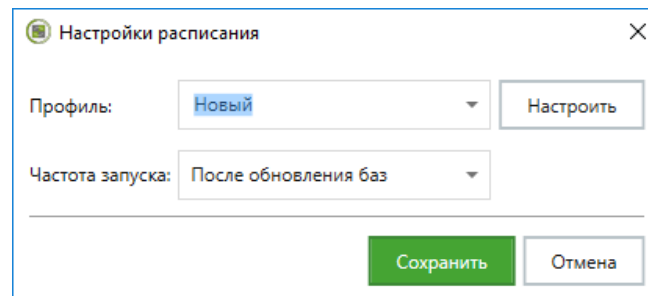
### Для настройки сканирования по расписанию:

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.



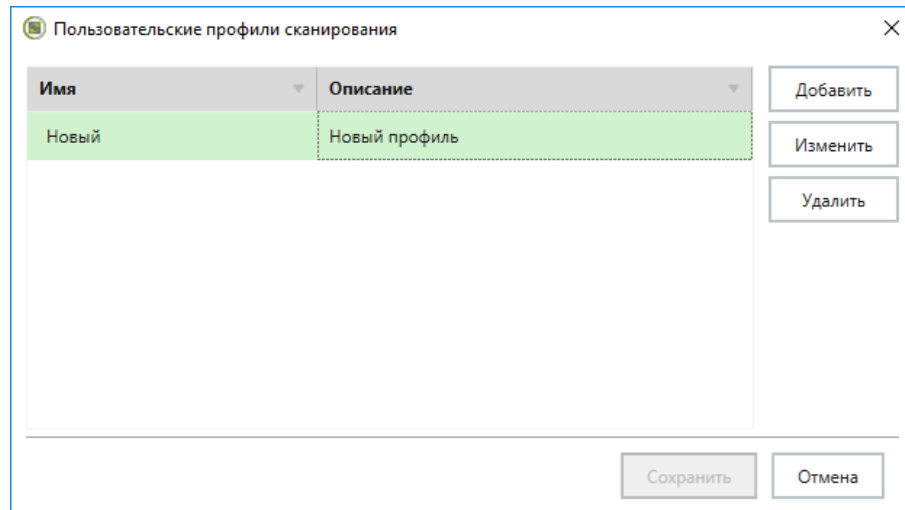
3. Выберите профиль сканирования, частоту запуска проверки и нажмите кнопку "Сохранить".

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

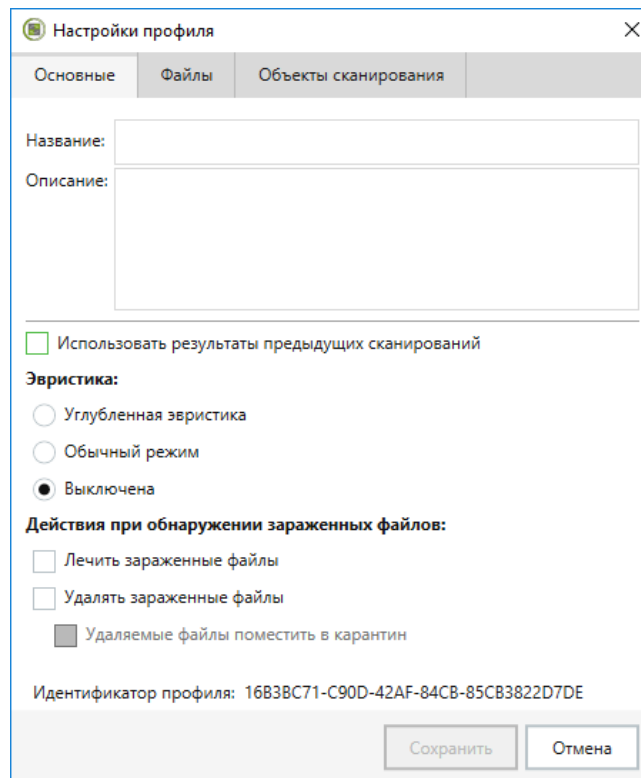
4. Нажмите кнопку "Применить" внизу вкладки "Настройки".

### 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.

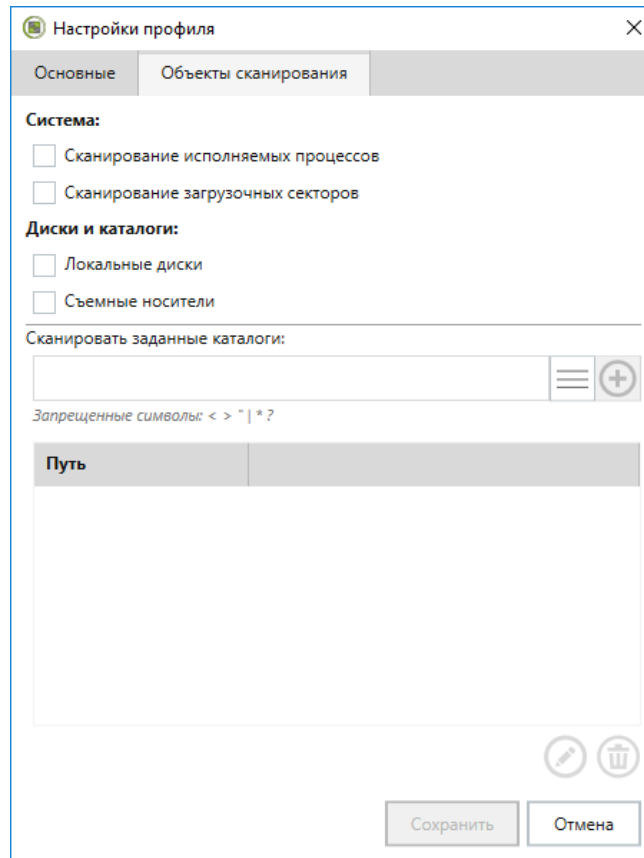


3. На вкладке "Основные" введите название и описание профиля сканирования и укажите значения параметров (см. стр. [12](#)).

