КОД БЕЗОПАСНОСТИ

Средство защиты информации

Secret Net Studio

Руководство администратора

Настройка и эксплуатация. Сетевая защита

RU.88338853.501400.001 91 6

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

Оглавление

Список сокращений ... **4**

Введение ... **5**

Общие сведения ... **6**
- Персональный межсетевой экран ... 6
- Механизм авторизации сетевых соединений ... 6

Персональный межсетевой экран ... **8**
- Порядок обработки сетевых пакетов ... 9
- Управление приоритетом правила ... 9
- Управление правилами доступа ... 10
  - Создание правила доступа ... 11
  - Управление работой правил доступа ... 17
  - Удаление правила доступа ... 18
- Управление системными правилами ... 19
  - Создание системного правила ... 20
  - Управление работой системных правил ... 21
- Управление прикладными правилами ... 22
  - Создание прикладного правила ... 24
  - Управление работой прикладных правил ... 28
- Управление правилами фильтрации сетевого потока ... 29
  - Подключение к серверу управления ... 30
  - Создание и редактирование правил фильтрации сетевого потока ... 30
  - Просмотр правил фильтрации сетевого потока ... 33
  - Удаление правила фильтрации сетевого потока ... 34
- Управление сетевыми протоколами ... 34
- Настройка режима защиты протокола ICMP ... 35
- Управление сетевыми сервисами ... 36
- Настройка режима обучения ... 37
- Управление работой межсетевого экрана на защищаемых компьютерах ... 39

Авторизация сетевых соединений ... **40**
- Настройка защиты соединений для группы everyone ... 41
- Настройка параметров обработки пакетов ... 41
- Настройка SMB-соединения ... 42
- Настройка параметров получения IP-адресов компьютера ... 43
- Управление работой механизма авторизации соединений на защищаемых компьютерах ... 44

Документация ... **45**

Список сокращений

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

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

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

Глава 1
Общие сведения

В состав сетевой защиты Secret Net Studio входят следующие подсистемы:

- персональный межсетевой экран;
- механизм авторизации сетевых соединений.

Персональный межсетевой экран

Персональный 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.

Персональный межсетевой экран выполняет следующие функции:

Функция	Описание
Фильтрация сетевого трафика	Для фильтрации сетевого трафика используются специальные правила, обладающие широким диапазоном настроек. Сетевые соединения можно ограничивать на следующих уровнях: • пользователи; • компьютеры; • группы пользователей (компьютеров); • параметры соединения — служебные и прикладные протоколы, порты, сетевые интерфейсы, приложения, дни недели, время суток
Режим обучения	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.

Функция	Описание
Авторизация сетевых соединений	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
Контроль неизменности передаваемых сетевых пакетов	Позволяет контролировать аутентичность, целостность и конфиденциальность передаваемых данных
Шифрование трафика	Обеспечивает криптографическую защиту сетевого трафика

Глава 2
Персональный межсетевой экран

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

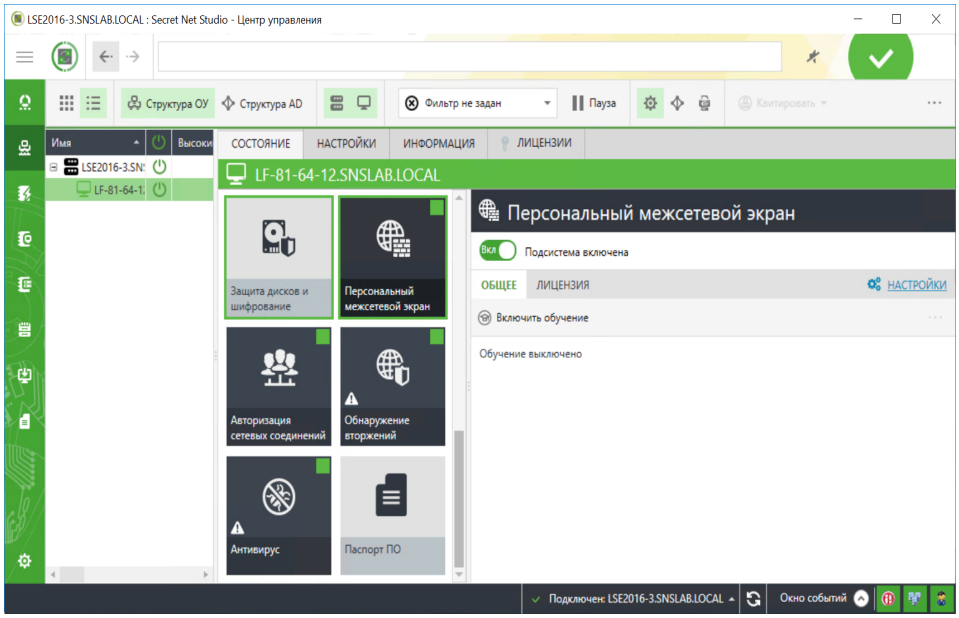
Примечание. В состав Secret Net Studio также входит компонент "Локальный центр управления". С помощью данного компонента можно только посмотреть настройки механизма межсетевого экрана непосредственно на защищаемом компьютере.

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.



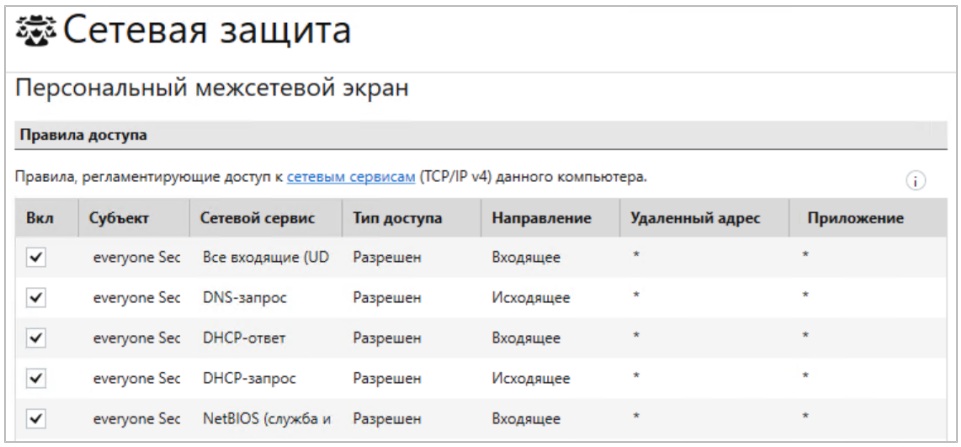
Совет. Для просмотра значений параметров межсетевого экрана непосредственно на защищаемом компьютере вызовите программу "Локальный центр управления", перейдите на вкладку "Настройки" и в разделе "Политики" выберите элемент "Персональный межсетевой экран". В локальном режиме управления редактирование 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" и нажмите при необходимости кнопку "Загрузить настройки", затем в разделе "Политики" выберите элемент "Персональный межсетевой экран".

В правой части экрана появится область настройки выбранных параметров.



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

Порядок обработки сетевых пакетов

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

- Входящие пакеты — первоначально выполняется проверка на соответствие настройкам сетевых протоколов, затем — на соответствие системным правилам, а затем, если пакет пропущен, — на соответствие правилам доступа.
- Исходящие пакеты — сначала выполняется 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.9).

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

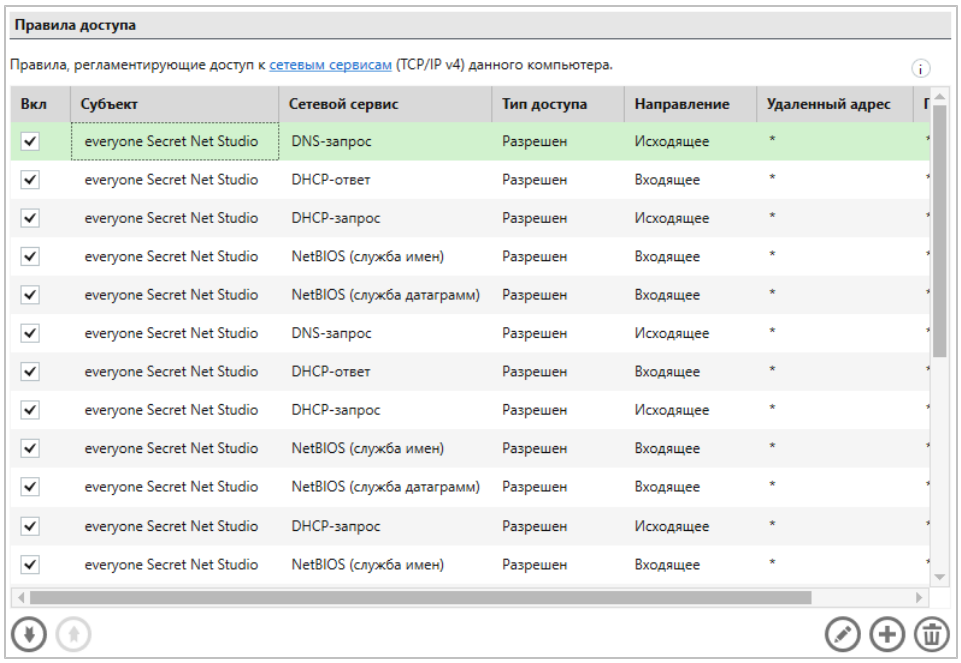
Правила доступа регулируют доступ аутентифицированных и анонимных пользователей к сетевым сервисам защищаемого компьютера. Данные правила имеют более высокий приоритет, чем прикладные правила (см. стр.22).

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".



