Киберсейф Межсетевой экран для Windows

Руководство пользователя

Содержание

Общая информация о программе Киберсейф Межсетевой экран 1

Назначение программы 5
Условные обозначения, используемые в этом Руководстве 5
Для кого предназначен этот документ 6
Лицензионное соглашение на использование изделия 6
Термины и определения 6
Предмет соглашения 7
Авторские права 7
Условия использования 7
Срок действия соглашения 8
Ответственность 8
Гарантии изготовителя (поставщика) 8
Помощь по работе с программой 9
Дополнительная информация о продукте 9
Контактная информация 9

Киберсейф Межсетевой экран. Основы 2

Основные функции программы 10

Установка Киберсейф Межсетевой экран 3

Перед установкой 12
Системные требования 12
Установка программы 12
Первый запуск программы 17
Запуск и завершение работы программы 17
Киберсейф Межсетевой экран и брандмауэр Windows 19
Первичная настройка 20
Деинсталляция программы 21

Пользовательский интерфейс 4

Основное окно программы 22
Активные соединения 23
Сетевые интерфейсы 23
Лог пакетов 26

Настройки программы 5

Общие параметры программы 30
Дополнительные параметры программы 31
Управление пользователями 32
Смена пользователя 33
Параметры протоколирования 33
Просмотр системного журнала 34

Настройка правил брандмауэра 6

Правила безопасности 36
Что такое правила безопасности? 36
Основные свойства правил безопасности 36
Просмотр правил безопасности 37
Создание правила безопасности 39

Правила переадресации 43
Правила шейпера: ограничение пропускной способности 44
Что такое правила шейпера? 44
Свойства правила шейпера 44
Создание правила шейпера 44

Маршрутизация и NAT 7

Преобразование сетевых адресов (NAT) 46
Маршрутизация 48
Сетевые псевдонимы 49

Киберсейф Удаленный сервер 8

Назначение программы 51
Первый запуск программы 51
Запуск сервера 52
Настройка клиентов 53
Просмотр общей информации и журнала 54
Назначение пользователя администратором 56
Создание сценария развертывания 57
Развертывание программы с помощью Active Directory 59

Панель администрирования 9

Интерфейс панели администрирования 67
Групповые и глобальные правила 69
Удаленное управление файрволом 70
Блокирование сайтов 71

Примеры и лучшая практика 10

Глобальная блокировка доступа к узлу Интернета по IP-адресу 73
Локальная блокировка доступа к узлу Интернета по URL 74
Запрещаем ICQ 74
Сервер шлюза 75
Запрет доступа к ресурсам Интернета только определенным узлам 76
Разграничение в ИСПД 77
Ограничение скорости для определенной группы 81
Третий уровень невидимости на сервере 82
Переадресация RDP 82

1 Общая информация о программе Киберсейф Межсетевой экран

Киберсейф Межсетевой экран - мощный межсетевой экран (файервол), разработанный для защиты компьютерных систем и локальной сети от внешних вредоносных воздействий. Программа защищает вашу систему от внешних атак. Эффективность защиты достигается путем фильтрации входящего и исходящего трафика на основе выбранной политики безопасности.

В этом разделе

Назначение программы 5
Условные обозначения, используемые в этом Руководстве 5
Для кого предназначен этот документ 6
Лицензионное соглашение 6
Помощь по работе с программой 9

Назначение программы

Программа разрабатывалась как комплексное решение, предназначенное для защиты систем на базе ОС Windows. Возможно использование программы, как на сервере (в качестве межсетевого экрана сети), так и на рабочей станции (в качестве персонального брандмауэра). Программа позволяет осуществлять мониторинг, устанавливать контроль трафика для Интернет-ресурсов и просматривать входящий и исходящий трафик с возможностью сортировки и экспорта в файл.

Программа сертифицирована ФСТЭК, с соответствующим сертификатом вы можете ознакомиться по адресу: http://cybersafesoft.com/rus/products/cybersafe-firewall/certificate/.

Условные обозначения, использующиеся в Руководстве

Примечания. Дополнительные, но важные сведения, которые обращают Ваше внимание на существенные моменты в работе с программой. Читая их, вы сможете использовать программу более эффективно.

Предупреждения. Указывают на возможность потери данных либо на незначительные нарушения безопасности. Предупреждения расскажут вам о ситуациях, в которых могут возникнуть проблемы, если не принять необходимые меры предосторожности. Уделите этим пунктам должное внимание.

Предостережения. Указывают на возможность значительной потери данных или возникновения серьезной бреши в безопасности, а также сообщают о существенных проблемах, которые могут возникнуть в том случае, если не будут предприняты своевременные меры по их предотвращению. Отнеситесь к Предостережениям очень серьезно.

Для кого предназначен этот документ

Это Руководство адресовано всем, кто намерен использовать Киберсейф Межсетевой экран для защиты компьютерных систем, работающих под управлением ОС Windows, и локальной сети от внешних вредоносных воздействий.

Документ содержит описание контролируемых функций, описание процедуры первого старта Киберсейф Межсетевой экран, краткие инструкции по настройке и конфигурированию. Так же в документе приводятся типовые примеры по настройке и конфигурированию межсетевого экрана.

Лицензионное соглашение на использование изделия

Настоящее Лицензионное соглашение является общей офертой ООО "КиберСофт" и Пользователем – физическим или юридическим лицом. Настоящее Лицензионное соглашение в случае согласия, выраженного в форме молчания в течение 7 дней с момента приобретения Изделия, в соответствии со ст. 433 ГК РФ, имеет силу договора.

Термины и определения

- Под Изделием понимается комплекс программ для ЭВМ, включая носители и документацию, который является объектом авторского права и охраняется законом.
- Везде в тексте под словом “документация” подразумеваются печатные материалы и носители, содержащие документацию в электронном виде. Документация является неотъемлемой частью Изделия.
- Данное Изделие (программный продукт), включая носители и печатные материалы, передается на условиях Лицензионного соглашения.
- Дальнейшая установка Изделия рассматривается как согласие с условиями Лицензионного соглашения и вступление его в законную силу.
- В случае несогласия с каким-либо из условий Лицензионного соглашения в течение семи дней со дня получения продукта, Пользователь должен

вернуть полный комплект Изделия, включая печатные материалы и упаковку с носителями, в компанию, предоставившую данное Изделие.

Предмет соглашения

- Предметом настоящего Лицензионного соглашения является возмездная передача Пользователю прав пользования и владения на Изделие.
- Все условия, оговоренные далее, относятся как к Изделию в целом, так и ко всем его компонентам в отдельности.

Авторские права

- Изделие и его компоненты являются интеллектуальной собственностью разработчика и защищаются законодательством об авторском праве © 2015 КиберСофт (ООО).
- Право использования Изделия предоставляется только конечному Пользователю как владельцу, и никаким иным третьим лицам, если нет письменного согласия ООО "КиберСофт" на обратное.

Условия использования

- Пользователь может хранить, установить и использовать только определенное количество экземпляров Изделия. Пользователь не имеет права хранить, устанавливать или использовать (в установленном или неустановленном виде) большее количество экземпляров Изделия, чем предоставлено ему и определено в соответствующих документах на право использования Изделия.
- Пользователь обязуется не распространять данное Изделие. Под распространением Изделия понимается предоставление доступа третьим лицам к воспроизведенным в любой форме компонентам Изделия путем продажи, проката, сдачи внаем, предоставления взаймы или иными другими способами отчуждения.
- Пользователь не имеет права осуществлять следующую деятельность:
  - допускать использование Изделия людьми, не имеющими прав на такое использование;
  - пытаться дизассемблировать, декомпилировать (преобразовывать объектный код в исходный текст) программы и другие компоненты Изделия;
  - вносить какие-либо изменения в объектный код программ за исключением тех, которые вносятся средствами, включенными в комплект Изделия и описанными в документации;
  - совершать относительно Изделия другие действия, нарушающие Российские и международные нормы по авторскому праву и использованию программных средств.

Примечание. Использование шифровальных средств криптографической защиты информации подлежит лицензированию в соответствии с действующим законодательством РФ.

Срок действия соглашения

- Настоящее Лицензионное соглашение вступает в силу с момента вскрытия упаковки с носителями Киберсейф Межсетевой экран или установки программного обеспечения из комплекта Изделия и действует на протяжении всего срока использования Изделия.
- В случае нарушения условий Лицензионного соглашения или неспособности далее выполнять его условия, все компоненты Изделия (включая печатные материалы, магнитные носители, файлы с информацией, архивные копии) должны быть уничтожены. Пользователь обязан подтвердить факт уничтожения Изделия в письменном виде. Лицензионное соглашение при этом прекращает свое действие.

Ответственность

- Пользователь приобретает Изделие и несет ответственность за его использование в соответствии с рекомендациями, изложенными в эксплуатационной документации.
- Нелегальное использование, распространение, воспроизведение для третьих лиц, копирование программного обеспечения является нарушением Закона Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" и преследуется по закону.
- В случае нарушения настоящего Лицензионного соглашения конечный Пользователь лишается права на использование Изделия, при этом гарантийные обязательства на обслуживание Изделия снимаются.

Гарантии изготовителя (поставщика)

- Изготовитель гарантирует работоспособность Изделия при соблюдении требований эксплуатации, транспортирования и хранения, корректном его пользовании и пользовании Изделия в "невирусной среде".
- В случае выявления дефектов в программах, не связанных с нарушением правил эксплуатации, транспортирования и хранения, изделие подлежит рекламации в 10-дневный срок с момента обнаружения, и изготовитель обязуется по получении уведомления о претензии в возможно короткий срок устранить дефекты своими силами и средствами вплоть до поставки экземпляров изделия.
- Гарантийный срок изделия устанавливается 12 месяцев.
- Начальной датой исчисления гарантийного срока изделия является дата поставки изделия, зафиксированная в формуляре.

- Изготовитель (поставщик) принимает претензии к качеству поставки Изделия в течение тридцати дней со дня поставки.
- Действие гарантийных обязательств прекращается по истечении гарантийного срока.

Помощь по работе с программой

Для более подробного изучения продукта ознакомьтесь, пожалуйста, со следующими разделами.

Дополнительная информация о программе

Для получения более подробной информации о программе посетите сайт программы www.cybersafesoft.com. На сайте доступны детальные видео-уроки по работе с программой и использованию ее основных функций.

На форуме сайта можно задать интересующие вас вопросы, узнать о методах устранения ошибок, а также ознакомиться с опытом работы других пользователей.

Контактная информация

Для связи с технической поддержкой, отправьте письмо на адрес электронной почты support@cybersafesoft.com или воспользуйтесь контактной формой на сайте: http://cybersafesoft.com/rus/contacts. *Обращаем Ваше внимание, что техническая поддержка по e-mail возможна лишь для пользователей, использующих платную версию программы.*

Адрес компании: Российская Федерация, Москва, ул. Марксистская, 32
Тел.: 8 (800) 555-28-43

2 Киберсейф Межсетевой экран

В этом разделе описывается основные функциональные возможности программы Киберсейф Межсетевой экран.

В этом разделе

Основные функции программы 10

Основные функции программы

Для того чтобы использовать программу максимально эффективно, вам следует ознакомиться с ее основными функциями, о которых пойдет речь в этом разделе.

Основные возможности Киберсейф Межсетевой экран:

- Статическая и динамическая маршрутизация для IPv4 и IPv6 (RIP, OSPF, BGP);
- Просмотр активных соединений, сетевых интерфейсов, а также протоколирование пакетов;
- Межсетевое экранирование для IPv4 и IPv6, включая фильтрацию p2p-трафика:
  - Фильтрация IP-пакетов на уровне сетевых адресов отправителя и получателя
  - Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств
  - Фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов
  - Фильтрация с учетом любых значимых полей сетевых пакетов
  - Фильтрация на транспортном уровне запросов на установление виртуальных соединений
  - Фильтрация на прикладном уровне запросов к прикладным сервисам
  - Фильтрация с учетом даты (времени)
- Трансляция сетевых адресов;
- Резервирование маршрутизаторов с синхронизацией таблицы состояний соединений;
- Удаленное управление межсетевыми экранами, установленными на

других компьютерах вашей сети;

- Создание сценария автоматического развертывания программы, что полезно при установке на целый парк компьютеров.
- Возможность развертывания программы с помощью Active Directory

3 Установка Киберсейф Межсетевой экран

В этом разделе описывается процесс инсталляции Киберсейф Межсетевой экран локальный компьютер, а также первые действия по работе с программой после ее установки.

В этом разделе

Перед установкой 12
Установка программы 12
Первый запуск программы 17
Запуск и завершение работы программы 17
Киберсейф Межсетевой экран и брандмауэр Windows 19
Первичная настройка 20
Деинсталляция программы 21

Перед установкой

В этом параграфе пойдет речь о минимальных системных требованиях, которые необходимы для успешной установки программы на локальный компьютер, работающий под управлением ОС Windows.

Системные требования

Перед началом установки программы убедитесь, что ваша операционная система удовлетворяет следующим минимальным требованиям:

- Операционная система Windows XP SP3, Windows Vista (x32/x64), Windows 7 (x32/x64), Windows 8.x (x32/x64), Windows Server 2003 (x32/x64), Windows Server 2008 (x32/x64), Windows Server 2008 R2 (x32/x64), Windows Server 2012 (x32/x64), Windows Server 2012 R2 (x32/x64).

Примечание. Программа будет полностью совместима с перечисленными выше операционными системами лишь в том случае, если на них установлены все последние обновления Microsoft.

- 512 MB оперативной памяти
- 210 MB свободного пространства на жестком диске

Установка программы

В этом параграфе содержится информация о том, как правильно установить и

настроить Киберсейф Межсетевой экран.

Примечание. Для того, чтобы установить программу вы должны обладать правами администратора. Перед началом установки рекомендуется закрыть все другие приложения и программы.

Запустите установочный файл и в появившемся окне (рис. 3.1) нажмите кнопку **Далее**.

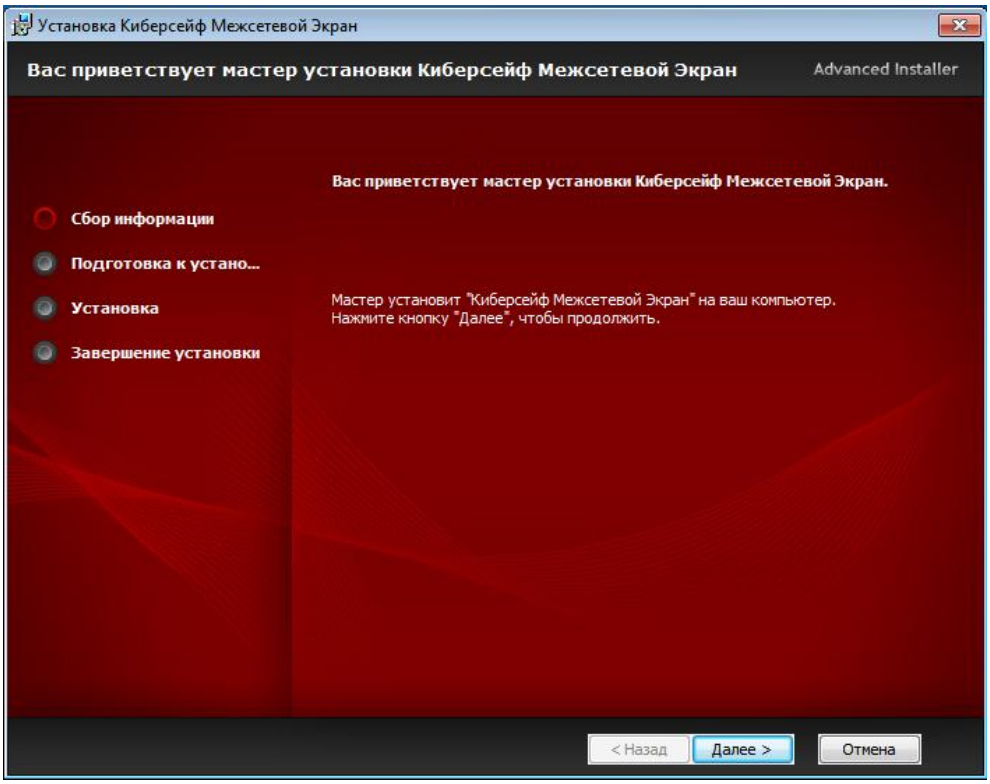

Рис. 3.1. Запуск инсталлятора программы

Затем нужно указать номер порта файрвола (по умолчанию используется номер 50001, но при желании вы можете изменить это значение), IP-адрес сервера удаленного доступа и номер порта, на котором работает сервер (по умолчанию также 50001), см рис. 3.2. Сервер удаленного доступа позволяет управлять другими межсетевыми экранами Киберсейф - вы будете видеть, запущен ли межсетевой экран на том или ином компьютере (поскольку межсетевой экран имеет смысл запускать при запуске Windows, то запуск межсетевого экрана также означает доступность компьютера в сети), а также сможете удаленно изменять правила файрвола на удаленном компьютере. Подробно об этом мы поговорим в разделах 8 и 9.

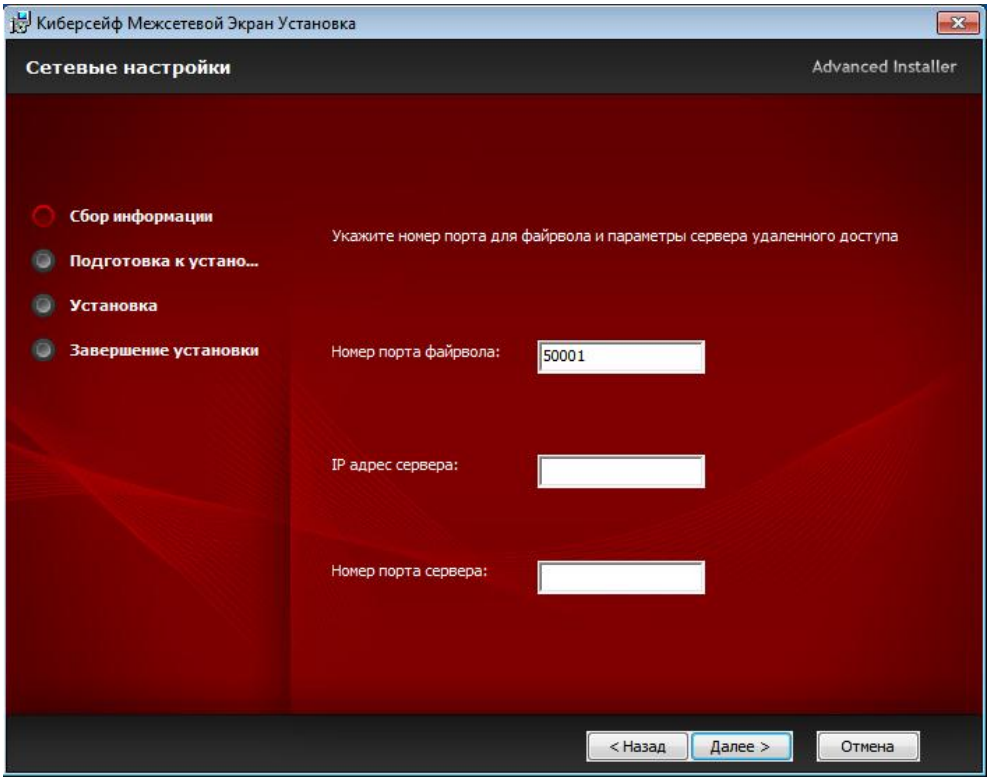

Рис. 3.2. Параметры удаленного доступа

Если вы пока не планируете использовать сервер удаленного доступа или пока его не настроили, можете оставить эти поля пустыми, вы сможете изменить эти параметры и после установки программы в окне настроек.

Следующее окно - ввод лицензионного ключа (рис. 3.3). Введите ключ и нажмите кнопку **Далее**.

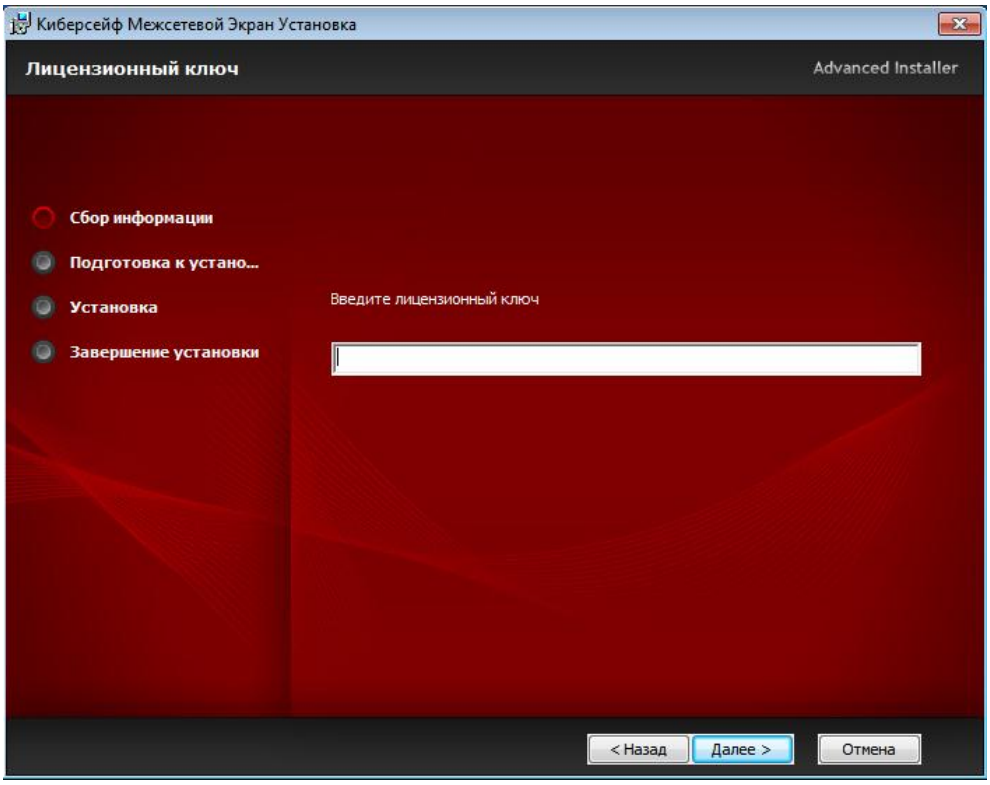

Рис. 3.3. Ввод лицензионного ключа

Выберите папку для установки программы и нажмите кнопку **Далее** (рис. 3.4). Обычно можно не изменять предлагаемое программой значение.

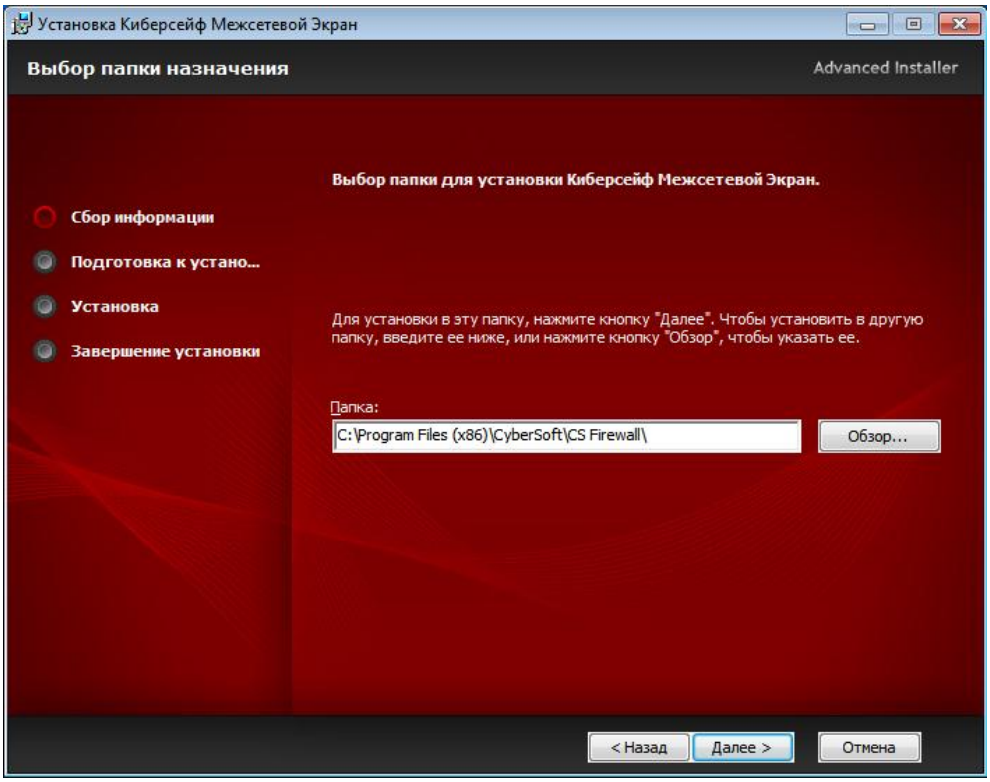

Рис. 3.4. Выбор папки для установки

Все готово к установке программы. Осталось только нажать кнопку **Установить** (рис. 3.5). При включенном UAC вы увидите окно, в котором нужно разрешить установку программы, нажав кнопку **Да** (рис. 3.6).

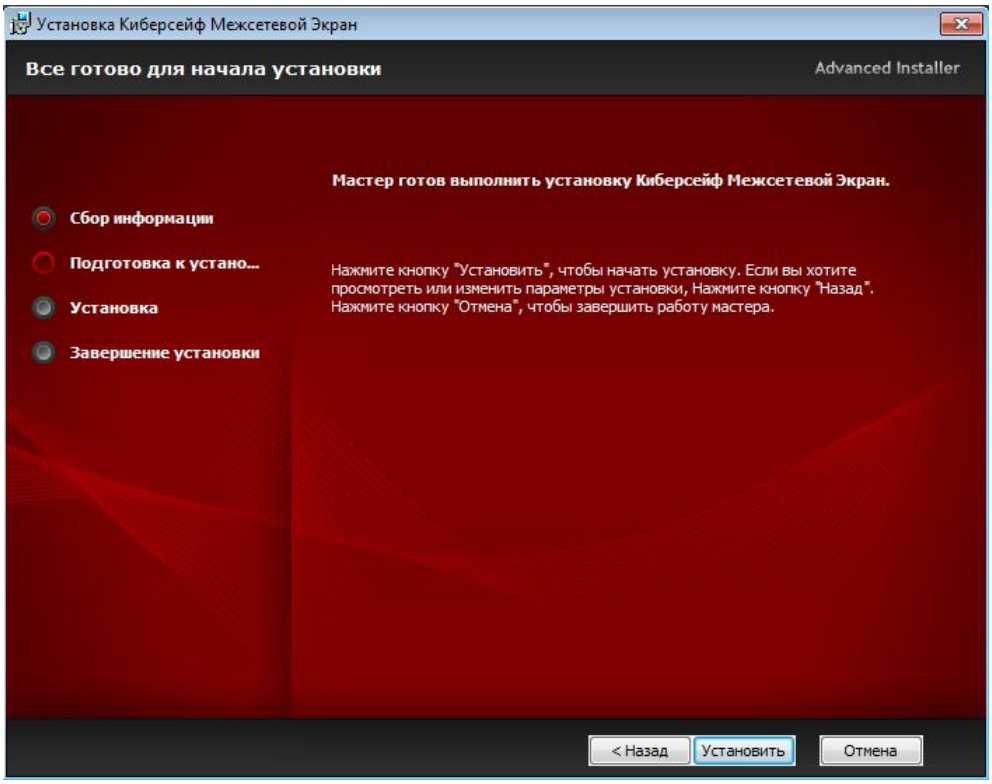

Рис. 3.5. Нажмите кнопку **Установить**

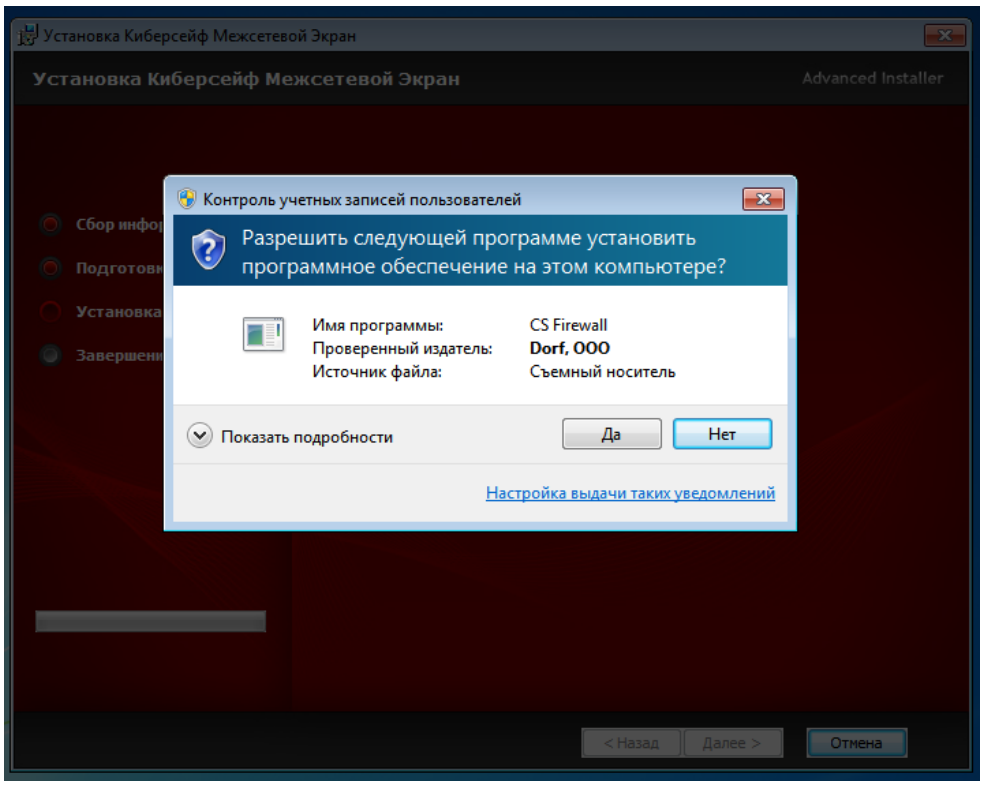

Рис. 3.6. Окно UAC: нажмите кнопку **Да**

Подождите, пока программа будет установлена и нажмите кнопку **Готово** (рис. 3.7) для выхода из инсталлятора.

