



КОД БЕЗОПАСНОСТИ

Средство защиты информации

# Secret Net Studio

**Руководство администратора**

Настройка и эксплуатация. Сетевая защита

RU.88338853.501400.001 91 6



## КОД БЕЗОПАСНОСТИ

© Компания "Код Безопасности", 2018. 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**

Web: **http://www.securitycode.ru**

# Оглавление

<b>Список сокращений</b> .....	<b>4</b>
<b>Введение</b> .....	<b>5</b>
<b>Общие сведения</b> .....	<b>6</b>
Межсетевой экран .....	6
Механизм авторизации сетевых соединений .....	6
<b>Межсетевой экран</b> .....	<b>8</b>
Порядок обработки сетевых пакетов .....	9
Управление приоритетом правила .....	10
Управление правилами доступа .....	10
Создание правила доступа .....	11
Управление работой правил доступа .....	17
Удаление правила доступа .....	18
Управление системными правилами .....	18
Создание системного правила .....	19
Управление работой системных правил .....	21
Управление прикладными правилами .....	22
Создание прикладного правила .....	23
Управление работой прикладных правил .....	27
Управление правилами фильтрации сетевого потока .....	27
Подключение к серверу управления .....	28
Создание и редактирование правил фильтрации сетевого потока .....	29
Просмотр правил фильтрации сетевого потока .....	31
Удаление правила фильтрации сетевого потока .....	32
Управление сетевыми протоколами .....	32
Настройка режима защиты протокола ICMP .....	33
Управление сетевыми сервисами .....	34
Настройка режима обучения .....	35
Управление работой меж сетевого экрана на защищаемых компьютерах .....	37
<b>Авторизация сетевых соединений</b> .....	<b>38</b>
Настройка защиты соединений для группы everyone .....	39
Настройка параметров обработки пакетов .....	39
Настройка SMB-соединения .....	40
Настройка параметров получения IP-адресов компьютера .....	41
Управление работой механизма авторизации соединений на защищаемых компьютерах .....	42
<b>Документация</b> .....	<b>44</b>

## Список сокращений

<b>AD</b>	Active Directory
<b>FAT</b>	File Allocation Table
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>LFN</b>	Long File Name
<b>MMC</b>	Microsoft Management Console
<b>NTFS</b>	New Technology File System
<b>PCMCIA</b>	Personal Computer Memory Card International Association
<b>PIN</b>	Personal Identification Number
<b>PKI</b>	Public Key Infrastructure
<b>RPC</b>	Remote Procedure Call
<b>RTF</b>	Rich Text Format
<b>TCP</b>	Transmission Control Protocol
<b>USB</b>	Universal Serial Bus
<b>АРМ</b>	Автоматизированное рабочее место
<b>БД</b>	База данных
<b>ЗПС</b>	Замкнутая программная среда
<b>КЦ</b>	Контроль целостности
<b>ЛБД</b>	Локальная база данных
<b>МД</b>	Модель данных
<b>ОС</b>	Операционная система
<b>ПАК</b>	Программно-аппаратный комплекс
<b>ПО</b>	Программное обеспечение
<b>ЦБД</b>	Центральная база данных

# 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 следующими механизмами защиты:

- персональный межсетевой экран;
- авторизация сетевых соединений.

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](mailto: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](mailto:education@securitycode.ru)).

# Глава 1

## Общие сведения

В состав сетевой защиты Secret Net Studio входят следующие защитные подсистемы:

- межсетевой экран;
- механизм авторизации сетевых соединений.

### Межсетевой экран

Межсетевой экран предназначен для защиты серверов и рабочих станций локальной сети от несанкционированного доступа и разграничения сетевого доступа в информационных системах.

Механизм защиты обеспечивает фильтрацию сетевого трафика на сетевом, транспортном и прикладном уровнях. Фильтрация трафика осуществляется на основе формируемых для приложений правил.

Межсетевой экран выполняет следующие функции:

Функция	Описание
<b>Фильтрация сетевого трафика</b>	Для фильтрации сетевого трафика используются специальные правила, обладающие широким диапазоном настроек. Сетевые соединения можно ограничивать на следующих уровнях: <ul style="list-style-type: none"> <li>• пользователи;</li> <li>• компьютеры;</li> <li>• группы пользователей (компьютеров);</li> <li>• параметры соединения — служебные и прикладные протоколы, порты, сетевые интерфейсы, приложения, дни недели, время суток</li> </ul>
<b>Режим обучения</b>	При включенном режиме обучения разрешается весь сетевой трафик. Для каждого пакета проверяется наличие правила фильтрации (правила с реакцией "по умолчанию" не проверяются). Если правила нет, оно добавляется как разрешающее для каждого из приложений. Однотипные правила заменяются одним правилом, включающим в себя все объединенные

### Механизм авторизации сетевых соединений

В Secret Net Studio реализован механизм защиты сетевого взаимодействия между авторизованными абонентами. Данный механизм базируется на открытых стандартах протоколов семейства IPsec и обеспечивает безопасность обмена данными.

Механизм авторизации абонентов основан на протоколе Kerberos. Данный протокол нечувствителен к попыткам перехвата паролей и атакам типа "Man in the Middle". С помощью этого механизма удостоверяются не только субъекты доступа, но и защищаемые объекты. Это предотвращает несанкционированную подмену (имитацию) защищаемой информационной системы с целью осуществления некоторых видов атак.

Механизм авторизации сетевых соединений выполняет следующие функции.

<b>Функция</b>	<b>Описание</b>
<b>Авторизация сетевых соединений</b>	Добавляет специальную служебную информацию для сетевых пакетов, удовлетворяющих правилам, полученным с сервера управления и авторизации. Осуществляет анализ специальной служебной информации входящих пакетов и передачу информации в модуль межсетевого экранирования для осуществления фильтрации по правилам
<b>Контроль неизменности передаваемых сетевых пакетов</b>	Позволяет контролировать аутентичность, целостность и конфиденциальность передаваемых данных
<b>Шифрование трафика</b>	Механизм авторизации сетевых соединений также выполняет криптографическую защиту сетевого трафика

## Глава 2

# Межсетевой экран

Настройка межсетевого экрана осуществляется централизованно в программе управления. Она выполняется на уровне объектов "Компьютер" по отдельности для каждого из защищаемых компьютеров.

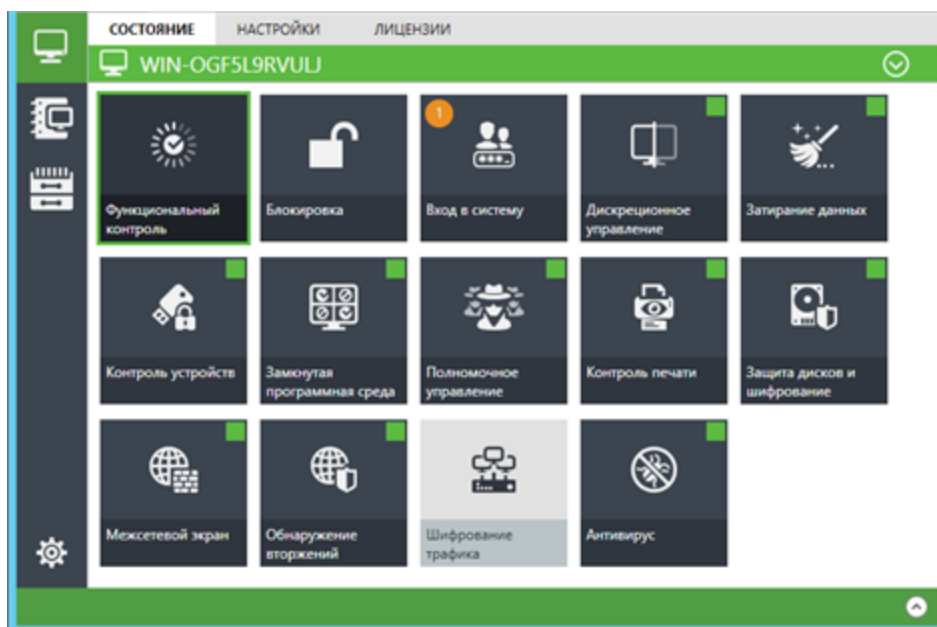
**Примечание.** В состав Secret Net Studio также входит компонент "Локальный центр управления". С помощью данного компонента можно только посмотреть настройки механизма межсетевого экрана непосредственно на защищаемом компьютере.

После установки Secret Net Studio на защищаемом компьютере первоначальная настройка межсетевого экрана разрешает прохождение всего сетевого трафика.

### Для настройки межсетевого экрана:

1. Вызовите программу управления Secret Net Studio.

На экране появится основное окно программы.



**Совет.** Для просмотра значений параметров межсетевого экрана непосредственно на защищаемом компьютере вызовите программу "Локальный центр управления", перейдите на вкладку "Настройки" и в разделе "Политики" выберите элемент "Межсетевой экран". В локальном режиме управления редактирование параметров недоступно.

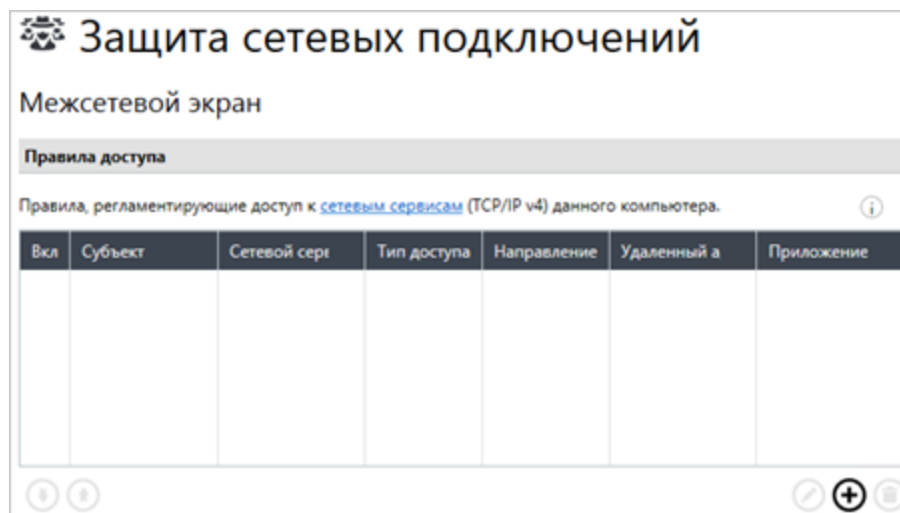
2. Откройте представление "Компьютеры", в левой части экрана в списке объектов управления найдите нужный компьютер, вызовите для него контекстное меню и активируйте в нем команду "Свойства".

В правой части экрана появится информация о состоянии компьютера.

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



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".

## Порядок обработки сетевых пакетов

Порядок обработки пакетов в Secret Net Studio зависит от направления сетевого трафика.

- Входящие пакеты — первоначально производится проверка на соответствие настройкам сетевых протоколов, затем — на соответствие системным правилам, а затем, если пакет пропущен, — на соответствие правилам доступа;
- Исходящие пакеты — сначала производится проверка на соответствие правилам доступа, затем — на соответствие системным правилам, а затем, если пакет пропущен, — на соответствие настройкам сетевых протоколов.

По умолчанию правила доступа к объектам обрабатываются в порядке их создания и расположения в таблице правил. Наивысшим приоритетом обладают правила, расположенные в начальных строках таблицы (см. стр. 10).

При совпадении характеристик сетевого пакета с его описанием в правиле выполняется заданное действие. Если доступ запрещен, дальнейшая проверка пакета на соответствие оставшимся правилам не выполняется. Если доступ разрешен, производится дальнейшая проверка пакета. Пакеты сетевого трафика, не попавшие под действие ни одного из правил, пропускаются.

**Примечание.** Служебные правила, пропускающие сетевой трафик, необходимый для работы Secret Net Studio, применяются даже если предыдущие уровни проверок заблокировали пакет.