Для каждого правила в таблице отображаются данные:

Столбец	Значение
Вкл	Управление работой правила: • отметка отсутствует — работа правила временно приостановлена; • отметка установлена — правило включено
Субъект	Имя учетной записи или группы учетных записей, для которых действует правило
Сетевой сервис	Наименование сетевого сервиса, для которого действует правило
Тип доступа	Тип доступа к защищаемому компьютеру: • "Разрешен"; • "Запрещен"
Направление	Направление трафика, для которого действует правило
Удаленный адрес	Имя или IP-адрес компьютера, для которого действует правило. Символ * (звездочка) означает, что правило действует для всех удаленных компьютеров

Столбец	Значение
Приложение	Путь к приложению, для которого действует правило. Символ * (звездочка) означает, что правило действует для всех приложений

Примечание. При добавлении правил доступа в режиме обучения в таблице будет отображаться столбец с признаком "Автообучение". Чтобы снять признак автообучения, нажмите кнопку "Снять признак самообучения".

2. Выполните нужные действия:
   - создайте правила (см. стр.**11**);
   - измените параметры правил (см. стр.**17**);
   - удалите ненужные правила (см. стр.**18**);
   - определите приоритет правил (см. стр.**9**).
3. Нажмите кнопку "Применить" внизу вкладки "Настройки".

Создание правила доступа

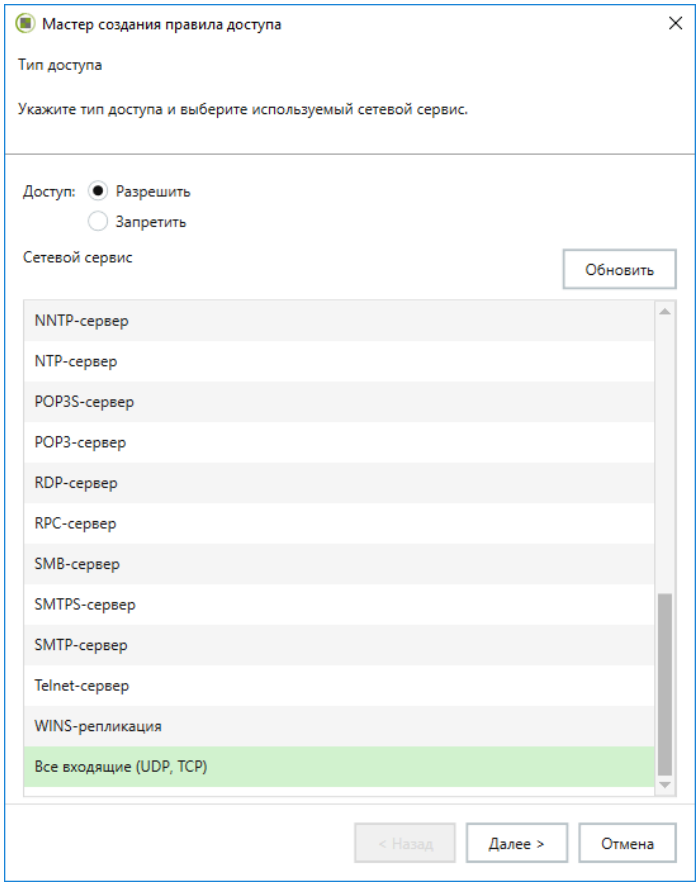
Для создания правила доступа используется специальная программа-мастер.

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.

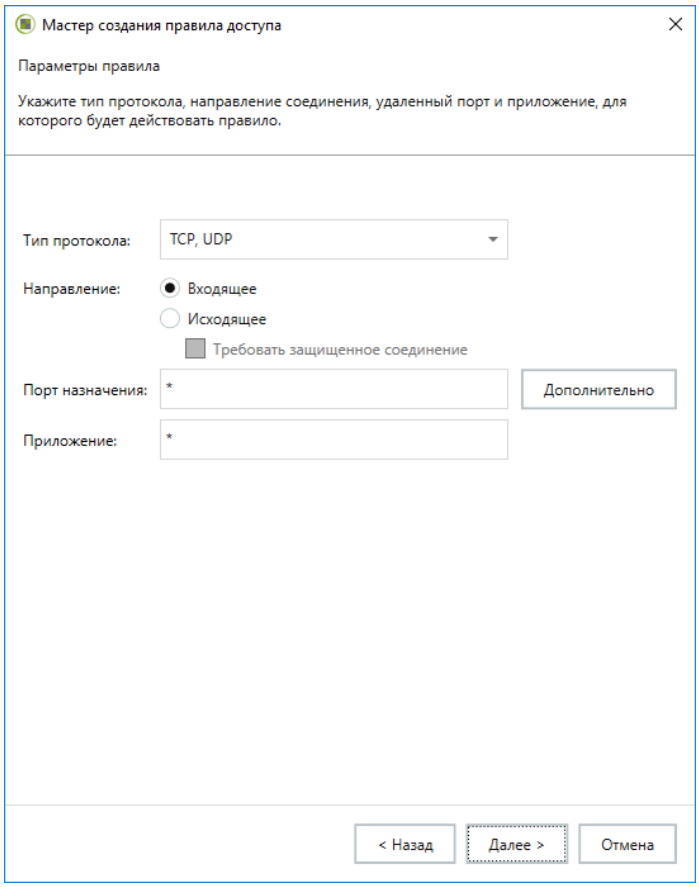


2. Настройте параметры и нажмите кнопку "Далее >".

Поле	Значение
Доступ	Выберите значение: • "Разрешить" — если при срабатывании правила требуется разрешить доступ к защищаемому объекту; • "Запретить" — если при срабатывании правила требуется запретить доступ к защищаемому объекту
Сетевой сервис	Выберите в списке название сетевого сервиса для типовой настройки параметров сетевых протоколов в создаваемом правиле. Если эти параметры предполагается настраивать вручную, выберите значение "<пусто>"

Примечание. В списке сетевых сервисов содержатся сервисы, заданные по умолчанию. Чтобы в списке появились сервисы, ранее созданные вручную (см. стр.36), нажмите кнопку "Обновить".

На экране появится следующий диалог мастера.



Пояснение. Если на предыдущем шаге мастера был выбран сетевой сервис, поля диалога будут настроены в соответствии с его параметрами. В этом случае при изменении данных параметров в полях диалога название выбранного сетевого сервиса будет заменено в правиле кратким описанием заданных параметров. При этом список сетевых сервисов изменен не будет.

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

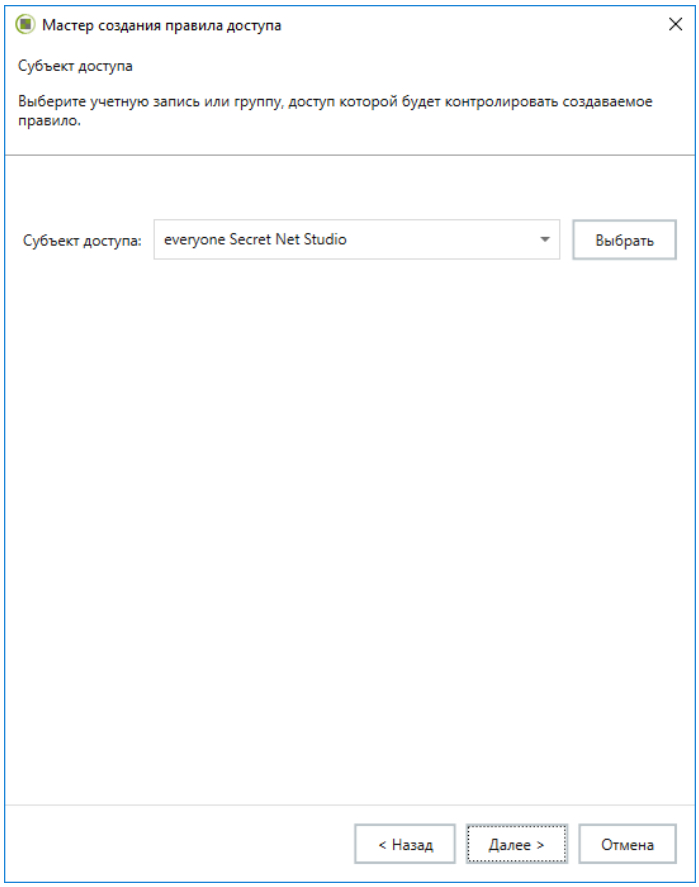
Поле	Значение
Тип протокола	Выберите тип протокола, для которого действует правило
Направление	Укажите направление трафика, для которого действует правило (по отношению к защищаемому объекту)

Поле	Значение
Требовать защищенное соединение	Отметьте поле, если для исходящего сетевого соединения требуется использовать защищенный канал передачи данных (см. стр.**41**)
Порт назначения	Укажите номера портов, для которых действует правило: • для входящего трафика укажите номера портов, на которые поступают IP-пакеты; • для исходящего трафика укажите номера портов, на которые отправляются IP-пакеты; • оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех портов. При вводе нескольких номеров портов разделяйте их символом "," (запятая). Для задания диапазона портов используйте символом "-" (дефис). Нажмите кнопку "Дополнительно", если требуется настроить перечень портов в диалоговом режиме.
Приложение	Укажите путь к исполняемому файлу приложения, для которого действует правило: • укажите путь к приложению. При указании пути к приложению можно также использовать системные переменные Windows; • оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех приложений. Созданное правило будет регулировать сетевой трафик для приложения, работающего непосредственно на защищаемом компьютере

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).