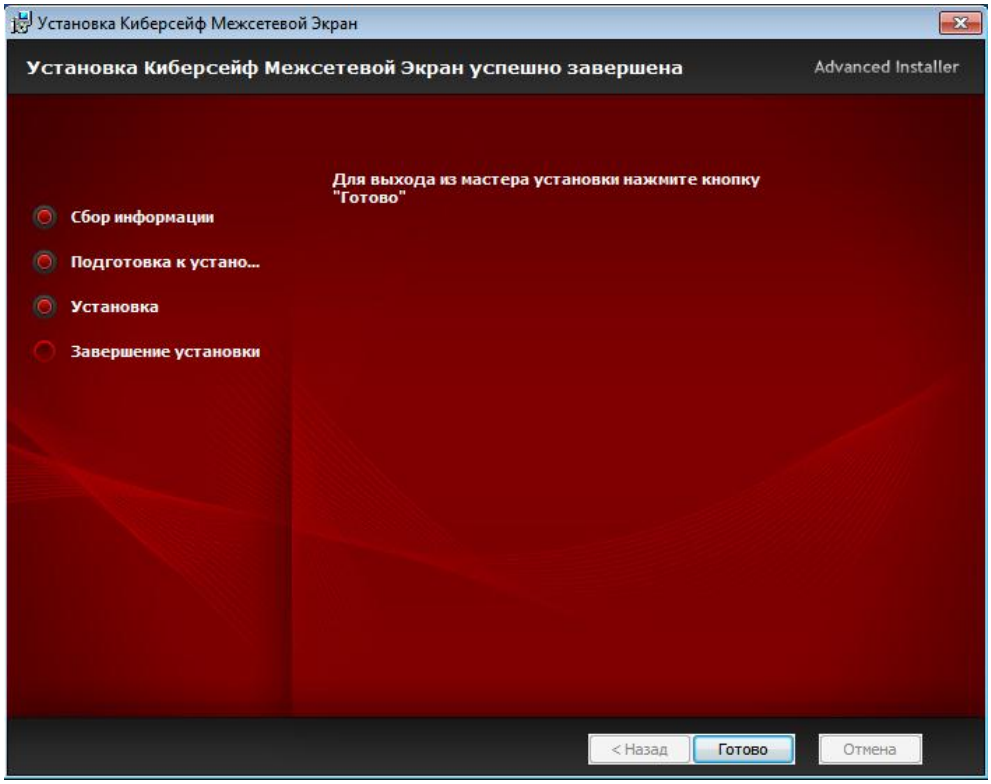

Рис. 3.7. Нажмите кнопку **Готово**

Первый запуск программы

При первом запуске программа предложит создать пользователя, под которым вы будете аутентифицированы в программе (рис. 3.8). Введите имя пользователя, его пароль и подтверждение пароля.

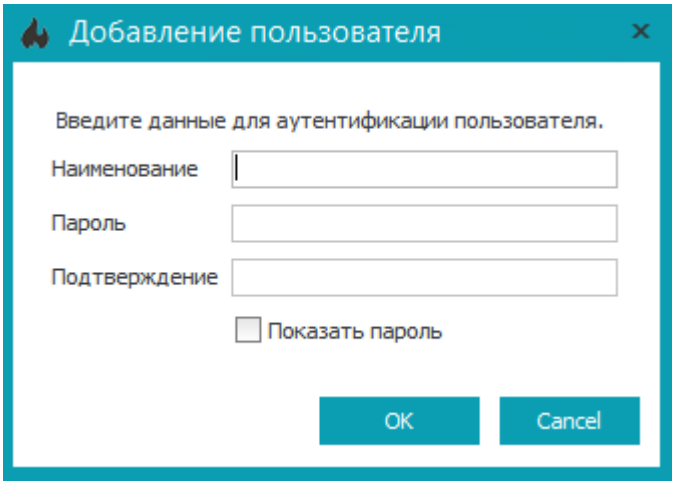

Рис. 3.8. Создание пользователя

Имейте в виду, что набор пользователей для конкретной машины свой собственный. Это означает, что под созданным пользователем вы сможете войти в программу только на этой машине. Если нужно входить под одним и тем же пользователем с одним и тем же паролем на всех машинах, на которых установлена программа, нужно или использовать сценарий развертывания (раздел 8) или же вручную создать одного и того же пользователя на всех машинах.

Запуск и завершение работы программы

Запуск программы может производиться вручную или автоматически. Для запуска программы вручную дважды щелкните по ее ярлыку на рабочем столе или выберите ярлык программы из меню **Пуск** (**Пуск, Все программы, CS Firewall, Киберсейф Межсетевой экран**). На рис. 3.9 показано основное окно программы и раздел **Активные соединения**, который отображается по умолчанию при запуске программы.

Для настройки автоматического запуска программы выполните следующие действия:

- Выберите команду **Инструменты, Настройки из меню программы**;
- Включите флажок **Запускать Файрвол при загрузке системы** (рис. 3.10);
- Нажмите кнопку **Применить**.

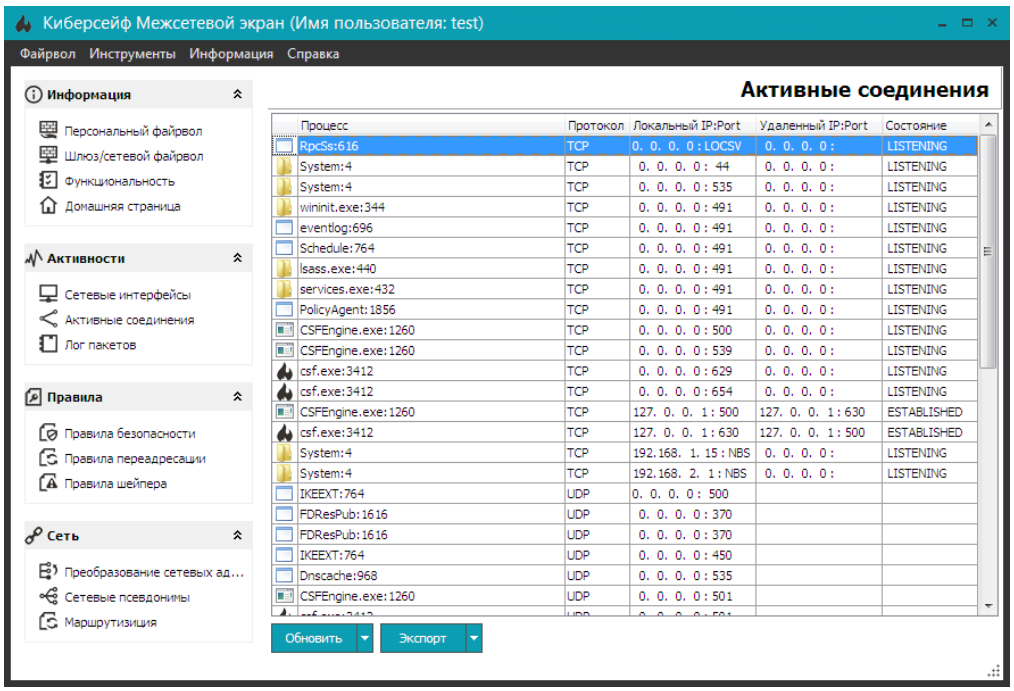

Рис. 3.9. Основное окно программы

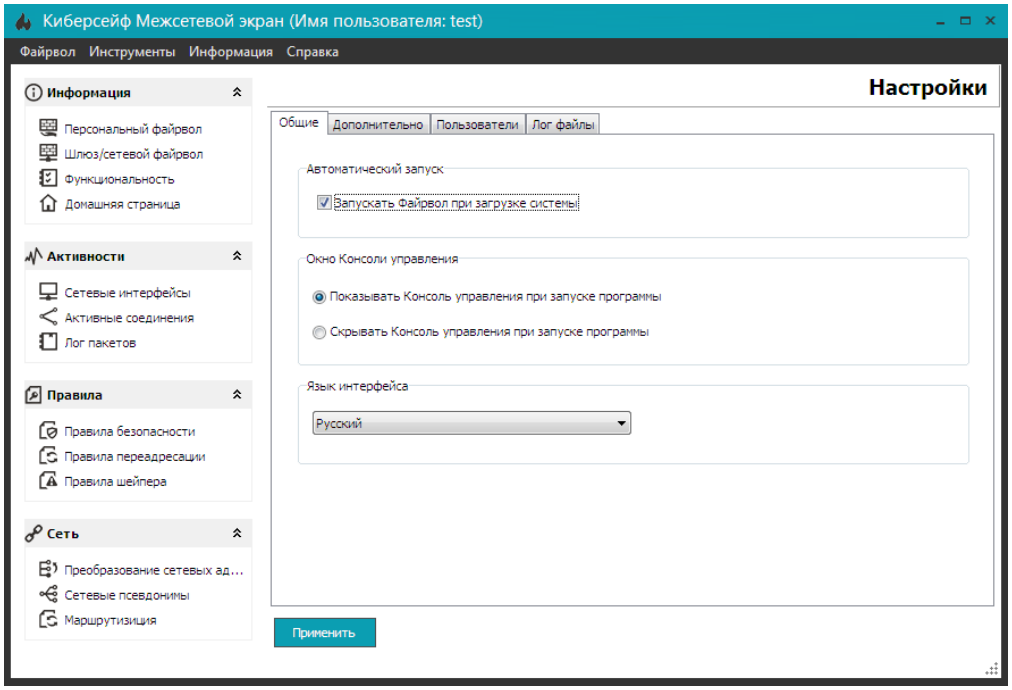

Рис. 3.10. Настройки программы

Для отключения автоматического запуска программы приведенные действия нужно повторить за тем лишь исключением, что флажок **Запускать Файрвол при загрузке системы** нужно выключить.

Для останова программы или закройте ее окно или щелкните правой кнопкой мыши на значке программы в системно трее и из появившегося меню выберите команду **Закрыть**.

Киберсейф Межсетевой экран и брандмауэр Windows

Во избежание конфликтов между двумя брандмауэрами - брандмауэр Windows и Киберсейф Межсетевой экран, брандмауэр Windows нужно отключить.

Для этого выполните следующие действия (на примере Windows 7):

- Нажмите кнопку **Пуск** и из главного меню Windows выберите команду **Панель управления**;
- Из списка **Просмотр** выберите значение **Крупные значки**;
- Запустите апплет **Брандмауэр Windows** (рис. 3.11);
- На панели слева выберите команду **Включение и отключение брандмауэра Windows**;
- Отключите брандмауэр для домашних и общественных сетей, как показано на рис. 3.12;
- Нажмите кнопку **ОК**.

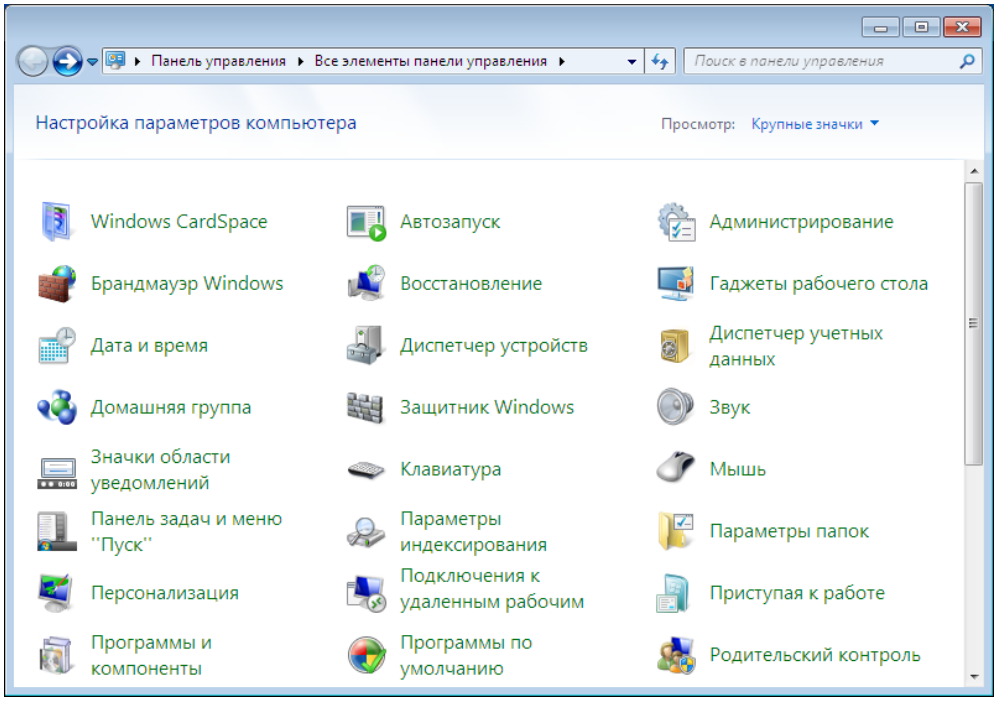

Рис. 3.11. Панель управления Windows 7

Примечание. В других выпусках Windows отключение брандмауэра с момента запуска Панели управления осуществляется аналогично.

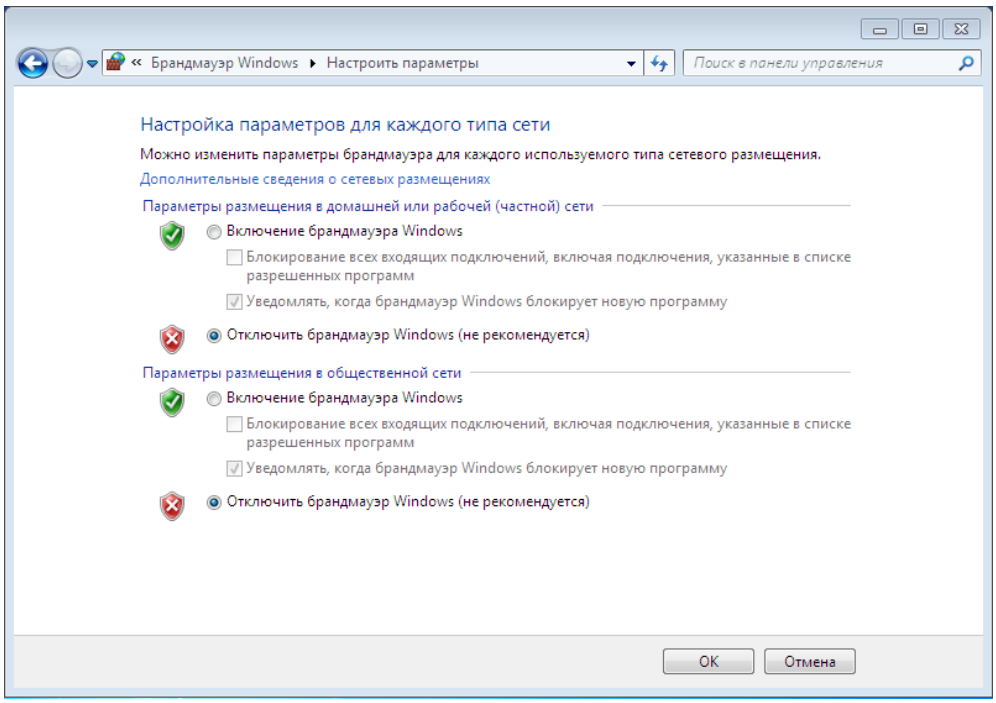

Рис. 3.12. Отключение брандмауэра Windows 7

Первичная настройка

Сразу после установки программа готова к работе. Однако вы можете настроить систему так, чтобы она в наибольшей степени удовлетворяла вашим запросам. Одной из наиболее важных характеристик программы является политика работы с сетью.

При первом запуске программа автоматически настраивает низкий уровень безопасности. Для просмотра и изменения уровня безопасности в дереве опций выбираем **Сетевые интерфейсы** (рис. 3.13).

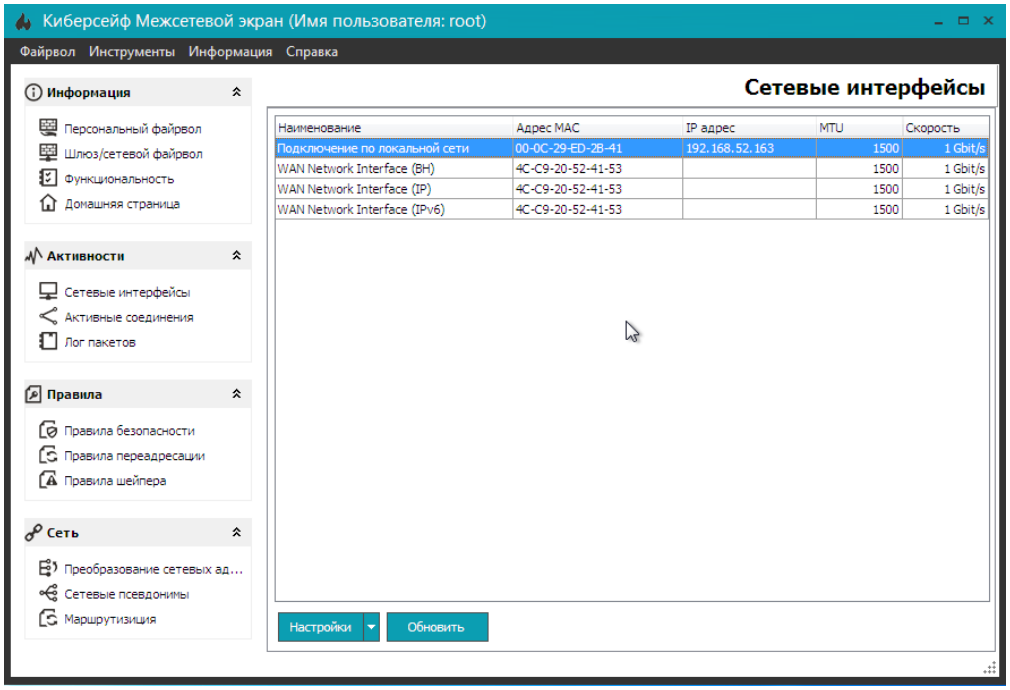

Рис. 3.13. Сетевые интерфейсы

Затем нужно выбрать соединение, уровень безопасности которого вам нужно изменить. Дважды щелкните по нужному соединению мышью. Вы перейдете в настройки уровней безопасности (рис. 3.14). Подробно об уровнях безопасности мы поговорим в следующем разделе.

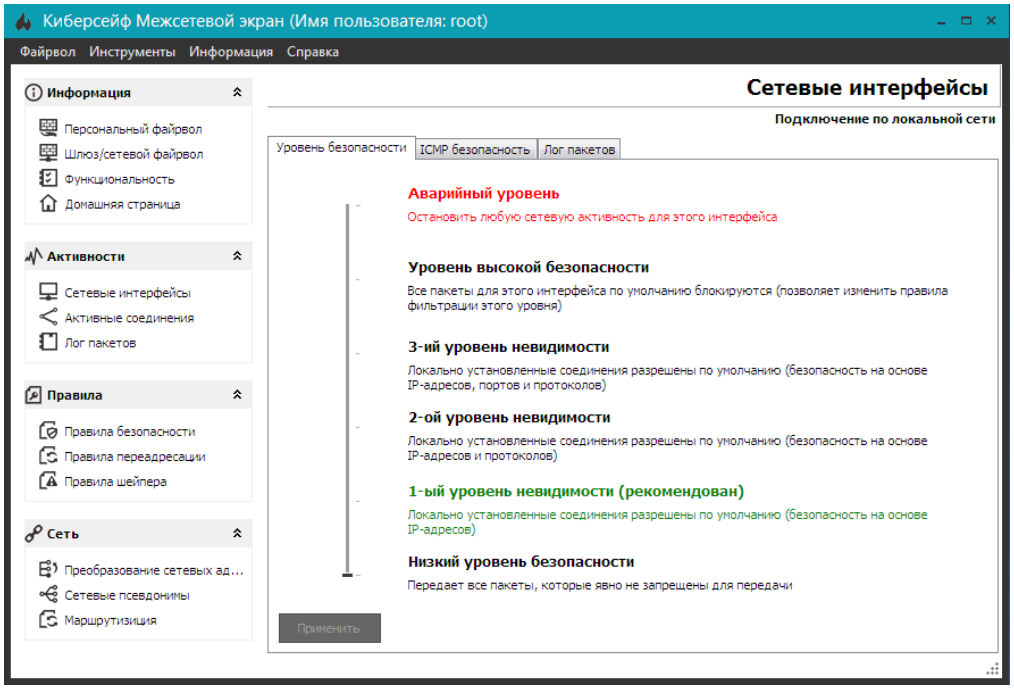

Рис. 3.14. Настройка уровня безопасности

Если Киберсейф Межсетевой экран планируется использовать как пограничный межсетевой экран между двумя одноранговыми сетями, то на ПК, на котором произведена установка системы, необходимо выполнить предварительную настройку статической маршрутизации сетевых пакетов между этими сетями. Для этого необходимо запустить командную строку от имени администратора системы и выполнить команды (в примере для Windows 7, для других версий ОС команды могут отличаться):

```
route –p add 10.10.10.0 mask 255.255.255.0 10.10.10.5
route –p add 192.168.20.0 mask 255.255.255.0 192.168.20.5
```

Деинсталляция программы

Для деинсталляции программы выполните следующие действия:

1. Нажмите кнопку Пуск и раскройте элемент меню **Все программы;**
2. Из группы **CS Firewall** выберите ярлык **Удалить;**
3. Следуйте инструкциям деинсталлятора.

4 Пользовательский интерфейс

В этом разделе описывается пользовательский интерфейс программы.

В этом разделе

Основное окно программы 22
Активные соединения 23
Сетевые интерфейсы 23
Лог пакетов 26

Основное окно программы

На рис. 4.1 изображено основное окно программы. Панель слева содержит следующие области:

- **Информация** - содержит команды доступа к информации о программе. Данные команды дублируют некоторые команды из меню **Информация** и **Справка**.
- **Активности** - содержит команды просмотра сетевых интерфейсов, активных соединений и команду доступа к журналу пакетов.
- **Правила** - здесь содержатся команды управления правилами брандмауэрами (см. раздел 6).
- **Сеть** - позволяет настроить преобразование сетевых адресов (NAT), сетевые псевдонимы, а также маршрутизацию.

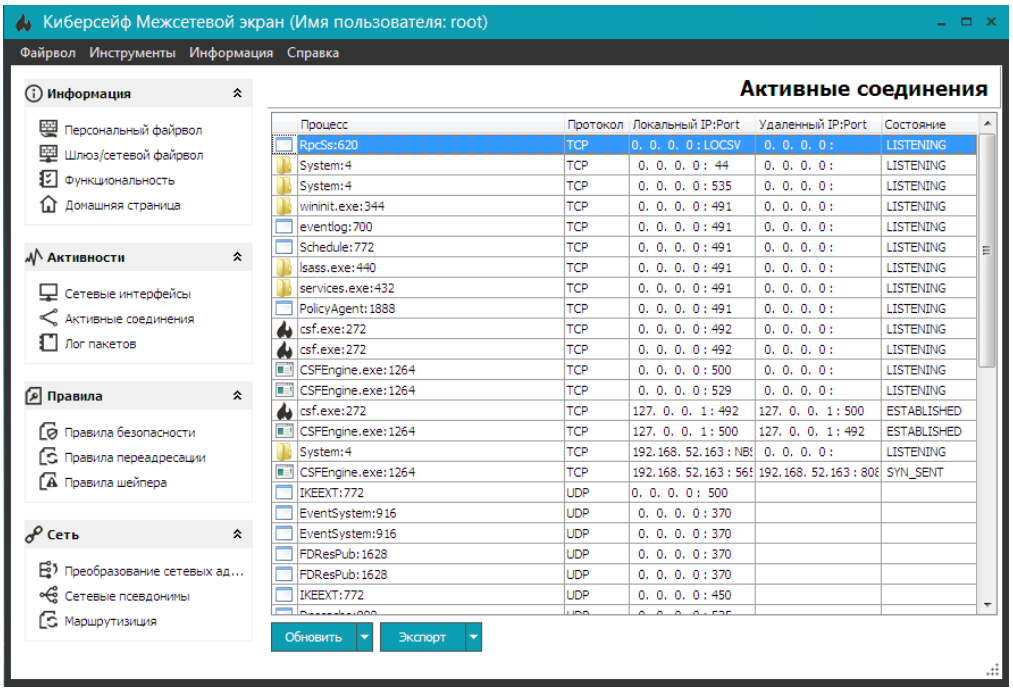

Рис. 4.1. Основное окно программы (активные соединения)

Активные соединения

По умолчанию отображается раздел программы **Активные соединения**, который и показан на рис. 4.1. Таблица с информацией об активных соединениях содержит следующие столбцы:

- **Процесс** - инициатор сетевого соединения. Имя процесса выводится в формате: <исполнимый файл>:<ИД процесса>, например, запись csf.exe:272 означает, что запущен процесс csf.exe с ИД процесса 272.
- **Протокол** - используемый протокол транспортного уровня (например, TCP или UDP).
- **Локальный IP:Port** - локальный IP-адрес и локальный порт;
- **Удаленный IP:Port** - удаленный IP-адрес и удаленный порт;
- **Состояние** - текущее состояние соединения.

Кнопка **Обновить** позволяет обновить таблицу активных соединений, а кнопка выпадающего списка справа - позволяет включить автоматическое обновление через каждый 10, 30 и 60 секунд (рис. 4.2).

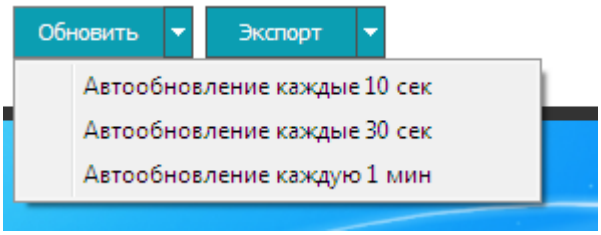

Рис. 4.2. Включение автоматического обновления

Кнопка **Экспорт** позволяет экспортировать список активных соединений в файл или буфер обмена (рис. 4.3).

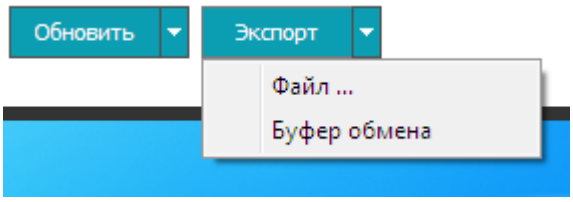

Рис. 4.3. Экспорт таблицы активных соединений

Сетевые интерфейсы

Настройка сетевых интерфейсов осуществляется средствами Windows-систем. Для просмотра списка сетевых интерфейсов, доступных в вашей системе, перейдите в раздел **Сетевые интерфейсы** в разделе **Активности** (рис. 4.4).