Порядок обработки пакетов для прикладных правил:

- сначала производится обработка пакетов, соответствующая обработке входящего трафика;
- после преобразования данных в операции над общими папками и именованными каналами производится проверка на соответствие прикладным правилам;
- после выполнения операций над общими папками и именованными каналами и последующего преобразования ответа в исходящие пакеты производится обработка, соответствующая проверке исходящего трафика.

Если операции над общими папками и именованными каналами выполняются непосредственно защищаемым компьютером, проверка на соответствие прикладным правилам не выполняется.

## Управление приоритетом правила

По умолчанию правила доступа к объектам обрабатываются в порядке их создания и расположения в таблице правил. Наивысшим приоритетом обладают правила, расположенные в начальных строках таблицы.

Средства Secret Net Studio позволяют изменять приоритет обработки правил.

### Для управления приоритетом правила:

1. Выберите в списке правило, приоритет которого требуется изменить.
2. Измените приоритет правила с помощью кнопок "Вниз" и "Вверх".

## Управление правилами доступа

Правила доступа регулируют доступ аутентифицированных и анонимных пользователей к сетевым сервисам защищаемого компьютера. Данные правила имеют более высокий приоритет, чем прикладные правила (см. стр. 22).



### Внимание!

- По умолчанию правила доступа применяются для всех сетевых интерфейсов компьютера.
- При изменении правил новые настройки вступают в силу в течение 4–6 минут после сохранения изменений.

### Для управления правилами:

1. В области настройки параметров межсетевого экрана перейдите к разделу "Правила доступа".

Вкл	Субъект	Сетевой серв	Тип доступа	Направление	Удаленный а	Приложение
<input checked="" type="checkbox"/>	everyone Secret	DNS-запрос	Разрешен	Исходящее	*	*
<input checked="" type="checkbox"/>	everyone Secret	DHCP-ответ	Разрешен	Входящее	*	*
<input checked="" type="checkbox"/>	everyone Secret	DHCP-запрос	Разрешен	Исходящее	*	*
<input checked="" type="checkbox"/>	everyone Secret	NetBIOS (служб	Разрешен	Входящее	*	*
<input checked="" type="checkbox"/>	everyone Secret	NetBIOS (служб	Разрешен	Входящее	*	*

Для каждого правила в таблице отображаются данные:

Столбец	Значение
<b>Вкл</b>	Управление работой правила: <ul style="list-style-type: none"> <li>• отметка отсутствует — работа правила временно приостановлена;</li> <li>• отметка установлена — правило включено</li> </ul>
<b>Субъект</b>	Имя учетной записи или группы учетных записей, для которых действует правило
<b>Сетевой сервис</b>	Наименование сетевого сервиса, для которого действует правило
<b>Тип доступа</b>	Тип доступа к защищаемому компьютеру: <ul style="list-style-type: none"> <li>• "Разрешен";</li> <li>• "Запрещен"</li> </ul>
<b>Направление</b>	Направление трафика, для которого действует правило
<b>Удаленный адрес</b>	Имя или IP-адрес компьютера, для которого действует правило. Символ * (звездочка) означает, что правило действует для всех удаленных компьютеров
<b>Приложение</b>	Путь к приложению, для которого действует правило

2. Выполните нужные действия:

- создайте правило (см. стр. **11**);
- измените свойства правила (см. стр. **17**);
- удалите правило (см. стр. **18**);
- определите приоритет правила (см. стр. **10**).

## Создание правила доступа

Для создания правила доступа используется специальная программа-мастер.



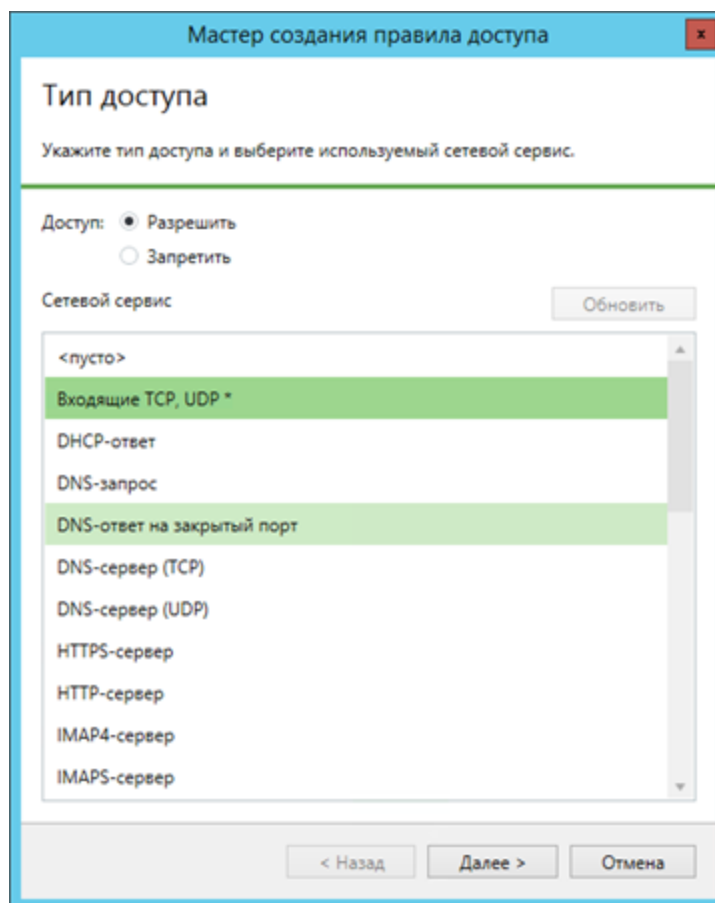
**Совет.** Для управления процедурой используйте кнопки:

- "< Назад" — для возврата к предыдущему диалогу;
- "Далее >" — для перехода к следующему диалогу;
- "Отмена" — для прекращения процедуры.

**Для создания правила доступа:**

1. Нажмите кнопку "Добавить".

На экране появится первый диалог мастера создания правила.



2. Укажите параметры и нажмите кнопку "Далее >".

Поле	Значение
<b>Доступ</b>	Выберите значение: <ul style="list-style-type: none"> <li>• "Разрешить" — если при срабатывании правила требуется разрешить доступ к защищаемому объекту;</li> <li>• "Запретить" — если при срабатывании правила требуется запретить доступ к защищаемому объекту</li> </ul>
<b>Сетевой сервис</b>	Выберите в списке название сетевого сервиса, для которого действует создаваемое правило. Если параметры сетевого сервиса требуется указать вручную, выберите значение "< пусто >"

**Примечание.** В списке сетевых сервисов отображаются сервисы, заданные по умолчанию. Чтобы в списке появились сервисы, ранее созданные вручную (см. стр. 34), нажмите кнопку "Обновить".

На экране появится следующий диалог мастера.

3. Заполните поля диалога и нажмите кнопку "Далее >".

Поле	Значение
<b>Тип протокола</b>	Выберите тип протокола, для которого действует правило
<b>Направление</b>	Укажите направление трафика, для которого действует правило (по отношению к защищаемому объекту)
<b>Требовать защищенное соединение</b>	Отметьте поле, если для исходящего сетевого соединения требуется использовать защищенный канал передачи данных
<b>Порт назначения</b>	<p>Укажите номер порта, для которого действует правило:</p> <ul style="list-style-type: none"> <li>оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех портов компьютера — отправителя или получателя IP-пакетов;</li> <li>для входящего трафика укажите номер порта компьютера — получателя IP-пакетов;</li> <li>для исходящего трафика укажите номер порта компьютера — отправителя IP-пакетов.</li> </ul> <p>Используйте кнопку "Дополнительно", если требуется настроить диапазон портов на защищаемом сервере или удаленном компьютере</p>
<b>Приложение</b>	<p>Укажите путь к исполняемому файлу приложения, для которого действует правило:</p> <ul style="list-style-type: none"> <li>укажите путь к приложению. При указании пути к приложению можно также использовать системные переменные Windows;</li> <li>оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех приложений.</li> </ul> <p>Созданное правило будет анализировать сетевой трафик для приложения, работающего непосредственно на защищаемом компьютере</p>

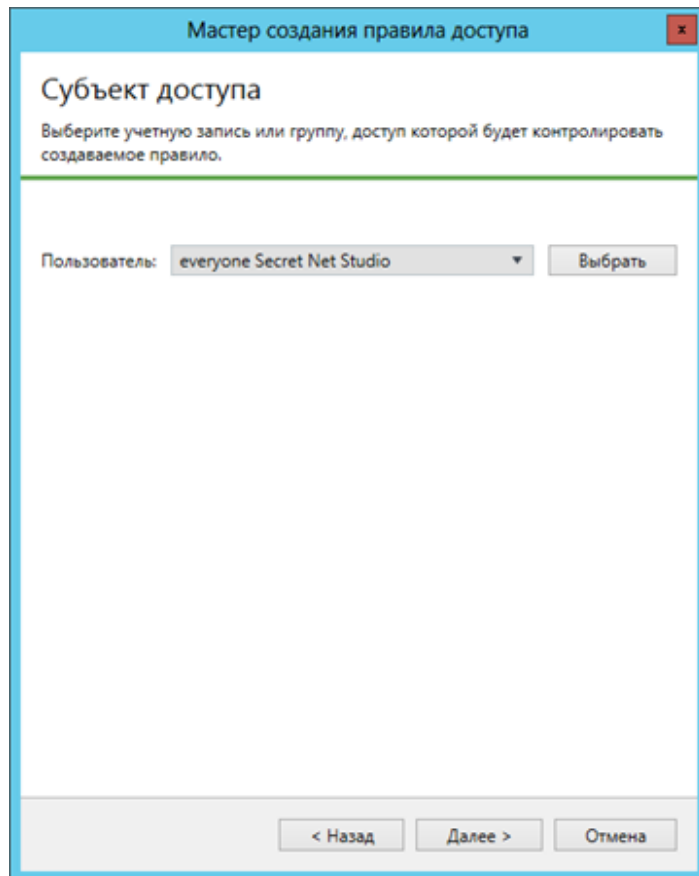


**Внимание!** Для корректной работы правил доступа рекомендуется указывать полный путь к исполняемому файлу приложения.



**Внимание!** При использовании параметра "Требовать защищенное соединение" сетевые соединения по незащищенному каналу не устанавливаются (при наличии лицензии на механизм авторизации сетевых соединений).

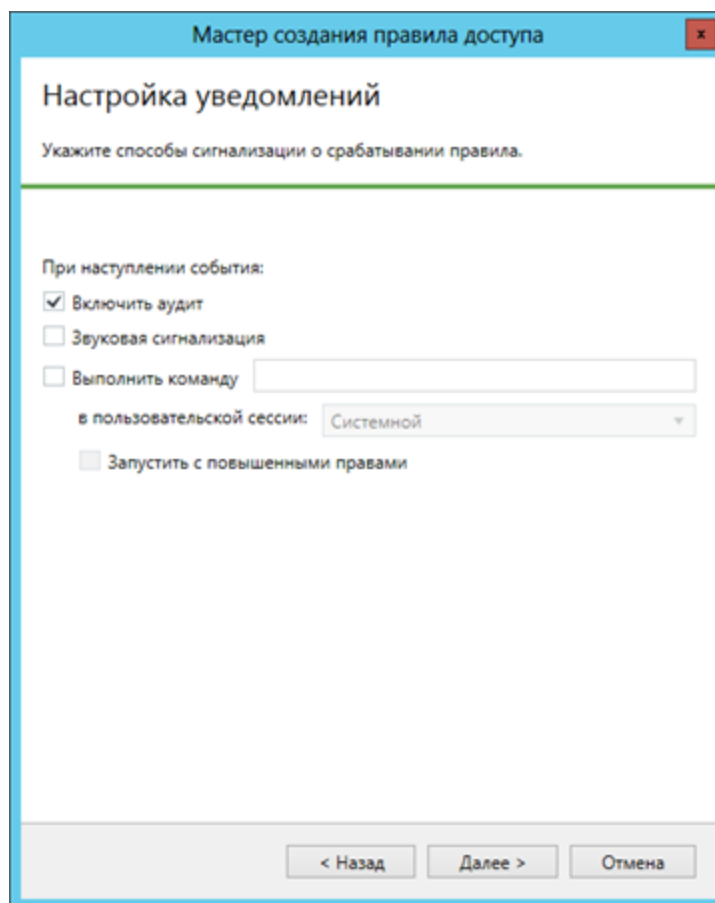
На экране появится диалог для выбора субъекта доступа.