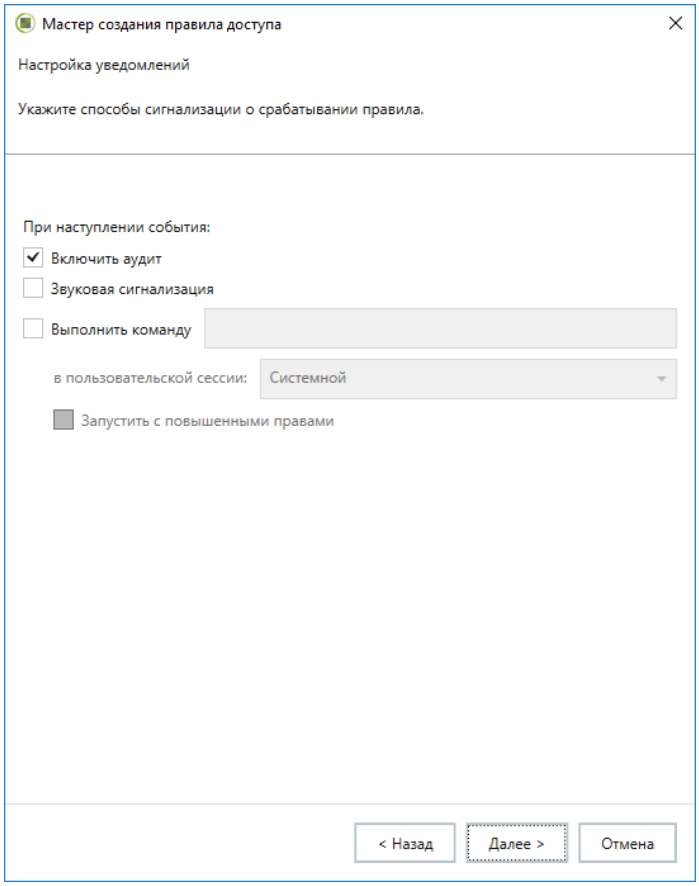
На экране появится диалог для выбора субъекта доступа.



Для выбора учетных записей в стандартном для Windows диалоге нажмите кнопку "Выбрать". Данная возможность есть только в сетевом режиме работы Secret Net Studio 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 настройки уведомлений о срабатывании правила.

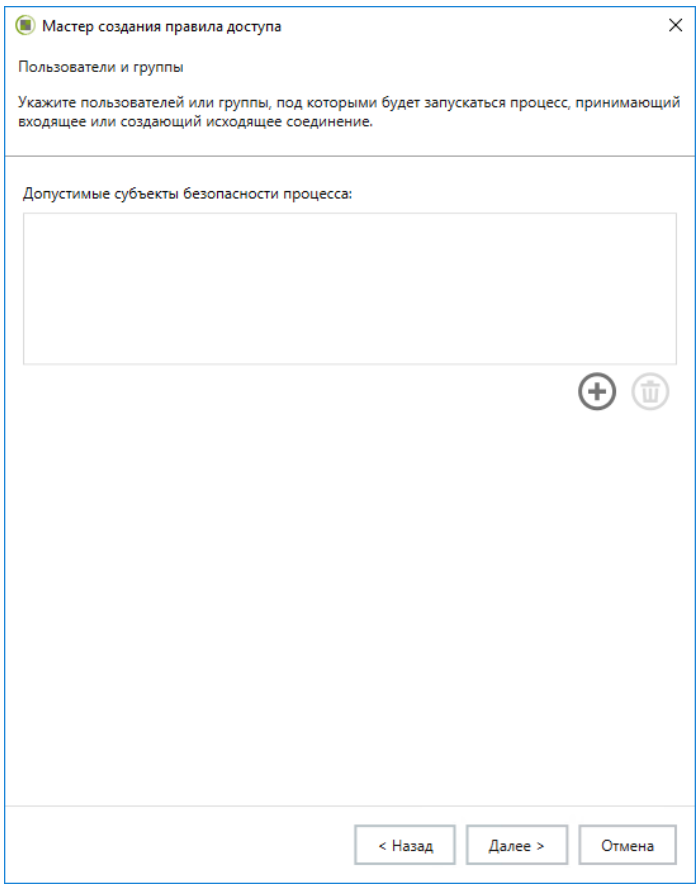


5. Укажите способы сигнализации о срабатывании правила, если это необходимо, и нажмите кнопку "Далее >".

Поле	Значение
Включить аудит	Поставьте отметку, если требуется фиксировать в журнале событие, возникающее при срабатывании правила. Если фиксировать событие не требуется — удалите отметку
Звуковая сигнализация	Поставьте отметку, если на защищаемом компьютере требуется подавать звуковой сигнал, оповещающий о срабатывании правила. Если подавать сигнал не требуется — удалите отметку
Выполнить команду	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
в пользовательской сессии	Поле доступно после выбора пункта "Выполнить команду". Выберите пользовательскую сессию, в которой необходимо выполнить указанную команду: • Системной — выполнить команду с правами системы; • Консольной — выполнить команду от имени пользователя в его сессии; • Всех сессиях пользователя — выполнить команду во всех пользовательских сессиях

Поле	Значение
Запустить с повышенными правами	Поставьте отметку, чтобы выполнить команду с полными правами пользователя, даже если для пользователя включен контроль учетных записей (UAC, User Account Control)

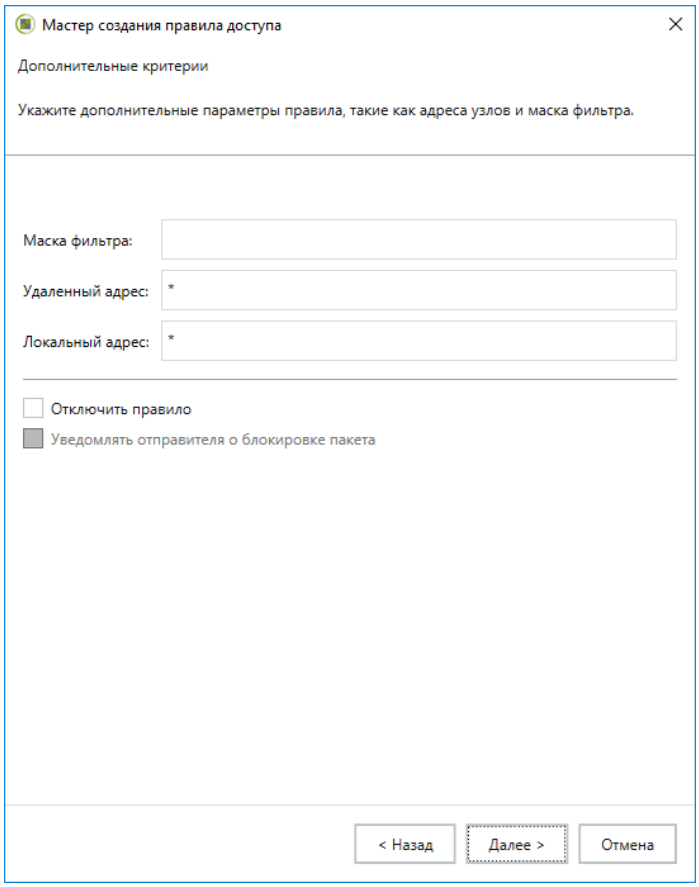
На экране появится диалог для выбора допустимых субъектов безопасности процессов.



Для выбора учетных записей в стандартном для Windows диалоге нажмите кнопку "Добавить". Чтобы удалить учетную запись из списка допустимых, выделите ее и нажмите кнопку "Удалить".

6. Укажите имя учетной записи или группы учетных записей, от имени которой будут запущены процессы, для которых будет действовать правило, и нажмите кнопку "Далее >".

На экране появится диалог для настройки дополнительных параметров.



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

Поле	Значение
Маска фильтра	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: • * — любое количество символов; • ? — один символ. Например, значению *abcd* будет соответствовать любой пакет, в теле которого встречается последовательность abcd
Удаленный адрес	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)
Локальный адрес	Укажите имя, IP-адрес компьютера, диапазон IP-адресов или подсеть, чтобы задать допустимый набор локальных адресов
Отключить правило	Управление работой правила: • отметка отсутствует — правило включено; • отметка установлена — работа правила временно приостановлена
Уведомлять отправителя о блокировке пакета	Управление оповещениями о блокировке пакетов в результате работы запрещающего правила: • отметка отсутствует — отправитель не получает уведомления о блокировке пакетов; • 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)

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.

8. 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, установленным для защищаемого компьютера.

Правило будет создано и отобразится в списке правил.

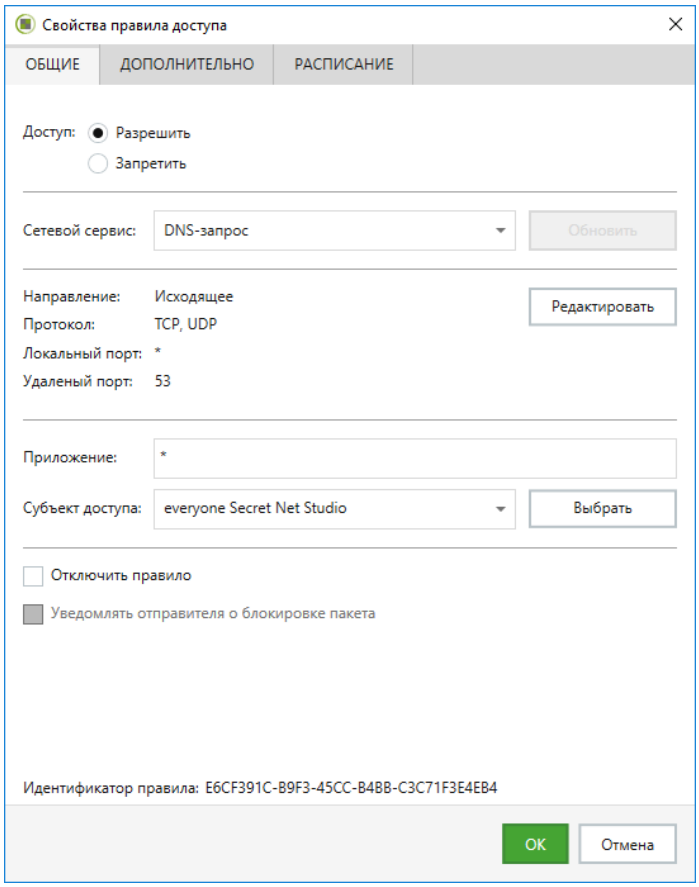
Управление работой правил доступа

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 "OK".