**Примечание.** Функция "Использовать результаты предыдущих сканирований" не применяется в Secret Net Studio версии 8.6.

4. На вкладке "Файлы" настройте параметры сканирования для файлов и выберите действия, которые будут выполнены при обнаружении зараженных объектов (см. стр. [12](#)).
5. Перейдите на вкладку "Объекты сканирования".  
Появится следующий диалог.





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

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

Параметр	Описание
<b>Система</b>	Выберите объекты, проверку которых нужно провести
<b>Диски и каталоги</b>	<ul style="list-style-type: none"> <li>Выберите диски и папки, которые необходимо проверять при запуске сканирования.</li> <li>Укажите путь к папке, 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 папки из списка нажмите "Удалить"</li> </ul>

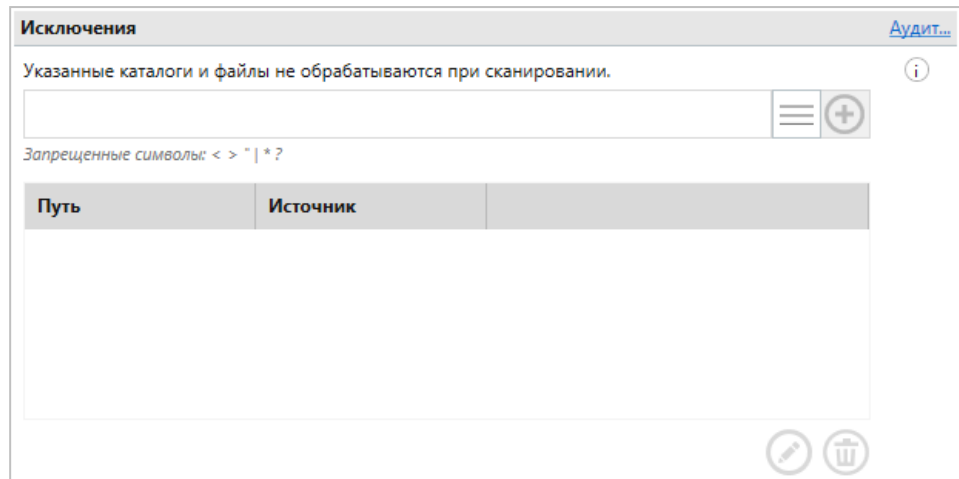
7. Нажмите кнопку "Применить" внизу вкладки "Настройки".

## Список исключений

Объекты из списка исключений пропускаются при сканировании всегда, независимо от используемого профиля сканирования.

### Для настройки списка исключений:

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



2. Чтобы внести в список папку или файл, укажите путь к объекту и нажмите кнопку "Добавить". При необходимости используйте переменные среды окружения из раскрывающегося списка.



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

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

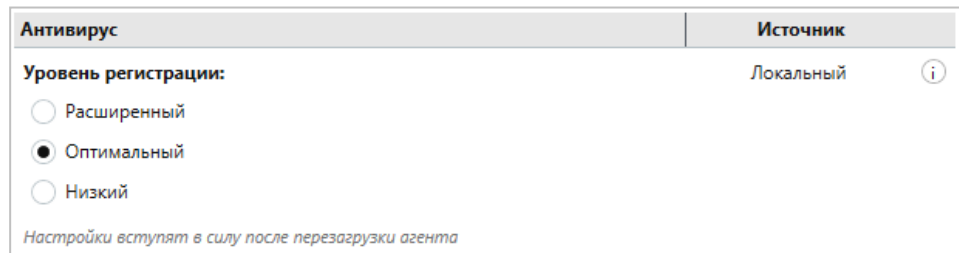
**Совет.** Для изменения пути к объекту выберите его в списке и нажмите кнопку "Редактировать". Для удаления объекта из списка нажмите кнопку "Удалить".

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;
- запуск процедуры обновления антивирусных баз;
- просмотр и управление содержимым карантина;
- просмотр информации о лицензии.

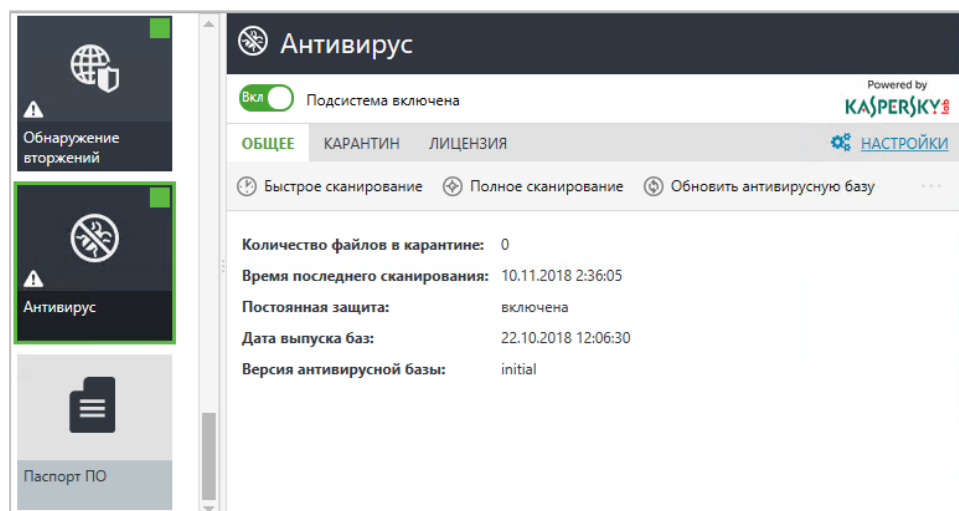
### Для управления работой антивируса:

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.