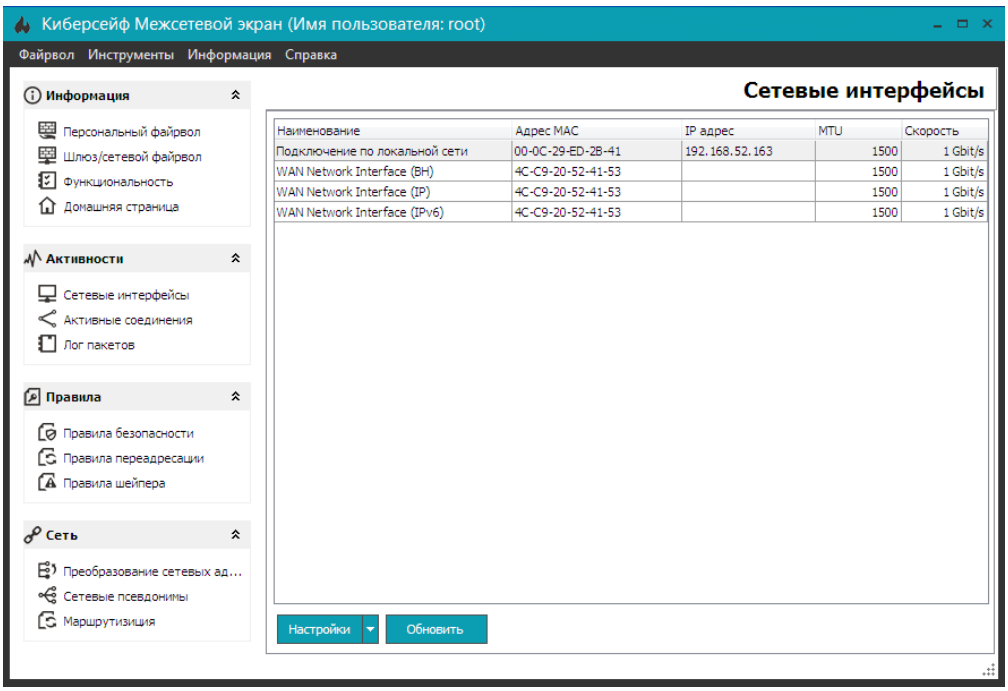

Рис. 4.4. Сетевые интерфейсы

Таблица, содержащая информацию о сетевых интерфейсах, имеет следующие столбцы:

- **Наименование** - название сетевого интерфейса, можно изменить, используя средства Windows;
- **Адрес MAC** - аппаратный (MAC) адрес сетевого интерфейса;
- **IP адрес** - IP-адрес, назначенный интерфейсу;
- **MTU** - максимальный размер полезного блока данных (Maximum Transmission Unit);
- **Скорость** - максимальная поддерживаемая скорость передачи данных по этому интерфейсу.

Ранее было показано (раздел 3), как вызвать окно изменения уровня безопасности сетевого интерфейса. Уровни безопасности должны быть установлены для каждого сетевого интерфейса, в соответствии с политикой безопасности. Входящие пакеты пропускаются или блокируются на основе этой установки.

Для каждого сетевого интерфейса в соответствии с политикой безопасности компьютера в сети можно установить один из следующих уровней безопасности (рис. 4.5):

- **Низкий уровень безопасности** - будут передаваться пакеты, которые явно не запрещены для передачи. Все, что не запрещено последующими правилами безопасности и протокольными защитами, разрешено.
- **1-ый уровень невидимости** - будут разрешены локально установленные соединения. Сетевой интерфейс работает по принципу контроля входящих пакетов и проверяет, чтобы адрес входящего

пакета соответствовали вашему запросу. Любой входящий пакет, который не соответствует вашему запросу, будет блокирован.

- **2-ой уровень невидимости** - сетевой интерфейс работает по принципу контроля входящих пакетов и проверяет, чтобы адрес, протокол входящего пакета соответствовали вашему запросу. Любой входящий пакет, который не соответствует вашему запросу, будет блокирован.
- **3-ий уровень невидимости** - сетевой интерфейс работает по принципу контроля входящих пакетов и проверяет, чтобы адрес, протокол и порт входящего пакета соответствовали вашему запросу. Любой входящий пакет, который не соответствует вашему запросу, будет блокирован.
- **Уровень высокой безопасности** - противоположен уровню низкой безопасности. Сетевой интерфейс действует по принципу : все что не разрешено, запрещено. На этом уровне блокируются все пакеты, которые не разрешены каким - либо правилом безопасности
- **Аварийный уровень** - останавливает любую сетевую активность для выбранного интерфейса.

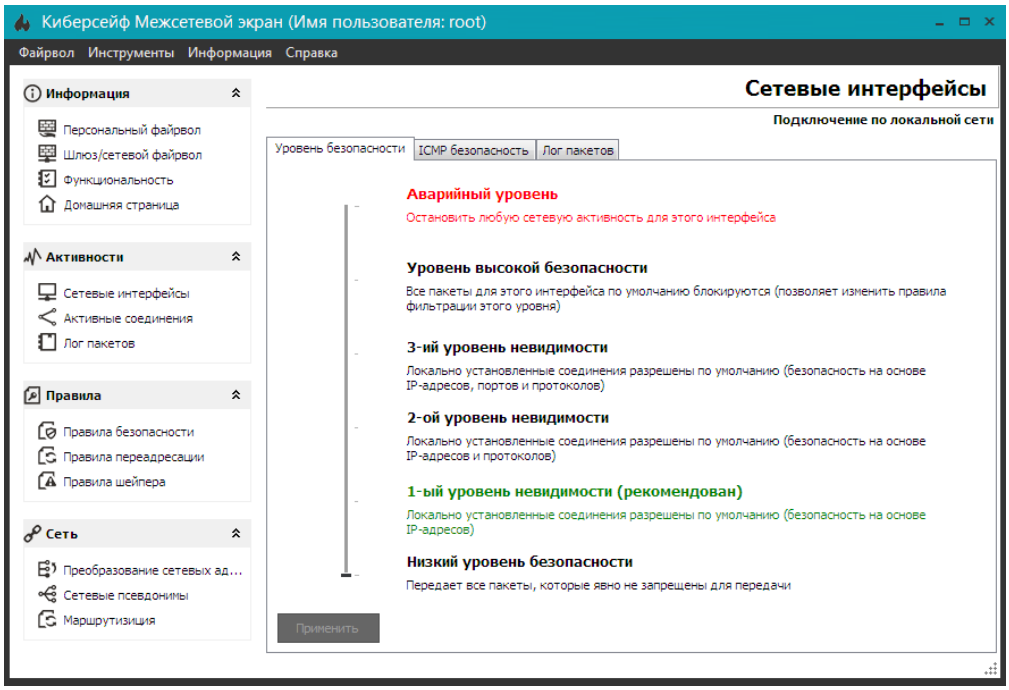

Рис. 4.5. Установка уровня безопасности

Примечание. Независимо от уровня безопасности сетевого интерфейса, пакет сначала подвергается проверке правилам безопасности, и только в случае, если ни одно из правил не способно решить: пропускать пакет или нет, пакет подвергается проверке уровня безопасности сетевых интерфейсов.

Предостережение. На аварийном уровне любой пакет блокируется, вне зависимости от правил безопасности!

Если щелкнуть правой кнопкой мыши на сетевом интерфейсе, то откроется следующее контекстное меню (рис. 4.6):

Уровень безопасности - открывает окно установки уровня безопасности, которое было рассмотрено ранее.

ICMP безопасность - открывает вкладку ICMP безопасность, где вы можете разрешать/блокировать входящие и исходящие сообщения ICMP (рис. 4.7). По умолчанию разрешены все сообщения ICMP.

Лог пакетов - открывает одноименную вкладку, где можно просмотреть журнал пакетов для выбранного интерфейса. Подробно журнал пакетов будет рассмотрен далее.

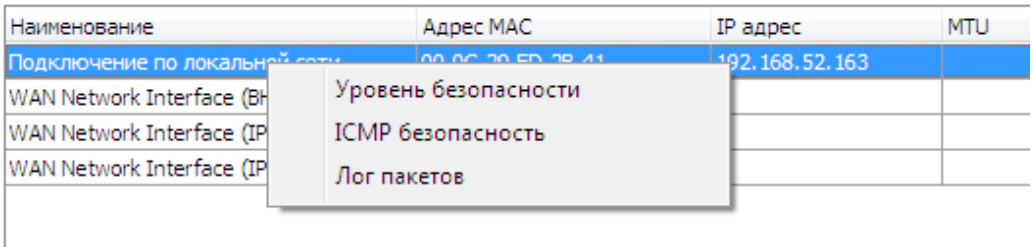

Рис. 4.6. Контекстное меню

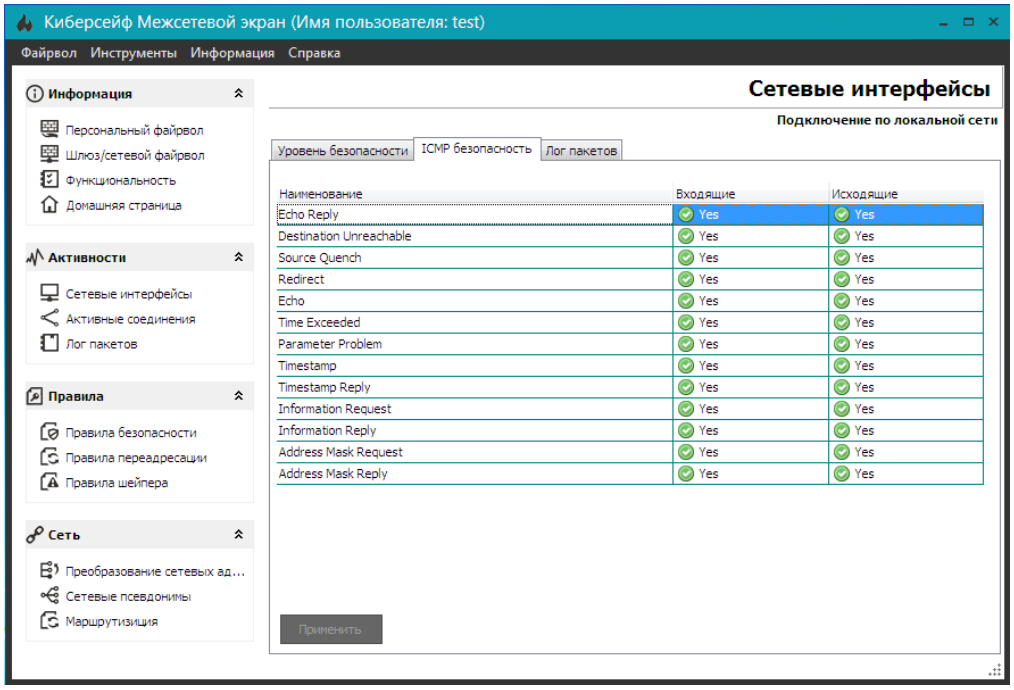

Рис. 4.7. ICMP безопасность

Кнопка **Обновить** внизу раздела **Сетевые интерфейсы** используется для обновления списка сетевых интерфейсов. Кнопка **Настройки** открывает вкладку **Уровень безопасности**, а кнопка выпадающего списка справа - дублирует команды контекстного меню (рис. 4.6).

Лог пакетов

В разделе **Лог пакетов** отображается журнал (рис. 4.8)

заблокированных/разрешенных пакетов для всех имеющихся интерфейсов. Если нужно просмотреть журнал пакетов для конкретного интерфейса, тогда перейдите в раздел **Сетевые интерфейсы**, щелкните правой кнопкой на интересующем вас интерфейсе и выберите команду **Лог пакетов**.

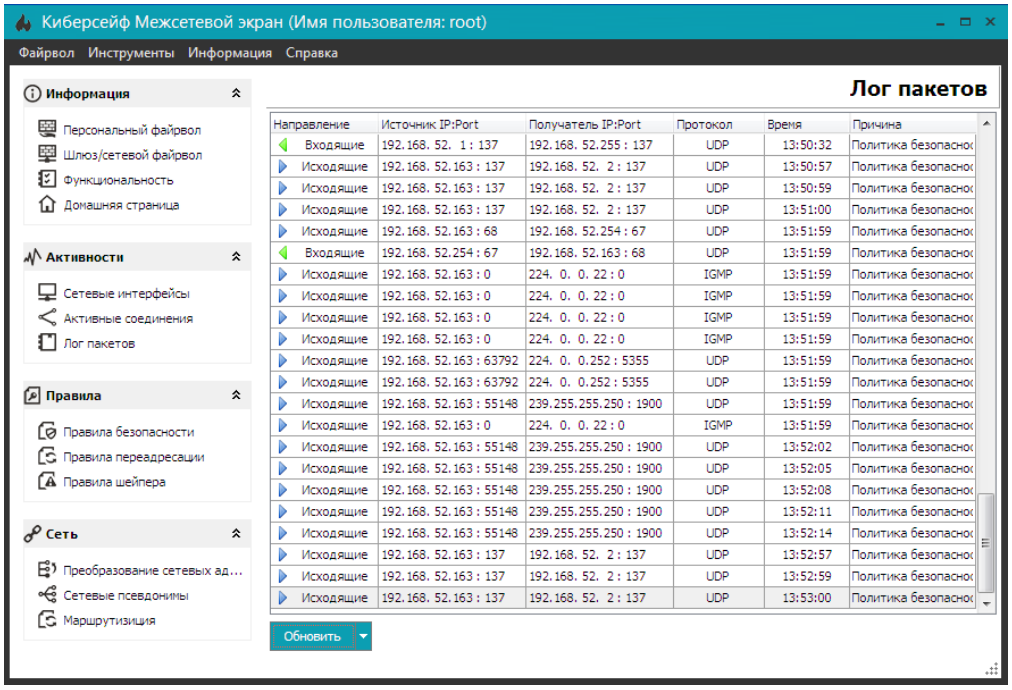

Рис. 4.8. Лог пакетов

Журнал пакетов обновляется автоматически, но вы можете обновить его принудительно, нажав кнопку **Обновить**. Кнопка выпадающего списка позволяет задать интервал автоматического обновления (2, 5 и 10 секунд).
Журнал пакетов представлен в виде таблицы со следующими столбцами:

- **Направление** - направление пакета - входящее или исходящее.
- **Источник IP:Port** - IP-адрес и порт источника пакета.
- **Получатель IP:Port** - IP-адрес и порт получателя пакета.
- **Протокол** - транспортный протокол (TCP, UDP, IGMP и др.)
- **Время** - время прохождения пакета через межсетевой экран.
- **Причина** - причина, по которой пакет был заблокирован или пропущен.

Записей в журнале пакетов может быть очень много, поэтому для облегчения поиска нужной записи в программе предусмотрены фильтры таблицы.
Щелкните по заголовку таблицы, по которому вы хотите отфильтровать лог пакетов (рис. 4.9). Далее нужно выбрать тип фильтра:

- **All** - отобразить все правила;
- **Custom** - открывает окно создания.
- **Blanks** - отображает правила, где свойство не установлено (пустые значения);
- **Nonblanks** - отображает правило, где свойство установлено (пустые

значения).

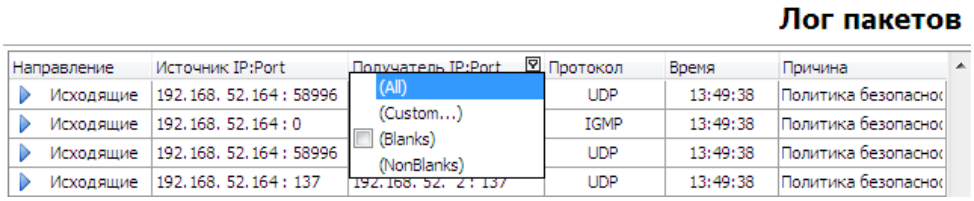

Рис. 4.9. Фильтр таблицы журнала пакетов по IP-адресу/порту получателя

Выберите тип фильтра **Custom** и в появившемся окне установите условие фильтра (рис. 4.10).

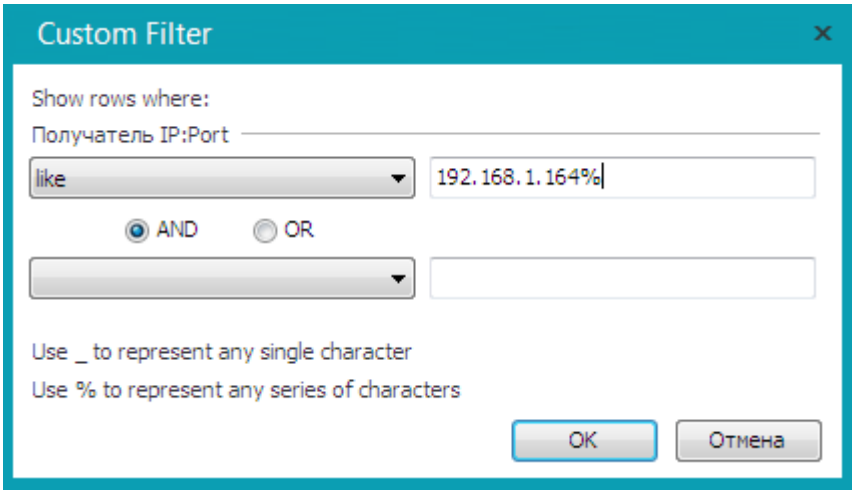

Рис. 4.10. Установка условия фильтра

Вы можете использовать символ _ для замены одного единственного символа (аналогично ? в маске имени файла) или символ % для представления любой последовательности символов (аналогично * в маске имени файла). Например, "192.168.1.164%" означает в нашем контексте указанный IP-адрес и любой порт, а "192.168.1.164:80__" означает указанный IP-адрес и порт, состоящих из четырех цифр, причем первые две из них - "80".

Оператор условия фильтра может быть следующим:

- **equals** - равен, лучше использовать для числовых значений;
- **does not equal** - не равен;
- **is less than** - меньше;
- **is less than or equal to** - меньше или равно;
- **is greater than** - больше;
- **is greater than or equal to** - больше или равно;
- **like** - подобен, лучше использовать для строковых значений;
- **not like** - не подобен;
- **is blank** - пусто;
- **is not blank** - не пусто (для поиска любого непустого значения).

Фильтр может содержать два условия, объединенные логическими операторами **AND** (И) или **OR** (ИЛИ).

Для применения фильтра нажмите кнопку **OK**. Чтобы вновь показать все записи выберите тип фильтра **All**. Дополнительная информация о работе с фильтрами будет также представлена в разделе 6, где мы будем использовать фильтры для фильтрации правил брандмауэра.

5 Настройки программы

В этом разделе описываются настройки программы, получить доступ к которым можно с помощью команды меню **Инструменты, Настройки**.

В этом разделе

Общие параметры программы 30
Дополнительные параметры программы 31
Управление пользователями 32
Параметры протоколирования 33
Просмотр системного журнала 34

Общие параметры программы

Для доступа к настройкам программы используется команда **Инструменты, Настройки**. На вкладке **Общие** (рис. 5.1) находятся общие параметры программы:

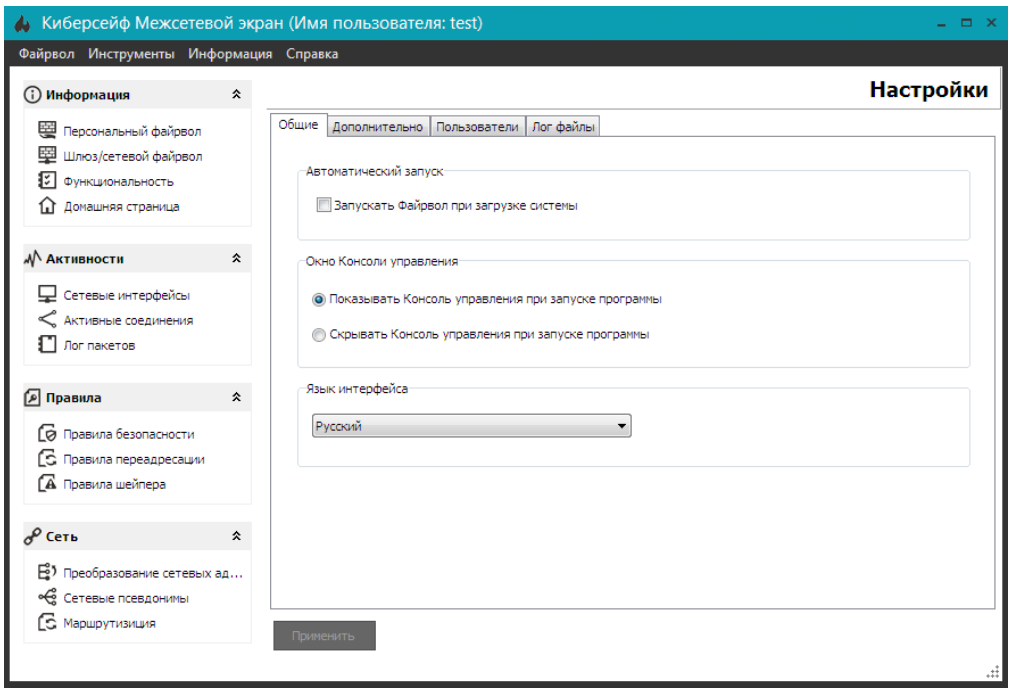

Рис. 5.1. Общие параметры программы

- **Автоматический запуск** - если включен переключатель **Запускать Файрвол при загрузке системы**, то программа будет загружаться автоматически.
- **Окно Консоли управления** - вы можете выбрать, нужно ли показывать консоль управления при запуске программы.
- **Язык интерфейса** - позволяет выбрать язык интерфейса программы

(русский или английский).

Примечание. Для сохранения параметров программы нужно обязательно нажать кнопку **Применить**.

Дополнительные параметры программы

На вкладке **Дополнительно** (рис. 5.2) находятся дополнительные параметры программы.

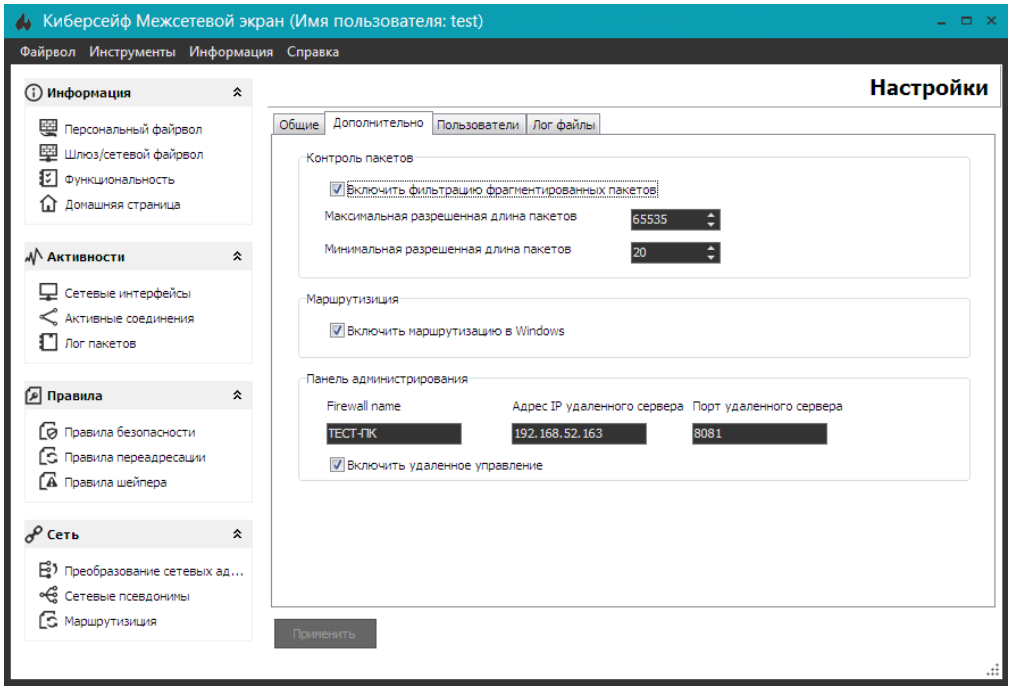

Рис. 5.2. Дополнительные параметры программы

Область **Контроль пакетов** содержит параметры, позволяющие включить фильтрацию фрагментированных пакетов, а также задать минимальную и максимальную разрешенную длину пакетов. Значения по умолчанию показаны на рис. 5.2.

Параметр **Включить маршрутизацию в Windows** позволяет включить маршрутизацию в Windows и превращает ваш компьютер в шлюз. Если планируется использование программы в качестве персонального брандмауэра (только для защиты одного компьютера), этот параметр можно выключить.

Очень важными являются параметры в группе **Панель администрирования**. Параметр **Firewall name** позволяет задать имя этого файрвола, которое будет отображаться в консоли удаленного управления файрволом. Параметр **Адрес IP** удаленного сервера позволяет указать IP-адрес удаленного сервера. Обычно удаленный сервер запускается на шлюзе сети, но может быть запущен на любом другом компьютере, с которого администратору удобно управлять другими файрволами.

Параметр **Порт удаленного сервера** позволяет задать порт сервера. По умолчанию используется порт 50001, на рис. 5.2 продемонстрирована возможность задания другого порта (задан порт 8081).

Переключатель **Включить удаленное управление** (если включен) разрешает удаленное управление этим файрволом с помощью удаленного сервера и Панели администрирования. О настройке удаленного сервера и удаленном администрировании мы поговорим в разделах 8 и 9 данного Руководства.

Управление пользователями

Для управления пользователями используется вкладка **Пользователи** (рис. 5.3).

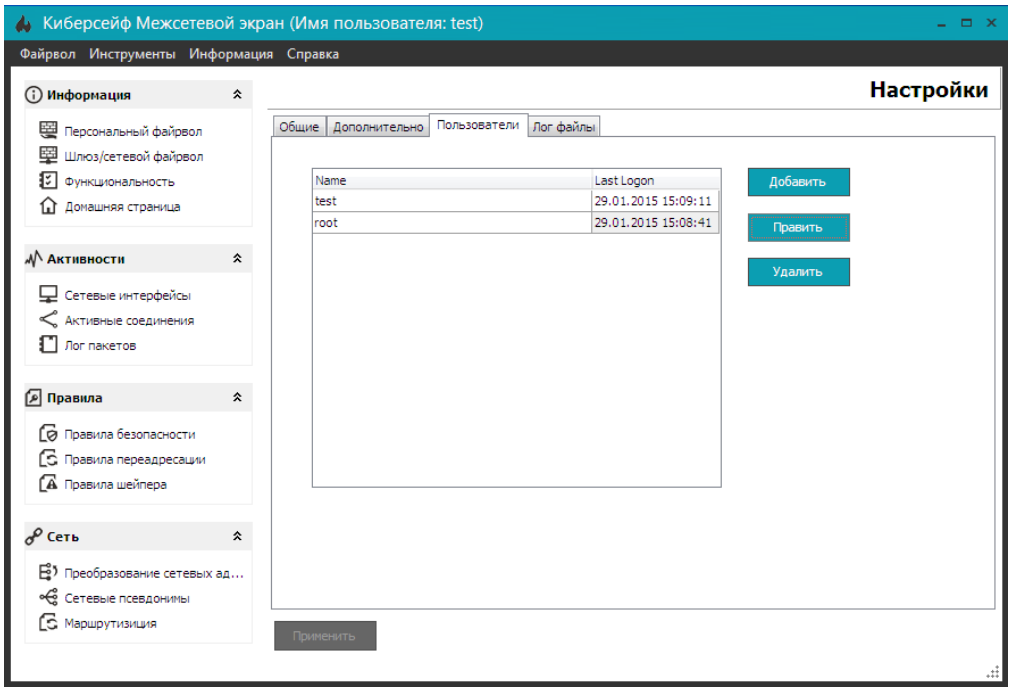

Рис. 5.3. Пользователи

Список пользователей хранится только на локальной машине и никак не синхронизируется с другими файрволами. На рис. 5.3 видно, что созданы пользователи test и root и отображается последняя дата входа каждого пользователя. Эти пользователи существуют только на этой машине. Если вам нужно входить под этими именами на другой машине, нужно создать на ней пользователей с такими же именами. Пароли при этом могут быть разными.

Если же вам нужно обеспечить вход под одним именем и одним паролем на все файрволы (на всех машинах), вам нужно использовать сценарий развертывания, процесс создания которого будет рассмотрен в разделе 8.

Кнопка **Добавить** позволяет добавить нового пользователя. При этом вам нужно ввести его логин, пароль и подтверждение пароля (рис. 5.4).

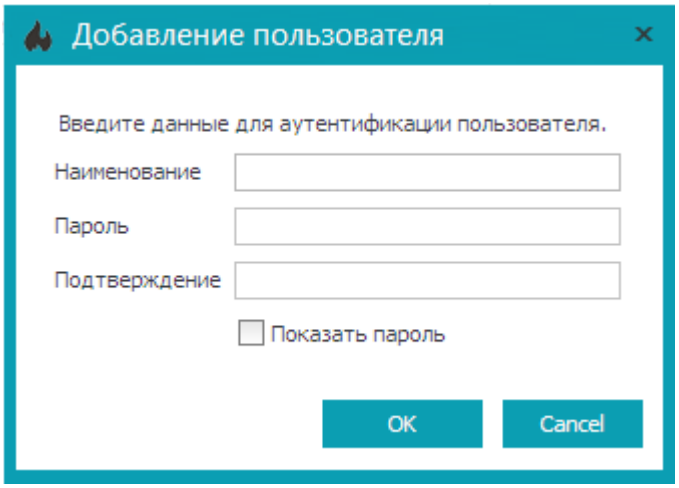

Рис. 5.4. Создание нового пользователя

Кнопка **Править** позволяет изменить логин и пароль пользователя, а кнопка **Удалить** - удаляет выделенного пользователя.

Примечание. Администраторам доступа **Панель администрирования** (команда **Файрвол, Панель администрирования**). Администратором считается пользователь, назначенный таковым с помощью программы Киберсейф Удаленный сервер (см. раздел 8).

Смена пользователя

Для изменения пользователя нужно выполнить команду меню **Файрвол, Сменить пользователя**. После этого нужно ввести логин и пароль пользователя, под которым вы хотите войти.

Параметры протоколирования

Вкладка **Лог файлы** (рис. 5.5) содержит параметры журналирования. Область **Системный лог** позволяет задать расположение системного журнала, указать периодичность удаления старых файлов журнала, а также выбрать будет ли сохранен системный журнал в файл. По умолчанию системный журнал сохраняется в папку C:\ProgramData\Cybersafe Firewall\SystemLog\, а старые файлы системного журнала будут удаляться каждые 3 дня.