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 нужно удалить такие 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.

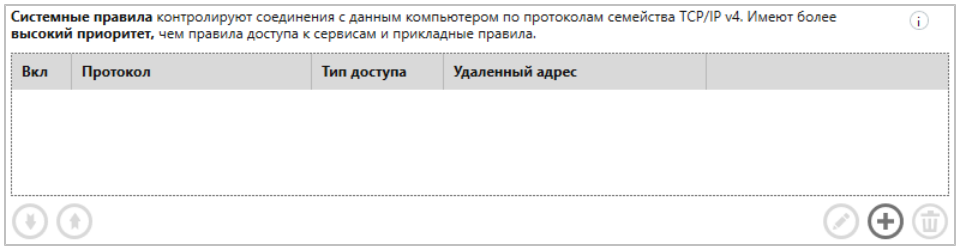
Управление системными правилами

Системные правила контролируют соединения с данным компьютером по протоколам семейства TCP/IP v4. Эти 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.



   Для каждого правила отображаются следующие данные.

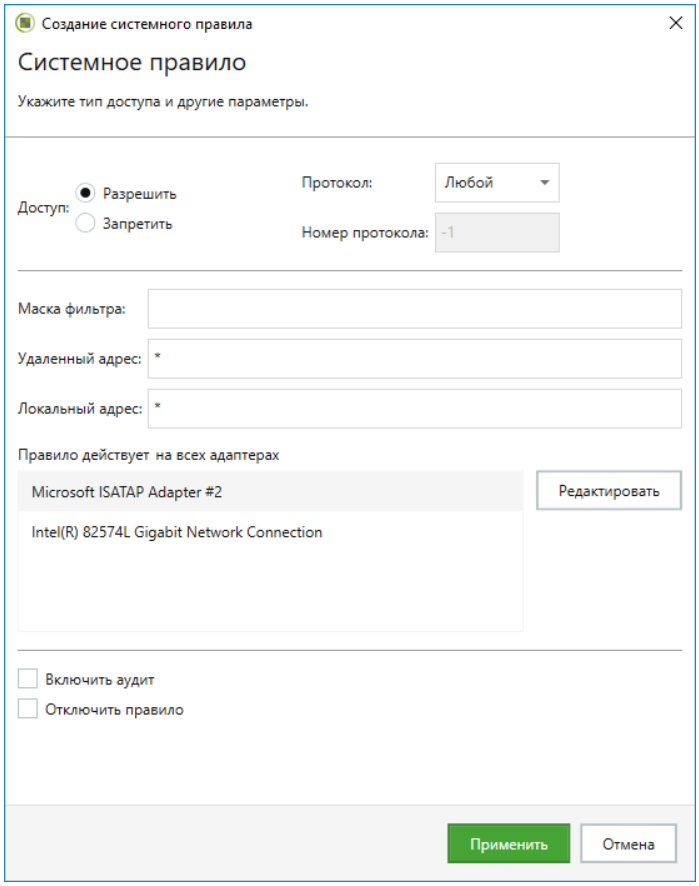
Столбец	Значение
Вкл	Управление работой правила: • отметка отсутствует — работа правила временно приостановлена; • отметка установлена — правило включено
Протокол	Наименование протокола, для которого действует правило
Тип доступа	Тип доступа к защищаемому компьютеру: • "Разрешен"; • "Запрещен"
Удаленный адрес	Адрес компьютера, для которого действует правило, или символ * (звездочка), если правило действует для всех удаленных компьютеров

2. Выполните нужные действия:
   - создайте правила (см. стр.**20**);
   - измените параметры правил (см. стр.**21**);
   - удалите ненужные правила (см. стр.**18**);
   - определите приоритет правил (см. стр.**9**);
   - настройте режим защиты протокола ICMP (см. стр.**35**).
3. Нажмите кнопку "Применить" внизу вкладки "Настройки".

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
Доступ	Выберите значение: • "Разрешить" — если при срабатывании правила требуется разрешить доступ к защищаемому объекту; • "Запретить" — если при срабатывании правила требуется запретить доступ к защищаемому объекту
Протокол	Выберите тип протокола, для которого действует правило, или: • "Любой" — если нужно, чтобы правило действовало для всех указанных в списке типов протоколов; • "Другой"— если нужный тип протокола отсутствует в списке. В этом случае станет доступным для изменения поле "Номер протокола"
Номер протокола	Если выбран тип протокола, то значение в этом поле устанавливается автоматически и изменить его нельзя. Если в поле "Протокол" выбрано значение "Другой", укажите номер протокола, для которого действует правило

Поле	Значение
Маска фильтра	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: • * — любое количество символов; • ? — один символ. Например, значению *abcd* будет соответствовать любой пакет, в теле которого встречается последовательность abcd
Удаленный адрес	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
Локальный адрес	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 локальных компьютеров
Правило действует ...	Чтобы правило действовало только на определенных адаптерах, нажмите кнопку "Редактировать" и выберите нужные адаптеры
Включить аудит	Управление регистрацией событий, возникающих при срабатывании данного правила: • отметка отсутствует — регистрация событий выключена; • отметка установлена — регистрация событий включена
Отключить правило	Управление работой правила: • отметка отсутствует — правило включено; • отметка установлена — работа правила временно приостановлена

Новое правило отобразится в списке правил.

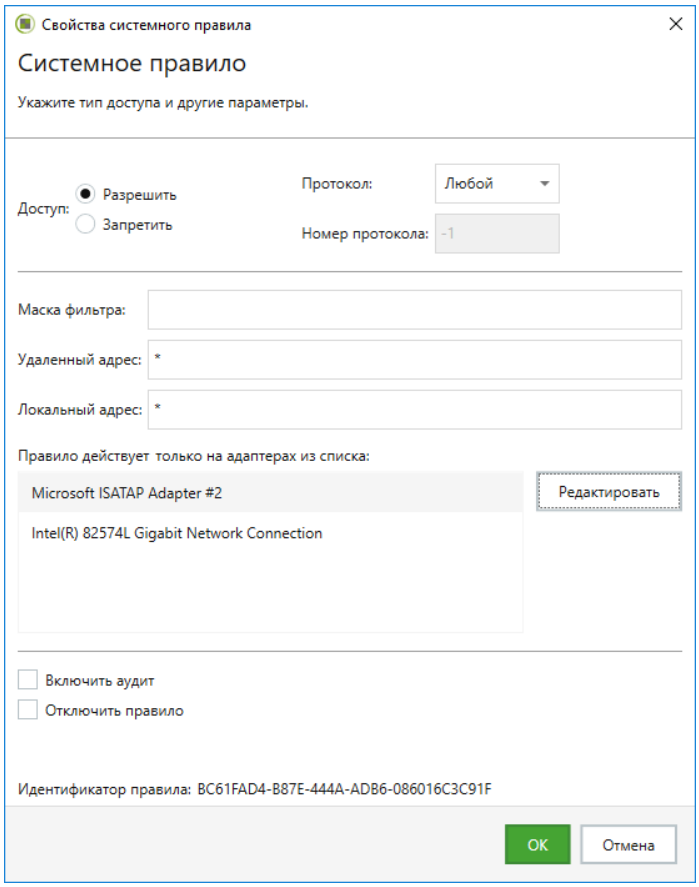
Управление работой системных правил

Параметры системного правила, указанные при его создании, можно изменить.

Для изменения параметров системного правила:

1. Выберите в таблице 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 "ОК".

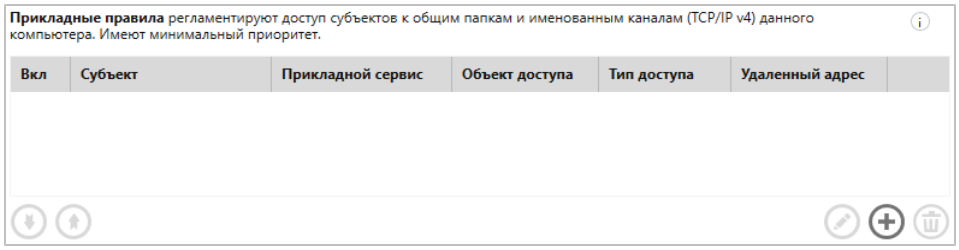
Управление прикладными правилами

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.