**Примечание.** В заголовке панели отображаются различные сообщения и предупреждения (например, предупреждение об истечении срока действия лицензии или сообщение об ошибке).

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. 34).

**Примечание.** Настройка параметров сканирования выполняется при настройке политик (см. стр. 8). Нажмите кнопку-ссылку "НАСТРОЙКИ", чтобы перейти к настройке политики антивируса.

### Просмотр лицензии

На вкладке "Лицензия" можно посмотреть информацию о сроках действия лицензии и технической поддержки.

**Примечание.** Для просмотра подробной информации о лицензии нажмите кнопку-ссылку "Перейти к информации о лицензии".

Зарегистрированная лицензия Secret Net Studio определяет вариант антивируса, используемый в данный момент: Антивирус, Антивирус (технология ESET) или Антивирус (технология Kaspersky).

**Примечание.** Одновременно может быть применена лицензия только на один вариант антивируса.

При смене лицензии используемого варианта антивируса на лицензию другого варианта происходит автоматическая установка нового антивируса и его баз, предыдущий антивирус при этом будет удален. Уже запущенные задания сканирования будут выполнены и корректно завершены предыдущим антивирусом до его удаления.

За 30 дней до истечения срока действия лицензии в программе управления Secret Net Studio начнут появляться ежедневные предупреждения об этом. После истечения срока действия зарегистрированной лицензии Антивирус и Антивирус (технология Kaspersky) перестанут получать обновления, а Антивирус (технология ESET) прекратит свою работу.

## Управление карантином

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

### Для управления карантином:

1. В панели управления работой антивируса перейдите на вкладку "Карантин".
2. Выполните нужные действия.

Кнопка	Описание
<b>Запросить</b>	Будет загружен список файлов, помещенных в карантин на данном компьютере
<b>Восстановить</b>	Выбранные файлы будут восстановлены из карантина. Чтобы восстановить сразу несколько файлов, выделите их в списке объектов и нажмите кнопку "Восстановить"
<b>Удалить</b>	Выбранный файл, находящийся в карантине, будет удален
<b>Удалить все</b>	Все файлы, находящиеся в карантине, будут удалены



**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 `sns.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 `sns.av_cli.exe`.

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

```
sns.av_cli.exe
```

### Управление карантином

Доступны следующие команды управления карантином.

- Отобразить объекты в карантине:

```
sns.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:

```
sns.av_cli.exe -c:remove_file_from_quarantine -quarantine_file_id:<идентификатор файла>
```

Например:

```
sns.av_cli.exe -c:remove_file_from_quarantine -quarantine_file_id:1
```

- Удалить старые файлы из карантина:

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

Например:

```
sns.av_cli.exe -c:remove_files_from_quarantine_older_than -days:2
```

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

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

Например:

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

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

С помощью утилиты sns.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 нужно установить антивирус Secret Net Studio и с помощью утилиты sns.av\_cli.exe выполнить команду восстановления файла из карантина, указав путь к файлу с расширением .quarantine.

## Устранение неисправностей

При возникновении проблем во время работы Secret Net Studio (например, медленная работа системы) следует изучить информацию о процессах, выполняемых антивирусом Secret Net Studio.

### Для просмотра информации о процессах:

1. Запустите "Диспетчер задач" ОС Windows и откройте вкладку "Процессы".
2. Каждое сканирование антивируса Secret Net Studio вызывает независимый процесс вида SNS.scan\_worker.exe. Найдите процессы в таблице и изучите подробную информацию о них в колонке "Командная строка". Строка может содержать следующие включения:
  - on\_access — процесс постоянной защиты;
  - on\_demand — процесс сканирования по требованию и по расписанию;
  - on\_mount — процесс сканирования подключаемых носителей;
  - on\_mail — процесс сканирования вложений сообщений электронной почты.

## 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 работой механизма обнаружения 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;
- блокировка доступа к опасным веб-ресурсам (фишинговые URL-адреса, ботнет URL-адреса, URL-адреса вымогателей, вредоносные IP-адреса). Базы опасных веб-ресурсов предоставляет Лаборатория Касперского при наличии соответствующей лицензии Secret Net Studio (см. стр. 33);
- блокировка сбора данных о системе средствами ОС Windows;
- контроль сетевых адаптеров.

### Для настройки и управления работой механизма:

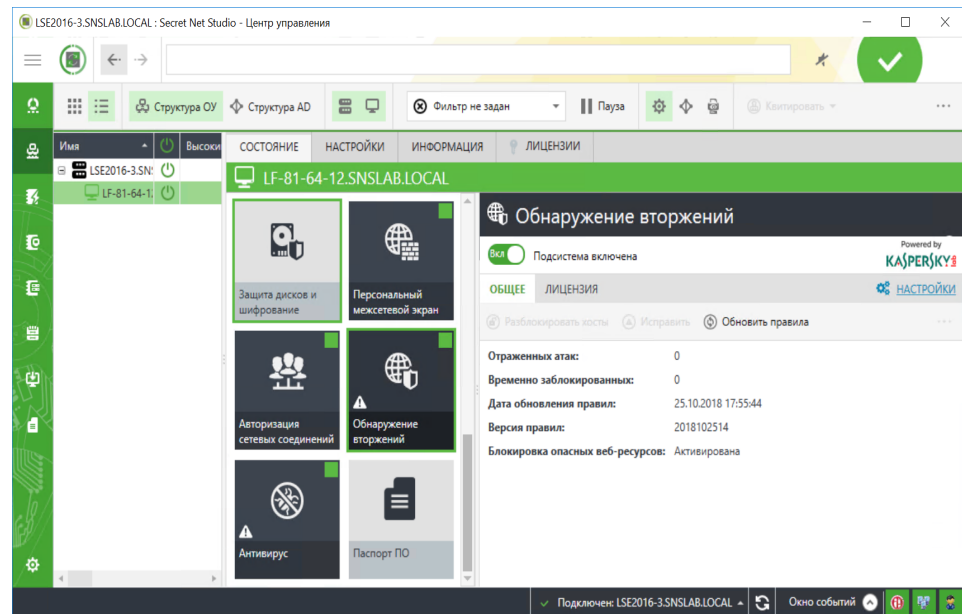
1. Вызовите программу управления Secret Net Studio.

**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.

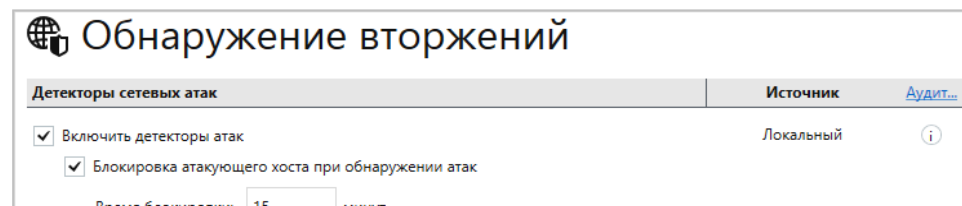
2. Откройте представление "Компьютеры", в левой части экрана в списке объектов управления найдите нужный компьютер (домен, сервер безопасности), вызовите для него контекстное меню и выберите в нем команду "Свойства".

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".

## Детекторы сетевых атак

Чтобы использовать детекторы сетевых атак, настройте их параметры, а затем включите нужные детекторы.

### Для настройки детекторов:

1. Настройте общие параметры детекторов сетевых атак (см. ниже).
2. При использовании детектора DoS настройте списки сетевых сервисов (стр.26).
3. Настройте параметры работы каждого используемого детектора (см. стр.25).

### Настройка общих параметров детекторов

#### Для настройки общих параметров:

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

## Обнаружение вторжений

Детекторы сетевых атак	Источник																								
<input checked="" type="checkbox"/> Включить детекторы атак	Локальный <span style="float: right;">(i)</span>																								
<input checked="" type="checkbox"/> Блокировка атакующего хоста при обнаружении атак Время блокировки: <input type="text" value="15"/> минут																									
<input checked="" type="checkbox"/> Использовать черный список IP-адресов																									
Белый список IP-адресов: <input style="width: 100%;" type="text"/> <span style="float: right;">+</span> <small>Указанные IP-адреса не будут блокироваться</small>																									
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Путь</th> <th>Источник</th> </tr> </thead> <tbody> <tr> <td style="height: 40px;"> </td> <td> </td> </tr> </tbody> </table> <div style="text-align: right;"> <span style="margin-right: 10px;">✎</span> <span>🗑</span> </div>	Путь	Источник																							
Путь	Источник																								
Используемые <a href="#">сетевые сервисы</a> :																									