Аналогично, область **Лог пакетов** задает параметры для журнала пакетов. По умолчанию журнал пакетов хранится в папке C:\ProgramData\Cybersafe Firewall\PacketsLog\, а старые файлы журналов удаляются каждые 3 дня.

Включение параметра **Сохранять в файл информацию о пакетах построчно** может снизить производительность системы, помните об этом, включая этот параметр.

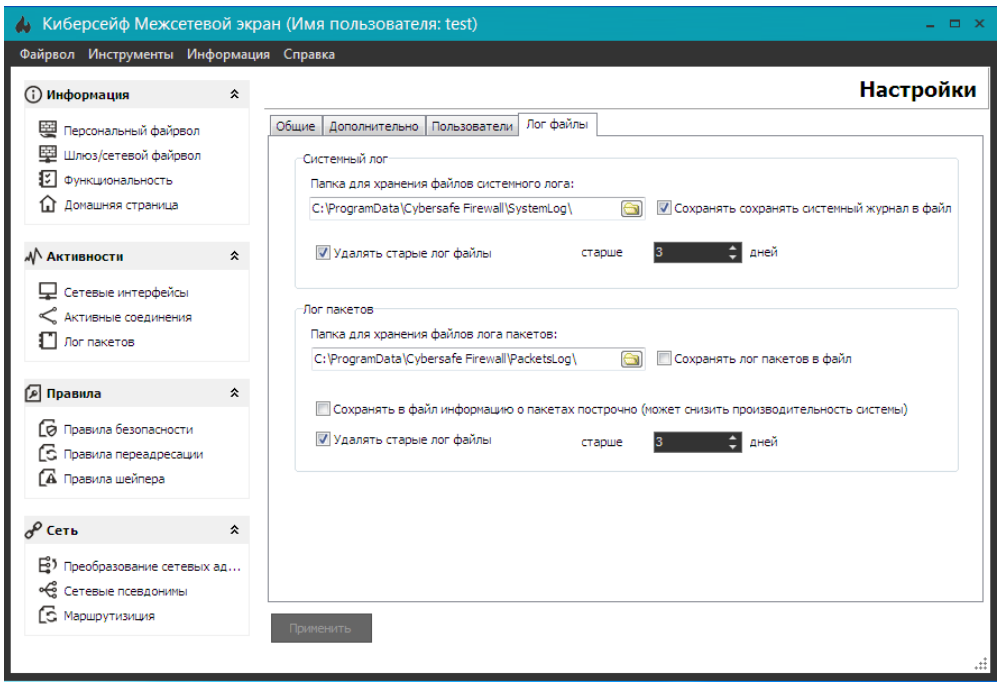

Рис. 5.5. Параметры протоколирования

Просмотр системного журнала

В системный журнал заносятся системные события, например, запуск программы и завершение работы программы, вход пользователя и т.д. (рис. 5.6). Для просмотра системного журнала используется команда **Инструменты, Системный лог**.

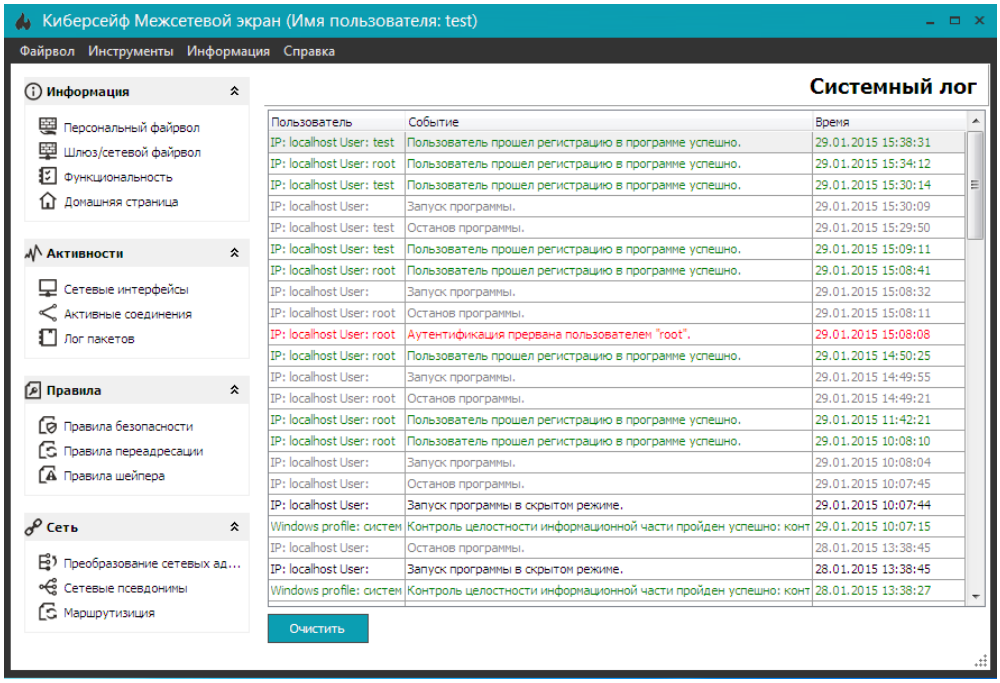

Рис. 5.6. Системный журнал

Кнопка **Очистить** позволяет удалить все записи из системного журнала.

Сохранение и восстановление конфигурации

Конфигурация Киберсейф Межсетевой экран хранится в файле конфигурации csf.fdb. По умолчанию файл хранится в каталоге C:\Users\Public\Documents\bp\. Необходимо производить регулярное резервное копирование файла конфигурации на резервный носитель данных. Для восстановления конфигурации Киберсейф Межсетевой экран после сбоя (переустановки) системы необходимо, перед запуском Киберсейф Межсетевой экран, скопировать актуальную версию файла csf.fdb с резервного носителя данных в каталог C:\Users\Public\Documents\bp\. После запуска Киберсейф Межсетевой экран будут применены последние сохраненные в файле csf.fdb настройки.

Вы можете также экспортировать правила и конфигурацию программу вручную с помощью команды меню **Инструменты, Экспорт настроек и правил**. Для импорта настроек используется другая команда - **Импорт настроек и правил**.

6 Настройка правил брандмауэра

В этом разделе описывается, как настроить правила брандмауэра Киберсейф Межсетевой экран.

В этом разделе

Правила безопасности 36

Правила переадресации. 43

Правила шейпера: ограничение пропускной способности. 44

Правила безопасности

Что такое правила безопасности?

Правила безопасности определяют правила, при которых пакеты либо передаются через брандмауэр, либо блокируются. Каждое правило имеет свой уникальный Идентификатор. Идентификатор определяет порядок применения правил для принимаемого пакета.

Чем меньше значение приоритета правила, тем выше его приоритет и тем быстрее оно будет применяться при анализе пакетов. Анализ пакетов прекращается, если пакет был заблокирован каким-либо правилом безопасности.

В случае, когда отсутствует правило, которое может быть применено к принятому пакету, он проверяется на соответствие уровня безопасности и передается далее. Подводя итоги сказанному - правила безопасности применяются до проверки пакета на соответствие настройкам уровня безопасности.

При разработке системы компьютерной безопасности важно, в первую очередь, определить правила безопасности и порядок их применения. При применении аварийного уровня безопасности, независимо от использования правил безопасности, блокируются все пакеты.

Основные свойства правил безопасности

Правило идентификатора (или правило приоритета) представляет собой числовое значение в диапазоне от 1 до 65535. Чем меньше значение приоритета правила, тем выше его приоритет и тем быстрее оно будет применяться при анализе пакетов.

Сетевой интерфейс - это сетевой адаптер, который принимает пакеты, впоследствии анализируемые на основе правил безопасности. В зависимости от типа, правила будут либо пропускать пакеты, либо блокировать их.

Направление пакетов - позволяет контролировать только входящие, только

исходящие, или все пакеты. Правила безопасности могут быть применены либо только к входящим пакетам, либо только к исходящим, либо и к тем и другим одновременно. Фильтр применяется к пакетам с выбранным протоколом.
Исходный IP-адрес и порт - контроль над пакетами с данного источника определяется правилами безопасности.
IP-адрес назначения и порт - контроль над пакетами на данное назначение определяется фильтром.

Примечание. Термин "Порт" применяется только к TCP и UDP сетевым протоколам.

Просмотр правил безопасности

Перейдите в раздел Правила безопасности (рис. 6.1). В нем содержится таблица описания правил безопасности, в которой имеются следующие столбцы:

- **Тип правила** - правило может разрешать или запрещать передачу пакетов;
- **Описание** - описание правила, при создании правила вы можете указать, для чего оно используется;
- **Приоритет** - приоритет правила (см. ранее);
- **Статус** - правило может быть или включено или выключено;
- **Протокол** - протокол, к которому применяется правило (TCP, IP, UDP, ICMP и т.д.);
- **Источник IP:Port, Получатель IP:Port** - IP-адреса и порты источника и получателя соответственно;
- **Направление** - отображает направление (входящее/исходящее/любое) пакетов;
- **Интерфейс** - отображает интерфейс, по которому передаются пакеты. Если интерфейс не задан, считается, что правило применяется ко всем имеющимся сетевым интерфейсам;
- **Логирование** - будет ли заноситься в журнал информация о применении правила к пакету.

Поскольку таблица правил безопасности может быть очень большой, предусмотрены фильтры правил. Для активации фильтра щелкните по заголовку, по которому вы хотите отфильтровать таблицу (рис. 6.2) и выберите одно из значений (значения могут меняться в зависимости от содержимого столбца):

- **All** - отобразить все правила;
- **Custom** - открывает окно создания фильтра (с подобным окном, возможно, вы работали в Excel). На рис. 6.3 показано, что я создаю фильтр, который должен показывать все правила, применяющиеся к протоколу TCP.
- **Blanks** - отображает правила, где свойство не установлено (пустые значения);

- **Nonblanks** - отображает правило, где свойство установлено (пустые значения).

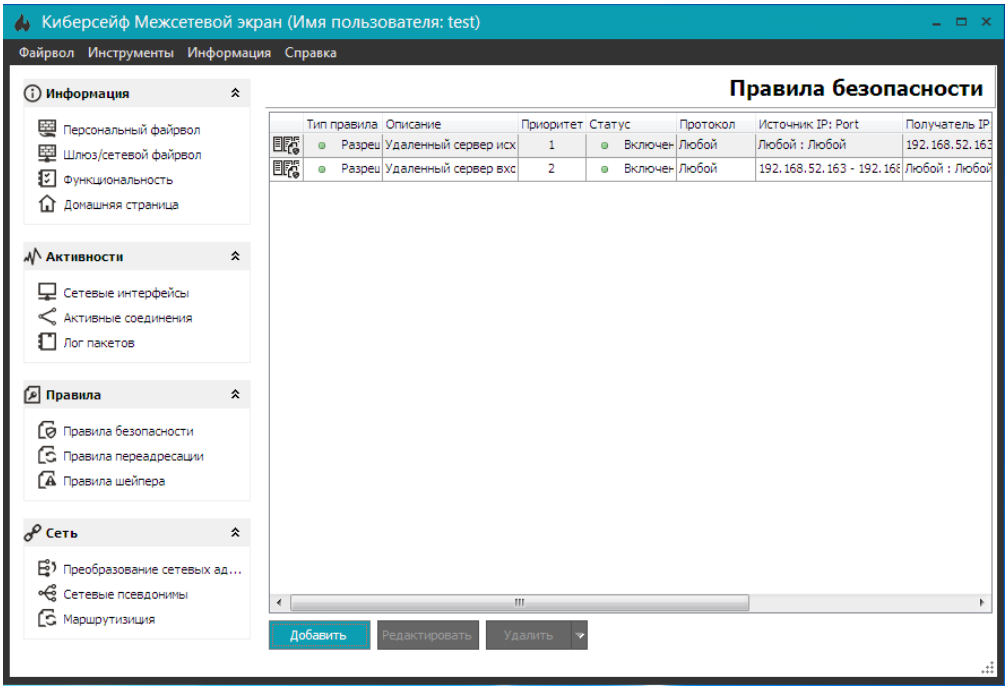

Рис. 6.1. Правила безопасности

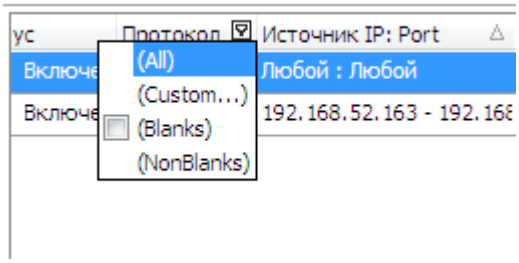

Рис. 6.2. Автоматический фильтр

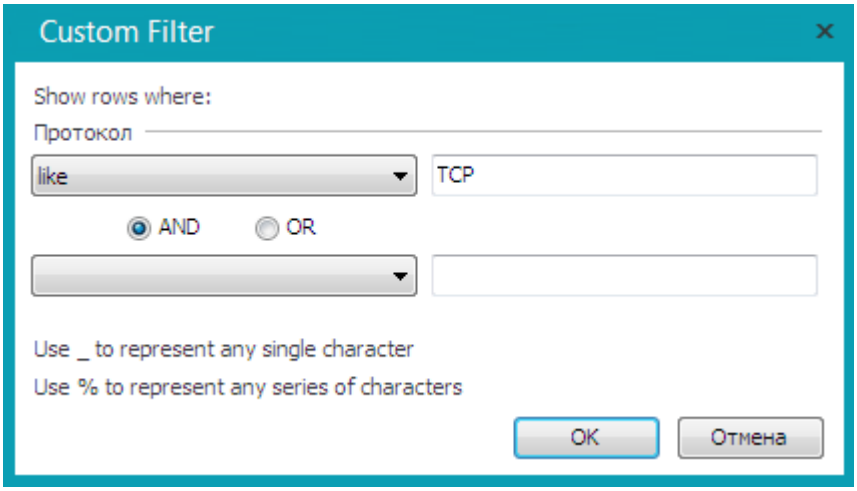

Рис. 6.3. Создание пользовательского фильтра

Если в данный момент применен фильтр, то в соответствующем столбце будет

отображен синий значок фильтра (рис. 6.4) и это означает, что возможно, вы видите не все возможные правила.

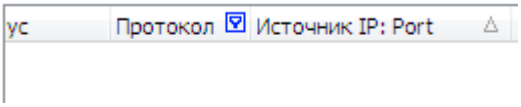

Рис. 6.4. Работает фильтр

Аналогично можно отфильтровать таблицы правил переадресации и правил шейпера, поэтому в соответствующих разделах мы больше не будем рассматривать эту возможность, чтобы не повторяться.

Создание правил безопасности

Для добавления правила безопасности перейдите в раздел **Правила безопасности** (рис. 6.1) и нажмите кнопку **Добавить**. Также можно щелкнуть по таблице правил и выберите команду **Добавить** из контекстного меню.

В появившемся окне (рис. 6.5) нужно установить свойства правила, а именно - описание, приоритет, сетевой интерфейс, тип правила, направление пакетов, протокол. Все эти свойства уже обсуждались ранее. Переключатель **Разрешить логирование** позволяет разрешить/запретить логирование применения правила.

Вкладки **Источник** и **Получатель**, соответственно, позволяют описать источник и получатель пакетов (рис. 6.6). Обратите внимание, что в качестве источника и получателя может быть подсеть (например, 192.168.1.0 и маска 255.255.255.0), диапазон IP-адресов (например, от 192.168.1.100 до 192.168.1.200), псевдоним или URL. Если нужно указать всего один IP-адрес, укажите его, как в поле **От**, так и в поле **До**.

Псевдоним можно выбрать из соответствующего списка, а создать псевдоним можно в разделе **Сеть, Сетевые псевдонимы**.

Вкладка **Дата Время** (рис. 6.7) позволяет указать дату и время, когда будут действовать правила. Например, вы можете запретить доступ к определенному ресурсу (URL) в рабочее время.

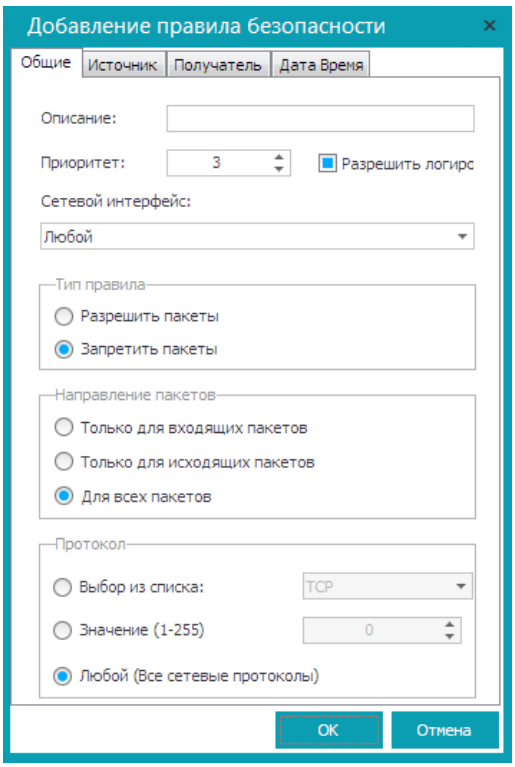

Рис. 6.5. Общие свойства правила безопасности

Примечание. Функция блокирования по URL работает только для сайтов с одним IP-адресом. У некоторых крупных сайтов есть несколько серверов, каждый со своим IP-адресом. Для блокировки таких сайтов нужно блокировать или диапазон IP-адресов или каждый IP-адрес сайта отдельно.

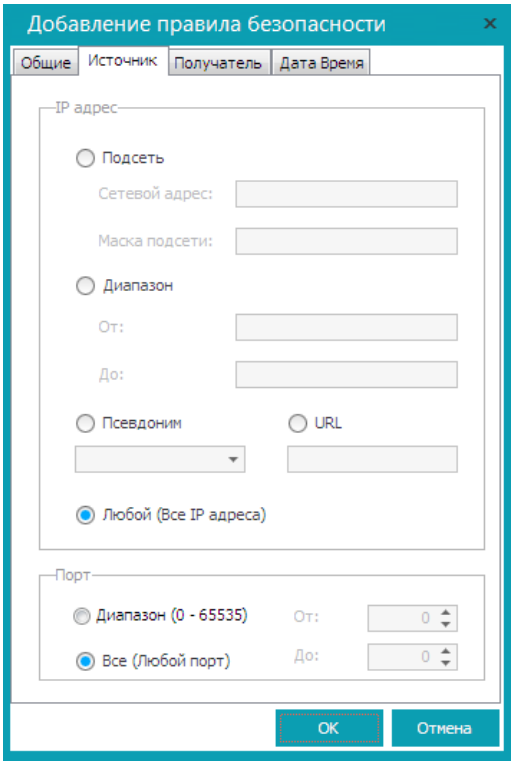

Рис. 6.6. Определение источника пакетов

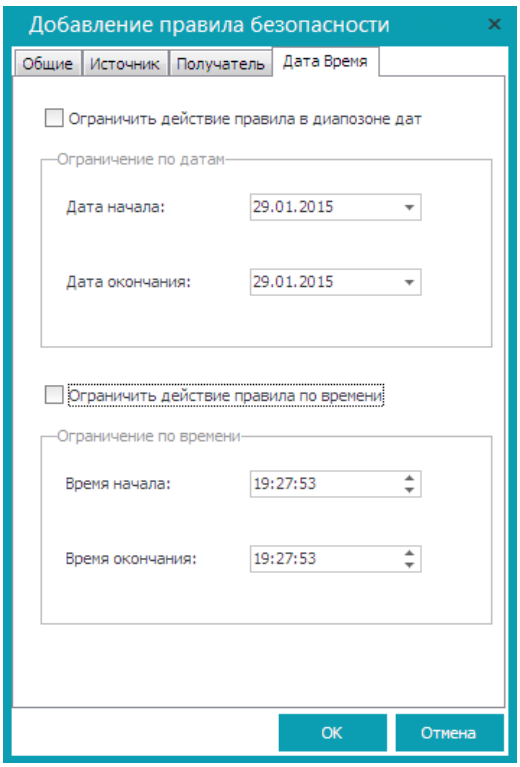

Рис. 6.7. Дата и время работы правила

Для добавления правила нажмите кнопку **OK**. Чтобы правило вступило в силу, щелкните по нему правой кнопкой мыши и выберите команду **Включить** (рис. 6.8). Аналогично, для выключения правила нужно щелкнуть по нему правой кнопкой мыши и выбрать команду **Выключить**.

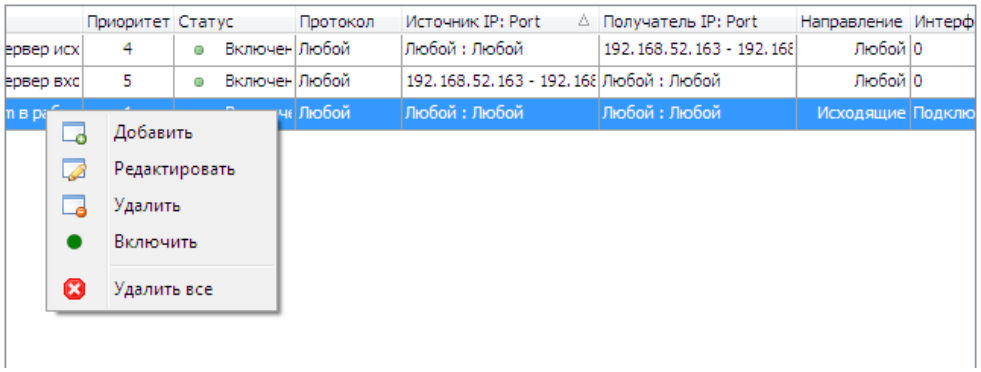

Рис. 6.8. Действия над правилами

Для редактирования правила нужно или дважды щелкнуть по нему мышкой или выделить его и нажать кнопку **Редактировать** (можно также щелкнуть по нему правой кнопкой мыши и выбрать команду **Редактировать**).
Кнопка **Удалить** удаляет правила. Из выпадающего списка справа можно выбрать команду **Удалить все**, которая удаляет все правила (рис. 6.9).

Примечание. Если правило активно, то сначала его нужно выключить, а уже потом - удалять.

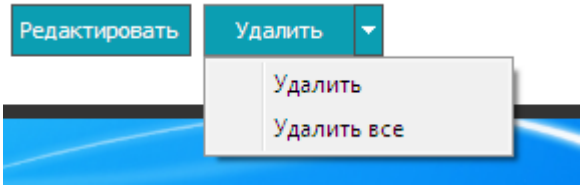

Рис. 6.9. Удаление всех правил

Удаленная активация правил

Киберсейф Межсетевой Экран позволяет удаленно активировать ранее определенные разрешающие правила. Принцип этой функции в следующем. Сначала администратор настраивает разрешающие правила, которые будут активированы по удаленному запросу. Чтобы создать такое правило, нужно в окне создания/редактирования правила на вкладке **Дополнительно** включить переключатель **Активация по удаленному запросу доступа** (рис. 6.10).

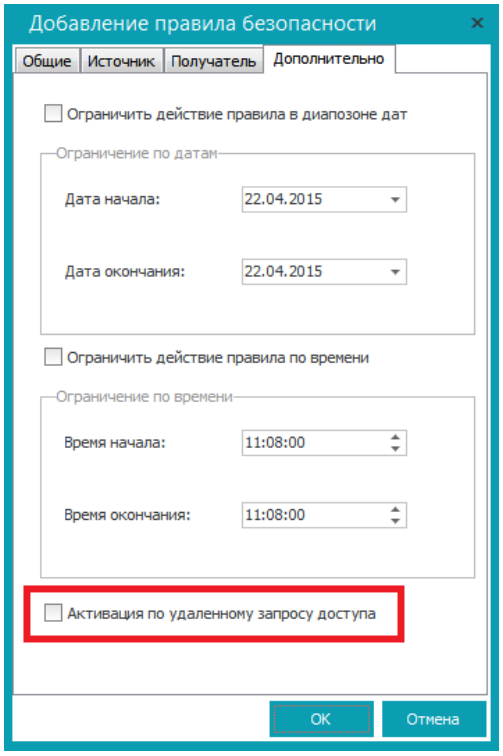

Рис. 6.10. Включение удаленной активации правила

Для удаленной активации правила нужно запустить утилиту **Удаленный доступ** (**Пуск, Все программы, CS Firewall, Киберсейф Удаленный доступ** или вручную запустить исполнимый файл rcsf.exe). Утилита удаленного доступа изображена на рис. 6.11. Администратору нужно ввести IP-адрес брандмауэра, на котором нужно удаленно активировать разрешающие правила, номер порта, имя пользователя и пароль. Если параметры введены правильно, на удаленном брандмауэре будут активированы правила, в настройках которых установлен переключатель Активация по адаленному запросу доступа.

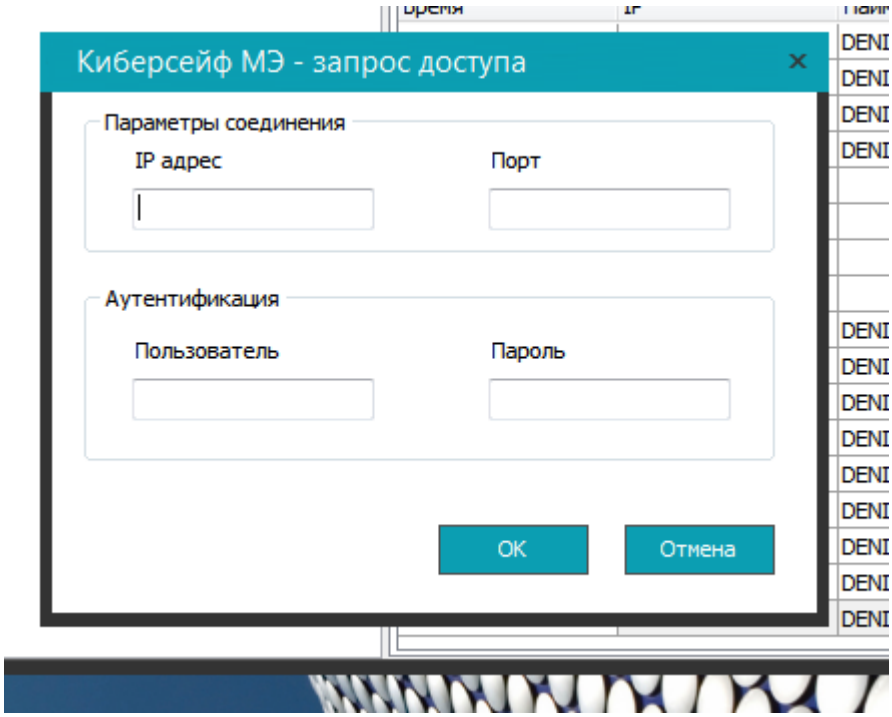

Рис. 6.11. Удаленный доступ

Правила будут активны до тех пор, пока работает утилита удаленного доступа. Как только администратор закроет утилиту, правила будут деактивированы.

Правила переадресации

Киберсейф Межсетевой Экран позволяет производить перенаправление портов (и даже конкретный IP/Протокол) на другой IP адрес. Другими словами, Киберсейф Межсетевой Экран может выполнить перенаправление пакетов, поступающих на определенный IP-адрес/порт, на другой IP-адрес/порт. Данный процесс называется Port Mapping или PAT (Port Address Translation).

Для того чтобы создать новое перенаправление, перейдите в раздел **Правила переадресации**. Затем нажмите кнопку **Добавить** и заполните необходимые свойства (рис. 6.12).

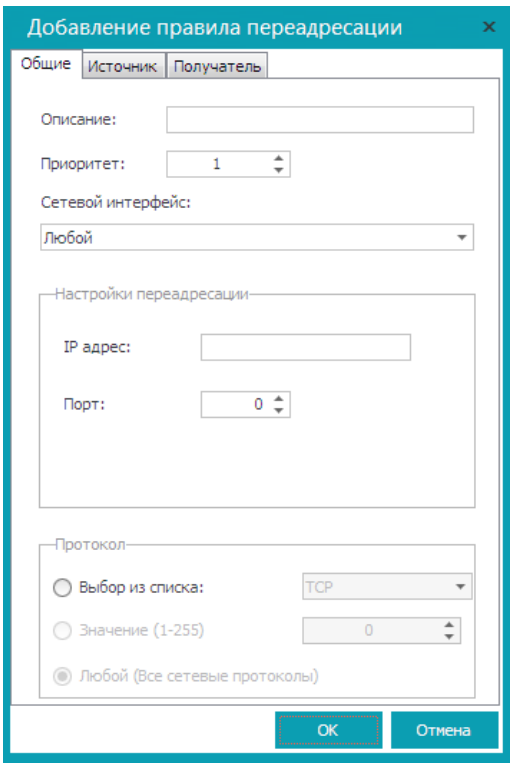

Рис. 6.12. Создание правила переадресации

Правила шейпера: ограничение трафика

Что такое правила шейпера?

Ограничение трафика является всего лишь способом контролировать трафик компьютерной сети в целях оптимизации и не гарантирует производительность и/или увеличение пропускной способности.

Ограничение трафика обеспечивается механизмом контроля объема трафика, передаваемого по сети, а также скорости, с которой он передается. Программа также служит для определения транспортных потоков для различных сервисов сети, который позволяет трафик-формирующим механизмам контролировать разделение трафика на отдельные потоки и по-разному их формировать.