Для каждого правила отображаются данные:

Столбец	Значение
Вкл	Управление работой правила: • отметка отсутствует — работа правила временно приостановлена; • отметка установлена — правило включено
Субъект	Имя учетной записи или группы учетных записей, для которых действует правило
Прикладной сервис	Наименование прикладного сервиса: • "Общие папки"; • "Именованные каналы"
Объект доступа	Наименование общей папки или именованного канала, для которого действует правило. Символ * (звездочка) означает, что правило действует для всех объектов этого типа
Тип доступа	Тип доступа к защищаемому компьютеру: • "Разрешен"; • "Запрещен"
Удаленный адрес	Имя или IP-адрес компьютера, для которого действует правило. Символ * (звездочка) означает, что правило действует для всех удаленных компьютеров

2. Выполните нужные действия:
   - создайте правила (см. стр.**24**);
   - измените параметры правил (см. стр.**28**);
   - удалите ненужные правила (см. стр.**18**);
   - определите приоритет правил (см. стр.**9**).
3. Нажмите кнопку "Применить" внизу вкладки "Настройки".

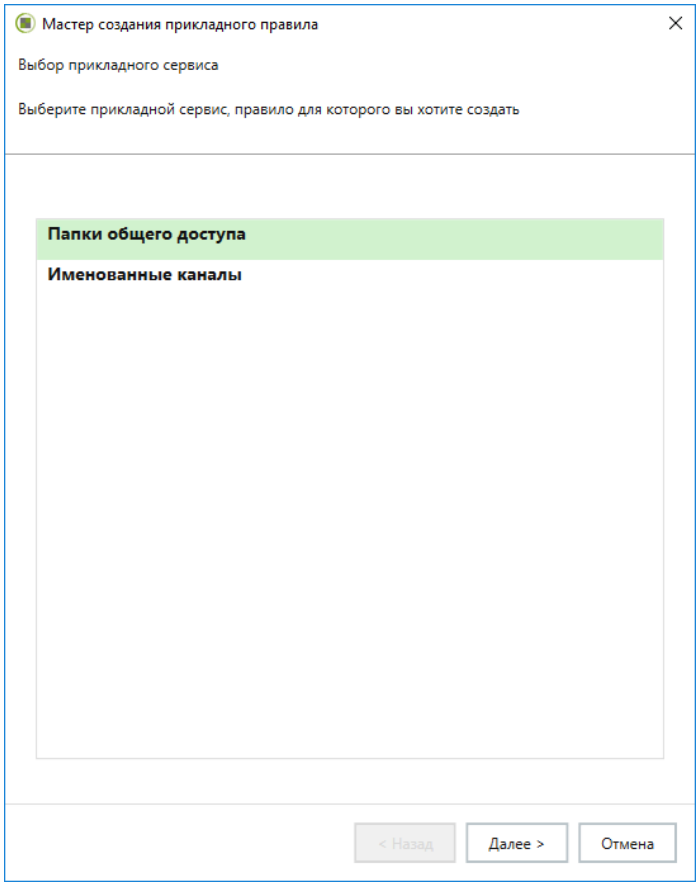
Создание прикладного правила

Для создания прикладного правила используется специальная программа-мастер.

Для создания правила:

1. Нажмите кнопку "Добавить".

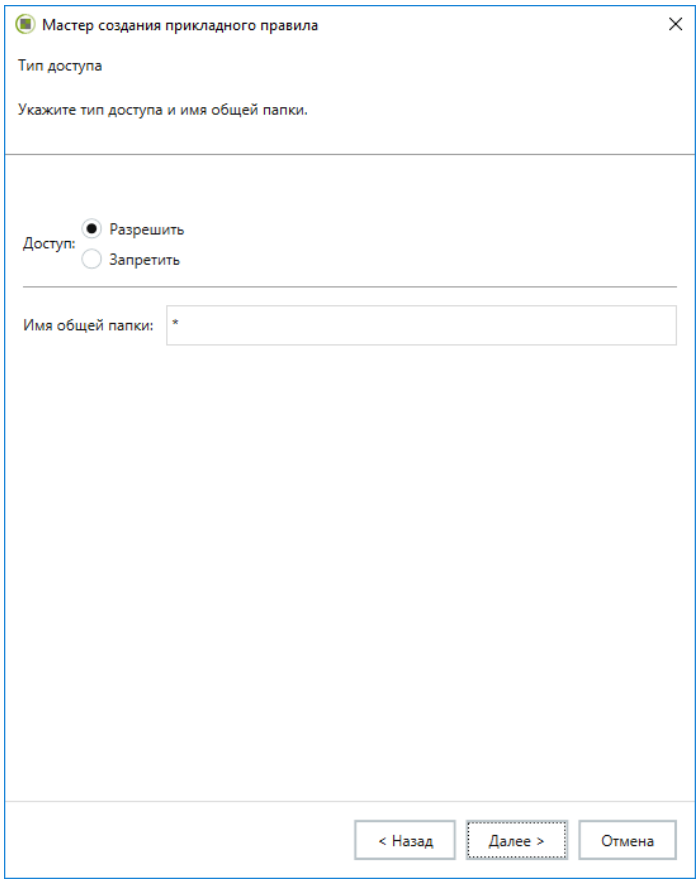
   На экране появится первый диалог мастера создания правила.



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 для настройки параметров правила.



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

Поле	Значение
Доступ	Выберите значение: • "Разрешить" — если при срабатывании правила требуется разрешить доступ к защищаемому объекту; • "Запретить" — если при срабатывании правила требуется запретить доступ к защищаемому объекту
Имя общей папки/ Именованный канал	Укажите название папки или канала, для которой(ого) действует правило. Оставьте символ * (звездочка), если правило будет действовать для всех папок или именованных каналов на данном компьютере

Пояснение.

- 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 символы: ? (вопросительный знак) — для замены одного символа и * (звездочка) — для замены нескольких символов, включая пробел.
- 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.

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

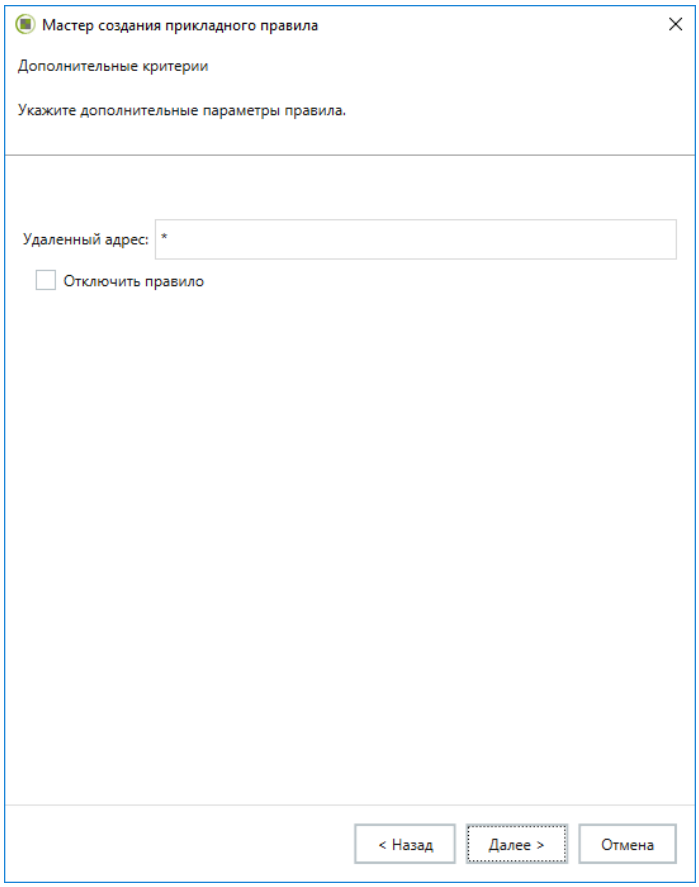
Совет. Для выбора учетных записей в стандартном для Windows диалоге нажмите кнопку "Выбрать".

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
Включить аудит	Отметьте, если требуется фиксировать в журнале событие, возникающее при срабатывании этого правила. Если фиксировать событие не требуется — удалите отметку
Звуковая сигнализация	Отметьте, если на защищаемом компьютере требуется подавать звуковой сигнал, оповещающий о срабатывании правила. Если подавать сигнал не требуется — удалите отметку
Выполнить команду	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
в пользовательской сессии	Поле доступно после выбора пункта "Выполнить команду". Выберите пользовательскую сессию, в которой необходимо выполнить указанную команду: • Системной — выполнить команду с правами системы; • Консольной — выполнить команду от имени пользователя в его сессии; • Всех сессиях пользователя — выполнить команду во всех пользовательских сессиях
Запустить с повышенными правами	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.



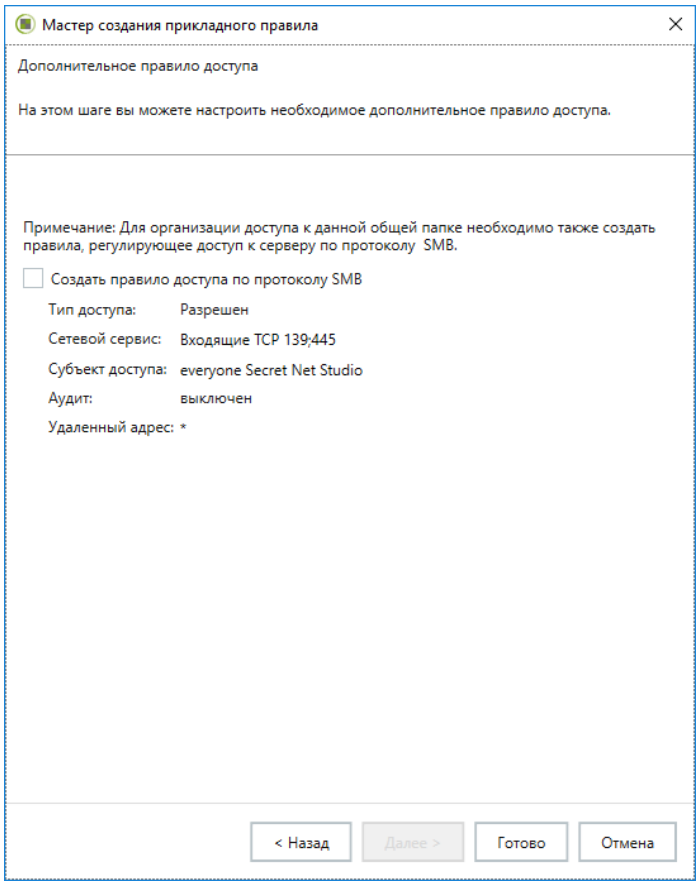
6. Укажите дополнительные параметры правила и нажмите кнопку "Далее >".