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Область адресации</th> <th>Протокол</th> <th>Порты</th> </tr> </thead> <tbody> <tr> <td colspan="3"><b>Сервис : Получатель ICMP</b></td> </tr> <tr> <td>AF_INET</td> <td>1</td> <td>*</td> </tr> <tr> <td>AF_INET6</td> <td>58</td> <td>*</td> </tr> <tr> <td colspan="3"><b>Сервис : SMB-сервер</b></td> </tr> <tr> <td>Любая</td> <td>IPPROTO_TCP</td> <td>139; 445</td> </tr> <tr> <td colspan="3"><b>Сервис : RDP-сервер</b></td> </tr> <tr> <td>Любая</td> <td>IPPROTO_TCP</td> <td>3389</td> </tr> </tbody> </table> <div style="text-align: right;">✎</div>	Область адресации	Протокол	Порты	<b>Сервис : Получатель ICMP</b>			AF_INET	1	*	AF_INET6	58	*	<b>Сервис : SMB-сервер</b>			Любая	IPPROTO_TCP	139; 445	<b>Сервис : RDP-сервер</b>			Любая	IPPROTO_TCP	3389	
Область адресации	Протокол	Порты																							
<b>Сервис : Получатель ICMP</b>																									
AF_INET	1	*																							
AF_INET6	58	*																							
<b>Сервис : SMB-сервер</b>																									
Любая	IPPROTO_TCP	139; 445																							
<b>Сервис : RDP-сервер</b>																									
Любая	IPPROTO_TCP	3389																							

2. Чтобы активировать детекторы сетевых атак, отметьте пункт "Включить детекторы атак" и настройте параметры, общие для всех детекторов.

Параметр	Описание
<b>Блокировка атакующего хоста при обнаружении атак</b>	При включении детекторов атак данная функция активируется по умолчанию для всех детекторов. В этом случае IP-адрес атакующего хоста будет заблокирован
<b>Время блокировки ... минут</b>	Длительность блокировки хоста. По умолчанию составляет 15 минут
<b>Использовать черный список IP-адресов</b>	При включении детекторов атак данная функция активируется по умолчанию для всех детекторов. В этом случае будут заблокированы вредоносные IP-адреса из базы опасных веб-ресурсов Kaspersky
<b>Белый список IP-адресов</b>	<p>Введите IP-адрес (например, 192.168.100.25) или маску подсети в нотации CIDR (например, 192.168.100.0/24) и нажмите кнопку "Добавить". IP-адрес будет добавлен в белый список. Адреса из белого списка не блокируются детекторами атак.</p> <p>Чтобы изменить или удалить IP-адрес, выделите его в таблице и нажмите кнопку "Редактировать" или "Удалить".</p> <p>Если белый список сформирован средствами групповой политики, его редактирование на уровне отдельного компьютера запрещено. При этом пополнение белого списка будет доступно (только для данного компьютера)</p>



После активации детекторов атак работать будут только те детекторы, которые также включены и настроены (см. ниже).

## Включение и настройка детекторов атак

### Для включения детекторов:

1. Включите необходимые детекторы и настройте параметры их работы.

Детектор, Параметр	Описание
<b>Сканирование портов</b>	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
<b>ARP-spoofing</b>	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: <ul style="list-style-type: none"> <li>• Игнорировать;</li> <li>• Логировать — записывать событие аудита;</li> <li>• Логировать и посылать ARP-ответы;</li> <li>• Активный детектор ARP-spoofing — на каждый ARP-ответ без ARP-запроса будет выдан ARP-запрос;</li> <li>• 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</li> </ul>
<b>SYN-FLOOD</b>	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. 24). Чтобы точно 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

Детектор, Параметр	Описание
<b>Аномальный трафик</b>	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. 24). Чтобы точно 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
<b>DDoS</b>	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
<b>DoS</b>	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. Данное значение не действует для настроенных сетевых сервисов
Максимальный размер данных, при превышении которого будет детектирована атака	По достижении указанного размера отправляемых с сервера данных за указанный отрезок времени сервер считается атакующим. Данное значение не действует для настроенных сетевых сервисов
Замедлять трафик с атакующего хоста	Отметьте данный пункт, чтобы автоматически уменьшать скорость передачи данных с атакующего сервера, специально теряя часть пакетов. После замедления трафика в 2 раза атакующий хост будет заблокирован