Ограничение трафика осуществляется посредством установки правила шейпера.

Свойства правила шейпера

Идентификатор фильтра (или приоритет фильтра) представляет собой числовое значение в диапазоне от 1 до 65535. Чем меньше значение приоритета фильтра, тем выше его приоритет и тем быстрее он будет применяться при анализе пакетов.

Сетевой интерфейс представляет собой сетевой адаптер, который принимает пакеты, и впоследствии анализирует их на основе фильтра.

Общее значение скорости передачи определяет среднюю скорость трафика в байтах в секунду.

Пиковое значение скорости передачи определяет пиковую скорость трафика в

байтах в секунду.

Фильтр применяется к пакетам с выбранным протоколом.

Создание правила шейпера

Перейдите в раздел **Правила шейпера** и нажмите кнопку **Добавить** для добавления нового правила шейпера (рис. 6.13). Заполните параметры на вкладке **Общие**. Назначение этих параметров было только что описано.

Затем перейдите на вкладку **Источник**, чтобы определить источника пакетов. Помните, что термин *порт* применяется только к TCP/UDP-соединениями. Аналогично, на вкладке **Получатель** можно задать получателя пакетов.

Примечание. Киберсейф Межсетевой экран контролирует объем и скорость передачи только исходящего трафика. Также важно определить порядок фильтров шейпера при разработке политики компьютера.

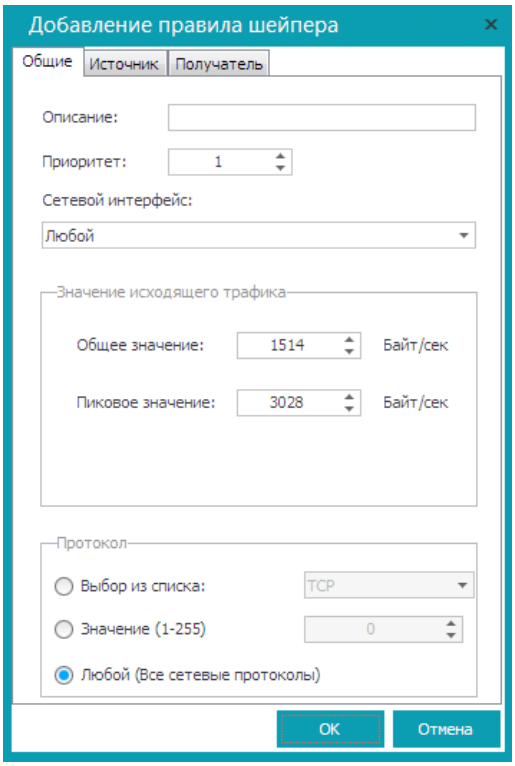

Рис. 6.13. Добавление правила шейпера

7 Маршрутизация и NAT

В этом разделе рассказывается о том, как превратить ваш компьютер в шлюз, настроить NAT и создать сетевые псевдонимы.

В этом разделе

Преобразование сетевых адресов (NAT) 46
Маршрутизация 48
Сетевые псевдонимы 49

Преобразование сетевых адресов (NAT)

Теория

Для начала определимся с терминологией, а потом уже перейдем к настройке межсетевого экрана. *Шлюзом* называется компьютер, предоставляющий компьютерам локальной сети доступ к Интернету. Шлюз выполняет как бы маршрутизацию пакетов. Но не нужно путать шлюз с обычным маршрутизатором. Маршрутизатор используется просто для пересылки пакетов, поэтому его можно использовать для соединения сетей одного типа, например, локальной и локальной, глобальной и глобальной. Шлюз используется для соединения сетей разных типов, например, локальной и глобальной, как в нашем случае.

Сложность в соединении сетей разных типов заключается в различной адресации. В локальной сети обычно используются локальные адреса, которые недопустимы в Интернете, например, 192.168.*.* (сеть класса C), 10.*.*.* (сеть класса A) и 172.16.*.*-172.31.*.* (класс B)). Поэтому шлюз должен выполнить преобразование сетевого адреса (NAT, Network Address Translation).

Предположим, у нас есть шлюз и локальная сеть с адресами 192.168.*.*. Реальный IP-адрес (который можно использовать в Интернете) есть только у шлюза – пусть это 193.254.219.1. У всех остальных компьютеров локальные адреса, поэтому при всем своем желании они не могут обратиться к Интернет-узлам.

Все узлы нашей локальной сети используют в качестве шлюза компьютер с адресом 192.168.1.1. Это означает, что все запросы будут переданы на узел 192.168.1.1. Запросы передаются в виде:

Назначение: IP-адрес узла Интернета
Источник: адрес компьютера локальной сети, пусть 192.168.1.10

Наш шлюз принимает запрос и перезаписывает его так:

Назначение: IP-адрес узла Интернета
Источник: 193.254.219.1

То есть шлюз подменяет адрес источника, устанавливая в качестве этого адреса свой реальный IP-адрес – иначе бы любой Интернет-узел не принял бы запрос с локального адреса. Получив ответ от узла, он направляет его нашему узлу:

Назначение: 192.168.1.10
Источник: IP-адрес узла Интернета

Нашему локальному узлу "кажется", что он получил ответ непосредственно от узла Интернета, а на самом деле ответ приходит от шлюза.
Кроме возможности компьютеров с локальными IP-адресами подключаться к глобальной сети, в которой используются реальные IP-адреса, NAT позволяет защищать локальную сеть, скрывая внутренние адреса, а также экономит сами IP-адреса, которых не так уж и много (если говорить об IPv4).

Включение NAT

Перейдите в раздел **Сеть, Преобразование сетевых адресов**. Очень важно правильно выбрать сетевой интерфейс, который будет являться NAT провайдером и публичным IP адресом для внешнего (интернет) трафика. Этот интерфейс выбирается из списка **Назначение интерфейса интернет-провайдера**. IP-адрес интерфейса изменять не нужно (за исключением лишь случаев, когда вы знаете, что делаете).
В таблице **Выбор интерфейсов, которые получат доступ в Интернет** нужно выбрать локальные интерфейсы, то есть те, которым нужно "раздать" Интернет. Весь трафик будет проходить через файрвол, поэтому к нему будут применяться правила и другие проверки.
После этого нажмите кнопку **Старт NAT** (рис. 7.1). После этого нужно изменить настройки всех клиентов вашей сети и указать в качестве шлюза IP-адрес компьютера, на котором запущена программа с включенным NAT. В настройках DHCP-сервера желательно указать IP-адрес шлюза (компьютера, на котором запущена программа Киберсейф Межсетевой экран в режиме NAT), чтобы вручную не настраивать каждый компьютер.
После включения NAT кнопка **Старт NAT** превратится в кнопку **Стоп NAT**. Ее нужно нажать для выключения NAT, если преобразование сетевых адресов больше вам не нужно.

Примечание. Перед включением NAT убедитесь, что в настройках программы включен переключатель **Включить маршрутизацию в Windows**.

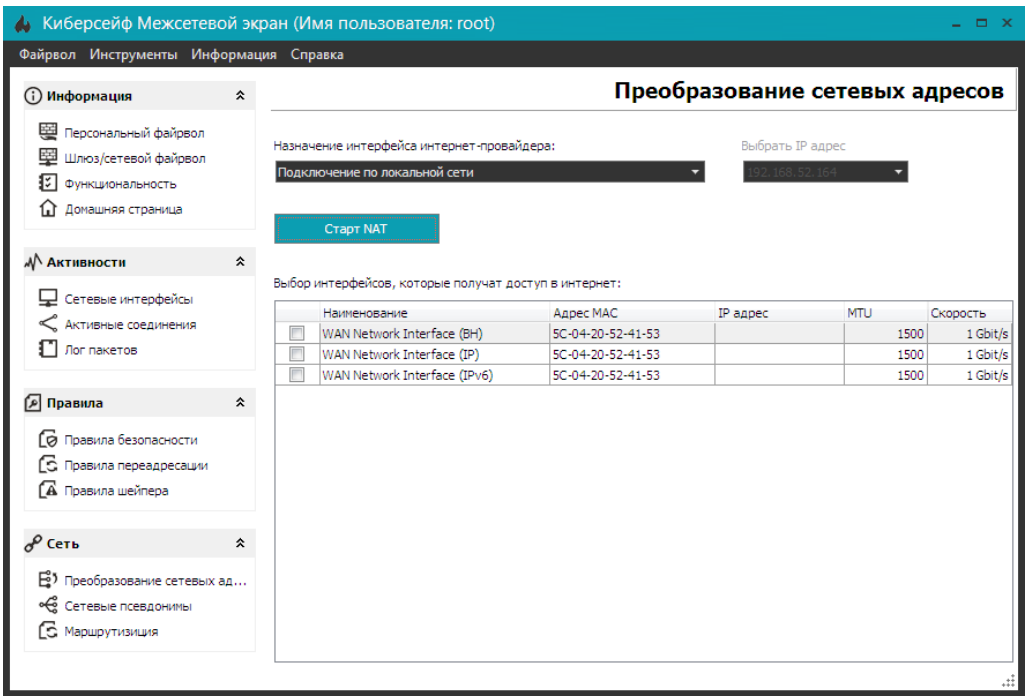

Рис. 7.1. Включение NAT

Маршрутизация

Маршрутизация - это процесс перенаправления пакета по различным сетям вплоть до места назначения.

В сетях TCP/IP информация маршрутизации хранится в виде таблицы маршрутизации. Таблица маршрутизации содержит ряд простых правил. Например, если пакет отправляется в сеть А он должен быть отправлен на маршрутизатор МА, если пакет отправляется в сеть Б, то его нужно отправить на маршрутизатор МБ. Пакет, отправляемый на любую другую сеть (не А и не Б), нужно отправить на маршрутизатор М (шлюз по умолчанию).

Раздел **Маршрутизация** позволяет редактировать таблицу маршрутизации (рис. 7.2). Для добавления маршрута нажмите кнопку **Добавить** и заполните форму, показанную на рис. 7.3.

В поле **IP адрес** нужно ввести IP-адрес сети, например, 10.0.0.0, в поле **Маска** - маску сети, например, 255.0.0.0, в поле **Шлюз** - маршрутизатор, который доставит пакеты в эту сеть (пусть это будет 10.0.0.1), а поле **Метрика** - это сколько маршрутизаторов будет на пути к этой сети.

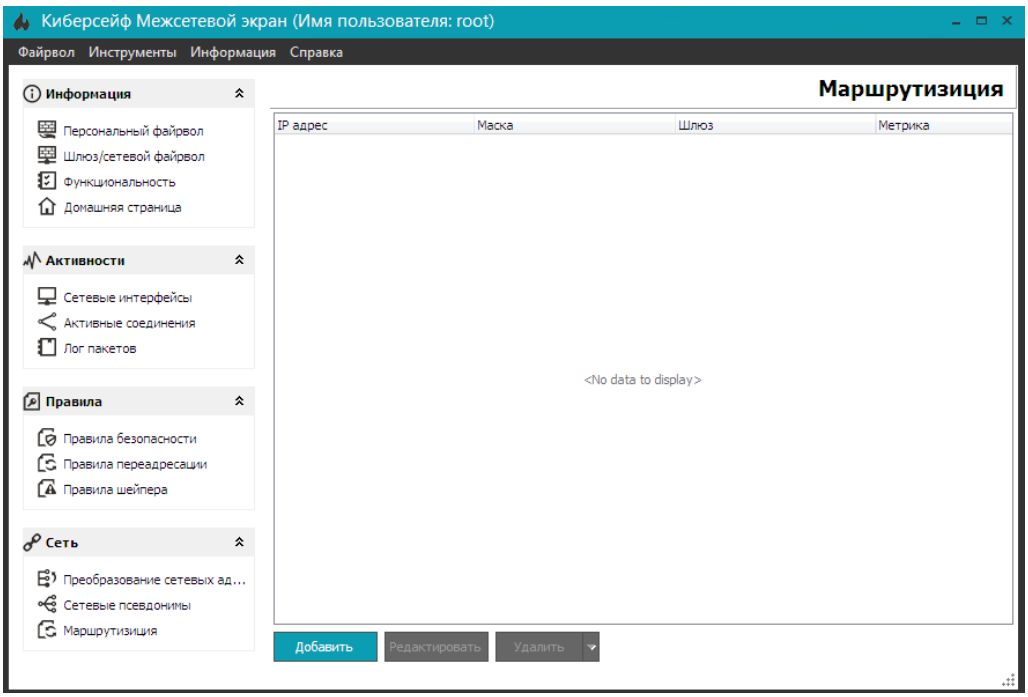

Рис. 7.2. Раздел Маршрутизация

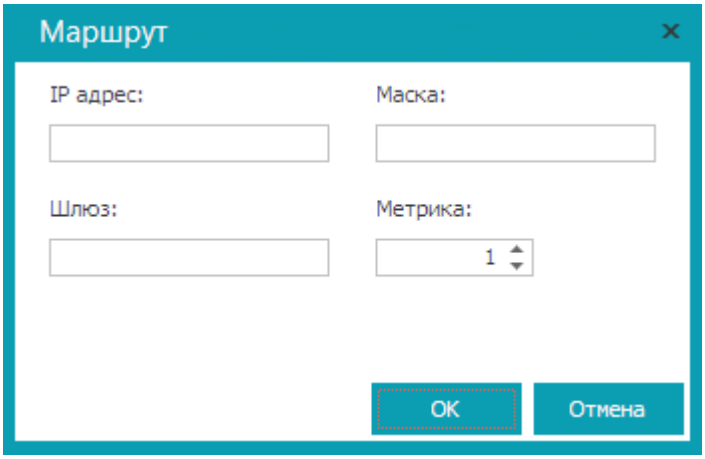

Рис. 7.3. Создание маршрута

Сетевые псевдонимы

Ранее было показано, что при указании источника и получателя можно использовать сетевые псевдонимы. Сетевые псевдонимы можно определить в разделы **Сеть, Сетевые псевдонимы**.

Перейдите в этот раздел и нажмите кнопку **Добавить**. В появившемся окне введите название псевдонима и определите, на что будет ссылаться псевдоним - или на всю подсеть (нужно задать IP-адрес сети и маску) или же на диапазон IP-адресов (рис. 7.4).

После этого созданный псевдоним можно будет использовать при создании правил брандмауэра (рис. 7.5).

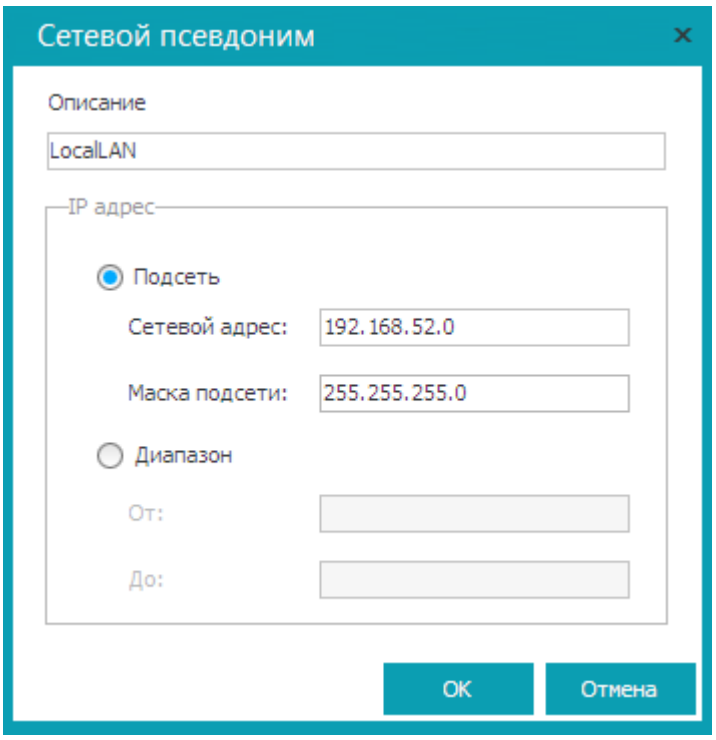

Рис. 7.4. Создание псевдонима

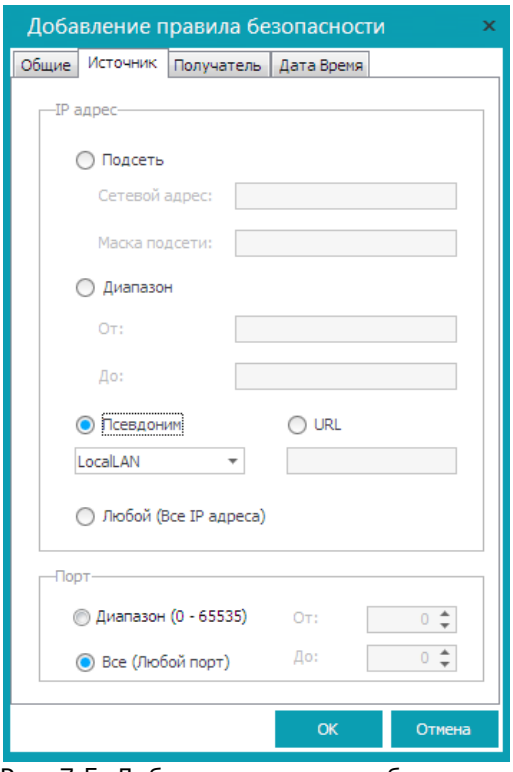

Рис. 7.5. Добавление правила брандмауэра с использованием псевдонима

8 Киберсейф Удаленный сервер

Данный раздел посвящен программе Киберсейф Удаленный сервер и удаленному управлению межсетевыми экранами с ее помощью.

В этом разделе

Назначение программы 50
Первый запуск программы 50
Запуск сервера 51
Настройка клиентов 52
Просмотр общей информации и журнала 53
Назначение пользователя администратором 55
Создание сценария развертывания 55
Развертывание программы с помощью Active Directory 57

Назначение программы

Программа Киберсейф Удаленный сервер позволяет администратору сети удаленно управлять программами Киберсейф Межсетевой экран, которые установлены на других компьютерах сети.

Примечание. Возможно удаленное управление программой Киберсейф Межсетевой экран без развертывания удаленного сервера. Для этого в командной строке введите команду

```
csf.exe /remote ipaddress port
```

Например:

```
csf.exe /remote 192.168.1.14 50001
```

После этого программа запросит имя пользователя (пользователь должен быть зарегистрирован на удаленной машине) и пароль, и вы сможете управлять программой Киберсейф Межсетевой экран, установленной на удаленном компьютере.

Первый запуск программы

При первом запуске программа просит проверить лицензионный ключ и активировать программы (рис. 8.1). Введите лицензионный ключ и нажмите кнопку **Активация через Интернет**. Конечно, на момент нажатия этой кнопки соединение с Интернетом должно быть установлено. Если ключ введен правильно, вы увидите сообщение об активации ключа (рис. 8.2).

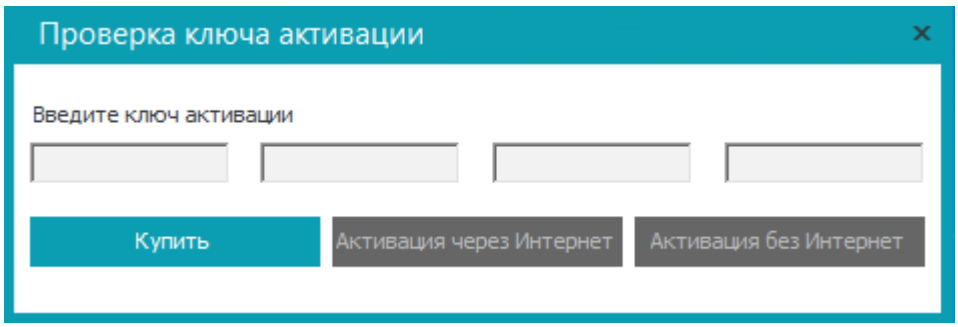

Рис. 8.1. Активация программы

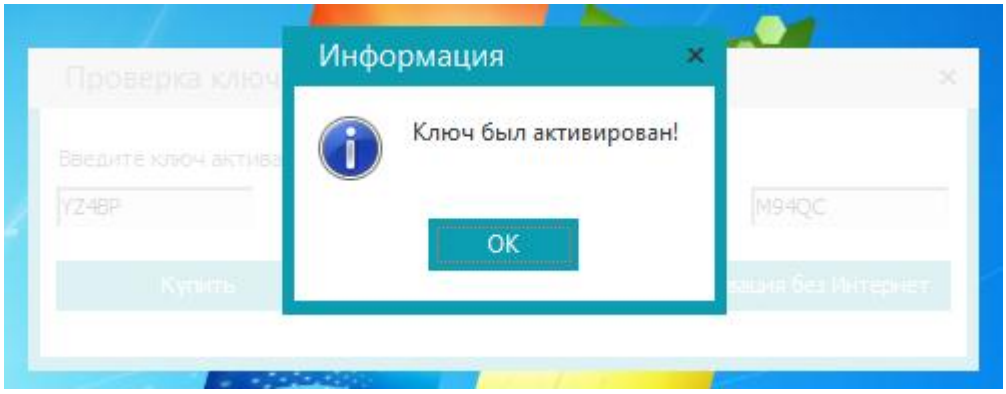

Рис. 8.2. Ключ активирован

Запуск сервера

В основном окне программы (рис. 8.3) установите порт, на котором будет работать сервер (по умолчанию используется порт 50005) и нажмите кнопку **Запуск сервера**. При желании вы можете установить другой номер порта. Номер порта при закрытии программы будет сохранен и вам не придется вводить его заново.

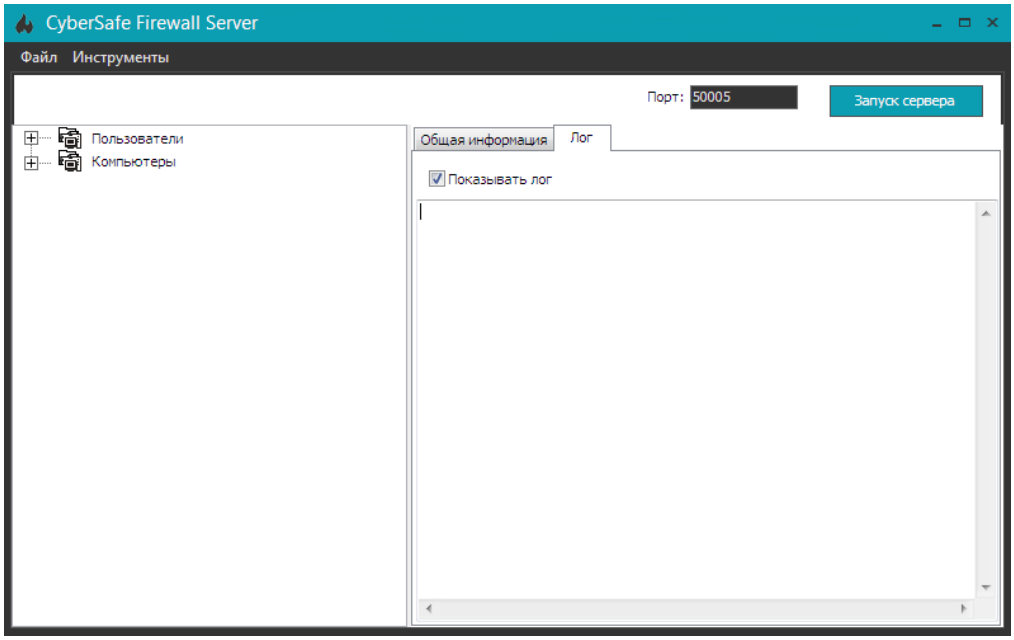

Рис. 8.3. Основное окно программы Киберсейф Удаленный сервер

После запуска сервера кнопка **Запуск сервера** будет переименована в **Останов сервера**. На рис. 8.4 продемонстрировано, что сервер запущен и что изменен порт по умолчанию. Особое внимание уделяется порту сервера, поскольку при неправильном указании номера порта клиенты не смогут подключиться к серверу.

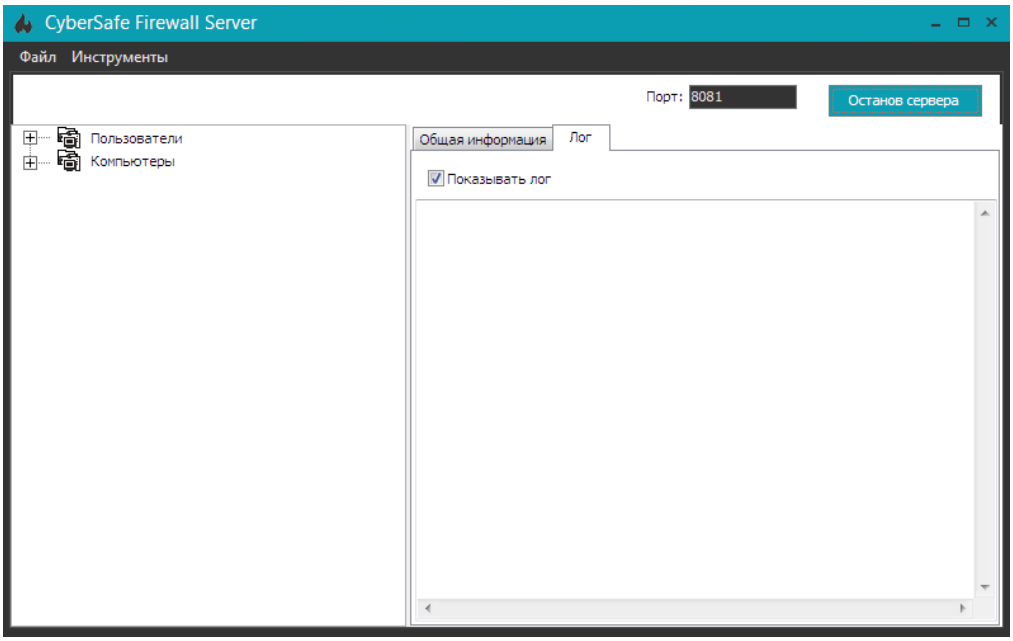

Рис. 8.4. Сервер запущен

Настройка клиентов

После того, как сервер запущен, нужно настроить клиенты. Для этого на каждом компьютере сети, где установлена программа Киберсейф Межсетевой экран нужно выбрать команду меню **Инструменты, Настройки**.

На вкладке **Дополнительно** укажите IP-адрес удаленного сервера (компьютера, на котором запущена программа Киберсейф Удаленный сервер) и порт удаленного сервера (который вы указали в программе Киберсейф Удаленный сервер), см. рис. 8.5.

Узнать IP-адрес удаленного сервера можно с помощью команды `ipconfig`, запущенной на самом удаленном сервере (рис. 8.6).

Напомним, что удаленный сервер используется исключительно для управления межсетевыми экранами Киберсейф в вашей сети и может отличаться от шлюза. Другими словами, компьютер А может быть шлюзом, предоставляющим доступ к Интернету (на нем запущена программа Киберсейф Межсетевой экран в режиме NAT), а программа Киберсейф Удаленный сервер может быть установлена на компьютере Б, откуда администратор сети управляет межсетевыми экранами.

Для применения настроек нажмите кнопку **Применить** в окне настройки программы Киберсейф Межсетевой экран.