Для выбора учетных записей в стандартном для Windows диалоге нажмите кнопку "Выбрать". Данная возможность есть только при наличии лицензии на использование механизма авторизации сетевых соединений.

4. Укажите имя учетной записи или группы учетных записей, для которой будет действовать правило, и нажмите кнопку "Далее >".

На экране появится диалог для настройки уведомлений о срабатывании правила.



5. Укажите способы сигнализации о срабатывании правила, если это необходимо, и нажмите кнопку "Далее >".

Поле	Значение
<b>Включить аудит</b>	Поставьте отметку, если требуется фиксировать в журнале событие, возникающее при срабатывании правила. Если фиксировать событие не требуется — удалите отметку
<b>Звуковая сигнализация</b>	Поставьте отметку, если на защищаемом компьютере требуется подавать звуковой сигнал, оповещающий о срабатывании правила. Если подавать сигнал не требуется — удалите отметку
<b>Выполнить команду</b>	Поставьте отметку, если на защищаемом компьютере при срабатывании правила требуется автоматически запускать исполняемый файл. В текстовом поле, которое станет доступным после установки отметки, укажите полный путь и имя исполняемого файла (с параметром). Например, C:\windows\notepad.exe 1.txt
<b>в пользовательской сессии</b>	Поле доступно после выбора пункта "Выполнить команду". Выберите пользовательскую сессию, в которой необходимо выполнить указанную команду: <ul style="list-style-type: none"> <li>• Системной — выполнить команду с правами системы;</li> <li>• Консольной — выполнить команду от имени пользователя его сессии;</li> <li>• Всех сессиях пользователя — выполнить команду во всех пользовательских сессиях</li> </ul>
<b>Запустить с повышенными правами</b>	Поставьте отметку, чтобы выполнить команду с полными правами пользователя, даже если для пользователя включен контроль учетных записей (UAC, User Account Control)

На экране появится диалог для настройки дополнительных параметров.

**Мастер создания правила доступа**

**Дополнительные критерии**

Укажите дополнительные параметры правила, такие как адреса узлов и маска фильтра.

Маска фильтра:

Удаленный адрес: \*

Локальный адрес: \*

Отключить правило

Уведомлять отправителя о блокировке пакета

6. Укажите дополнительные параметры правила и нажмите кнопку "Далее >".

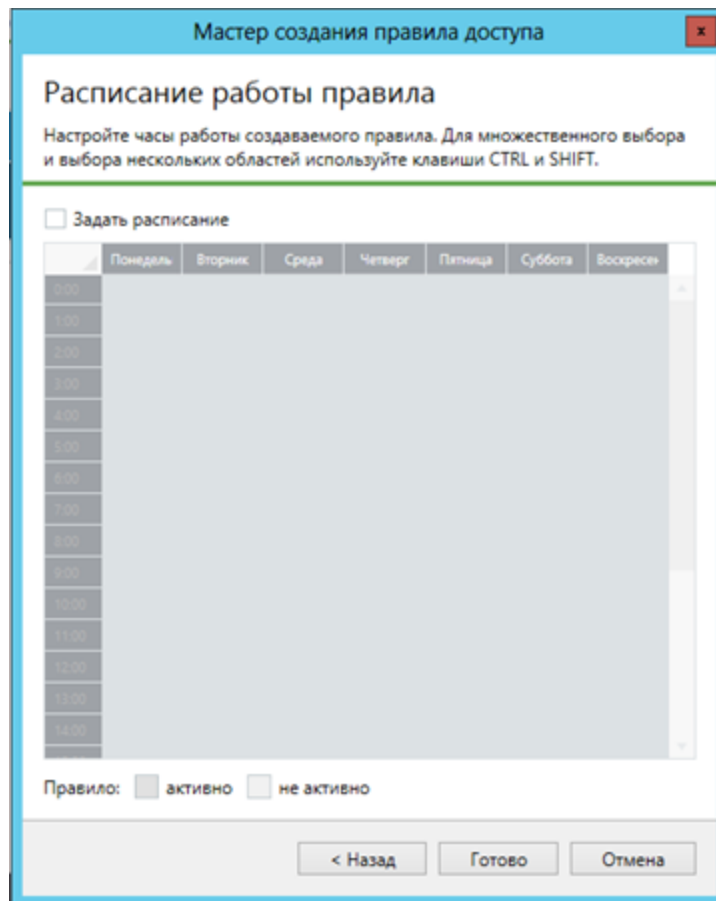
Поле	Значение
<b>Маска фильтра</b>	<p>Введите значение, определяющее необходимость обработки IP-пакета. Если поле заполнено, правилом обрабатываются только IP-пакеты, содержимое которых соответствует маске фильтра. Поле поддерживает следующие специальные символы:</p> <ul style="list-style-type: none"> <li>* — любое количество символов;</li> <li>? — один символ.</li> </ul> <p>Например, значению *abcd* будет соответствовать любой пакет, в теле которого встречается последовательность abcd</p>
<b>Удаленный адрес</b>	<p>Чтобы задать допустимый набор удаленных адресов, укажите имя, IP-адрес компьютера, диапазон IP-адресов (например, 192.168.0.3-192.168.0.9) или подсеть (например, 192.168.1.0/24 или 10.10.0.0/255.255.0.0)</p>
<b>Локальный адрес</b>	<p>Укажите имя, IP-адрес компьютера, диапазон IP-адресов или подсеть, чтобы задать допустимый набор локальных адресов</p>
<b>Отключить правило</b>	<p>Управление работой правила:</p> <ul style="list-style-type: none"> <li>отметка отсутствует — правило включено;</li> <li>отметка установлена — работа правила временно приостановлена</li> </ul>
<b>Уведомлять отправителя о блокировке пакета</b>	<p>Управление оповещениями о блокировке пакетов в результате работы запрещающего правила:</p> <ul style="list-style-type: none"> <li>отметка отсутствует — отправитель не получает уведомления о блокировке пакетов;</li> <li>отметка установлена — отправитель получает уведомления о блокировке пакетов. В случае срабатывания правила для протокола TCP будут генерироваться RST-пакеты, для всех остальных протоколов (кроме ICMP, AH, ESP) — пакеты ICMP (тип Destination Unreachable)</li> </ul>



**Совет.** Оставьте в поле "Удаленный адрес" или "Локальный адрес" символ \* (звездочка), если требуется, чтобы правило действовало для любых адресов.  
Указать несколько IP-адресов, диапазонов адресов или подсетей можно с помощью разделителя ";", (точка с запятой).

**Примечание.** Поле "Уведомлять отправителя о блокировке пакета" доступно для изменений в правилах с типом доступа "Запретить" и направлением трафика "Входящее".

На экране появится диалог для настройки расписания работы правила.



7. Настройте расписание работы правила, если это необходимо, и нажмите кнопку "Готово":
  - отметьте поле "Задать расписание". Станет доступной для изменения таблица, с помощью которой настраиваются параметры расписания;
  - выделите нажатием левой кнопки мыши ячейки, соответствующие дням недели и времени, в которое требуется разрешить (правило "активно") или запретить (правило "неактивно") работу правила.

**Примечание.** Время работы правила определяется часовым поясом защищаемого компьютера.

Правило будет создано и отобразится в списке правил.

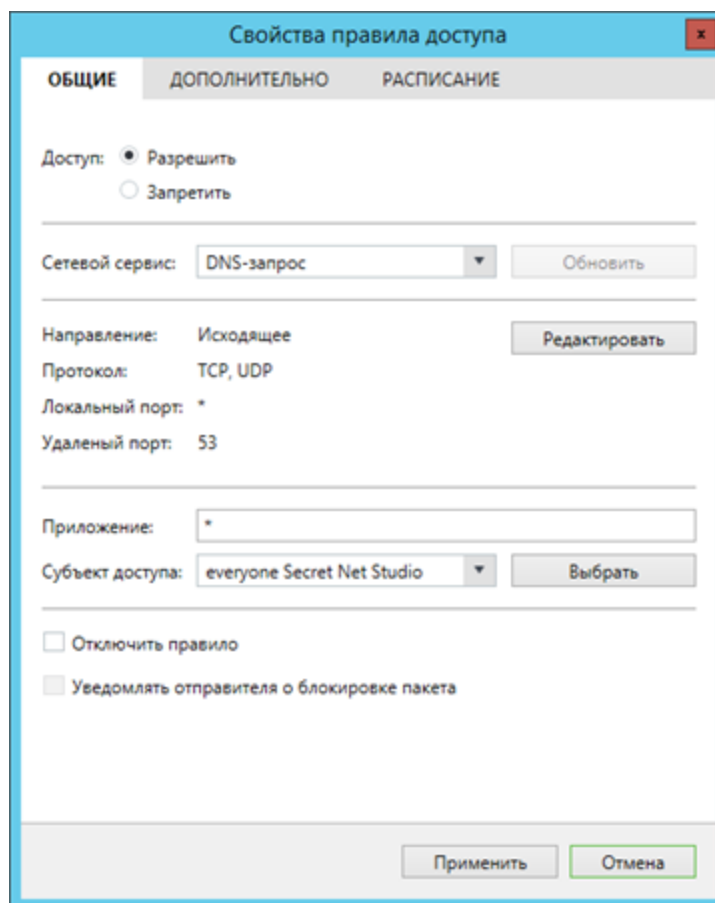
## Управление работой правил доступа

Параметры правила доступа, указанные при его создании, могут быть изменены.

### Для изменения параметров правила:

1. Выберите в таблице правило доступа, параметры которого нужно изменить.
2. Нажмите кнопку "Редактировать".

На экране появится диалог для настройки параметров правила.



Параметры правила, содержащиеся в диалоге, аналогичны тем, что описаны в процедуре создания правила.

3. Для управления работой правила:
  - если требуется приостановить работу правила — отметьте поле "Отключить правило". Правило будет отключено;
  - для восстановления работоспособности правила — удалите отметку из поля "Отключить правило". Правило будет включено.
4. Укажите нужные значения параметров и нажмите кнопку "Применить".



**Внимание!** При ошибочном создании правил, осуществляющих блокировку служебных протоколов (DNS, DHCP и т.д.), возможна потеря связи с агентом на удаленном компьютере. В этом случае необходимо удалить правила в Программе управления (см. ниже), а затем на защищаемом компьютере в командной строке выполнить следующую команду под именем локального администратора:  
`C:\Program Files\Secret Net Studio\Client\Components\Network Protection\ScAuthModCfg.exe /r`

## Удаление правила доступа

**Для удаления правила доступа:**

1. Выберите правила, которые требуется удалить.

**Совет.** Для выбора нескольких правил используйте клавиши <Ctrl> и <Shift>.

2. Нажмите кнопку "Удалить".  
 Выбранные правила будут удалены.

## Управление системными правилами

Системные правила контролируют соединения с данным компьютером по протоколам семейства TCP/IP. Данные правила имеют более высокий приоритет, чем правила доступа к сетевым сервисам и прикладные правила.

**Для управления системными правилами:**

1. В области настройки параметров межсетевого экрана в разделе "Правила доступа" нажмите кнопку-ссылку "Показать специализированные правила доступа".

На экране появится таблица с перечнем системных правил.