Поле	Значение
Удаленный адрес	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, осуществляющих попытку доступа
Отключить правило	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.

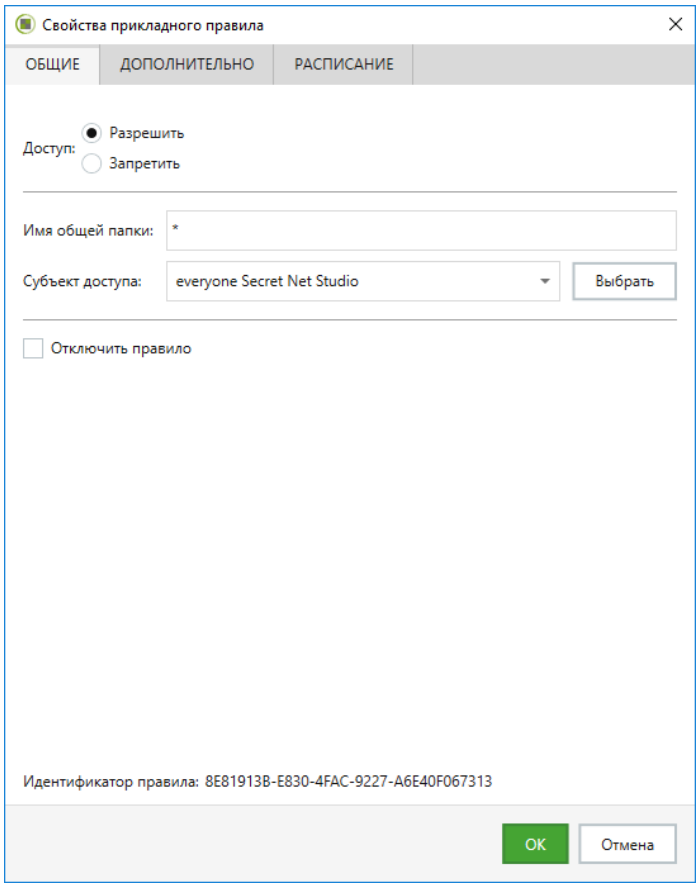
Управление работой прикладных правил

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 "OK".

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 папке установки, по умолчанию — 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 папке установки, по умолчанию — 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.exe [@argfile] [/?|h|help] [/v|version]
<domain> [/local] [kdc] [/p|password <value>] [/a|admin
<value>] [/q <value>] [/s <value>]
```

где:

- @argfile — прочитать 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 данном 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 введите следующую команду в командной строке утилиты:

```
add network_stream_filtration_rule <protected_computer>
/filter <value> [/flt-case-insensetive | /flt-case-sensetive]
[/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 команды и параметры правила:

Параметр	Описание	Возможные значения
add network_stream_ filtration_rule или add nsfr	Команда для создания правила фильтрации	
modify network_ stream_filtration_rule или modify nsfr	Команда для редактирования правила фильтрации	
protected_computer	Полное доменное имя защищаемого компьютера, для которого будет действовать правило	

Параметр	Описание	Возможные значения
filter	Маска фильтра	• * — заменяет любое количество символов; • ? — заменяет один символ
flt-case-insensetive	Регистронезависимый поиск	
flt-case-sensetive	Регистрозависимый поиск. Применяется по умолчанию	
at (access type)	Тип правила доступа	• deny — при обнаружении последовательности, попадающей под маску фильтра, соединение будет разорвано. Значение задано по умолчанию; • allow — при обнаружении последовательности, попадающей под маску фильтра, будет выполнен только аудит (если он разрешен)
direction	Список направлений соединений (сетевого трафика), для которых будет применяться это правило. В качестве разделителя используется ";"	• in — правило будет применяться для входящих соединений, для входящего трафика. Значение задано по умолчанию; • in_reply — правило будет применяться для входящих соединений, для ответного трафика; • out — правило будет применяться для исходящих соединений, для исходящего трафика; • out_reply — правило будет применяться для исходящих соединений, для ответного трафика
local_addrs	Список локальных адресов/сетей/диапазонов, для которых действует правило. В качестве разделителя используется ";"	
local_ports	Список локальных портов/диапазонов, для которых действует правило. В качестве разделителя используется ";"	
remote_addrs	Список удаленных адресов/сетей/диапазонов, для которых действует правило. В качестве разделителя используется ";"	
remote_ports	Список удаленных портов/диапазонов, для которых действует правило. В качестве разделителя используется ";"	

Параметр	Описание	Возможные значения
audit	Включение/выключение аудита при срабатывании правила	• 1 — аудит включен; • 0 — аудит выключен
order	Порядок применения правил. Параметр влияет только на порядок срабатывания правил	
enable	Текущий статус правила	• 1 — правило включено; • 0 — правило выключено

Для редактирования правила фильтрации используется следующая команда:

```
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
JavaScript	Content-Type: text/javascript Content-Type: text/jscript 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
Adobe Flash	Content-Type: application/x-shockwave-flash
VBScript	Content-Type: text/vbscript
Java	Content-Type: application/java-archive Content-Type: application/jar
ActiveX	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-insensetive /direction out_reply /remote_ports 80
add nsfr SP-VM01 /filter "Content-Type: application/x-ms"
/flt-case-insensetive /direction out_reply /remote_ports 80
add nsfr SP-VM01 /filter " Content-Disposition*filename*ocx"
/flt-case-insensetive /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:

```
show network_stream_filtration_rules(nsfrs) <protected_
computer>
```

где <protected_computer> — имя защищаемого компьютера.

Пример

```
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:

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

где:

- <protected_computer> — имя защищаемого компьютера;
- <id> — идентификатор правила.