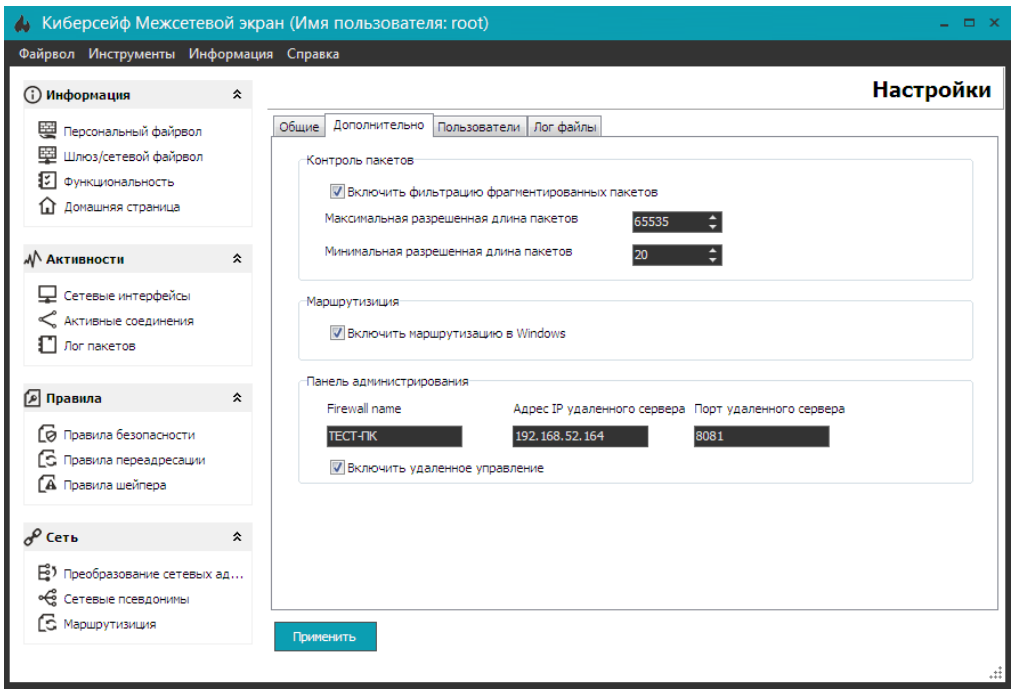

Рис. 8.5. Настройка клиента

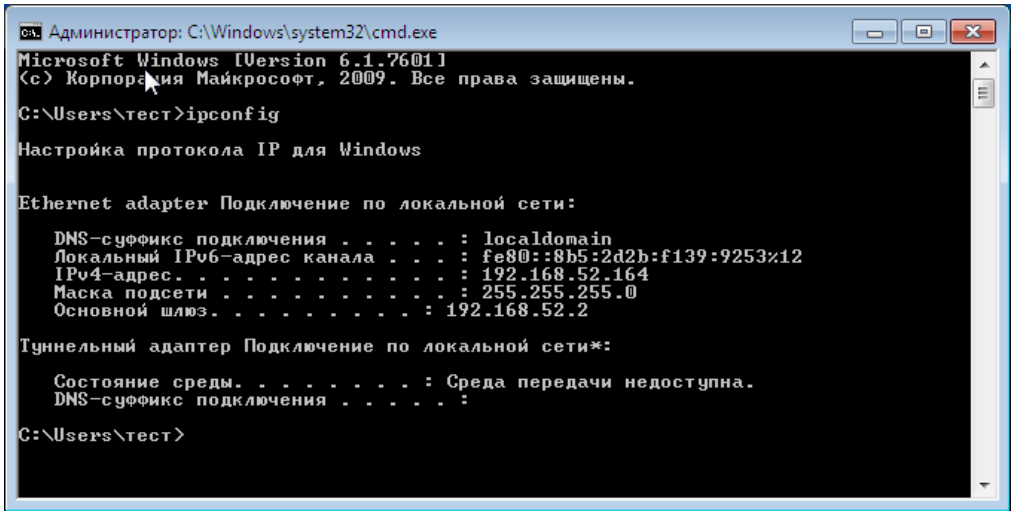

Рис. 8.6. Адрес удаленного сервера

Просмотр общей информации и журнала

На рис. 8.7 видно, что из трех компьютеров активен сейчас только один. Причины неактивности остальных компьютеров могут быть следующими:

- Компьютер выключен;
- Неправильно настроена программа Киберсейф Межсетевой экран. Проверьте правильность указания IP-адреса удаленного сервера и номера порта.
- Программа Киберсейф Межсетевой экран не запущена.

На вкладке **Общая информация** отображается название брандмауэра (указывается в настройках программы Киберсейф Межсетевой экран), IP-

адрес компьютера, время лицензии и название лицензии.

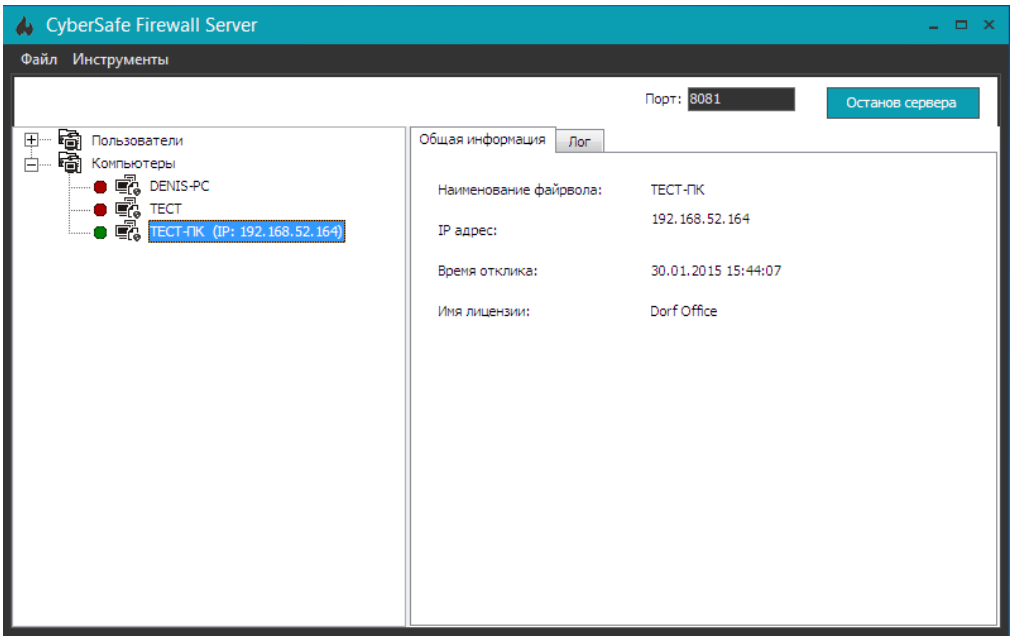

Рис. 8.7. Список компьютеров

На вкладке **Лог** отображается журнал событий, например, опрос (пинг) компьютера, вход того или иного пользователя и т.д. (рис. 8.8). В большой сети можно отключить переключатель **Показывать лог**, чтобы попросту не тратить ресурсы компьютера.

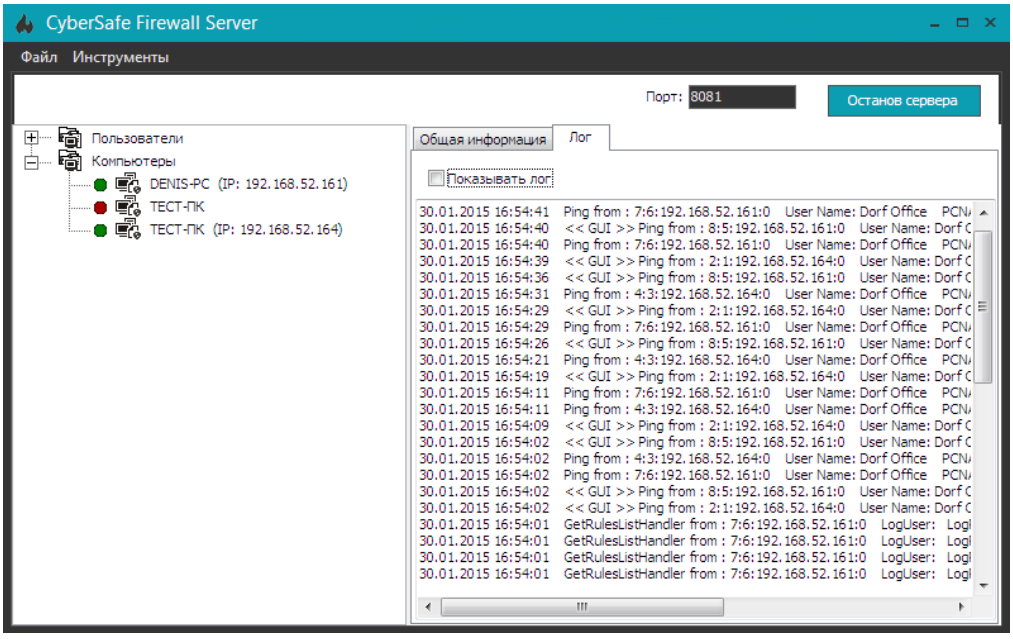

Рис. 8.8. Журнал удаленного сервера

Назначение пользователя администратором

С помощью программы Киберсейф Удаленный сервер вы можете назначить пользователя администратором. Администратор может с помощью панели администрирования управлять удаленным брандмауэром. О том, как управлять правилами удаленного брандмауэра, будет показано в следующем разделе, а пока разберемся, как назначить пользователя администратором.

Разверните узел **Пользователи** и выберите пользователя, которого вы хотите сделать администратором и включите переключатель **Администратор** (рис. 8.9).

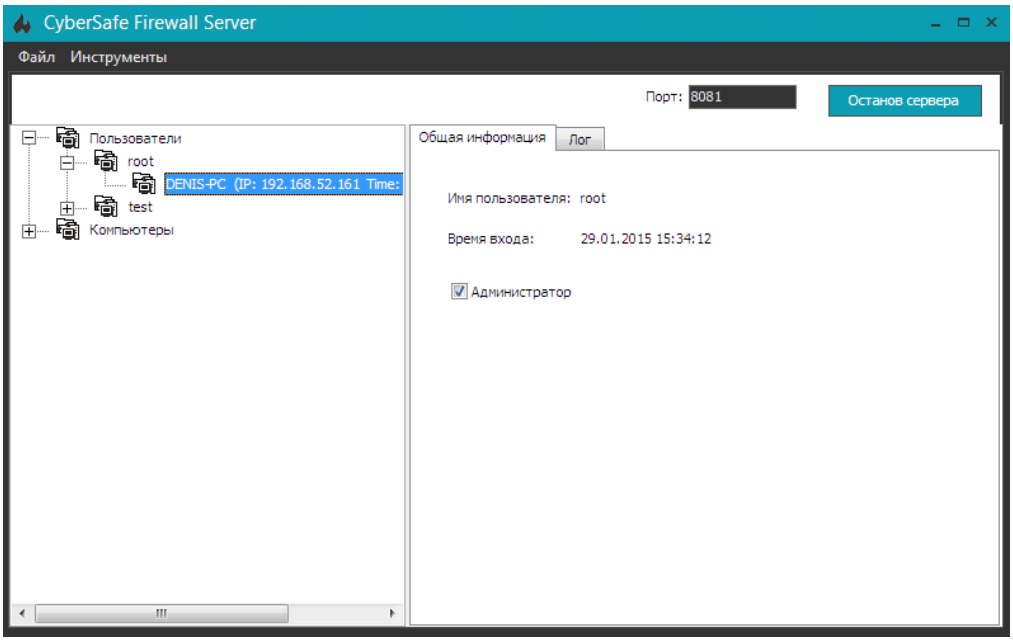

Рис. 8.9. Пользователь назначен администратором

После этого, если войти под этим пользователем в программу Киберсейф Межсетевой экран, то станет активной команда меню **Файрвол, Панель администрирования**.

Создание сценария развертывания

Ранее было сказано, что список пользователей уникален для каждой машины. Если вы хотите автоматизировать настройку программу Киберсейф Межсетевой экран и создать на каждой машине одинакового пользователя с одним и тем же паролем (для личного удобства), вы можете использовать сценарий развертывания.

Для создания сценария развертывания выполните следующие действия:

1. Откройте программу Киберсейф Удаленный сервер;
2. Выберите команду меню **Инструменты, Установочный скрипт файл**;
3. Заполните параметры, которые будут занесены в сценарий

развертывания, а именно порт, на котором будет работать файрвол (обычно 50001), порт удаленного сервера, IP-адрес удаленного сервера, ключ активации, e-mail администратора, пользователь и пароль по умолчанию (рис. 8.10);

4. Нажмите кнопку **Сохранить скрипт**;
5. В окне сохранения файла выберите формат сценария - или *.bat или *.mst (рис. 8.11).

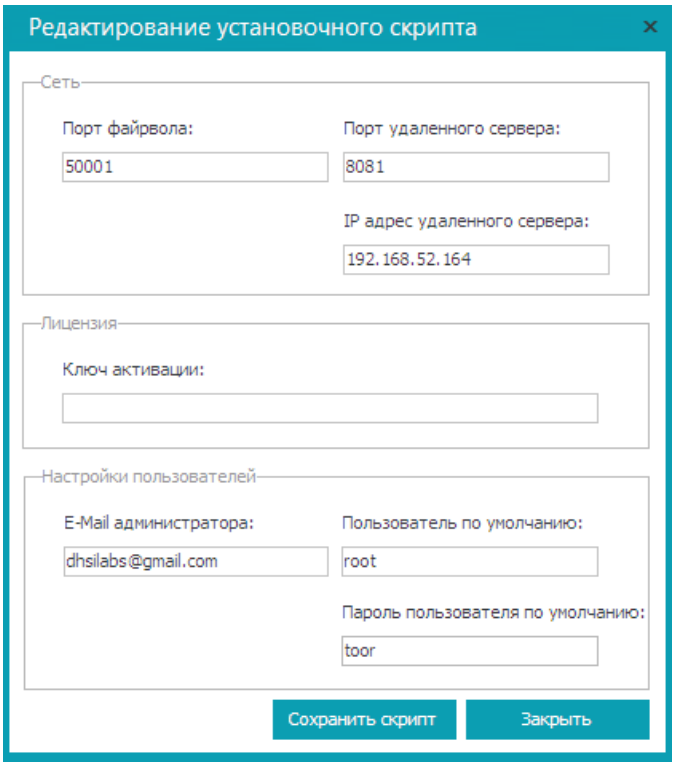

Рис. 8.10. Создание сценария развертывания

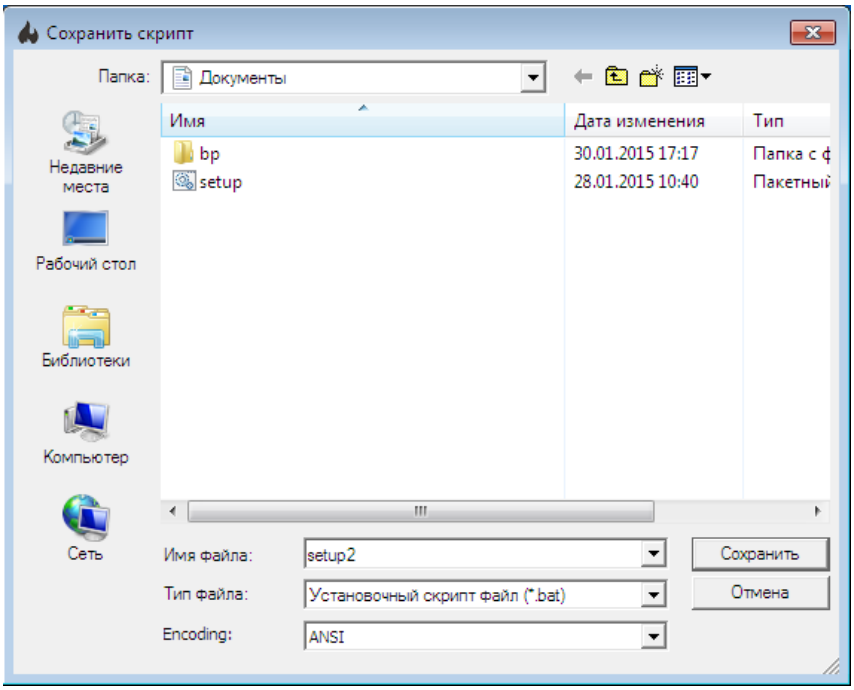

Рис. 8.11. Сохранение сценария развертывания

Созданный сценарий развертывания нужно поместить в одну папку с инсталлятором программы. Если просмотреть установочный bat-файл, то в него заносится строка вызова программы-инсталлятора с определенными параметрами, которые в качестве значений содержат введенными вами данные:

```
msiexec.exe /i "csfirewall.msi" CS_PORT_PROP="50001"
REMOTE_IP_PROP="192.168.52.164" REMOTE_PORT_PROP="8081"
LICENSE_KEY_PROP="" ADMIN_EMAIL_PROP="dhsilabs@gmail.com"
USER_NAME_PROP="root" USER_PASS_PROP="toor"
```

Затем, используя созданный сценарий развертывания, нужно установить программу на всех компьютерах вашей сети (или только на тех, на которых планировалось использование программы Киберсейф Межсетевой экран).

Развертывание программы с помощью Active Directory

В этом разделе речь пойдет о развертывании программы Киберсейф Межсетевой экран с помощью ActiveDirectory. Все иллюстрации для этого раздела были созданы в Microsoft Windows Server 2012 R2, но все приведенные инструкции будут работать и в более старых версиях (Microsoft Windows Server 2003/2008), возможно, немного будут отличаться иллюстрации.

Первым делом нужно создать папку для развертывания программного обеспечения. Она будет содержать все MSI-пакеты, развертывания которых вам нужно выполнить (не нужно создавать отдельную папку для программы Киберсейф Межсетевой экран).

Пусть это будет папка C:\Install. В этой папке создайте подпапку CSFirewall. В нее нужно поместить установочный файл csfirewall.msi и файл трансформации csfirewall.mst, который вы создали в предыдущем разделе (bat-сценарий в данном случае не подходит).

К папке C:\Install нужно предоставить общий доступ (рис. 8.12). Для этого щелкните правой кнопкой по папке и выберите команду **Свойства**. На вкладке Доступ нажмите кнопку **Общий доступ** и предоставьте доступ на чтение и запись администратору и доступ только на чтение всем остальным пользователям сети (рис. 8.13).

Далее запустите редактор групповой политики `gpmc.msc`. Мы предполагаем, что программу Киберсейф Межсетевой экран нужно будет установить не на всех компьютерах домена, а только на компьютерах подразделения CSFirewall Computers. Если у вас нет этого подразделения, создайте его (или подразделение с другим именем по вашему усмотрению).

Щелкните правой кнопкой мыши на подразделении CSFirewall Computers и выберите команду **Создать объект групповой политики** в этом домене и связать его (рис. 8.14).

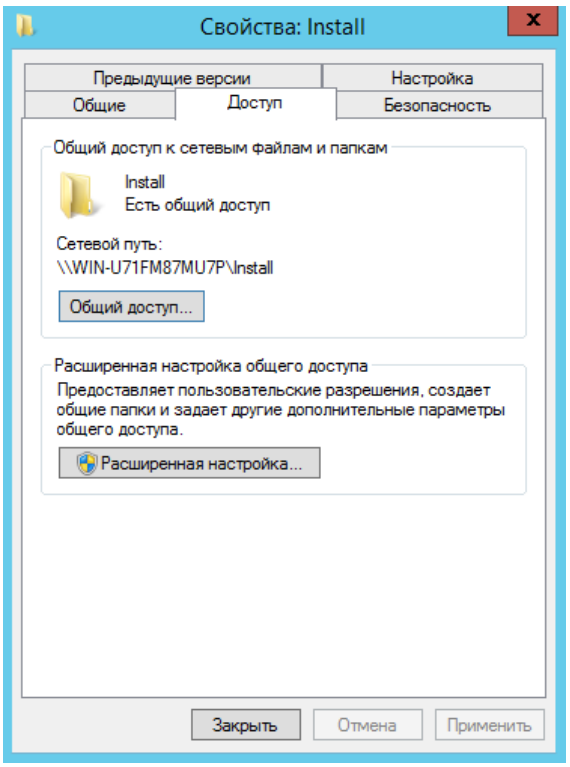

Рис. 8.12. Общий доступ к папке предоставлен

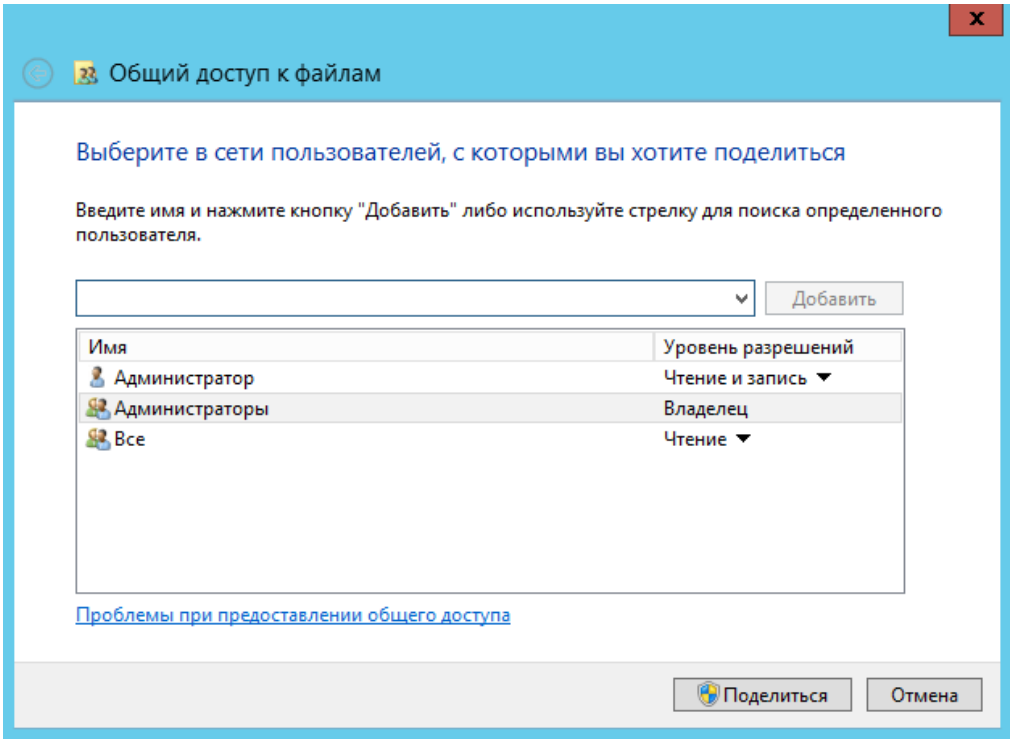

Рис. 8.13. Параметры общего доступа

Примечание. Если вам нужно установить программу на все компьютеры домена, тогда создавать отдельное подразделение не нужно. Просто щелкните правой кнопкой мыши на названии вашего домена и создайте GPO для всего домена.

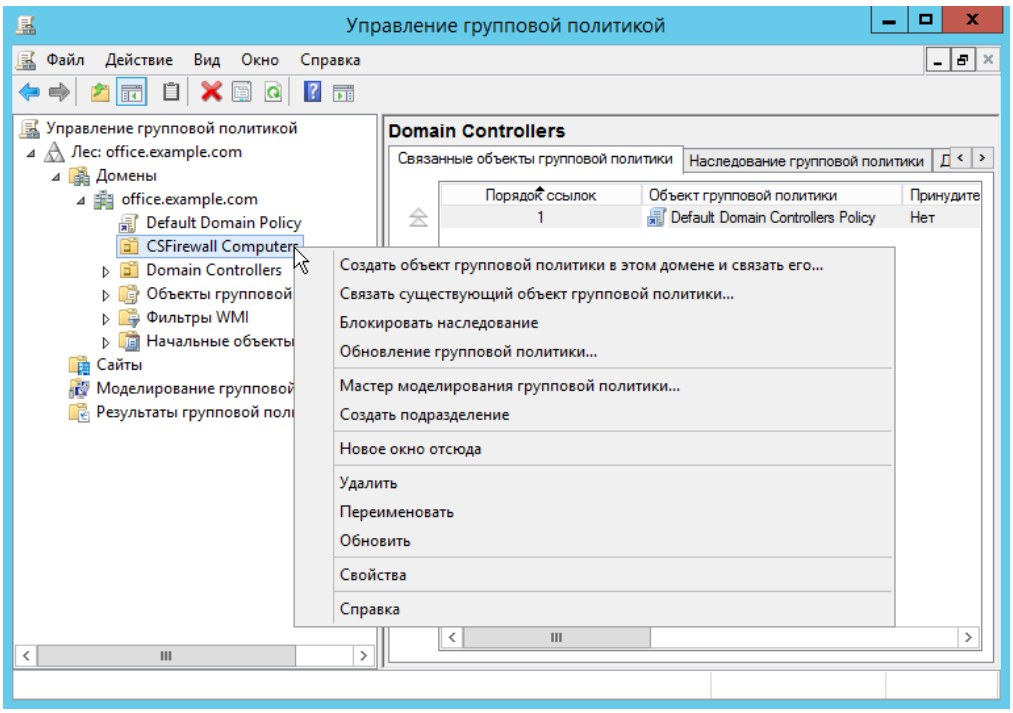

Рис. 8.14. Редактор групповой политики

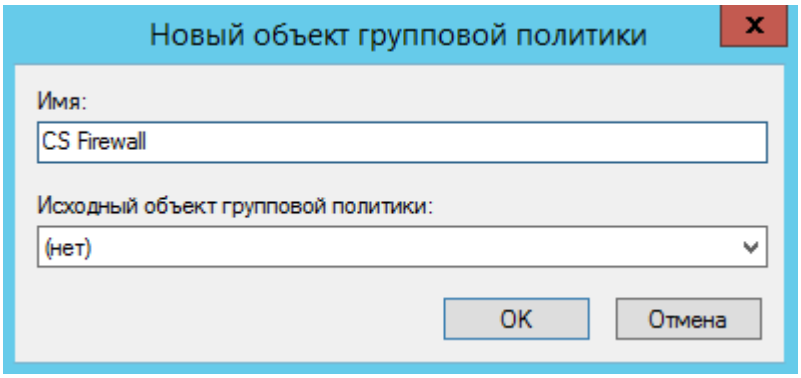

Рис. 8.15а. Создание нового объекта GPO

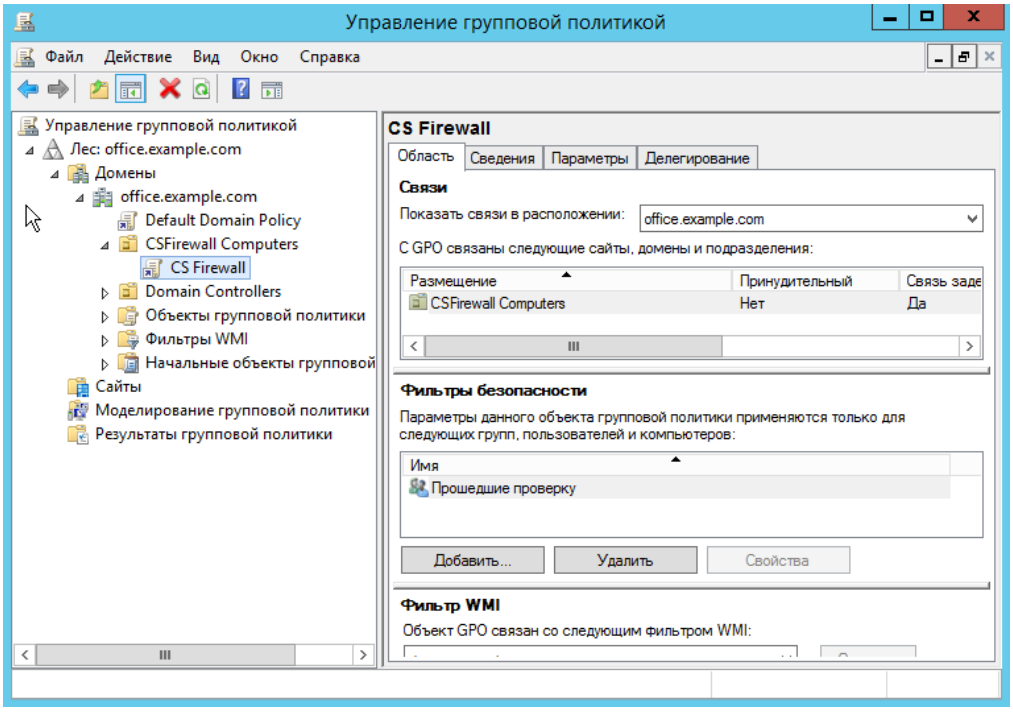

Рис. 8.15б. Созданный объект GPO

Назовите новый объект групповой политики CS Firewall (рис. 8.15а). Созданный GPO изображен на рис. 8.15б. В разделе **Фильтры безопасности** удалите группу **Прошедшие проверку** и добавьте компьютеры, группы и пользователей, к которым будут применены параметры данного объекта групповой политики. Другими словами добавьте компьютеры, на которые должна быть установлена программа.

Щелкните правой кнопкой мыши на только что созданном GPO (CS Firewall) и выберите команду **Изменить** (рис. 8.16).

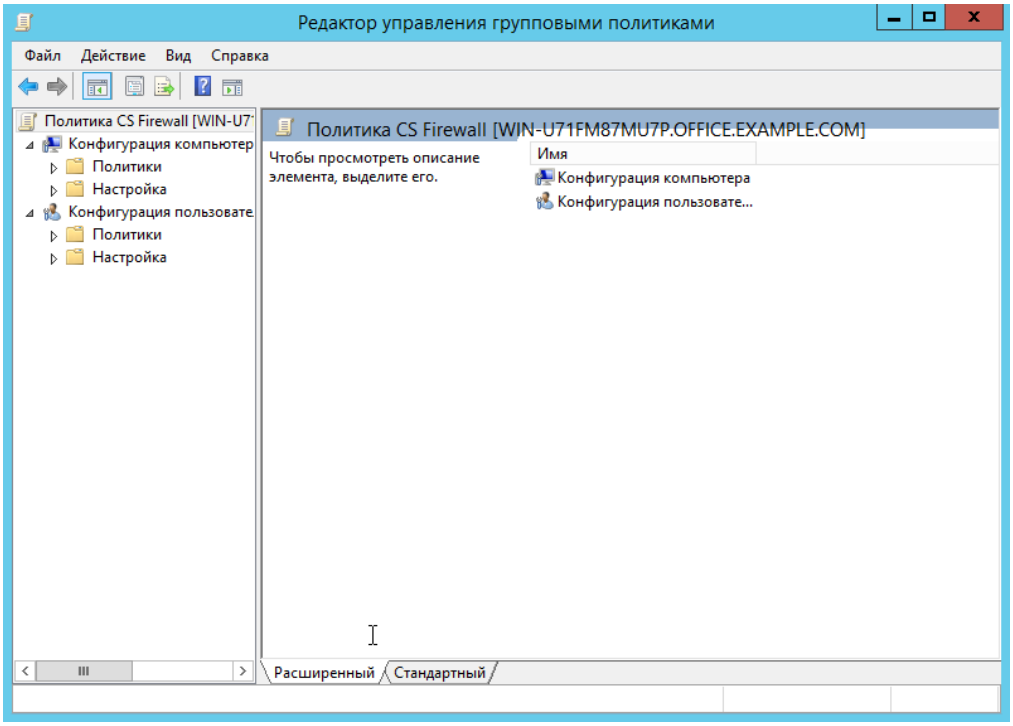

Рис. 8.16. Редактирование GPO

Перейдите в раздел **Конфигурация пользователя, Политики, Конфигурация программ, Установка программ** (рис. 8.17).