Вкл	Протокол	Тип доступа	Удаленный адрес

Для каждого правила отображаются данные:

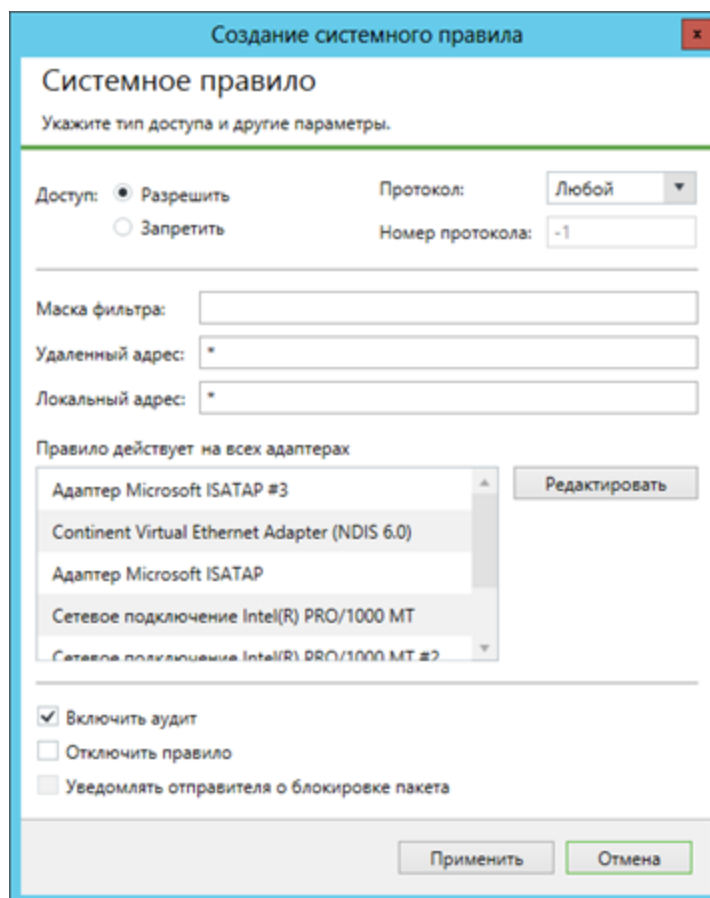
Столбец	Значение
<b>Вкл</b>	Управление работой правила: <ul style="list-style-type: none"> <li>• отметка отсутствует — работа правила временно приостановлена;</li> <li>• отметка установлена — правило включено</li> </ul>
<b>Протокол</b>	Наименование протокола, для которого действует правило
<b>Тип доступа</b>	Тип доступа к защищаемому компьютеру: <ul style="list-style-type: none"> <li>• "Разрешен";</li> <li>• "Запрещен"</li> </ul>
<b>Удаленный адрес</b>	Адрес компьютера, для которого действует правило, или символ * (звездочка), если правило действует для всех удаленных компьютеров

2. Выполните нужные действия:
  - создайте правило (см. стр. **19**);
  - измените свойства правила (см. стр. **21**);
  - удалите правило (см. стр. **18**);
  - определите приоритет правила (см. стр. **10**);
  - настройте режим защиты протокола ICMP (см. стр. **33**).

**Создание системного правила****Для создания правила:**

1. Нажмите кнопку "Добавить".

На экране появится диалог для создания системного правила.



2. Настройте параметры правила и нажмите кнопку "Применить".

Поле	Значение
<b>Доступ</b>	<p>Выберите значение:</p> <ul style="list-style-type: none"> <li>"Разрешить" — если при срабатывании правила требуется разрешить доступ к защищаемому объекту;</li> <li>"Запретить" — если при срабатывании правила требуется запретить доступ к защищаемому объекту</li> </ul>
<b>Протокол</b>	<p>Выберите тип протокола, для которого действует правило:</p> <ul style="list-style-type: none"> <li>"Любой" — если нужно, чтобы правило действовало для всех типов протоколов;</li> <li>"Другой" — если нужный тип протокола отсутствует в списке. В этом случае станет доступным для изменения поле "Номер протокола"</li> </ul>
<b>Номер протокола</b>	<p>Если выбран тип протокола, то значение в этом поле устанавливается автоматически и изменить его нельзя.</p> <p>Если в поле "Протокол" выбрано значение "Другой", укажите номер протокола, для которого действует правило</p>
<b>Маска фильтра</b>	<p>Введите значение, определяющее необходимость обработки IP-пакета. Если поле заполнено, правилом обрабатываются только IP-пакеты, содержимое которых соответствует маске фильтра. Поле поддерживает следующие специальные символы:</p> <ul style="list-style-type: none"> <li>* — любое количество символов;</li> <li>? — один символ.</li> </ul> <p>Например, значению *abcd* будет соответствовать любой пакет, в теле которого встречается последовательность abcd</p>
<b>Удаленный адрес</b>	<p>Укажите имя, IP-адрес компьютера, диапазон IP-адресов (например, 192.168.0.3-192.168.0.9) или подсеть (например, 192.168.1.0/24 или 10.10.0.0/255.255.0.0), чтобы задать допустимый набор удаленных адресов. Оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех удаленных компьютеров</p>

Поле	Значение
<b>Локальный адрес</b>	Укажите имя, IP-адрес компьютера, диапазон IP-адресов или подсеть, чтобы задать допустимый набор локальных адресов. Оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех удаленных компьютеров
<b>Правило действует на всех адаптерах</b>	Чтобы правило действовало только на определенных адаптерах, нажмите кнопку "Редактировать" и выберите нужные адаптеры
<b>Включить аудит</b>	Управление регистрацией событий, возникающих при срабатывании правила: <ul style="list-style-type: none"> <li>отметка отсутствует — регистрация событий выключена;</li> <li>отметка установлена — регистрация событий включена</li> </ul>
<b>Отключить правило</b>	Управление работой правила: <ul style="list-style-type: none"> <li>отметка отсутствует — правило включено;</li> <li>отметка установлена — работа правила временно приостановлена</li> </ul>

Новое правило отобразится в списке правил.

## Управление работой системных правил

Параметры системного правила, указанные при его создании, могут быть изменены.

### Для изменения параметров правила:

1. Выберите в таблице системное правило, параметры которого нужно изменить.
2. Нажмите кнопку "Редактировать".

На экране появится диалог для настройки параметров правила.

Свойства системного правила

Системное правило

Укажите тип доступа и другие параметры.

Доступ:  Разрешить  Запретить

Протокол: Любой

Номер протокола: -1

Маска фильтра:

Удаленный адрес: \*

Локальный адрес: \*

Правило действует на всех адаптерах

Microsoft Hyper-V Network Adapter Редактировать

Включить аудит

Отключить правило

Уведомлять отправителя о блокировке пакета

Применить Отмена

Параметры правила, содержащиеся в диалоге, аналогичны тем, что описаны в процедуре создания правила.

3. Для управления работой правила:
  - если требуется приостановить работу правила — отметьте поле "Отключить правило". Правило будет отключено;
  - для восстановления работоспособности правила — удалите отметку из поля "Отключить правило". Правило будет включено.
4. Укажите нужные значения параметров и нажмите кнопку "Применить".

## Управление прикладными правилами

Прикладные правила регулируют доступ аутентифицированных и анонимных пользователей к общим папкам и именованным каналам на данном компьютере. Данные правила имеют минимальный приоритет.

### Для управления правилами:

1. В области настройки параметров межсетевого экрана в разделе "Правила доступа" нажмите кнопку-ссылку "Показать специализированные правила доступа".

На экране появится таблица с перечнем прикладных правил.

Вкл	Субъект	Прикладной сервис	Объект доступа	Тип доступа	Удаленный адрес

Для каждого правила отображаются данные:

Столбец	Значение
<b>Вкл</b>	Управление работой правила: <ul style="list-style-type: none"> <li>• отметка отсутствует — работа правила временно приостановлена;</li> <li>• отметка установлена — правило включено</li> </ul>
<b>Субъект</b>	Имя учетной записи или группы учетных записей, для которых действует правило
<b>Прикладной сервис</b>	Наименование прикладного сервиса: <ul style="list-style-type: none"> <li>• "Общие папки";</li> <li>• "Именованные каналы"</li> </ul>
<b>Объект доступа</b>	Наименование общей папки или именованного канала, для которого действует правило. Символ * (звездочка) означает, что правило действует для всех объектов этого типа
<b>Тип доступа</b>	Тип доступа к защищаемому компьютеру: <ul style="list-style-type: none"> <li>• "Разрешен";</li> <li>• "Запрещен"</li> </ul>
<b>Удаленный адрес</b>	Имя или IP-адрес компьютера, для которого действует правило. Символ * (звездочка) означает, что правило действует для всех удаленных компьютеров

2. Выполните нужные действия:
  - создайте правило (см. стр. **23**);
  - измените свойства правила (см. стр. **27**);
  - удалите правило (см. стр. **18**);
  - определите приоритет правила (см. стр. **10**).

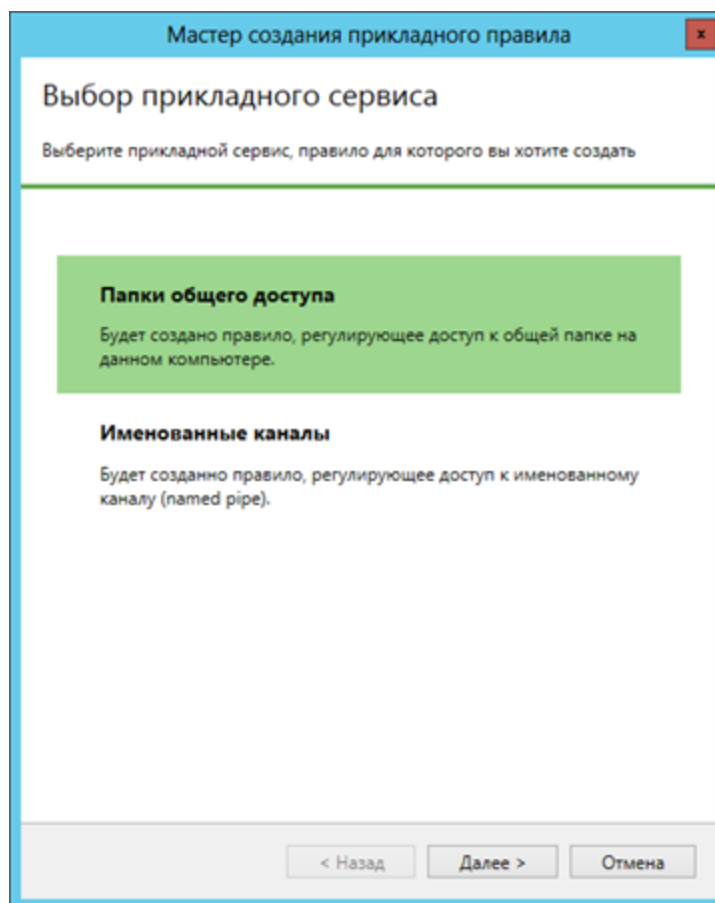
## Создание прикладного правила

Для создания прикладного правила используется специальная программа-мастер.

### Для создания правила:

1. Нажмите кнопку "Добавить".

На экране появится первый диалог мастера создания правила.



2. Выберите прикладной сервис, правило для которого вы хотите создать, и нажмите кнопку "Далее >":
  - "Папки общего доступа" — новое правило будет контролировать доступ пользователей к указанной сетевой общей папке по протоколу SMB;
  - "Именованные каналы" — новое правило будет контролировать доступ пользователей к указанному именованному каналу по протоколу Named Pipes.

**Примечание.** Прикладные правила позволяют разграничить доступ пользователей к общим папкам со всем их содержимым (например, `\\server\share`). Гранулярное разграничение доступа к подпапкам общих папок (например, `\\server\share\folder`) не обеспечивается.

На экране появится диалог задания параметров правила.

3. Укажите параметры и нажмите кнопку "Далее >".