Сервис	В таблице отображаются сетевые сервисы, настроенные ранее (см. стр. 26). Для каждого сервиса укажите допустимое максимальное количество пакетов и их максимальный размер в килобайтах. Указанные значения будут действовать только для данного сервиса

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

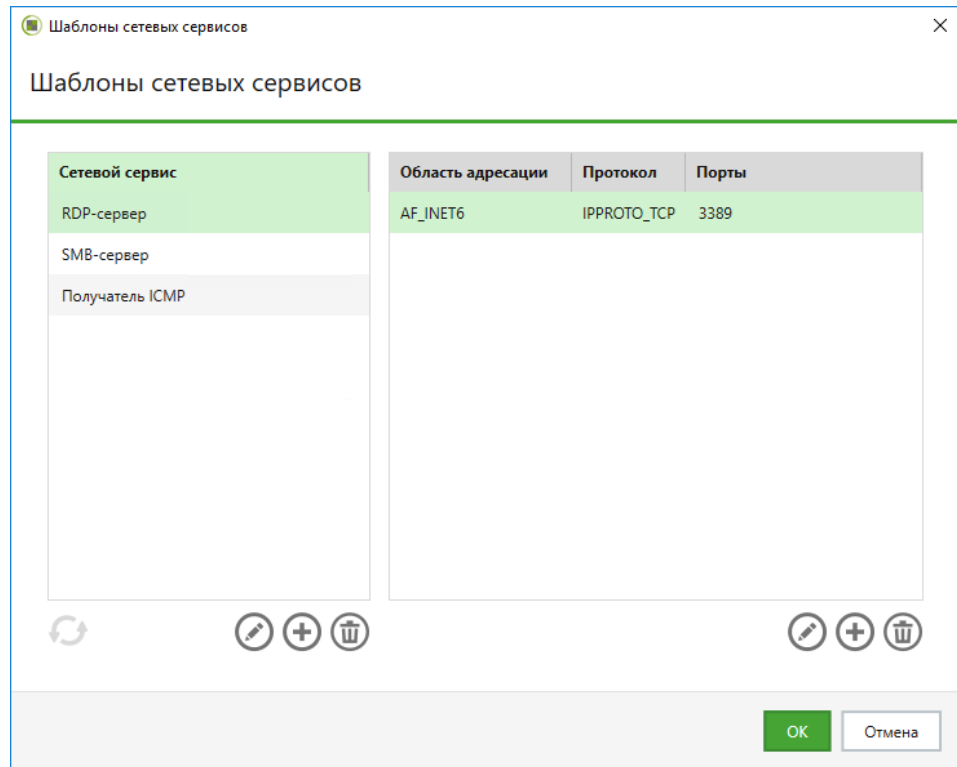
### Настройка сетевых сервисов

Чтобы можно было указывать индивидуальные параметры срабатывания детектора DoS для разных протоколов и портов, настройте список сетевых сервисов. Сетевые сервисы могут быть созданы с помощью шаблонов.

**Примечание.** Список шаблонов сетевых сервисов является общим для всех компьютеров, входящих в домен безопасности.

**Для управления шаблонами сетевых сервисов:**

1. В области настройки параметров нажмите кнопку-ссылку "сетевые сервисы". На экране появится следующий диалог.



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

- Нажмите кнопку "Редактировать", чтобы изменить имя шаблона.
- Нажмите кнопку "Удалить" для удаления выбранного шаблона.
- Нажмите кнопку "Обновить", чтобы обновить список шаблонов.

**Совет.** Для настройки шаблона 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.

2. Для создания нового шаблона сетевого сервиса нажмите кнопку "Добавить" в левой части диалога, в появившемся диалоге укажите имя сервиса и нажмите кнопку "Добавить".

Шаблон сетевого сервиса появится в списке.

3. Чтобы настроить созданный шаблон, выделите его в левой части диалога и выполните нужные действия, используя кнопки в правой части диалога. Например, для добавления новой настройки сервиса нажмите кнопку "Добавить".

На экране появится следующий диалог.

The screenshot shows a dialog box titled "Настройка для сетевого сервиса "RDP-сервер"". It contains three input fields: "Область адресации:" with a dropdown menu showing "AF\_INET", "Протокол:" with a text box containing "1", and "Порты:" with a text box containing "\*". At the bottom right, there are two buttons: "Добавить" (Add) and "Отмена" (Cancel).

4. Укажите нужные значения параметров и нажмите кнопку "Добавить".

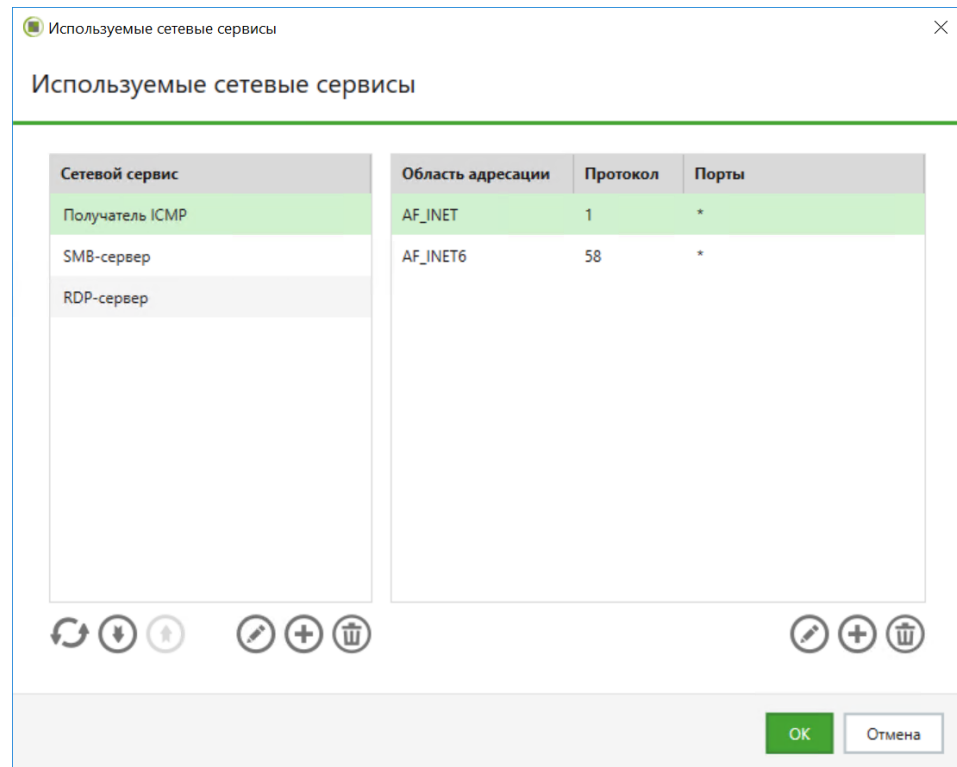
Параметр	Описание
<b>Область адресации</b>	Выберите область адресации для сетевого сервиса: <ul style="list-style-type: none"> <li>AF_INET — семейство протоколов IPv4;</li> <li>AF_INET6 — семейство протоколов IPv6;</li> <li>любая — семейства протоколов IPv4 и IPv6</li> </ul>
<b>Протокол</b>	Укажите номер протокола транспортного уровня, для которого действует сервис
<b>Порты</b>	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

5. Для сохранения изменений нажмите кнопку "ОК" в диалоге настройки шаблонов сетевых сервисов, затем нажмите кнопку "Применить" внизу вкладки "Настройки".

#### Для управления сетевыми сервисами:

1. В области настройки параметров механизма обнаружения вторжений нажмите кнопку "Редактировать", расположенную под таблицей с используемыми сетевыми сервисами.

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 изменить название сетевого сервиса. Это действие не влияет на шаблоны сервиса.
- Нажмите кнопку "Удалить" для удаления выбранного сетевого сервиса.
- Нажмите кнопку "Обновить", чтобы обновить настройки сетевых сервисов, добавленных из списка шаблонов.

**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.

2. 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. Настройка выполняется аналогично настройке шаблонов сетевых сервисов (см. стр. 28).
3. Для сохранения изменений нажмите кнопку "ОК" в диалоге настройки используемых сетевых сервисов, затем нажмите кнопку "Применить" внизу вкладки "Настройки".

Новые сервисы появятся в таблице.

## Сигнатурные анализаторы

### Для настройки анализаторов:

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

Сигнатурные анализаторы
[Аудит...](#)

Включить сигнатурные анализаторы (i)

**Анализаторы**

Анализатор HTTP

Максимальный уровень  
 Оптимальный уровень  
 Базовый уровень

Контроль входящего трафика

Контроль исходящего трафика

Список портов:

80; 8080; 3128

Блокировать фишинговые URL-адреса

Блокировать ботнет сети

Белый список URL-адресов:

+

Указанные веб-адреса не будут блокироваться

Путь	Источник
test.ru	Локальный

2. Настройте параметры.

Параметр	Описание
<b>Включить сигнатурные анализаторы</b>	Отметьте данный пункт, чтобы активировать сигнатурные анализаторы