Щелкните правой кнопкой на разделе **Установка программ** и выберите команду **Создать, Пакет**. В появившемся окне нужно выбрать путь к MSI-файлу программы. Обратите внимание, что вводить нужно не локальный путь, а сетевой, поскольку пользователи будут получать доступ к пакету по сети (рис. 8.18).

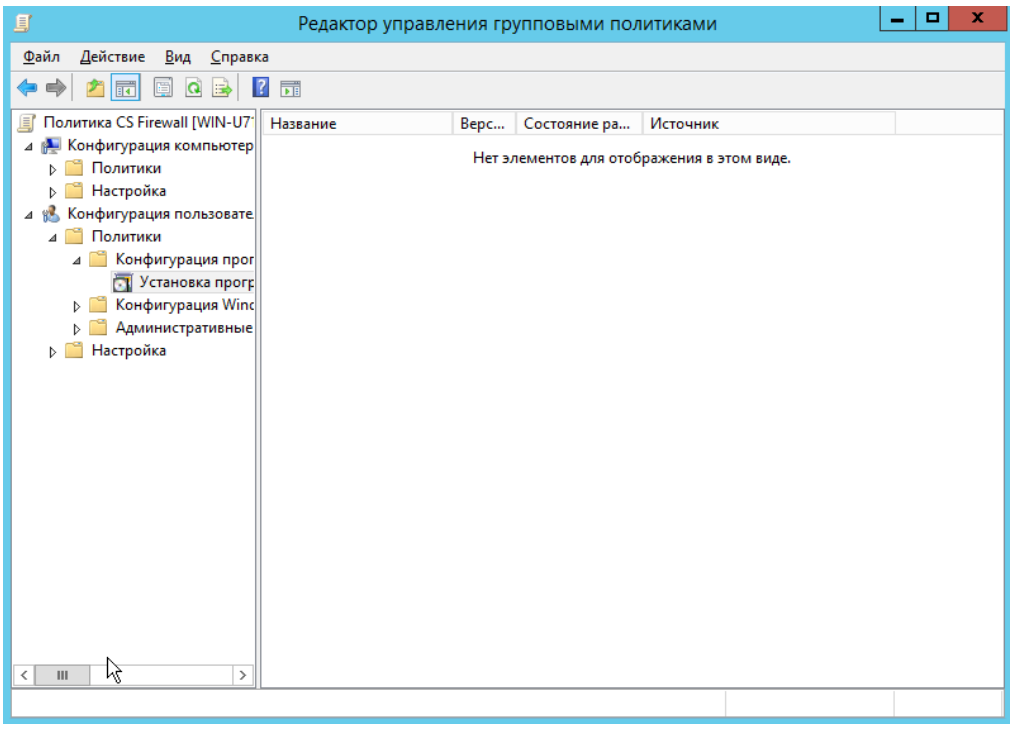

Рис. 8.17. Раздел **Конфигурация пользователя, Политики, Конфигурация программ, Установка программ**

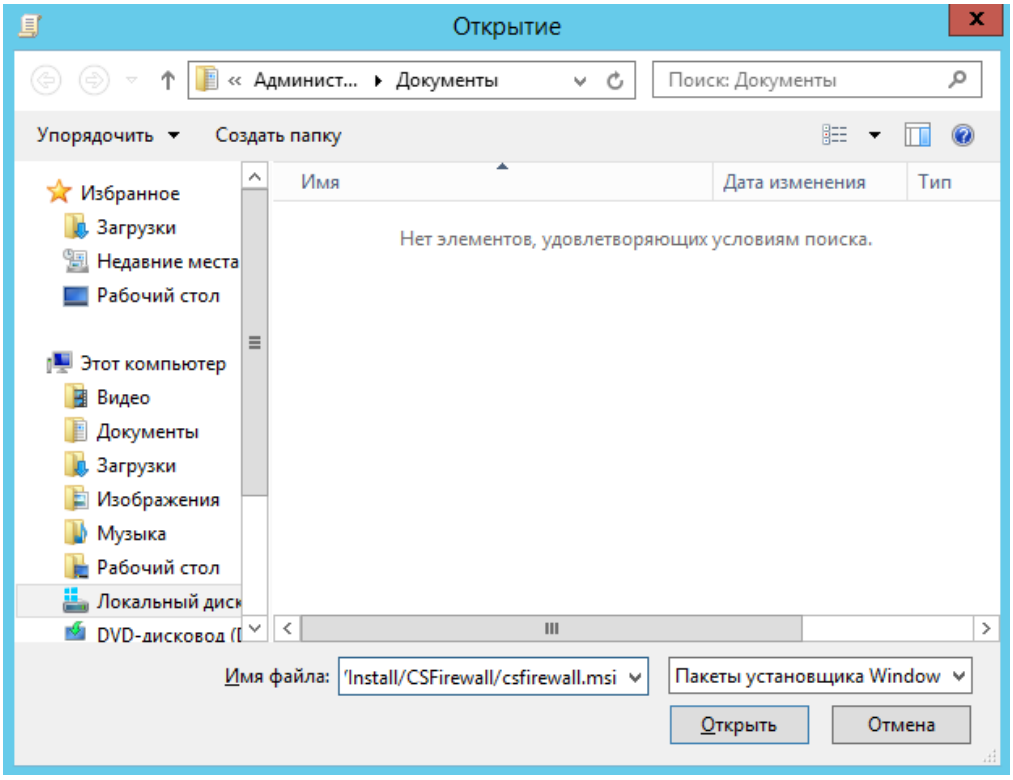

Рис. 8.18. Указываем сетевой путь к MSI-файлу

Следующий шаг - выбор метода развертывания. Поскольку мы хотим предоставить файл трансформации (mst-файл, созданный программой Киберсейф Удаленный сервер), то нужно выбрать особый метод развертывания (рис. 8.19). Благодаря этому будет открыто окно настройки

пакета развертывания (рис. 8.20). Затем перейдите на вкладку **Модификации**, нажмите кнопку **Добавить** и выберите файл трансформации (.mst-файл), рис. 8.21.

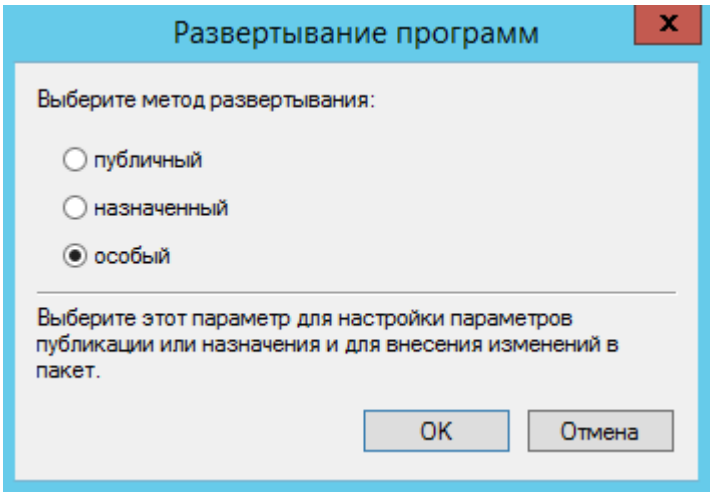

Рис. 8.19. Выбор метода развертывания

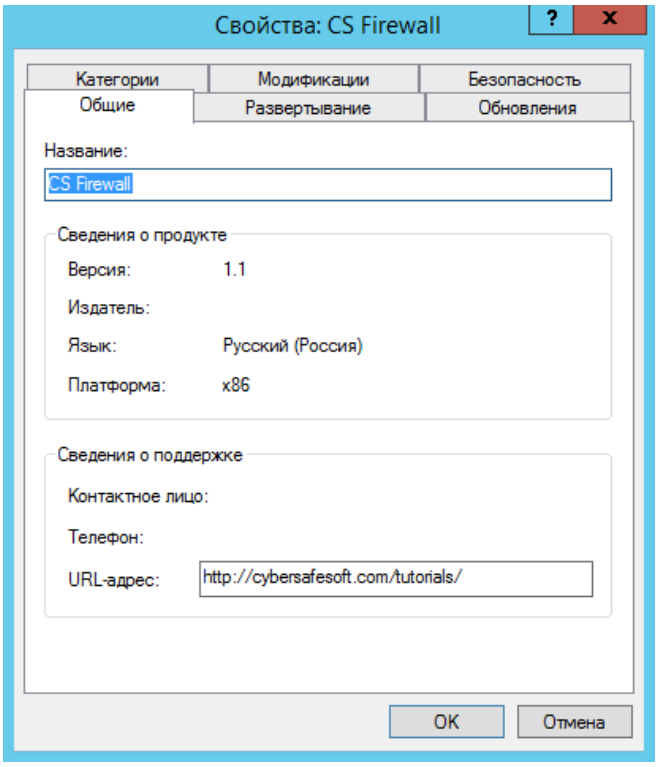

Рис. 8.20. Окно настройки пакета развертывания

Не спешите нажимать **OK**. Нужно еще настроить права доступа, поэтому перейдите на вкладку **Безопасность** (рис. 8.22) и предоставьте полный доступ к необходимым пользователям и группам. Также удалите группу **Прошедшие проверку**, если вы этого еще не сделали в разделе **Фильтры безопасности**. Только после настройки прав доступа можно нажать кнопку **OK**.

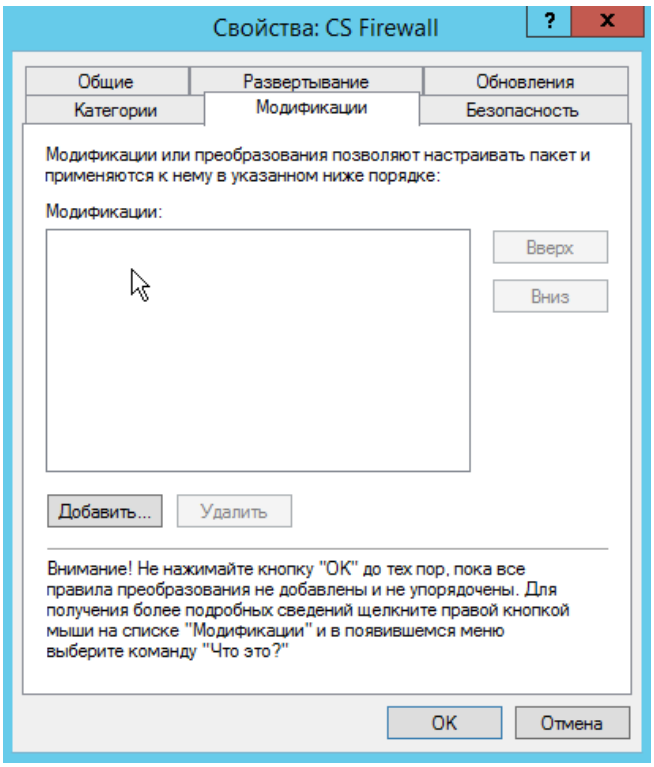

Рис. 8.21. Вкладка **Модификации**

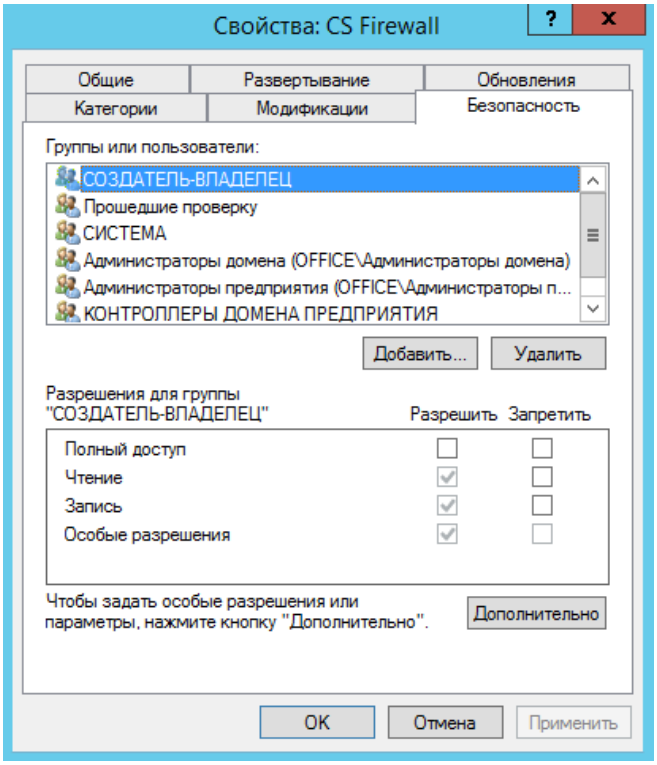

Рис. 8.22. Вкладка **Безопасность**

Примечание. После нажатия кнопки **ОК** пакет и файл трансформации (файлы .msi и .mst соответственно) будут прокэшированы. Если вам понадобится изменить файл трансформации после создания пакета, то придется создавать пакет развертывания заново.

На этом работа с редактором групповой политики завершена. Закройте все окна, откройте командую строку (или хотя бы окно **Выполнить**, нажав комбинацию клавиш Win + R) и введите команду:

```
gpupdate /force
```

На этом все. Программа будет автоматически установлена на компьютеры после их перезагрузки и до отображения окна входа в систему. Пользователь ни на что не может повлиять и ни в чем не может ошибиться.

Иногда программа не устанавливается автоматически. Чаще всего такая проблема наблюдается на рабочих станциях под управлением Windows XP. Чтобы произвести ее установку, нужно вручную ввести на ней команду `gpupdate /force`.

9 Панель администрирования

Данный раздел содержит информацию об использовании панели администрирования для удаленного управления межсетевыми экранами.

В этом разделе

Интерфейс панели администрирования. 65
Групповые и глобальные правила. 68
Удаленное управление файрволом. 69
Блокирование сайтов. 71

Интерфейс панели администрирования

Если пользователь, запустивший программу Киберсейф Межсетевой экран, является администратором, в меню **Файрвол** станет доступной команда **Панель администрирования** (рис. 9.1). Сама же панель администрирования изображена на рис. 9.2.

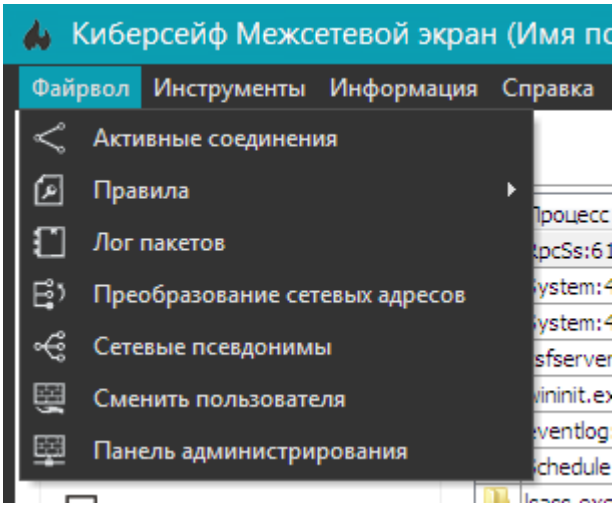

Рис. 9.1. Вызов панели администрирования

Как видно из рис. 9.2, сейчас есть три компьютера, на которых установлена программа Киберсейф Межсетевой экран. Компьютеры можно объединять в группы. Для этого щелкните правой кнопкой мыши на рабочей области программы и выберите команду **Добавить группу** (рис. 9.3).

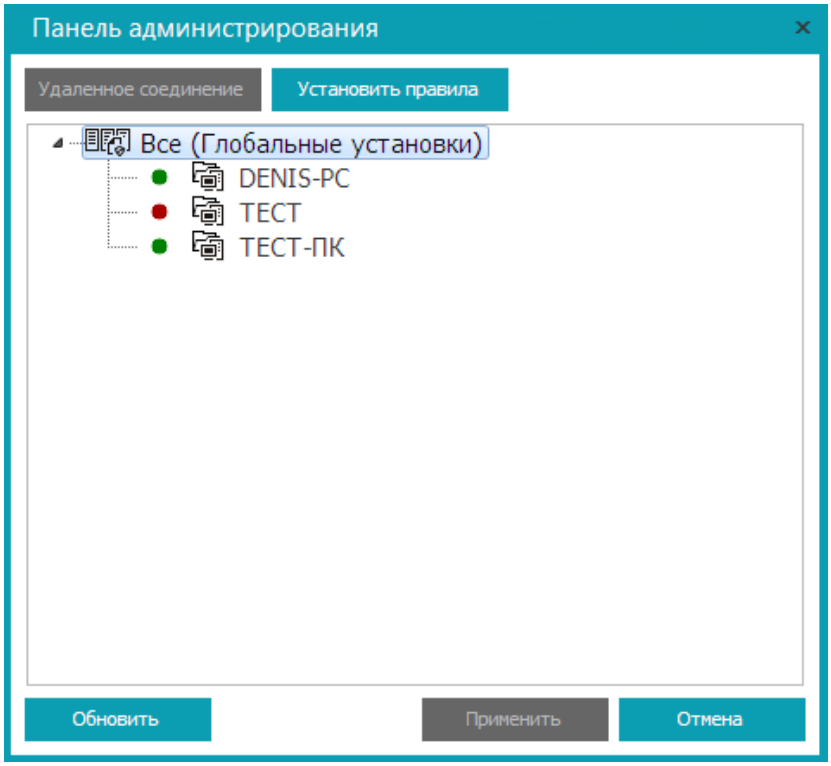

Рис. 9.2. Панель администрирования

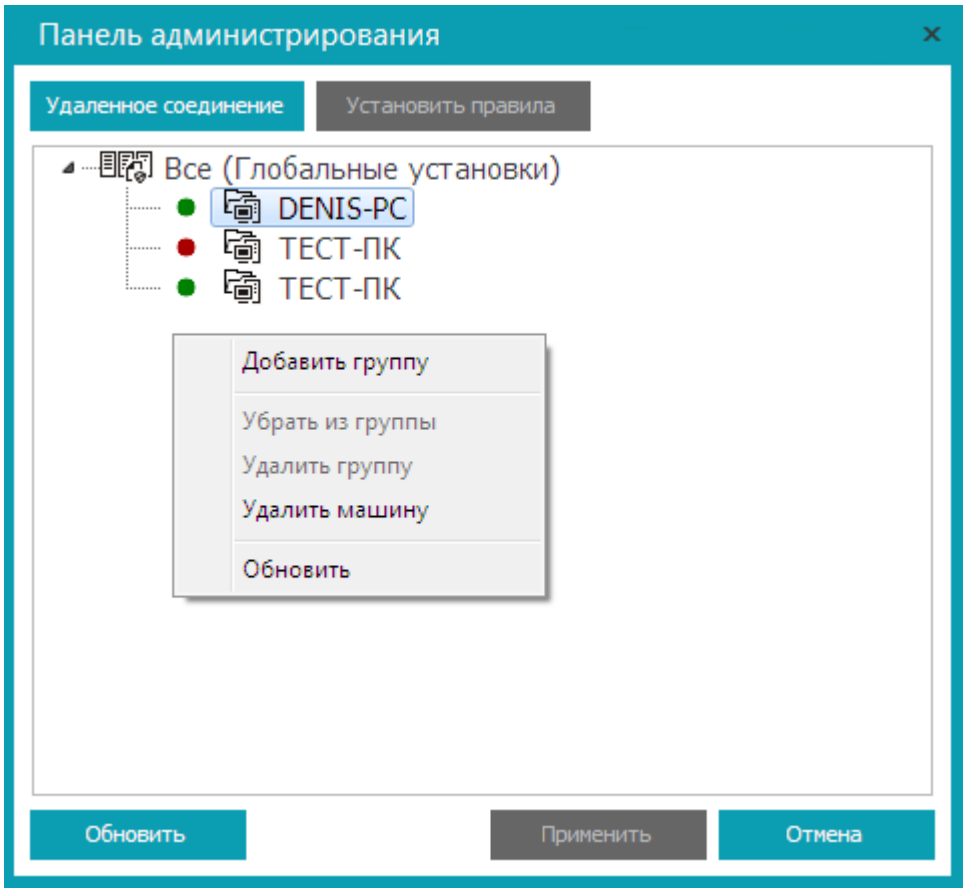

Рис. 9.3. Контекстное меню

Введите название группы и нажмите кнопку **Принять** (рис. 9.4). Созданная группа появится в дереве групп и компьютеров (рис. 9.5).

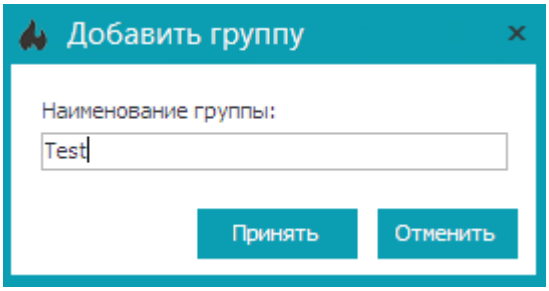

Рис. 9.4. Создание группы

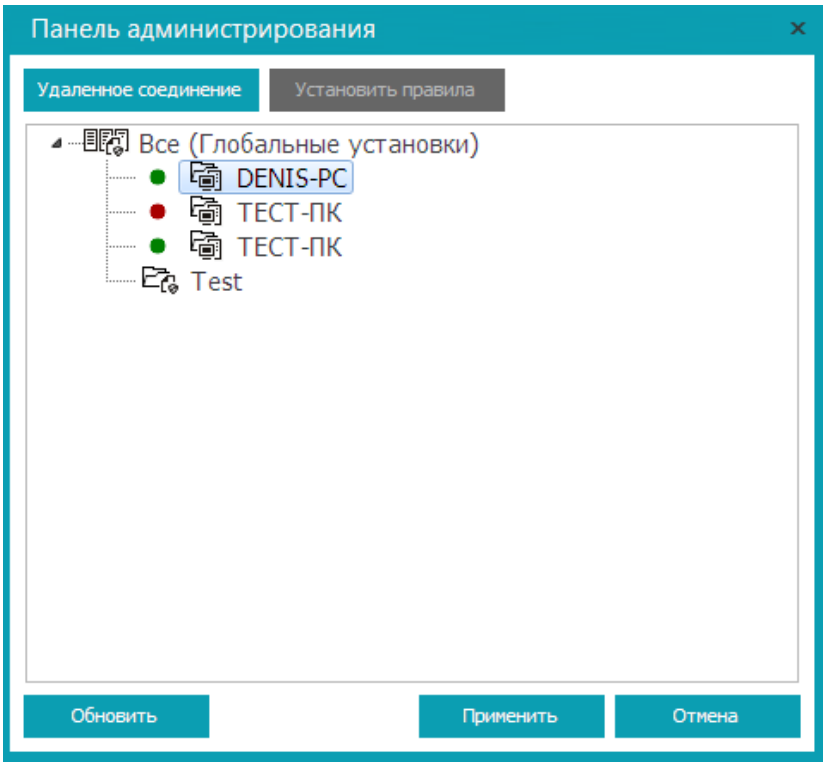

Рис. 9.5. Созданная группа

Чтобы добавить компьютер в группу, просто перетяните мышкой его значок на значок группы (рис. 9.6).

Обратите внимание на контекстное меню. Кроме команды **Добавить группу**, в нем есть следующие команды:

- **Убрать из группы** - используется для удаления компьютера из группы. После удаления из группы компьютер окажется в группе **Все** (глобальная группа).
- **Удалить группу** - удаляет группу.
- **Удалить машину** - удаляет машину из дерева панели администрирования.
- **Обновить** - обновляет дерево панели администрирования.

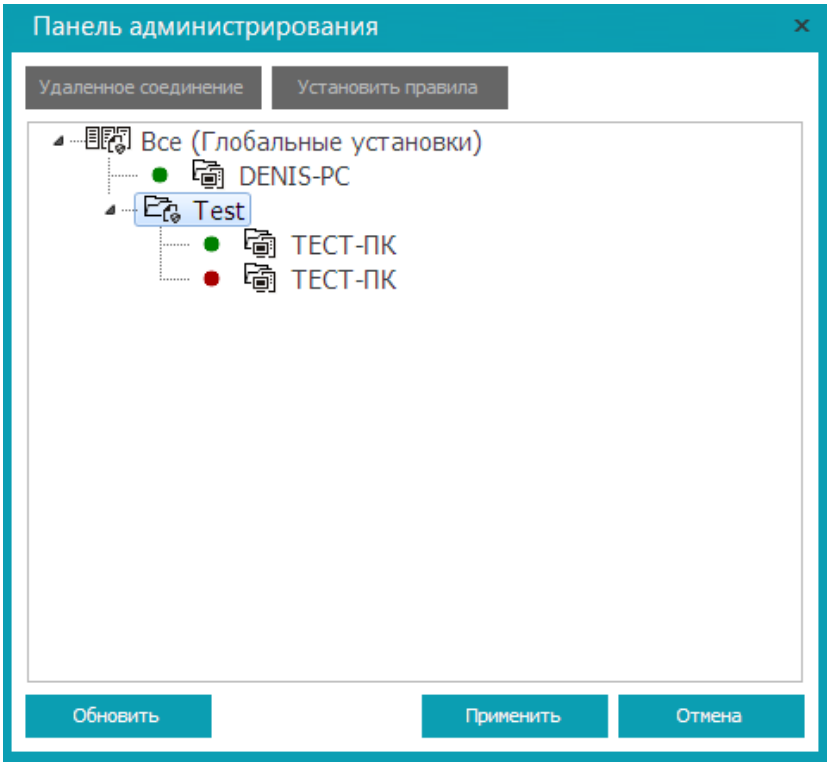

Рис. 9.6. Компьютеры перемещены в созданную группу

Предостережения. После изменения списка групп, например, после добавления или удаления группы обязательно нажмите кнопку **Применить**. Если вы этого не сделаете, а сразу приступите к установке правил (то есть выделите группу и нажмете кнопку **Установить правила**), то окно редактора правил будет содержать старую конфигурацию групп - новые группы в нем будут отсутствовать (созданные после последнего нажатия кнопки **Применить**), а удаленные - присутствовать (если после удаления вы не нажали кнопку **Применить**).

Групповые и глобальные правила

Вы можете установить правила как для целой группы (групповые правила), так и для всех компьютеров (глобальные правила). Для установки правил группы выделите группу и нажмите кнопку **Установить правила**. Откроется окно с названием группы, в котором вы сможете установить правила безопасности, правила переадресации и правила шейпера (рис. 9.7). Групповые правила брандмауэра устанавливаются аналогично установке обычных правил, что уже было продемонстрировано в этом Руководстве ранее (раздел 6).

Для установки глобальных правил, щелкните на узле **Все** и нажмите кнопку **Установить правила**. Откроется окно установки глобальных правил, в котором вы сможете установить правила, распространяющиеся на все брандмауэры Киберсейф Межсетевой экран в сети (рис. 9.8).