Поле	Значение
<b>Доступ</b>	Выберите значение: <ul style="list-style-type: none"> <li>• "Разрешить" — если при срабатывании правила требуется разрешить доступ к защищаемому объекту;</li> <li>• "Запретить" — если при срабатывании правила требуется запретить доступ к защищаемому объекту</li> </ul>
<b>Имя общей папки/ Именованный канал</b>	Укажите название папки или канала, для которой(ого) действует правило. Оставьте символ * (звездочка), если правило действует для всех папок или именованных каналов на данном компьютере

- Имя общей папки указывается без имени компьютера, на котором она находится. Например, если сетевой путь к папке на сервере \\server\share, то укажите в поле только ее имя: share.
- В имени папки или канала могут быть использованы подстановочные знаки: ? (вопросительный знак) — для замены одного символа и \* (звездочка) — для замены нескольких символов, включая пустой.
- Если доступ к общим папкам защищаемого объекта запрещен для всех пользователей (создано запрещающее правило для учетной записи everyone, в котором в качестве имени общей папки указан символ \* (звездочка)), то для того чтобы пользователи имели возможность просматривать список общих папок на данном компьютере, необходимо создать разрешающее правило для общей папки IPC\$.

На экране появится диалог для выбора учетных записей, для которых действует правило.

**Совет.** Для выбора учетных записей в стандартном для Windows диалоге нажмите кнопку "Выбрать".

4. Укажите имя учетной записи или группы учетных записей, для которой будет действовать правило, и нажмите кнопку "Далее >".



На экране появится диалог для настройки уведомлений о срабатывании правила.

5. Укажите способы сигнализации о срабатывании правила, если это необходимо, и нажмите кнопку "Далее >":

Поле	Значение
<b>Включить аудит</b>	Отметьте, если требуется фиксировать в журнале событие, возникающее при срабатывании правила. Если фиксировать событие не требуется — удалите отметку
<b>Звуковая сигнализация</b>	Отметьте, если на защищаемом компьютере требуется подавать звуковой сигнал, оповещающий о срабатывании правила. Если подавать сигнал не требуется — удалите отметку
<b>Выполнить команду</b>	Отметьте, если на защищаемом компьютере при срабатывании правила требуется автоматически запускать исполняемый файл. В текстовом поле, которое станет доступным после установки отметки, укажите полный путь и имя исполняемого файла (с параметром). Например, C:\windows\notepad.exe 1.txt
<b>в пользовательской сессии</b>	Поле доступно после выбора пункта "Выполнить команду". Выберите пользовательскую сессию, в которой необходимо выполнить указанную команду: <ul style="list-style-type: none"> <li>• Системной — выполнить команду с правами системы;</li> <li>• Консольной — выполнить команду от имени пользователя в его сессии;</li> <li>• Всех сессиях пользователя — выполнить команду во всех пользовательских сессиях</li> </ul>
<b>Запустить с повышенными правами</b>	Поставьте отметку, чтобы выполнить команду с полными правами пользователя, даже если для пользователя включен контроль учетных записей (UAC, User Account Control)

На экране появится диалог для настройки дополнительных параметров.

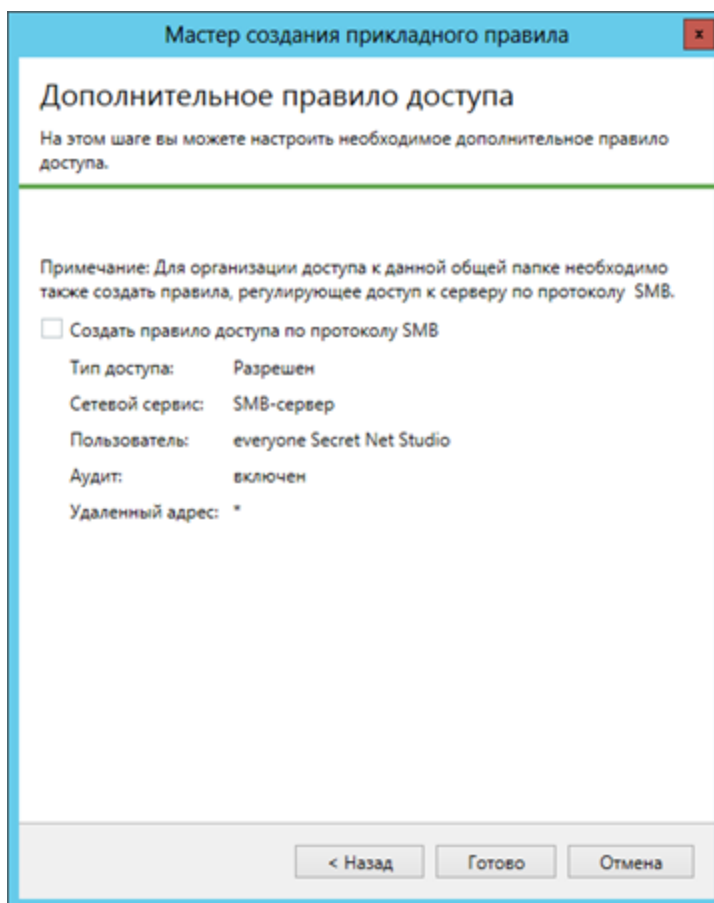
6. Укажите дополнительные параметры правила и нажмите кнопку "Далее >".

Поле	Значение
<b>Удаленный адрес</b>	Укажите имя или IP-адрес компьютера (маску подсети), к которому будет применяться правило при попытке доступа к общей папке или именованному каналу на защищаемом компьютере. Оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех компьютеров — отправителей IP-пакетов
<b>Отключить правило</b>	Отметьте поле, если требуется ввести правило в эксплуатацию позднее

На экране появится диалог для настройки расписания работы правила.

7. Настройте расписание работы правила, если это необходимо, и нажмите кнопку "Далее >":
  - отметьте поле "Задать расписание". Станет доступной для изменения таблица, с помощью которой настраиваются параметры расписания;
  - выделите нажатием левой кнопки мыши ячейки, соответствующие дням недели и времени, в которое требуется разрешить (правило "активно") или запретить (правило "неактивно") работу правила.

На экране появится диалог создания дополнительного правила доступа.



Для корректной работы прикладных правил необходимо также настроить правила прохождения IP-пакетов на транспортном уровне — по протоколу SMB. Для этого требуется создать правило доступа, разрешающее прохождение пакетов по протоколу TCP на порт 445 (и/или 139) для учетной записи (группы), указанной в прикладном правиле.



**Внимание!** Если прохождение пакетов по протоколу SMB запрещается, прикладные правила не работают, так как на транспортном уровне IP-пакеты блокируются.

8. Если требуется создать разрешающее правило доступа по протоколу SMB — отметьте поле "Создать правило доступа по протоколу SMB".
9. Нажмите кнопку "Готово".

Новое правило будет добавлено в список прикладных правил.

При использовании функции создания дополнительного SMB-правила в списке правил доступа также отобразится правило, разрешающее использование SMB для учетной записи (группы), указанной в прикладном правиле.

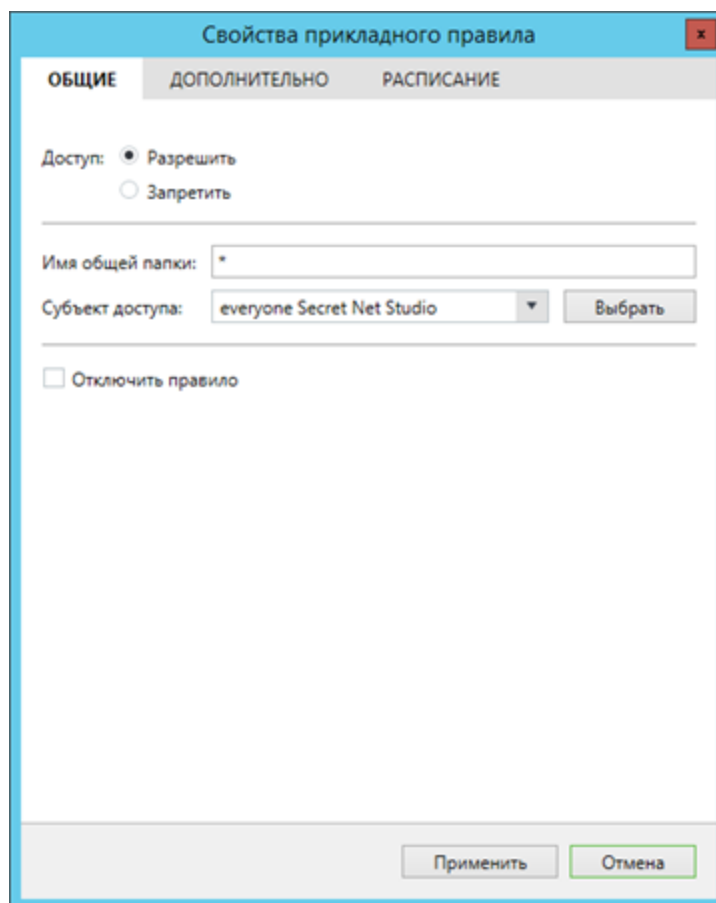
## Управление работой прикладных правил

Параметры прикладного правила, указанные при его создании, могут быть изменены.

### Для изменения параметров правила:

1. Выберите в таблице прикладное правило, параметры которого нужно изменить.
2. Нажмите кнопку "Редактировать".

На экране появится диалог для настройки параметров правила.



Параметры правила, содержащиеся в диалоге, аналогичны тем, что описаны в процедуре создания правила.

3. Для управления работой правила:
  - если требуется приостановить работу правила — отметьте поле "Отключить правило". Правило будет отключено;
  - для восстановления работоспособности правила — удалите отметку из поля "Отключить правило". Правило будет включено.
4. Укажите нужные значения параметров и нажмите кнопку "Применить".

## Управление правилами фильтрации сетевого потока

Правила фильтрации сетевого потока предназначены для осуществления фильтрации команд сетевых протоколов, параметров команд, а также для управления доступом к ресурсам, содержащим отдельные типы мобильного кода.

Управление правилами фильтрации сетевого потока осуществляется с помощью утилиты командной строки ScAuthSrvConfig.exe (в сетевом режиме работы Secret Net Studio) или ScLocalSrvConfig.exe (в автономном режиме работы).

Утилита ScAuthSrvConfig.exe располагается на сервере безопасности в каталоге установки Secret Net Studio\Server\Authentication Server\.

**Примечание.** Для входа в режим управления конфигурацией утилите ScAuthSrvConfig.exe нужно передать параметры для подключения к серверу управления (см. ниже).

Утилита ScLocalSrvConfig.exe располагается на защищаемом компьютере в каталоге установки Secret Net Studio\Client\Components\Network Protection\.



**Внимание!** Для изменения локальной конфигурации с помощью утилиты ScLocalSrvConfig.exe требуется наличие прав локального администратора.

## Подключение к серверу управления

Для входа в режим управления конфигурацией утилите ScAuthSrvConfig.exe нужно передать параметры для подключения к серверу управления. Для этого откройте командную строку и выполните следующую команду:

```
ScAuthSrvConfig [@argfile] [/?|h|help] [/v|version] <domain>
[/local] [kdc] [/p|password <value>] [/a|admin <value>] [/q
<value>] [/s <value>]
```

где:

- @argfile — прочесть аргументы из файла;
- /? — показать подробную информацию об утилите;
- /v — показать номер версии утилиты;
- domain — домен Kerberos;
- /local — локальный режим (восстановление конфигурации);
- kdc — расположение KDC (Key Distribution Center);
- /p <value> — пароль администратора домена;
- /a <value> — имя администратора домена;
- /q <value> — команда выполнения запроса;
- /s <value> — путь к script-файлу для исполнения.

### Пример

Подключение к серверу управления, запущенному на текущем компьютере:

```
ScAuthSrvConfig.exe DOMAINNAME 127.0.0.1 /admin Administrator
```

где:

- DOMAINNAME — домен безопасности;
- 127.0.0.1 — сетевой адрес сервера конфигурации;
- Administrator — имя администратора Secret Net Studio.