<b>Анализатор HTTP</b>	Отметьте данный пункт, чтобы включить анализатор HTTP-трафика. Выберите уровень защиты анализатора: <ul style="list-style-type: none"> <li>Максимальный уровень — проверяются все типы сигнатур;</li> <li>Оптимальный уровень — проверяются основные сигнатуры;</li> <li>Базовый уровень — проверяются только критически важные сигнатуры</li> </ul>
<b>Контроль входящего трафика</b>	Входящий трафик будет контролироваться на наличие сигнатур, зарегистрированных в базе решающих правил

Параметр	Описание
<b>Контроль исходящего трафика</b>	Исходящий трафик будет контролироваться на наличие сигнатур, зарегистрированных в базе решающих правил
<b>Список портов</b>	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. При использовании в организации прокси-сервера для корректной работы анализатора в этот список необходимо добавить порт прокси-сервера
<b>Блокировать фишинговые URL-адреса</b>	Отметьте данный пункт, чтобы блокировать URL-адреса фишинговых сайтов, находящихся в базе опасных веб-ресурсов Kaspersky
<b>Блокировать ботнет сети</b>	Отметьте данный пункт, чтобы блокировать ботнет URL-адреса, находящиеся в базе опасных веб-ресурсов Kaspersky
<b>Белый список URL-адресов</b>	Введите URL-адрес без префикса протокола и параметров (например, test.ru) или маску URL-адреса (например, *.test.ru, где * — любая последовательность символов) и нажмите кнопку "Добавить". Адрес будет добавлен в белый список. Адреса из белого списка не будут блокироваться сигнатурными анализаторами при обработке списков опасных веб-ресурсов Kaspersky. Чтобы изменить или удалить URL-адрес, выделите его в таблице и нажмите кнопку "Редактировать" или "Удалить". Если белый список сформирован средствами групповой политики, его редактирование на уровне отдельного компьютера запрещено. При этом пополнение белого списка будет доступно (только для данного компьютера)

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

## Блокировка телеметрии Windows

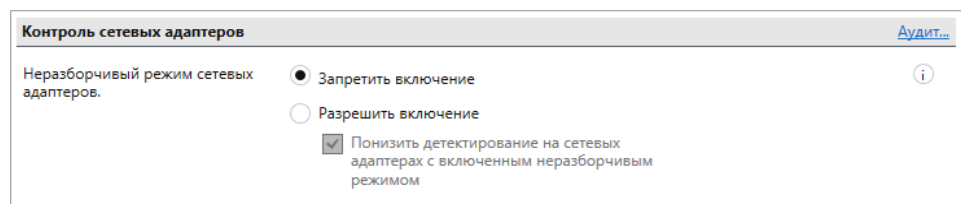
Чтобы заблокировать сбор данных о системе средствами ОС Windows и отправку этих данных в корпорацию Microsoft, в области настройки параметров механизма обнаружения вторжений перейдите к разделу "Блокировка телеметрии Windows" и отметьте пункт "Включить блокировку телеметрии Windows".

## Контроль сетевых адаптеров

При включенном неразборчивом режиме сетевой адаптер принимает все пакеты вне зависимости от того, кому они адресованы. Secret Net Studio позволяет контролировать изменение режима работы сетевых адаптеров на защищаемом компьютере.

### Для настройки контроля неразборчивого режима:

1. В области настройки параметров механизма обнаружения вторжений перейдите к разделу "Контроль сетевых адаптеров".



2. Настройте параметры:

- "Запретить включение" — включение неразборчивого режима для сетевых адаптеров на защищаемом компьютере будет недоступно;

- "Разрешить включение" — неразборчивый режим будет доступен для включения на защищаемом компьютере;
- "Понизить детектирование на сетевых адаптерах с включенным неразборчивым режимом" — будет изменен алгоритм обнаружения атак на сетевых адаптерах с включенным неразборчивым режимом для исключения ложных срабатываний детекторов сетевых атак.

## Управление работой механизма обнаружения вторжений

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

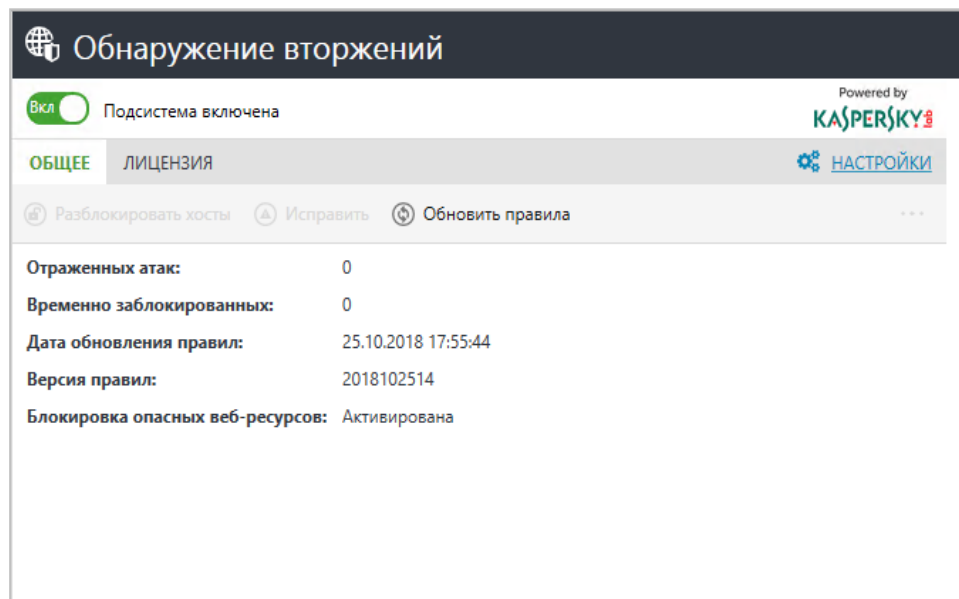
### Для управления работой механизма:

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.



**Примечание.** В заголовке панели отображаются различные сообщения и предупреждения (например, предупреждение об истечении срока действия лицензии или сообщение об ошибке).

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
<b>Разблокировать хосты</b>	Все хосты, заблокированные механизмом обнаружения вторжений на данном компьютере, будут разблокированы
<b>Исправить</b>	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
<b>Обновить правила</b>	Будет выполнено обновление базы решающих правил и баз опасных веб-ресурсов (см. стр. 34)

**Примечание.** Нажмите кнопку-ссылку "НАСТРОЙКИ", чтобы перейти к настройке политик механизма обнаружения вторжений (см. стр. 22).



## Просмотр лицензии

На вкладке "Лицензия" можно посмотреть информацию о сроках действия лицензии и технической поддержки.