Пример

```
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:

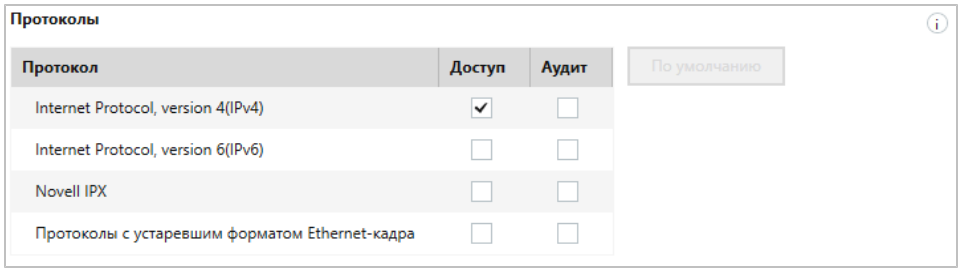
```
delete network_stream_filtration_rule(nsfr) <protected_
computer> <id>
```

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".



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" внизу вкладки "Настройки".

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

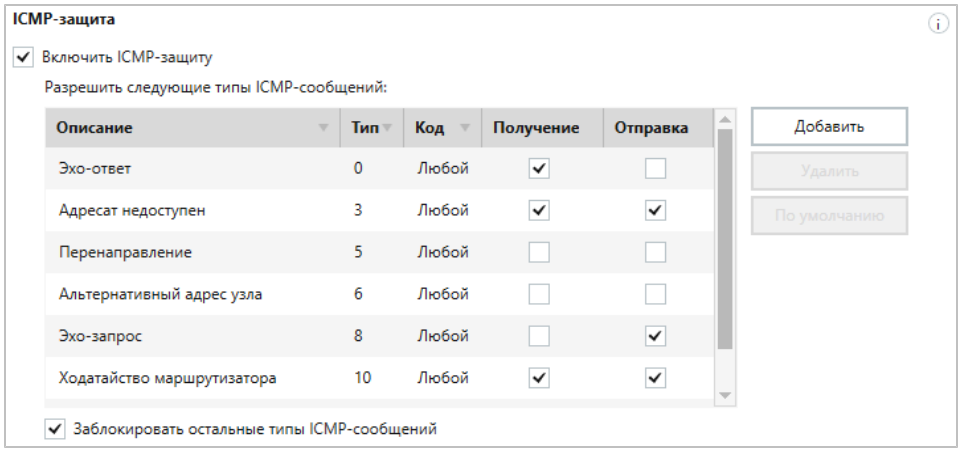
Настройка "Протоколы с устаревшим форматом Ethernet-кадра" позволяет заблокировать Ethernet-кадры, в заголовке которых вместо типа кадра содержится значение его длины. Посредством таких кадров на защищаемый сервер может пройти трафик IPX, SMB поверх NetBEUI и даже IP-трафик.

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".



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
Включить ICMP-защиту	Отметьте поле, если требуется включить защиту ICMP
Столбцы "Получение" и "Отправка"	Разрешите или запретите прохождение входящих и исходящих пакетов. Чтобы разрешить — поставьте отметку в нужную ячейку, чтобы запретить — удалите ее
Заблокировать остальные типы ICMP-сообщений	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 выбранных строк ("Удалить" – нельзя удалить строки, содержащиеся в таблице по умолчанию) или возврата таблицы к первоначальному состоянию ("По умолчанию").

3. Для сохранения новых значений параметров нажмите кнопку "Применить" внизу вкладки "Настройки".

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

Управление сетевыми сервисами

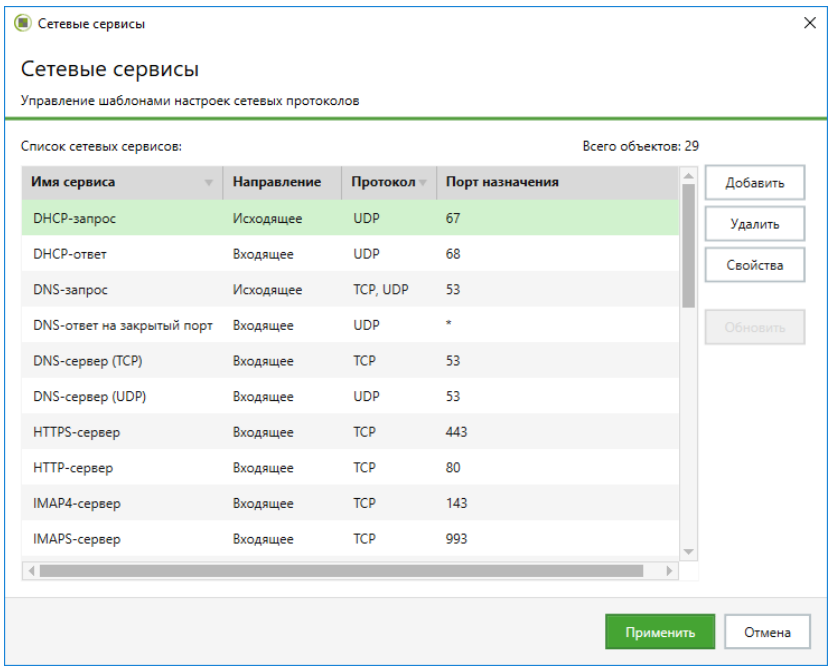
Сетевые сервисы — это список шаблонов наиболее распространенных настроек сетевых протоколов. Для каждого сервиса указываются следующие данные:

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

Для управления сетевыми сервисами:

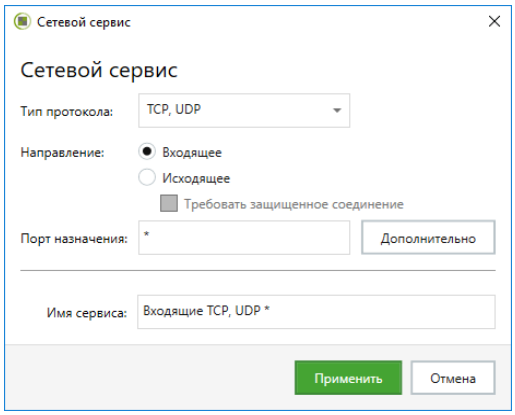
1. В области настройки параметров межсетевого экрана в разделе "Правила доступа" нажмите кнопку-ссылку "сетевым сервисам".

   На экране появится следующий диалог.



2. Для создания сетевого сервиса нажмите кнопку "Добавить".

   На экране появится диалог для настройки параметров сервиса.



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

Параметр	Значение
Тип протокола	Выберите тип протокола для этого сетевого сервиса
Направление	Укажите направление трафика для этого сетевого сервиса: • "Входящее"; • "Исходящее"
Требовать защищенное соединение	Отметьте это поле, если для этого сетевого сервиса требуется использовать защищенное соединение (см. стр.**41**)
Порт назначения	Укажите номера портов для этого сетевого сервиса: • для входящего трафика укажите номера портов, на которые поступают IP-пакеты; • для исходящего трафика укажите номера портов, на которые отправляются IP-пакеты; • оставьте символ ***** (звездочка), если требуется, чтобы сетевой сервис действовал для всех портов. При вводе нескольких номеров портов разделяйте их символом "," (запятая). Для задания диапазона портов используйте символ "-" (дефис). Нажмите кнопку "Дополнительно", если требуется настроить перечень портов в диалоговом режиме
Имя сервиса	Введите название, под которым требуется сохранить шаблон сетевого сервиса

Сетевой сервис будет создан и отобразится в списке сетевых сервисов.

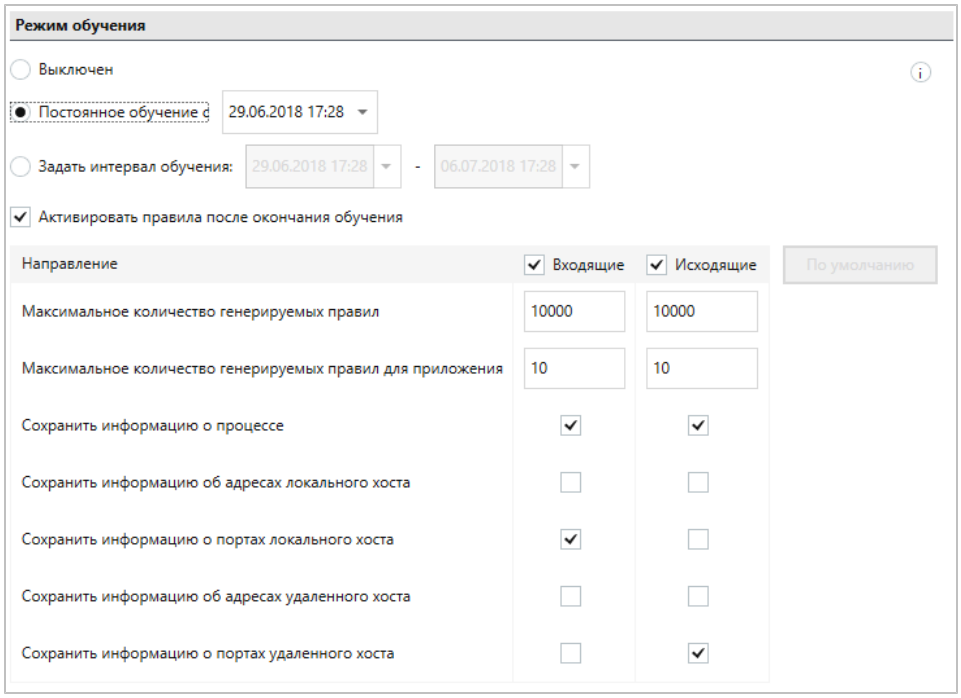
4. Для удаления сетевого сервиса выберите его в списке и нажмите кнопку "Удалить".
5. Для изменения параметров сетевого сервиса выберите его в списке и нажмите кнопку "Свойства". В появившемся диалоге измените параметры сервиса, руководствуясь описанием, приведенным в п.**3** данной процедуры, и нажмите кнопку "Применить".
6. Для сохранения изменений нажмите кнопку "Применить" в диалоге настройки сетевых сервисов.
7. Для сохранения новых значений параметров нажмите кнопку "Применить" внизу вкладки "Настройки".

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".



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

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

4. Для сохранения новых значений параметров нажмите кнопку "Применить" внизу вкладки "Настройки".

Режим обучения будет настроен в соответствии с указанными параметрами.

Управление работой межсетевого экрана на защищаемых компьютерах

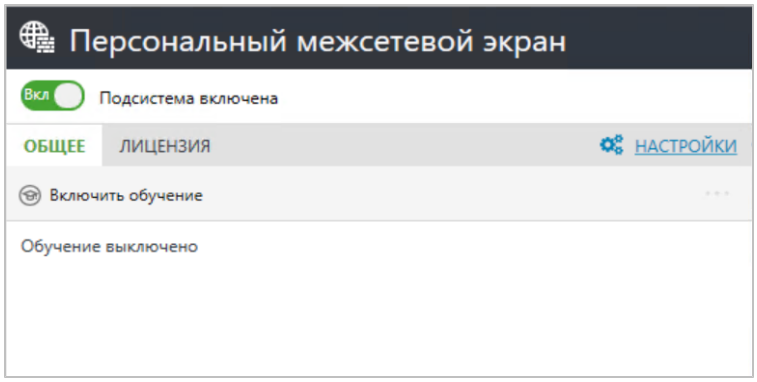
Программа управления Secret Net Studio позволяет осуществлять для отдельного компьютера управление режимом обучения.

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" выберите объект "Персональный межсетевой экран".

   В правой части экрана появится панель управления межсетевым экраном.



3. Для включения или отключения межсетевого экрана переведите в нужное положение переключатель в левом верхнем углу панели.
4. Для управления работой режима обучения нажмите кнопку:
   - "Включить обучение" — для включения режима обучения. После этого в панели появятся две следующие кнопки;
   - "Прервать обучение и сохранить правила" — для отключения режима обучения и сохранения всех уже сформированных правил;
   - "Прервать обучение без сохранения правил" — для отключения режима обучения и удаления всех сформированных в ходе обучения правил.

   Режим обучения позволяет сформировать базовый набор правил доступа (см. стр.**37**).

Примечание. Нажмите кнопку-ссылку "НАСТРОЙКИ", чтобы перейти к настройке политик межсетевого экрана (см. стр.**9**).

Перейдите на вкладку "Лицензия" и нажмите кнопку-ссылку "Перейти к информации о лицензии", чтобы просмотреть сведения о действующей лицензии.