## Создание и редактирование правил фильтрации сетевого потока

Для добавления нового правила фильтрации сетевого потока откройте командную строку и введите следующую команду:

```
config> add network_stream_filtration_rule(nsfr) <protected_computer> /filter <value> [/flt-case-insensitive | /flt-case-sensitive] [/at allow|deny] [/order <value>] [/local_addrs <value>] [/local_ports <value>] [/remote_addrs <value>] [/remote_ports <value>] [/direction <value>] [/audit 1|0] [/enable 1|0]
```

Доступны следующие параметры правила:

Параметр	Описание	Возможные значения
<b>filter</b>	Маска фильтра	<ul style="list-style-type: none"> <li>* — заменяет любое количество символов;</li> <li>? — заменяет один символ</li> </ul>
<b>flt-case-insensitive</b>	Регистронезависимый поиск	
<b>flt-case-sensitive</b>	Регистрозависимый поиск. Применяется по умолчанию	
<b>at (access type)</b>	Тип правила доступа	<ul style="list-style-type: none"> <li>deny — при обнаружении последовательности, попадающей под маску фильтра, соединение будет разорвано. Значение задано по умолчанию;</li> <li>allow — при обнаружении последовательности, попадающей под маску фильтра, будет выполнен только аудит (если он разрешён)</li> </ul>
<b>direction</b>	Список направлений соединений (сетевого трафика), для которых будет применяться это правило. В качестве разделителя используется ";"	<ul style="list-style-type: none"> <li>in — правило будет применяться для входящих соединений, для входящего трафика. Значение задано по умолчанию;</li> <li>in_reply — правило будет применяться для входящих соединений, для ответного трафика;</li> <li>out — правило будет применяться для исходящих соединений, для исходящего трафика;</li> <li>out_reply — правило будет применяться для исходящих соединений, для ответного трафика</li> </ul>

Параметр	Описание	Возможные значения
<b>local_addrs</b>	Список локальных адресов/сетей/диапазонов, для которых действует правило. В качестве разделителя используется ","	
<b>local_ports</b>	Список локальных портов/диапазонов, для которых действует правило. В качестве разделителя используется ";"	
<b>remote_addrs</b>	Список удалённых адресов/сетей/диапазонов, для которых действует правило. В качестве разделителя используется ","	
<b>remote_ports</b>	Список удалённых портов/диапазонов, для которых действует правило. В качестве разделителя используется ";"	
<b>audit</b>	Включение/выключение аудита при срабатывании правила	<ul style="list-style-type: none"> <li>• 1 — аудит включен;</li> <li>• 0 — аудит выключен</li> </ul>
<b>order</b>	Порядок применения правил. Параметр влияет только на порядок срабатывания правил	
<b>enable</b>	Текущий статус правила	<ul style="list-style-type: none"> <li>• 1 — правило включено;</li> <li>• 0 — правило выключено</li> </ul>

Для редактирования правила фильтрации используется следующая команда:

```
config> modify network_stream_filtration_rule(nsfr)
<protected_computer> <rule_id> [/filter <value>] [/at
allow|deny] [/order <value>] [/local_addrs <value>] [/local_
ports <value>] [/remote_addrs <value>] [/remote_ports
<value>] [/direction <value>] [/audit 1|0] [/enable 1|0]
```

где <rule\_id> — идентификатор правила, которое нужно модифицировать.

## Примеры

### Пример 1. Фильтрация одиночной команды

Создание правила, действующего на исходящие сетевые соединения через 23 порт. Правило срабатывает при обнаружении в отправляемой команде "cmd":

```
add nsfr SP-VM01 /filter "cmd1" /direction out /remote_ports
23
```

### Пример 2. Фильтрация последовательности команд

Создание правила, действующего на исходящие сетевые соединения через 23 порт. Правило срабатывает при обнаружении в отправляемых данных последовательности команд "cmd1", "cmd2" и "cmd3", между которыми может быть любое количество символов.

```
add nsfr SP-VM01 /filter "cmd1*cmd2*cmd3" /direction out
/remote_ports 23
```

### Пример 3. Фильтрация параметра команды

Создание правила, действующего на исходящие сетевые соединения через 23 порт. Правило срабатывает при обнаружении в отправляемых данных команды "cmd" с параметром "param".

```
add nsfr SP-VM01 /filter "cmd*param" /direction out /remote_
ports 23
```

#### Пример 4. Фильтрация доступа к ресурсам, содержащим отдельные типы мобильного кода

Для фильтрации доступа к ресурсам, содержащим отдельные типы мобильного кода, применяются правила фильтрации сетевого потока, в которых в качестве фильтра используются текстовые последовательности, характерные для мобильного кода определенного типа. Например, в протоколе HTTP для запрета мобильного кода необходимо создавать правила для исходящих соединений, для ответного трафика, с фильтрацией по заголовку "Content-Type". Дополнительно фильтрация может быть выполнена с помощью проверки заголовка "Content-Disposition" и его параметра "filename".

Список заголовков "Content-Type" для разных типов мобильного кода:

Тип мобильного кода	Строка для фильтрации
<b>JavaScript</b>	Content-Type: text/javascript Content-Type: text/jsript Content-Type: text/x-javascript Content-Type: text/ecmascript Content-Type: text/x-ecmascript Content-Type: application/javascript Content-Type: application/x-javascript Content-Type: application/ecmascript Content-Type: application/x-ecmascript
<b>Adobe Flash</b>	Content-Type: application/x-shockwave-flash
<b>VBScript</b>	Content-Type: text/vbscript
<b>Java</b>	Content-Type: application/java-archive Content-Type: application/jar
<b>ActiveX</b>	Content-Type: application/ocx Content-Type: application/x-ms

Пример создания набора правил для фильтрации мобильного кода:

```
add nsfr SP-VM01 /filter "Content-Type: application/ocx"
/flt-case-insensitive /direction out_reply /remote_ports 80
add nsfr SP-VM01 /filter "Content-Type: application/x-ms"
/flt-case-insensitive /direction out_reply /remote_ports 80
add nsfr SP-VM01 /filter " Content-Disposition*filename*ocx"
/flt-case-insensitive /direction out_reply /remote_ports 80
```

Правила блокируют загрузку ActiveX- компонентов по протоколу HTTP, работающему через 80 порт.

#### Просмотр правил фильтрации сетевого потока

Чтобы просмотреть список правил фильтрации сетевого потока выполните команду:

```
config> show network_stream_filtration_rules(nsfrs)
<protected_computer>
```

где <protected\_computer> — имя защищаемого компьютера.

#### Пример

```
config> show nsfrs SP-VM01
id {ca541ade-b955-4cf2-8894-d020aac9d9ac}
order 124000
access deny
content-filter cmd1*cmd2*cmd3
direction out
proto 6
local-addr *(*)
remote-addr *(23)
```

Просмотреть детальную информацию об отдельном правиле фильтрации сетевого потока можно с помощью команды:

```
config> show network_stream_filtration_rule(nsfr) <protected_
computer> <id>
```

где:

- <protected\_computer> — имя защищаемого компьютера;
- <id> — идентификатор правила.

#### Пример

```
config>show nsfr SP-VM01 {ca541ade-b955-4cf2-8894-
d020aac9d9ac}
server: sp-vm01
id {ca541ade-b955-4cf2-8894-d020aac9d9ac}
order 124000
access deny
content-filter cmd1*cmd2*cmd3
enabled 1
direction out
proto 6
local-addr *(*)
remote-addr *(23)
audit 1
```

## Удаление правила фильтрации сетевого потока

Чтобы удалить правило фильтрации сетевого потока выполните команду:

```
config> delete network_stream_filtration_rule(nsfr)
<protected_computer> <id>
```

## Управление сетевыми протоколами

Средства Secret Net Studio позволяют настроить доступ к защищаемым компьютерам по протоколам сетевого уровня IPv4, IPv6, Novell IPX, а также некоторым протоколам с устаревшим форматом Ethernet-кадра (LLC, IPX). По умолчанию работа этих протоколов запрещается, за исключением протокола IPv4. Эти настройки имеют более высокий приоритет, чем правила доступа к сетевым сервисам, прикладные правила и системные правила.

#### Для управления сетевыми протоколами:

1. В области настройки параметров межсетевого экрана перейдите к разделу "Настройки|Протоколы".

Протокол	Доступ	Аудит	По умолчанию
Internet Protocol, version 4(IPv4)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Internet Protocol, version 6(IPv6)	<input type="checkbox"/>	<input type="checkbox"/>	
Novell IPX	<input type="checkbox"/>	<input type="checkbox"/>	
Протоколы с устаревшим форматом Ethernet-кадра	<input type="checkbox"/>	<input type="checkbox"/>	

2. В столбце "Доступ" удалите отметки из ячеек протоколов, которые требуется отключить. Для включения протоколов поставьте отметки.



**Внимание!** По умолчанию доступ к защищаемым компьютерам разрешен только по протоколу IPv4. Не рекомендуется разрешать доступ по остальным протоколам, так как сетевой трафик по ним не контролируется межсетевым экраном Secret Net Studio.



3. В столбце "Аудит" отметьте ячейки тех протоколов, для которых требуется фиксировать в журнале события прохождения каждого пакета. Если фиксировать события не требуется — удалите отметку.

По умолчанию режим аудита для всех протоколов выключен.



**Внимание!** При включенном режиме аудита количество регистрируемых в журнале Secret Net Studio событий будет очень большим. Это может замедлить работу системы.

**Пояснение.** Значение поля "Аудит" в настройках сетевых протоколов не связано со значением поля "Включить аудит" в свойствах правил доступа.

4. Для сохранения новых значений параметров нажмите кнопку "Применить" в верхней части вкладки "Настройки".

**Совет.** Для возврата таблицы к первоначальному состоянию используйте кнопку "По умолчанию".

Настройка "Протоколы с устаревшим форматом Ethernet-кадра" позволяет заблокировать Ethernet-кадры, в заголовке которых вместо типа кадра содержится значение его длины. Посредством таких кадров на защищаемый сервер может пройти трафик IPX, SMB поверх NetBEUI и даже IP-трафик.

## Настройка режима защиты протокола ICMP

Режим защиты протокола ICMP используется для организации обмена сообщениями по данному протоколу. По умолчанию режим управления пакетами протокола ICMP выключен.

### Для настройки параметров режима:

1. В области настройки параметров межсетевого экрана перейдите к разделу "Настройки|ICMP-защита".

ICMP-защита

Включить ICMP-защиту

Разрешить следующие типы ICMP-сообщений:

Описание	Тип	Код	Получение	Отправка
Эхо-ответ	0	Любой	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Адресат недоступен	3	Любой	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Перенаправление	5	Любой	<input type="checkbox"/>	<input type="checkbox"/>
Альтернативный адрес узла	6	Любой	<input type="checkbox"/>	<input type="checkbox"/>
Эхо-запрос	8	Любой	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ходатайство маршрутизатора	10	Любой	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Превышение временного интервала	11	Любой	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Заблокировать остальные типы ICMP-сообщений

Добавить  
Удалить  
По умолчанию

Типы пакетов протокола ICMP представлены в виде таблицы. Для каждого типа отображаются следующие данные:

- описание типа пакета;
- тип пакета;
- код пакета;
- средства управления прохождением пакетов.

2. Настройте нужные параметры.

Параметр	Значение
<b>Включить ICMP-защиту</b>	Отметьте поле, если требуется включить защиту ICMP
<b>Столбцы "Получение" и "Отправка"</b>	Разрешите или запретите прохождение входящих и исходящих пакетов. Чтобы разрешить — поставьте отметку в нужную ячейку, чтобы запретить — удалите ее

Параметр	Значение
<b>Заблокировать остальные типы ICMP-сообщений</b>	Отметьте поле, чтобы запретить прохождение всех типов пакетов протокола ICMP, за исключением типов, указанных в таблице. Если требуется снять запрет на прохождение пакетов — удалите отметку

**Совет.** Используйте кнопки справа от таблицы для добавления типов ICMP-сообщений ("Добавить"), удаления добавленных строк ("Удалить") или возврата таблицы к первоначальному состоянию ("По умолчанию").

- Для сохранения новых значений параметров нажмите кнопку "Применить" в верхней части вкладки "Настройки".

Режим обработки пакетов протокола ICMP будет настроен в соответствии с указанными параметрами.