**Примечание.** Для просмотра подробной информации о лицензии нажмите кнопку-ссылку "Перейти к информации о лицензии".

Зарегистрированная лицензия Secret Net Studio определяет для компонента "Обнаружение вторжений" наличие или отсутствие функции блокировки доступа к опасным веб-ресурсам с использованием баз Kaspersky.

За 30 дней до истечения срока действия лицензии в программе управления Secret Net Studio начнут появляться ежедневные предупреждения об этом. После истечения срока действия зарегистрированной лицензии компонент "Обнаружение вторжений" продолжит работу, но базы решающих правил и опасных веб-ресурсов перестанут получать обновления.

## Глава 4

# Обновление

Для полноценной защиты от вредоносных программ в Secret Net Studio предусмотрена возможность автоматического обновления на защищаемых компьютерах антивирусных баз, базы решающих правил и баз опасных веб-ресурсов для механизма обнаружения вторжений. Также имеется возможность выполнить автономное обновление антивирусных баз вручную средствами специальной утилиты (см. стр.36).

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
<b>Без прокси</b>	Выберите данный пункт, если соединение с сервером обновлений происходит напрямую (без прокси-сервера)
<b>Использовать системные настройки прокси</b>	Используется автоматическое определение прокси-сервера (не рекомендуется)
<b>Ручная настройка прокси-сервера</b>	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, `https://192.168.10.1` или `https://us.domain.loc`;
  - путь к сетевой или локальной папке с обновлениями (см. стр. 36). 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. 36).

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

## Загрузка обновлений с сетевого ресурса

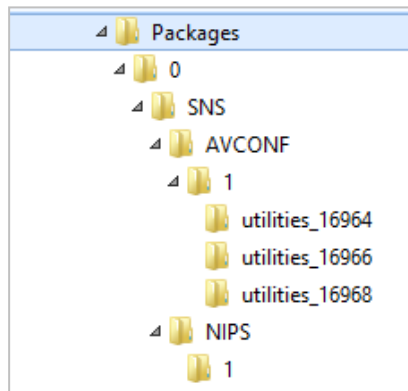
### Для загрузки обновлений с сетевого ресурса:

1. Установите ПО сервера обновлений на компьютере с доступом к интернету и настройте обновление с сервера компании "Код Безопасности" (см. документ [9]).
2. Создайте сетевой ресурс и предоставьте авторизованным пользователям доступ к нему.
3. Настройте клиенты Secret Net Studio или каскадные серверы обновлений на обновление из созданного сетевого ресурса.
4. Настройте синхронизацию содержимого папки C:\ProgramData\Security Code\Secret Net Studio\Server\Update Server\Packages, находящейся на установленном сервере обновлений, с созданным 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 содержимое папки C:\ProgramData\Security Code\Secret Net Studio\Server\Update Server\Packages или синхронизируемой с ней папки (см. выше) на съемный носитель информации и перенесите это содержимое на сервер обновлений в закрытой сети в аналогичную папку.



**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.

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"



**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 `sns.av_cli.exe` (см. стр. 20) или программы управления сервером обновлений (см. документ [9]).

## Документация

<b>1.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Принципы построения	RU.88338853.501400.001 91 1
<b>2.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Установка, обновление, удаление	RU.88338853.501400.001 91 2
<b>3.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Основы и базовая защита	RU.88338853.501400.001 91 3
<b>4.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Централизованное управление, мониторинг и аудит	RU.88338853.501400.001 91 4
<b>5.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Локальная защита	RU.88338853.501400.001 91 5
<b>6.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Сетевая защита	RU.88338853.501400.001 91 6
<b>7.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Антивирус и средство обнаружения вторжений	RU.88338853.501400.001 91 7
<b>8.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Настройка и эксплуатация. Доверенная среда	RU.88338853.501400.001 91 8
<b>9.</b> Средство защиты информации Secret Net Studio. Руководство администратора. Сервер обновлений. Установка и настройка	
<b>10.</b> Средство защиты информации Secret Net Studio. Руководство пользователя	RU.88338853.501400.001 92