Глава 3
Авторизация сетевых соединений

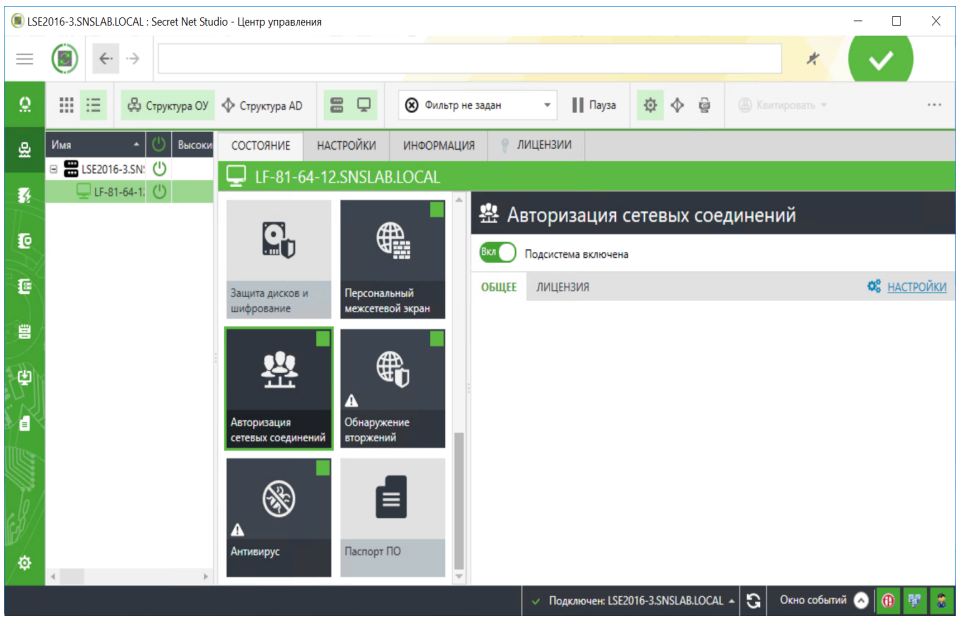
Настройка механизма авторизации сетевых соединений осуществляется централизованно в программе управления. Она выполняется на уровне объектов "Компьютер" по отдельности для каждого из защищаемых компьютеров.

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.



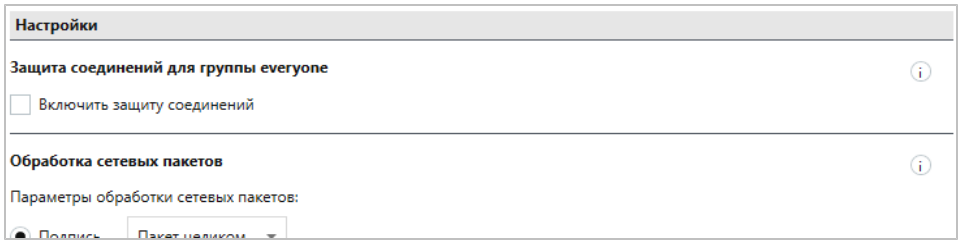
Совет. Для просмотра значений параметров механизма авторизации сетевых соединений непосредственно на защищаемом компьютере вызовите программу "Локальный центр управления", перейдите на вкладку "Настройки" и в разделе "Политики" выберите элемент "Авторизация сетевых соединений". В локальном режиме управления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

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

   В правой части экрана появится область настройки выбранных параметров.



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

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
Протокол AH (Authentication Header)	Позволяет гарантировать аутентичность и целостность передаваемых данных каждого IP-пакета. Обеспечивает защиту от атак типа "Man in the Middle"
Протокол ESP (Encapsulating Security Payload)	Используется для кодирования и контроля целостности передаваемых данных
Протокол ISAKMP	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.

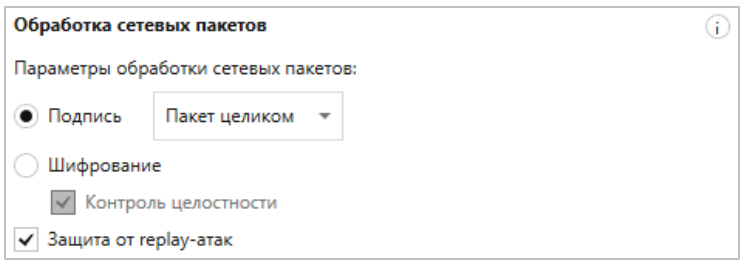
Защита и целостность передаваемых данных обеспечивается следующими средствами:

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

Примечание. В текущей версии Secret Net Studio 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
Подпись	Отметьте поле для включения режима добавления служебной информации к пакетам и выберите в списке уровень анализа: • "Только маркировка" — служебная информация формируется на основе первого сетевого пакета из серии, остальные пакеты получают метку принадлежности к аутентифицированной серии; • "Заголовки пакетов" — служебная информация формируется на основе заголовков пакетов; • "Пакет целиком" — служебная информация формируется для каждого пакета полностью. 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-получателю, будут дополнены служебной информацией
Шифрование	Отметьте поле для включения режима кодирования данных
Контроль целостности	Поставьте отметку, чтобы включить режим контроля целостности закодированных пакетов. Если требуется отключить режим контроля целостности закодированных пакетов — удалите отметку из поля "Контроль целостности"
Защита от replay-атак	Отметьте поле для включения режима защиты, с помощью которого предотвращается пассивный захват данных и их пересылка

3. Для сохранения новых значений параметров нажмите кнопку "Применить" внизу вкладки "Настройки".

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.

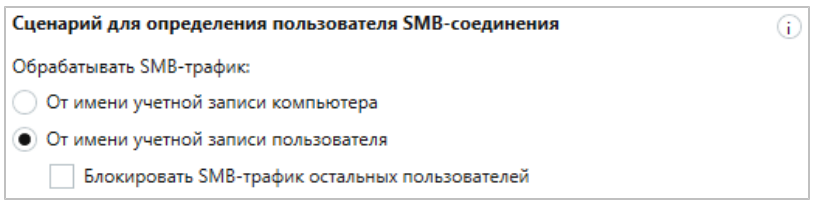
Приоритет предоставления SMB-соединений (от низшего к высшему): анонимные пользователи, сервисы, авторизованные пользователи Secret Net Studio.

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. В области настройки параметров механизма авторизации сетевых соединений перейдите к разделу "Настройки | Сценарий для определения пользователя SMB-соединения".



Примечание. Если SMB-соединение создается до начала работы компонентов механизма (например, mapped drive с флагом 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
От имени учетной записи компьютера	Отметьте поле, если SMB-соединения требуется устанавливать под учетной записью компьютера
От имени учетной записи пользователя	Отметьте поле, если SMB-соединения требуется устанавливать под учетной записью пользователя
Блокировать SMB-трафик остальных пользователей	Поставьте отметку, если требуется запретить использование SMB-соединения всем пользователям, кроме пользователя — инициатора соединения

Пояснение. Все пользователи получат 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 получат доступ к защищаемому объекту под одной и той же учетной записью.

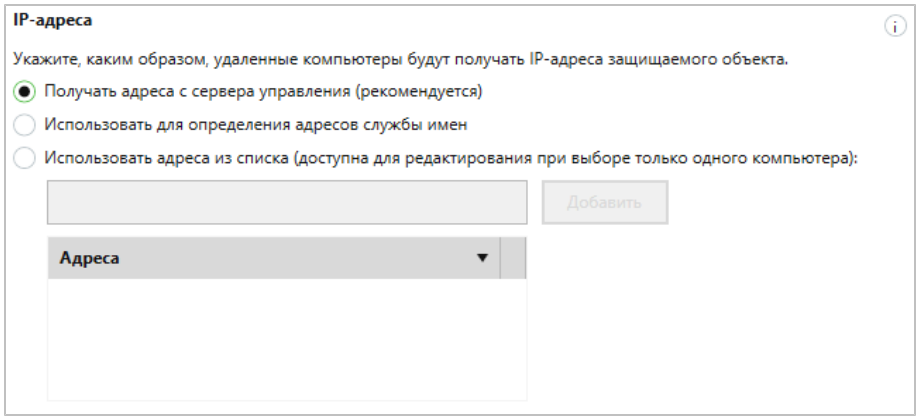
3. Для сохранения новых значений параметров нажмите кнопку "Применить" внизу вкладки "Настройки".

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".



2. Настройте параметры.

Поле	Значение
Получать адреса с сервера управления	По умолчанию клиенты будут получать IP-адреса данного защищаемого компьютера автоматически с сервера безопасности, которому компьютер подчинен
Использовать для определения адресов службы имен	Отметьте это поле, чтобы за адресами клиенты обращались к службам DNS, WINS и NetBIOS
Использовать адреса из списка	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. Нажмите кнопку "Применить" внизу 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.

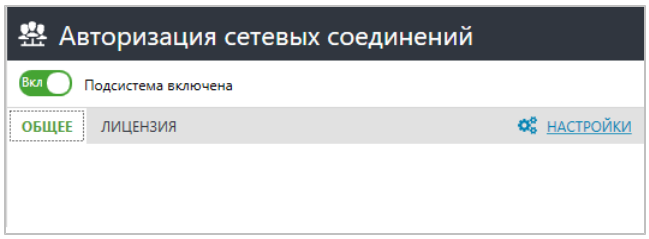
Для управления работой механизма авторизации соединений:

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".

   В правой части экрана появится панель управления данным механизмом.



3. Для включения или отключения механизма переведите в нужное положение переключатель в левом верхнем углу панели.

Примечание. Нажмите кнопку-ссылку "НАСТРОЙКИ", чтобы перейти к настройке политик механизма авторизации сетевых соединений (см. стр.40).
Перейдите на вкладку "Лицензия" и нажмите кнопку-ссылку "Перейти к информации о лицензии", чтобы просмотреть сведения о действующей лицензии.

Документация

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