## Управление сетевыми сервисами

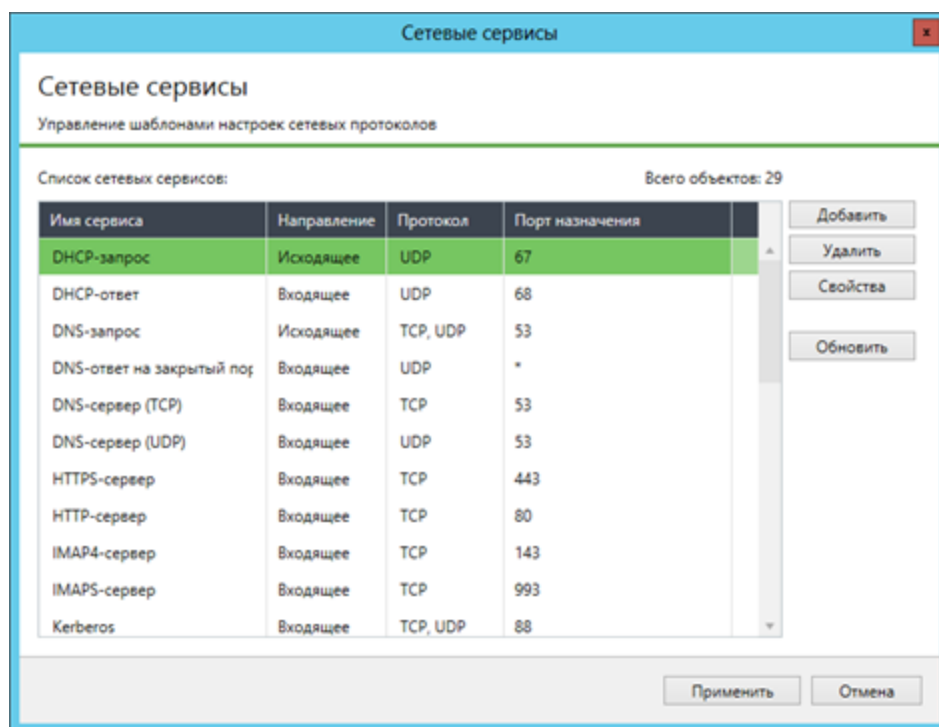
Сетевые сервисы — это список шаблонов наиболее распространенных настроек сетевых протоколов. Для каждого сервиса указываются следующие данные:

- наименование сетевого сервиса;
- направление трафика, для которого действует сетевой сервис;
- тип протокола сетевого сервиса;
- порт компьютера, для которого действует сетевой сервис.

### Для управления сетевыми сервисами:

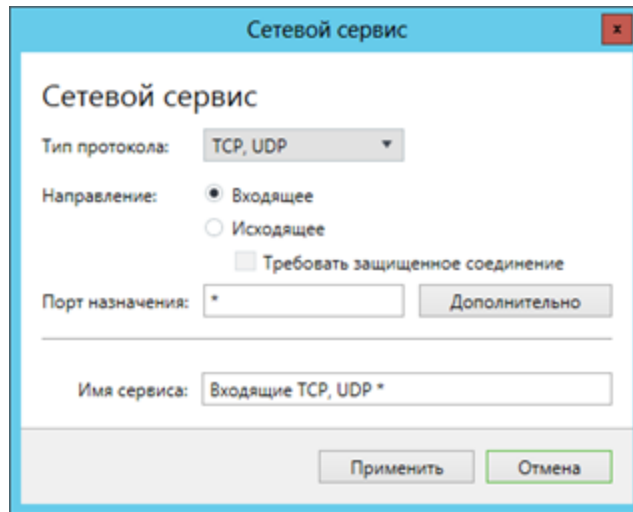
- В области настройки параметров межсетевого экрана в разделе "Правила доступа" нажмите кнопку-ссылку "сетевым сервисам".

На экране появится окно.



- Для создания сетевого сервиса нажмите кнопку "Добавить".

На экране появится диалог для ввода параметров сервиса.



3. Укажите параметры сервиса и нажмите кнопку "Применить".

Параметр	Значение
<b>Тип протокола</b>	Выберите тип протокола, для которого действует сетевой сервис
<b>Направление</b>	Укажите направление трафика, для которого действует сетевой сервис: <ul style="list-style-type: none"> <li>• "Входящее";</li> <li>• "Исходящее"</li> </ul>
<b>Требовать защищенное соединение</b>	Отметьте это поле, если при использовании сервиса требуется использовать защищенное соединение (см. стр. 39)
<b>Порт назначения</b>	Укажите номер порта, для которого действует сетевой сервис: <ul style="list-style-type: none"> <li>• оставьте символ * (звездочка), если сетевой сервис действует для всех портов компьютера — отправителя или получателя IP-пакетов;</li> <li>• для входящего трафика укажите номер порта компьютера получателя IP-пакетов;</li> <li>• для исходящего трафика укажите номер порта компьютера — отправителя IP-пакетов.</li> </ul> Чтобы указать диапазон портов назначения, нажмите кнопку "Дополнительно", расположенную рядом с полем "Порт назначения", и в появившемся диалоге добавьте диапазон портов
<b>Имя сервиса</b>	Введите название, под которым требуется сохранить шаблон сетевого сервиса

Сетевой сервис будет создан и отобразится в списке сетевых сервисов.

4. Для удаления одного или нескольких сетевых сервисов выберите сетевой сервис, который требуется удалить, и нажмите кнопку "Удалить". Выбранные сетевые сервисы будут удалены.
5. Для изменения параметров сетевого сервиса выберите его в списке и нажмите кнопку "Свойства". В появившемся окне измените параметры сервиса, руководствуясь описанием, приведенным в п.3 данной процедуры.

## Настройка режима обучения

Режим обучения используется на этапе ввода системы защиты в эксплуатацию. Данный режим позволяет составить базовый набор правил доступа, необходимый для функционирования защищаемого компьютера. Правила доступа составляются на основе информации о сетевой активности приложений на данном компьютере.

**Для настройки параметров режима:**

1. В области настройки параметров межсетевого экрана перейдите к разделу "Режим обучения".

Направление	<input checked="" type="checkbox"/> Входящие	<input checked="" type="checkbox"/> Исходящие
Максимальное количество генерируемых правил	10000	10000
Максимальное количество генерируемых правил для приложения	10	10
Сохранить информацию о процессе	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Сохранить информацию об адресах локального хоста	<input type="checkbox"/>	<input type="checkbox"/>
Сохранить информацию о портах локального хоста	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Сохранить информацию об адресах удаленного хоста	<input type="checkbox"/>	<input type="checkbox"/>
Сохранить информацию о портах удаленного хоста	<input type="checkbox"/>	<input checked="" type="checkbox"/>

2. Если требуется включить режим обучения — отметьте поле "Постоянное обучение с" или "Задать интервал обучения:" и укажите дату начала обучения или временной интервал.
3. Настройте параметры режима обучения.

Поле	Значение
<b>Активировать правила после окончания обучения</b>	Отметьте поле, чтобы по окончании периода обучения все составленные в его ходе правила доступа начали применяться
<b>Направление</b>	Отметьте направление трафика, для которого будет действовать режим обучения
<b>Максимальное количество генерируемых правил</b>	Укажите максимальное количество правил, генерируемых во время работы режима обучения
<b>Максимальное количество генерируемых правил для приложения</b>	Укажите максимальное количество правил, генерируемых во время работы режима обучения для каждого приложения
<b>Сохранить информацию о процессе</b>	Отметьте поле, чтобы созданные правила действовали для конкретных приложений, процессы которых вызывали сетевую активность. Если поле не отмечено, правила будут созданы для всех приложений
<b>Сохранить информацию о портах/адресах локального/удаленного хоста</b>	Отметьте соответствующие поля для сохранения необходимой информации

4. Для сохранения новых значений параметров нажмите кнопку "Применить" в верхней части вкладки "Настройки".

Режим обучения будет настроен в соответствии с указанными параметрами.

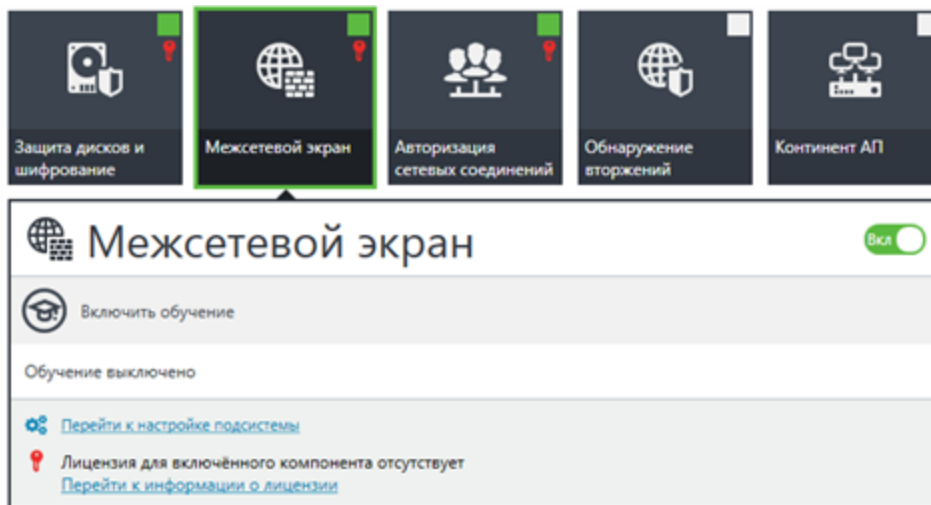
**Совет.** Для возврата таблицы к первоначальному состоянию используйте кнопку "По умолчанию".

## Управление работой межсетевого экрана на защищаемых компьютерах

Программа управления Secret Net Studio позволяет осуществлять для отдельного компьютера управление режимом обучения.

### Для управления работой межсетевого экрана:

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 "Межсетевой экран".  
Откроется панель управления работой межсетевого экрана.



3. Нажмите кнопку "Включить обучение"/"Выключить обучение" для управления работой режима обучения. Режим обучения позволяет составить базовый набор правил доступа (см. стр. **35**).

**Примечание.** Нажмите кнопку-ссылку "Перейти к настройке подсистемы", чтобы перейти к настройке локальных политик межсетевого экрана.

Нажмите кнопку-ссылку "Перейти к информации о лицензии", чтобы просмотреть сведения о действующей лицензии.

## Глава 3

# Авторизация сетевых соединений

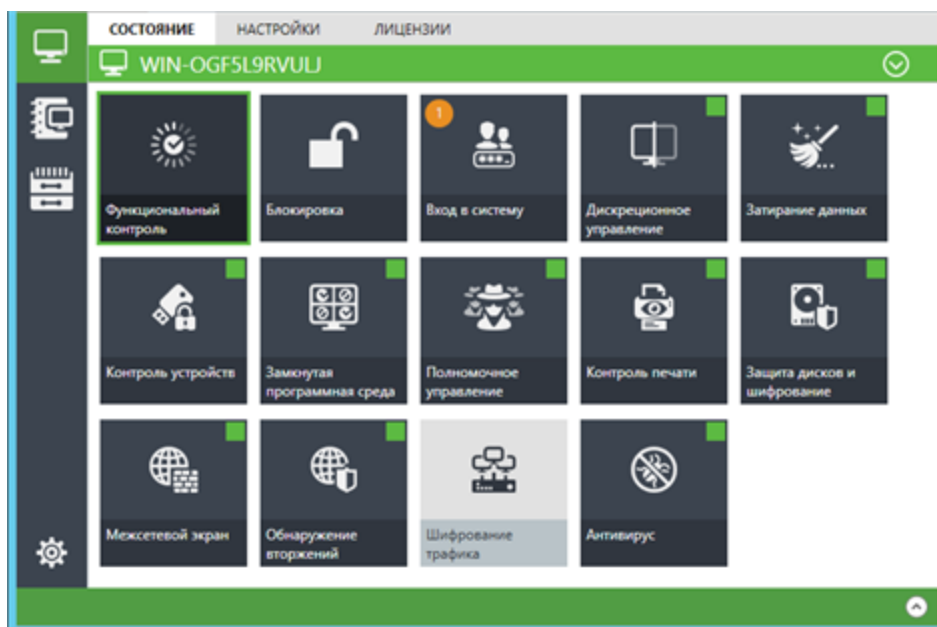
Настройка механизма авторизации сетевых соединений осуществляется централизованно в программе управления. Она выполняется на уровне объектов "Компьютер" по отдельности для каждого из защищаемых компьютеров.

**Примечание.** В состав Secret Net Studio также входит компонент "Локальный центр управления". С помощью данного компонента можно только посмотреть настройки механизма авторизации сетевых соединений непосредственно на защищаемом компьютере.

### Для настройки параметров:

1. Вызовите программу управления Secret Net Studio.

На экране появится основное окно программы.



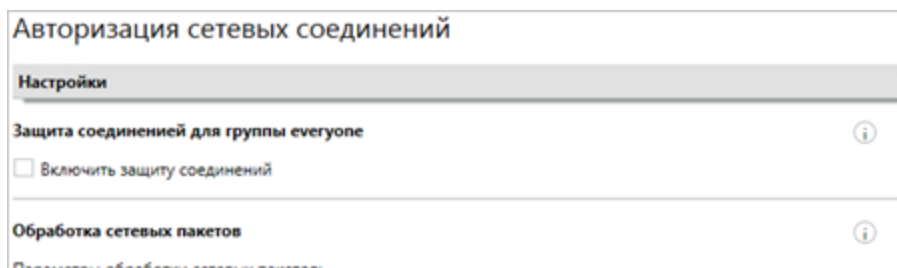
**Совет.** Для просмотра значений параметров механизма авторизации сетевых соединений непосредственно на защищаемом компьютере вызовите программу "Локальный центр управления", перейдите на вкладку "Настройки" и в разделе "Политики" выберите элемент "Авторизация сетевых соединений". В локальном режиме управления редактирование параметров недоступно.

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

В правой части экрана появится список параметров и политик данного компьютера.

3. Перейдите на вкладку "Настройки", затем в разделе "Политики" выберите элемент "Авторизация сетевых соединений".

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 защиты соединений для группы everyone

Чтобы разрешить защиту сетевых соединений в правилах доступа, настроенных для группы everyone, отметьте поле "Включить защиту соединений".

## Настройка параметров обработки пакетов

В Secret Net Studio реализован механизм защиты сетевого взаимодействия между авторизованными абонентами. Данный механизм базируется на открытых стандартах протоколов семейства IPsec и обеспечивает безопасность обмена данными.

В текущей версии используются следующие протоколы.

Название	Значение
<b>Протокол AH (Authentication Header)</b>	Позволяет гарантировать аутентичность и целостность передаваемых данных каждого IP-пакета. Обеспечивает защиту от атак типа "Man in the Middle"
<b>Протокол ESP (Encapsulating Security Payload)</b>	Используется для кодирования и контроля целостности передаваемых данных
<b>Протокол ISAKMP</b>	Предназначен для обмена ключами и согласования параметров соединения

Реализовано несколько режимов настройки. Администратор может для каждого защищаемого компьютера указать индивидуальный режим защиты.

По умолчанию параметры механизма авторизации сетевых соединений настроены следующим образом:

- включен режим добавления служебной информации в пакеты с уровнем анализа "Пакет целиком";
- включен режим защиты от replay-атак;
- сценарий определения пользователя SMB-соединения — от имени учетной записи пользователя.

Защита и целостность передаваемых данных обеспечивается следующими средствами:

- режим добавления служебной информации в пакеты;
- режим шифрования и контроля целостности;
- режим защиты от replay-атак.

**Примечание.** В текущей версии системы одновременное использование протоколов AH и ESP не предусмотрено.

### Для настройки параметров:

1. В области настройки параметров механизма авторизации сетевых соединений перейдите к разделу "Настройки | Обработка сетевых пакетов".



2. Настройте параметры защиты сетевых пакетов.



**Внимание!** Для установки защищенного соединения необходимо:

- настроить для удаленного компьютера-получателя правила доступа, необходимые для обмена данными с компьютером-отправителем (см. стр. 10);
- включить режим добавления служебной информации на компьютере-отправителе.

При невыполнении одного из этих условий установить защищенное соединение невозможно.

Поле	Значение
<b>Подпись</b>	<p>Отметьте поле для включения режима добавления служебной информации к пакетам и выберите в списке уровень анализа:</p> <ul style="list-style-type: none"> <li>• "Только маркировка" — служебная информация формируется на основе первого сетевого пакета из серии, остальные пакеты получают метку принадлежности к аутентифицированной серии;</li> <li>• "Заголовки пакетов" — служебная информация формируется на основе заголовков пакетов;</li> <li>• "Пакет целиком" — служебная информация формируется для каждого пакета полностью.</li> </ul> <p>Будет ли добавляться служебная информация к исходящему пакету или нет, определяется параметрами безопасности удаленного компьютера-получателя IP-пакетов. Если на компьютере-получателе пакетов разрешен обмен данными с компьютером-отправителем и настроены соответствующие правила, то при включении режима добавления служебной информации к пакетам на компьютере-отправителе все пакеты, отправленные данному компьютеру, будут дополнены служебной информацией</p>
<b>Шифрование</b>	Отметьте поле для включения режима кодирования данных
<b>Контроль целостности</b>	Поставьте отметку, чтобы включить режим контроля целостности закодированных пакетов. Если требуется выключить режим контроля целостности закодированных пакетов — удалите отметку из поля "Контроль целостности"
<b>Защита от replay-атак</b>	Отметьте поле для включения режима защиты, с помощью которого предотвращается пассивный захват данных и их пересылка

## Настройка SMB-соединения

Для определения пользователя SMB-соединения в Secret Net Studio реализовано несколько сценариев:

- пользователем соединения всегда считается учетная запись компьютера;
- пользователем соединения считается учетная запись пользователя — инициатора соединения. При этом остальным пользователям либо разрешается, либо запрещается пользоваться установленным SMB-соединением.

Деятельность всех пользователей, которым разрешается использовать SMB-соединение, осуществляется от имени пользователя — инициатора соединения. Если инициатор соединения неактивен более 30 секунд, то пользователем соединения считается следующий по порядку пользователь или сервис, которым требуется SMB-соединение.

Приоритет предоставления SMB- соединений (от низшего к высшему): анонимные пользователи, сервисы, авторизованные пользователи Secret Net Studio.

При реализации сценария, при котором пользователем соединения считается инициатор соединения, остальным пользователям:

- разрешается пользоваться SMB-соединением — деятельность всех низкоприоритетных абонентов осуществляется от имени высокоприоритетного абонента;
- запрещается пользоваться SMB-соединением — при запросе SMB- соединения высокоприоритетным абонентом SMB- соединения низкоприоритетных абонентов запрещаются.



**Для выбора сценария:**

1. Перейдите к разделу "Настройки|Сценарий для определения пользователя SMB-соединения".

**Сценарий для определения пользователя SMB-соединения**

Обрабатывать SMB-трафик:

От имени учетной записи компьютера

От имени учетной записи пользователя

Блокировать SMB-трафик остальных пользователей

**Примечание.** Если SMB-соединение создается до начала работы компонентов механизма (например, mapped drive с флажком reconnect at logon), то приоритет сервисов становится равным приоритету пользователей и все дальнейшие подключения будут происходить от имени учетной записи компьютера.

2. Укажите сценарий для определения пользователя SMB-соединения.

Поле	Значение
<b>От имени учетной записи компьютера</b>	Отметьте поле, если SMB-соединения требуется устанавливать под учетной записью компьютера
<b>От имени учетной записи пользователя</b>	Отметьте поле, если SMB-соединения требуется устанавливать под учетной записью пользователя
<b>Блокировать SMB-трафик остальных пользователей</b>	Поставьте отметку, если требуется запретить использование SMB-соединения всем пользователям, кроме пользователя — инициатора соединения

**Пояснение.** Все пользователи получают доступ к объекту под одной учетной записью (первой, которая осуществила доступ на терминальный сервер) при условии, что:

- доступ к защищаемому объекту осуществляется через терминальный сервер;
- SMB-соединение устанавливается под учетной записью пользователя;
- не включен параметр "Блокировать SMB-трафик остальных пользователей".

Если параметр "Блокировать SMB-трафик остальных пользователей" включен, то доступ получит только пользователь — инициатор соединения с данным терминальным сервером. В случае использования учетных записей компьютеров все пользователи терминального сервера получают доступ к защищаемому объекту под одной и той же учетной записью.

3. Для сохранения новых значений параметров нажмите кнопку "Применить" в верхней части вкладки "Настройки".

## Настройка параметров получения IP-адресов компьютера

Средства сетевой защиты Secret Net Studio позволяют идентифицировать компьютер не только по имени, но и по его IP-адресу. Эта возможность может быть использована, например, в случае, если имя компьютера по каким-либо причинам автоматически не преобразуется в IP-адрес.

**Для настройки параметров:**

1. В области настройки параметров механизма авторизации сетевых соединений перейдите к разделу "Настройки|IP-адреса".

**IP-адреса** i

Укажите, каким образом, удаленные компьютеры будут получать IP-адреса защищаемого объекта.

Получить адреса с сервера управления (рекомендуется)  
 Использовать для определения адресов службы имен  
 Использовать адреса из списка (доступна для редактирования при выборе только одного компьютера):

Адреса

## 2. Настройте параметры.

Поле	Значение
<b>Получать адреса с сервера управления</b>	По умолчанию клиенты будут получать IP-адреса данного защищаемого компьютера автоматически с сервера безопасности, которому компьютер подчинен
<b>Использовать для определения адресов службы имен</b>	Отметьте это поле, чтобы за адресами клиенты обращались к службам DNS, WINS и NetBIOS
<b>Использовать адреса из списка</b>	Отметьте это поле, если необходимо явно задать адреса. Введите IP-адрес данного защищаемого компьютера в поле ввода и нажмите кнопку "Добавить". Если требуется удалить введенный IP-адрес, выберите его в списке и нажмите кнопку "Удалить".

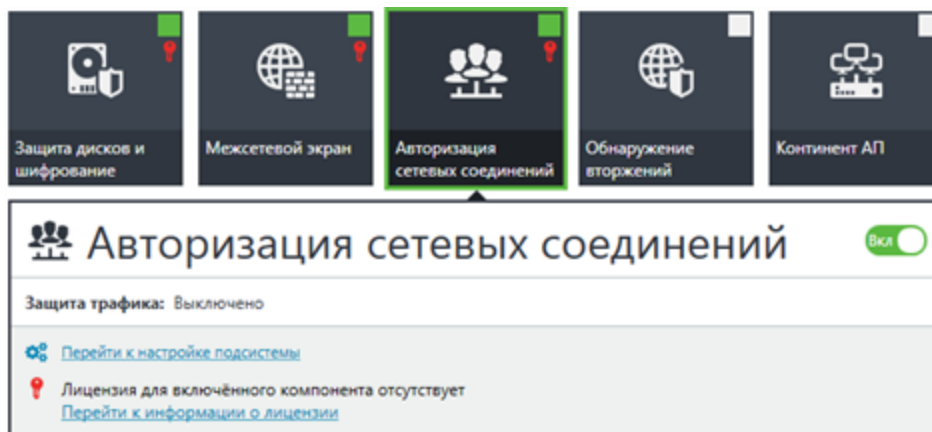
3. Для сохранения новых значений параметров нажмите кнопку "Применить" в верхней части вкладки "Настройки".

## Управление работой механизма авторизации соединений на защищаемых компьютерах

Программа управления Secret Net Studio позволяет осуществлять для отдельного компьютера управление работой механизма авторизации соединений.

### Для управления работой механизма авторизации соединений:

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 "Авторизация сетевых соединений".  
Откроется панель управления работой механизма авторизации соединений.



3. Чтобы включить авторизацию сетевых соединений на защищаемом компьютере, переведите переключатель в позицию "Вкл".

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

## 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	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. Шифрование сетевого трафика	RU.88338853.501400.001 91 8
<b>9.</b> Средство защиты информации Secret Net Studio. Руководство пользователя	RU.88338853.501400.001 92