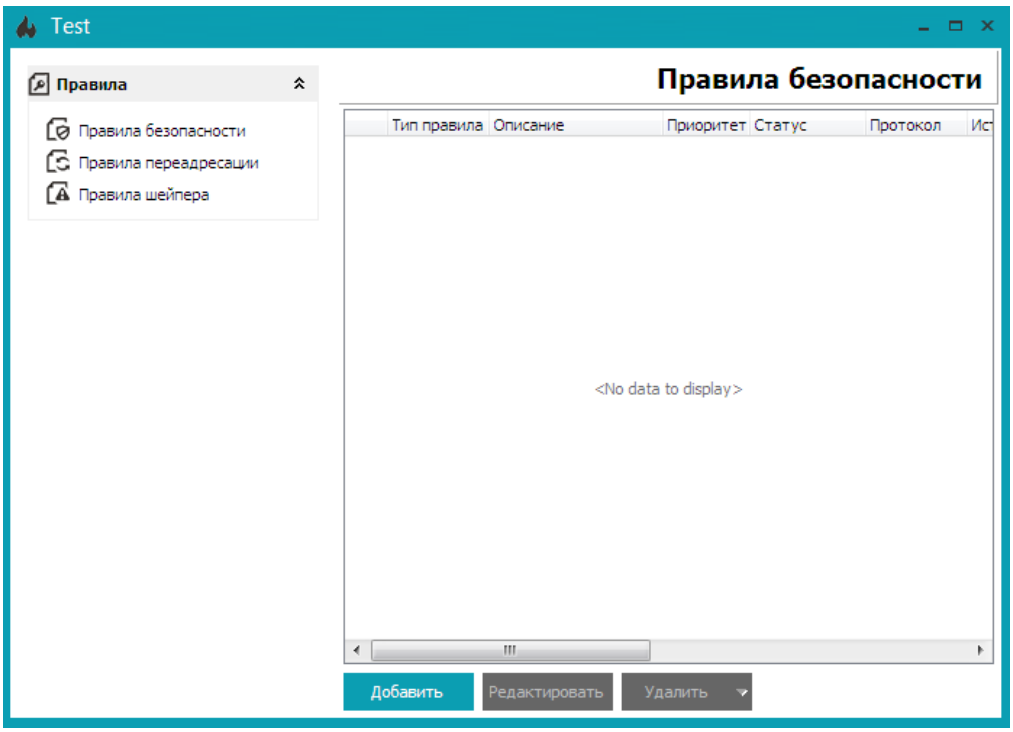

Рис. 9.7. Установка групповых (для группы Test) правил брандмауэра

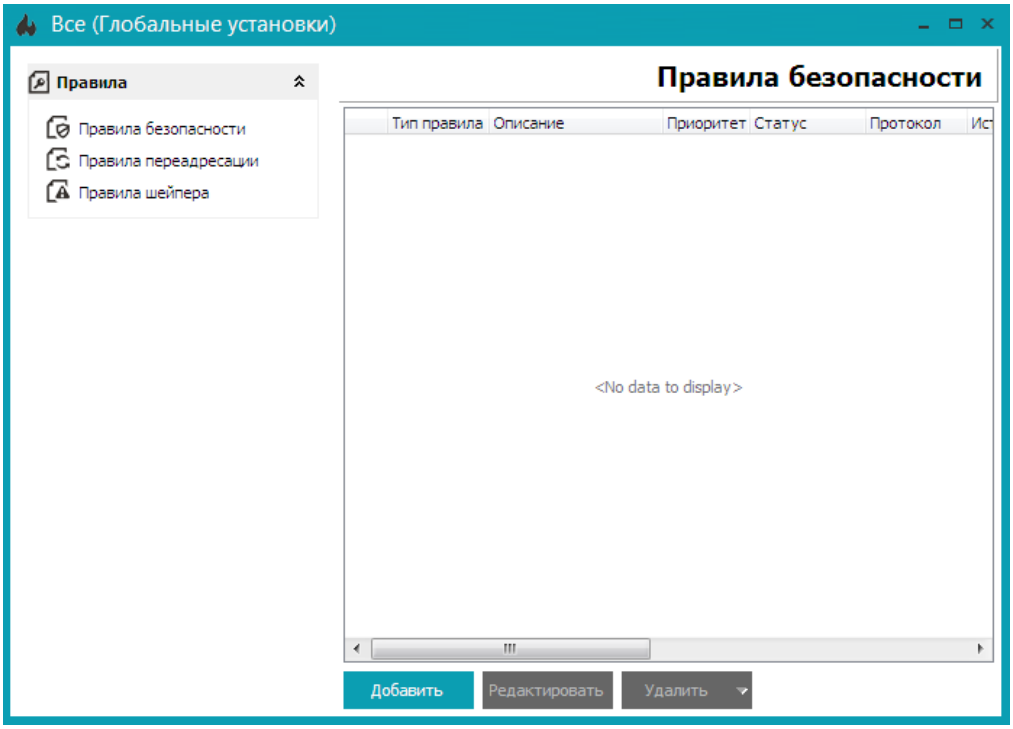

Рис. 9.8. Установка глобальных правил брандмауэра

Удаленное управление файрволом

Чтобы удаленно настроить какой-то отдельный брандмауэр (на котором работает программа Киберсейф Межсетевой экран и при условии, что она настроена правильно), выделите его название и нажмите **кнопку Удаленное соединение**. В появившемся окне нужно будет ввести имя пользователя программы Киберсейф Межсетевой экран, которое зарегистрировано на

удаленном компьютере (рис. 9.9).

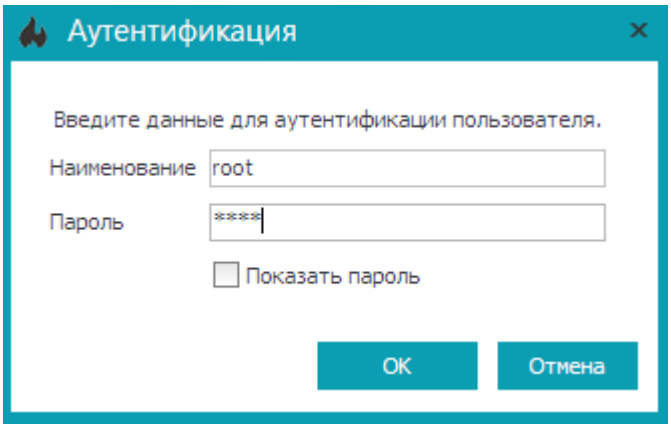

Рис. 9.9. Аутентификация на удаленном компьютере

Далее откроется окно удаленного управления брандмауэром. Обратите внимание на заголовок окна: в нем отображается, каким компьютером вы управляете, и под каким пользователем зарегистрировались (рис. 9.10).

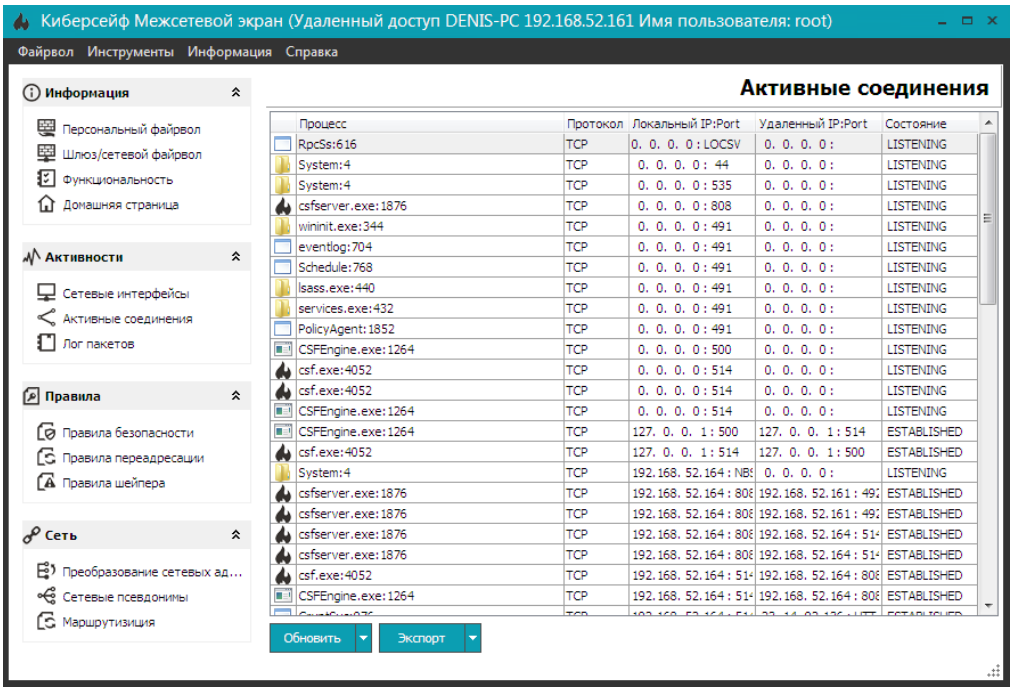

Рис. 9.10. Удаленная настройка определенного брандмауэра

Также обратите ваше внимание на функцию удаленной активации правил, описанную в разделе 6.

Блокирование сайтов

Довольно часто возникает необходимость закрытия доступа сотрудникам предприятия к определенным сайтам, например, к сайтам социальных сетей. Решить данную задачу можно путем настройки запрещающих правил, но чтобы облегчить работу администратора в продукте Киберсейф Межсетевой экран предусмотрен более удобный способ, подразумевающий, что

администратору не нужно будет создавать никакие правила, а лишь ввести адреса запрещенных сайтов.

Для редактирования запрещенных сайтов нужно перейти в раздел Интернет-сайты окна редактирования глобальных/групповых правил (рис. 9.11).

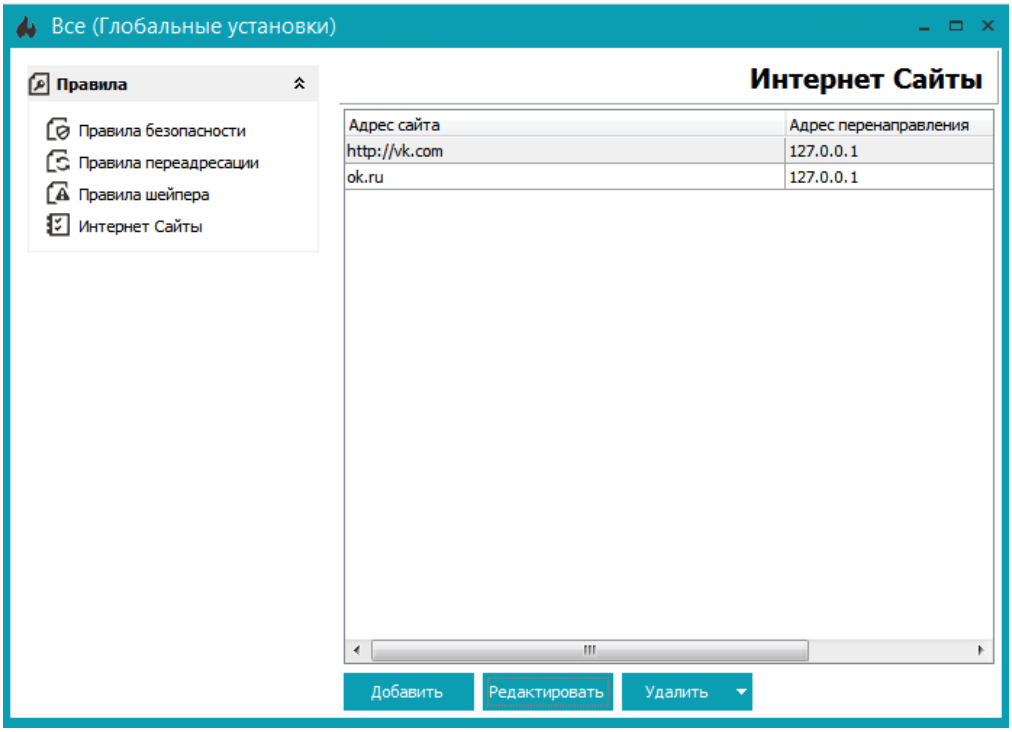

Рис. 9.11. Список блокируемых сайтов

Для блокирования сайта нужно нажать кнопку Добавить. В появившемся окне нужно ввести адрес сайта (можно без http, например, просто ok.ru) и IP-адрес перенаправления – куда будет перенаправлен пользователь при попытке открыть сайт. Для простого блокирования можно перенаправить пользователей на 127.0.0.1, но при желании можно перенаправлять пользователей на IP-адрес корпоративного веб-сервера.

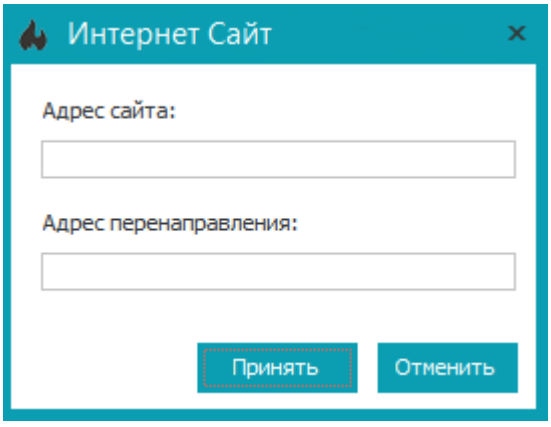

Рис. 9.12. Ввод адреса блокируемого сайта и IP-адреса перенаправления

10 Примеры и лучшая практика

В данном разделе рассмотрены некоторые полезные примеры использования программы.

В этом разделе

Глобальная блокировка доступа к узлу Интернета по IP-адресу 71
Локальная блокировка доступа к узлу Интернета по URL 72
Запрещаем ICQ 72
Сервер шлюза 73
Запрет доступа к ресурсам Интернета только определенным узлам 74
Разграничение в ИСПД 75
Ограничение скорости для определенной группы 79
Третий уровень невидимости на сервере 80
Переадресация RDP 80

Глобальная блокировка доступа к узлу Интернета по IP-адресу

Для блокирования доступа к определенному узлу Интернета по его IP-адресу, выполните следующие действия:

1. Войдите в программу, как администратор.
2. Выполните команду меню **Файрвол, Панель администрирования**.
3. Выберите группу **Все** и нажмите кнопку **Установить правила**
4. Перейдите в раздел окна **Правила, Правила безопасности**
5. Нажмите кнопку **Добавить**
6. На вкладке **Общие** введите название правила, например, "Блокирование доступа к ресурсу <название ресурса>"
7. Остальные параметры на вкладке **Общие** оставьте по умолчанию, убедившись, что выбран тип правила **Запретить пакеты**.
8. На вкладке **Источник** установите переключатель **Диапазон** и введите IP-адрес ресурса в поля **От** и **До** - для блокирования исходящих от этого узла пакетов.
9. На вкладке **Получатель** установите переключатель **Диапазон** и введите IP-адрес ресурса в поля **От** и **До** - чтобы локальный компьютер не смог подключиться к блокируемому узлу.
10. Нажмите кнопку **ОК**.
11. Найдите правило в таблице правил, щелкните по нему правой кнопкой мыши и выберите команду **Включить**.

Примечание. Для блокировки узла по URL в шагах 8 и 9 нужно выбрать переключатель URL и ввести адрес сайта, например, www.example.com.

Локальная блокировка доступа к узлу Интернета по URL

Для блокировки доступа к узлу Интернета по его URL выполните следующие действия:

- Перейдите в раздел программы **Правила, Правила безопасности;**
- Нажмите кнопку **Добавить**;
- На вкладке **Общие** введите название правила, например, "Блокирование доступа к сайту <сайт>";
- Остальные параметры на вкладке **Общие** оставьте по умолчанию, убедившись, что выбран тип правила **Запретить пакеты**;
- На вкладке **Получатель** установите переключатель **URL** и введите адрес сайта, например, www.example.com;
- Нажмите кнопку **ОК**;
- Найдите правило в таблице правил, щелкните по нему правой кнопкой мыши и выберите команду **Включить**.

Некоторые большие сайты заблокировать таким образом не получится, поскольку они расположены на нескольких серверах, у каждого из которых есть свой IP-адрес. Нужно заблокировать все IP-адреса ресурса. Но сначала их нужно узнать. Для этого можно воспользоваться какой-либо утилитой разрешения доменного имени или же сайтом http://2ip.ru/lookup/, который сообщит все IP-адреса сайта, доступ к которому нужно заблокировать. После этого создайте правила, которое блокирует все IP-адреса сайта. Если IP-адреса сайта выделены по порядку, можно блокировать диапазон IP-адресов, например, от 192.168.1.100 до 192.168.1.105 (в Руководстве специально используются локальные IP-адреса, чтобы не было претензий со стороны владельца IP-адреса).

Запрещаем ICQ

В корпоративной среде часто есть потребность запретить все, что не относится к производственным нуждам. В качестве примера рассмотрим, как можно заблокировать ICQ. Данный мессенджер использует TCP-порт 5190, который и нужно заблокировать. После этого любой ICQ-клиент не сможет подключиться к сети.

Для блокировки ICQ выполните следующие действия:

Войдите в программу, как администратор.

1. Выполните команду меню **Файрвол, Панель администрирования**;
2. Выберите группу **Все** и нажмите кнопку **Установить правила**;
3. Перейдите в раздел окна **Правила, Правила безопасности**;
4. Нажмите кнопку **Добавить**;
5. На вкладке **Общие** введите название правила, например, "Блокирование ICQ";
6. На вкладке **Общие** выберите протокол TCP (параметр **Выбор из списка**, значение TCP);
7. На вкладках **Источник** и **Получатель** в области **Порт** установите переключатель **Диапазон** и в поля **От** и **До** введите значение 5190;
8. Нажмите кнопку **ОК**;
9. Найдите правило в таблице правил, щелкните по нему правой кнопкой мыши и выберите команду **Включить**.

Для работы этого примера нужно установить уровень безопасности 3, то есть безопасность на основе IP-адресов, портов и протоколов.

Сервер шлюза

Чтобы превратить компьютер, на котором установлена программа Киберсейф Межсетевой экран в шлюз, выполните следующие действия:

1. Выполните команду **Инструменты, Настройки**;
2. На вкладке **Общие** включите переключатели **Запускать Файрвол** при загрузке системы и **Скрывать Консоль управления при загрузке программы**;
3. На вкладке **Дополнительно** включите переключатель **Включить маршрутизацию в Windows**;
4. Нажмите кнопку **Применить** и перейдите в раздел **Сеть**, **Преобразование сетевых адресов**;
5. Из списка вверху (**Назначение интерфейса интернет-провайдера**) выберите сетевой интерфейс к провайдеру;
6. В списке внизу выберите локальный сетевой интерфейс, по которому Интернет будет "раздаваться" в локальную сеть;
7. Нажмите кнопку **Старт NAT**;
8. Настройте ваш DHCP-сервер так, чтобы компьютер, на котором

запущена программа Киберсейф Межсетевой экран в режиме NAT, использовался как шлюз по умолчанию или же пропишите IP-адрес этого компьютера в качестве шлюза по умолчанию на каждом компьютере вашей локальной сети.

Запрет доступа к ресурсам Интернета только определенным узлам

Некоторым отделам на предприятии иногда нужно запретить просмотр веб-сайтов. Задача очень упрощается, если IP-адреса выделяются последовательно, например, 192.168.1.1 - 192.168.1.10 для IT-отдела, 192.168.1.11 - 192.168.1.20 - для бухгалтерии и т.д.

Выполните следующие действия:

1. Перейдите в раздел программы **Сеть, Сетевые псевдонимы**;
2. Нажмите кнопку **Добавить** и в появившемся окне введите название отдела, например, Бухгалтерия, установите переключатель **Диапазон** и в поля **От** и **До** введите начальный и конечный IP-адреса диапазона;
3. Нажмите кнопку **ОК**;
4. Перейдите в раздел программы **Правила, Правила безопасности**;
5. Нажмите кнопку **Добавить**;
6. На вкладке **Общие** введите название правила, например, "Блокирование HTTP для бухгалтерии";
7. Остальные параметры на вкладке **Общие** оставьте по умолчанию, убедившись, что выбран тип правила **Запретить пакеты**;
8. На вкладке **Источник** установите переключатель **Псевдоним** и выберите только что созданный псевдоним;
9. В области **Порт** установите переключатель в **Диапазон** и введите в поля **От** и **До** значение 80;
10. Нажмите кнопку **ОК**;
11. Найдите правило в таблице правил, щелкните по нему правой кнопкой мыши и выберите команду **Включить**;
12. Повторите действия 5-11 для порта 443 для блокирования протокола HTTPS;.
13. Повторите действия 1-12 для других подразделений компании.

Предостережение. В качестве побочного эффекта вы также можете заблокировать программу Skype, которая также использует порты 80 и 443.

В этом примере мы отключили подключение к портам 80 и 443, то есть запретили протоколы HTTP и HTTPS соответственно. Однако пользователи смогут использовать другие службы Интернета, например, электронную почту, поскольку мы не блокировали порты 25, 110 и некоторые другие, необходимые для работы почты.

Примечание. Все описанные в этом разделе правила нужно добавлять или на шлюзе или же установить их, как глобальные правила для всего предприятия, но правильнее их добавить на шлюзе.

Разграничение в ИСПД

Этот пример демонстрирует разграничение доступа в информационных системах персональных данных. Вот как можно ограничить доступ одной группы компьютеров к другой:

1. Войдите в программу, как администратор;
2. Выполните команду меню **Файрвол, Панель администрирования**;
3. Создайте группы и поместите в них компьютеры. В окне панели администрирования будут отображены все компьютеры, на которых установлена программа Киберсейф Межсетевой экран. Представим, что вы создали группы **ИСПДн №1** и **Рабочие станции**. Вам нужно запретить доступ компьютеров из группы **ИСПДн №1** к группе **Рабочие станции** (рис. 10.1);
4. Выберите группу **ИСПДн №1** и нажмите кнопку **Установить правила**;
5. Перейдите в раздел **Правила безопасности** и нажмите кнопку **Добавить** (рис. 10.2);
6. На вкладке **Общие** добавьте описание правила "Запрет подключения ИСПДн №1 к группе Рабочие станции" (рис. 10.3);
7. Установите тип правила **Запретить пакеты**;
8. На вкладке **Источник** установите переключатель **Псевдоним** и выберите название группы - **ИСПДн №1** (рис. 10.4);
9. На вкладке **Получатель** установите переключатель **Псевдоним** и

выберите название другой группы **- Рабочие станции** (рис. 10.5);

10. Нажмите кнопку **ОК**;
11. Найдите правило в таблице правил, щелкните по нему правой кнопкой мыши и выберите команду **Включить** (рис. 10.6);
12. Закройте окно редактирования правил безопасности;
13. В окне **Панель администрирования** нажмите кнопку **Применить**.

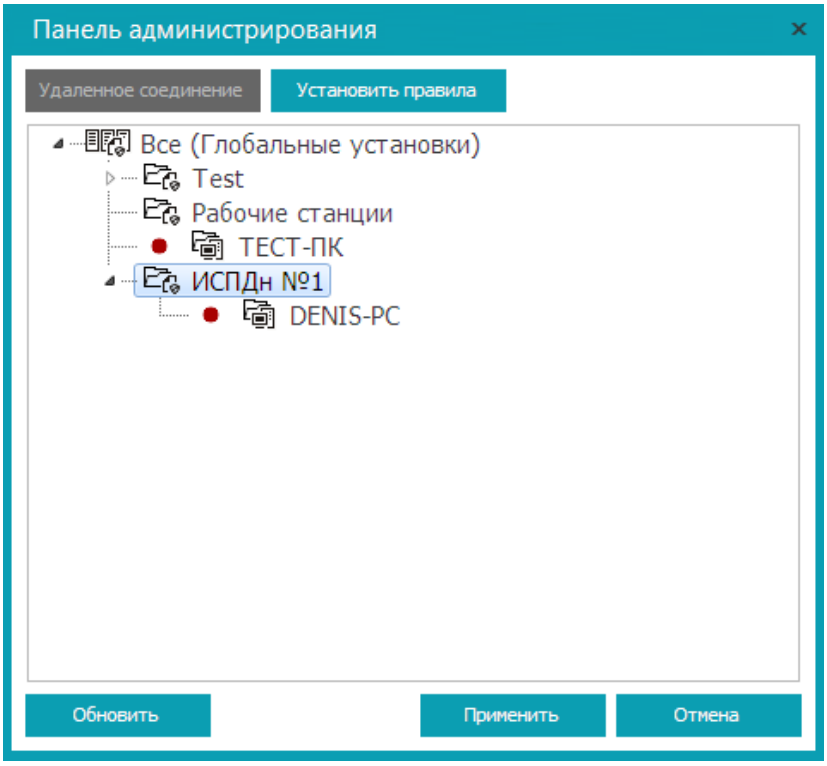

Рис. 10.1. Созданные группы

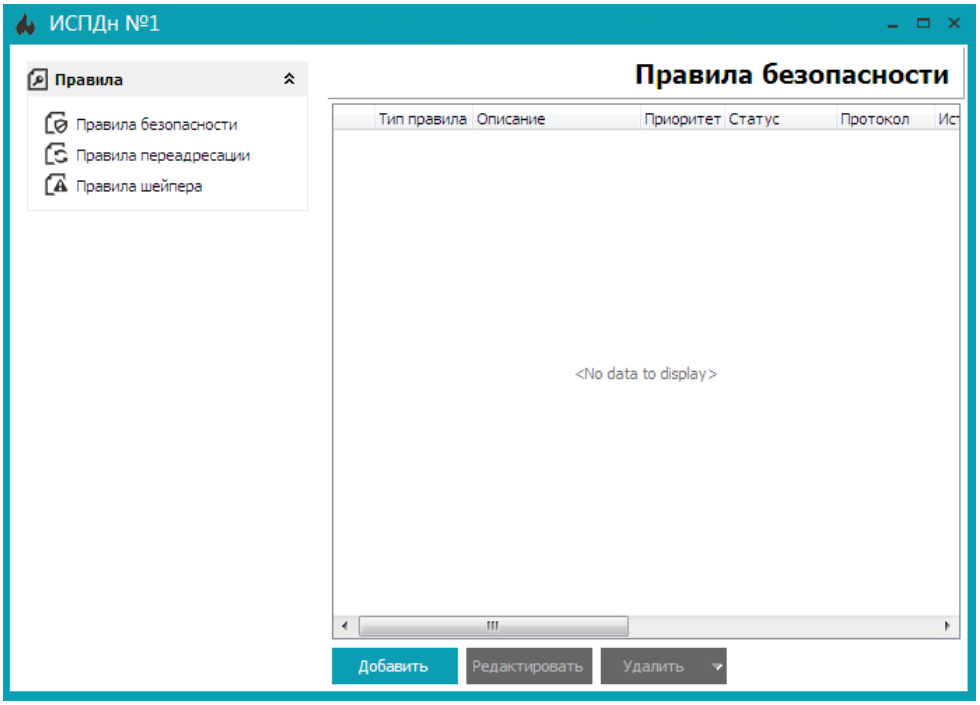

Рис. 10.2. Правила безопасности для группы ИСПДн №1

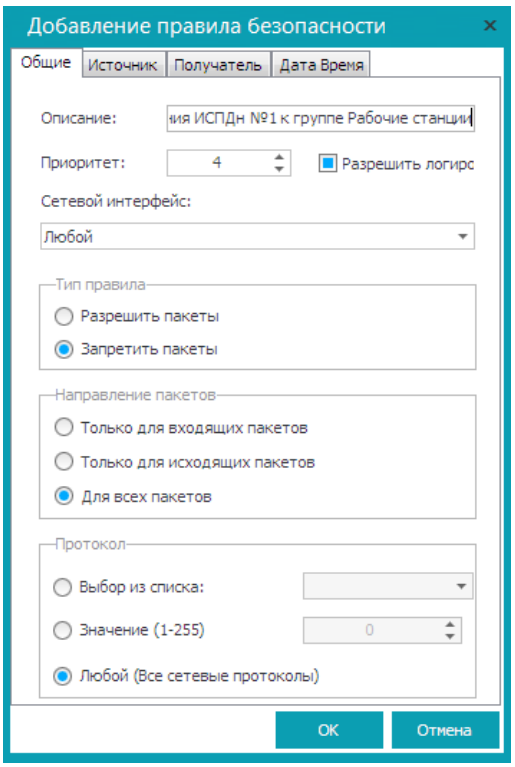

Рис. 10.3. Вкладка **Общие**

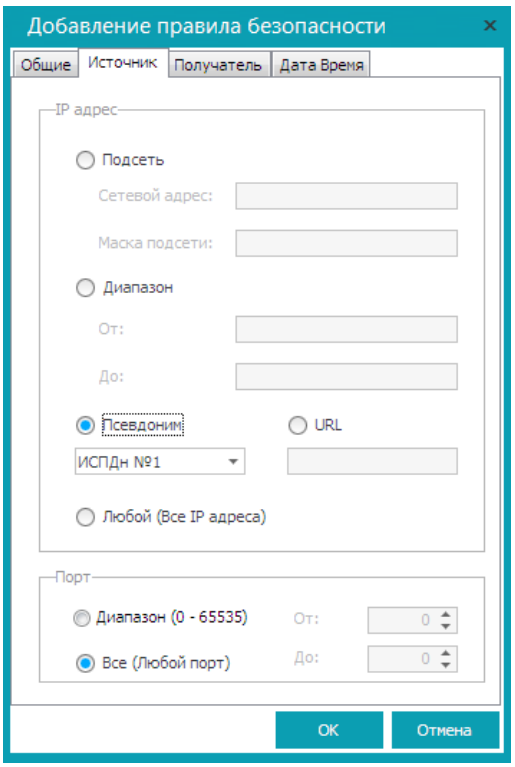

Рис. 10.4. Определяем источник

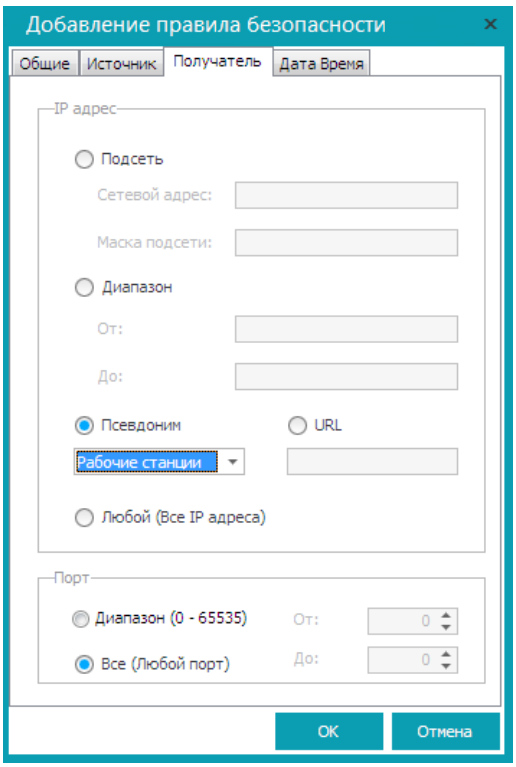

Рис. 10.5. Определяем получателя

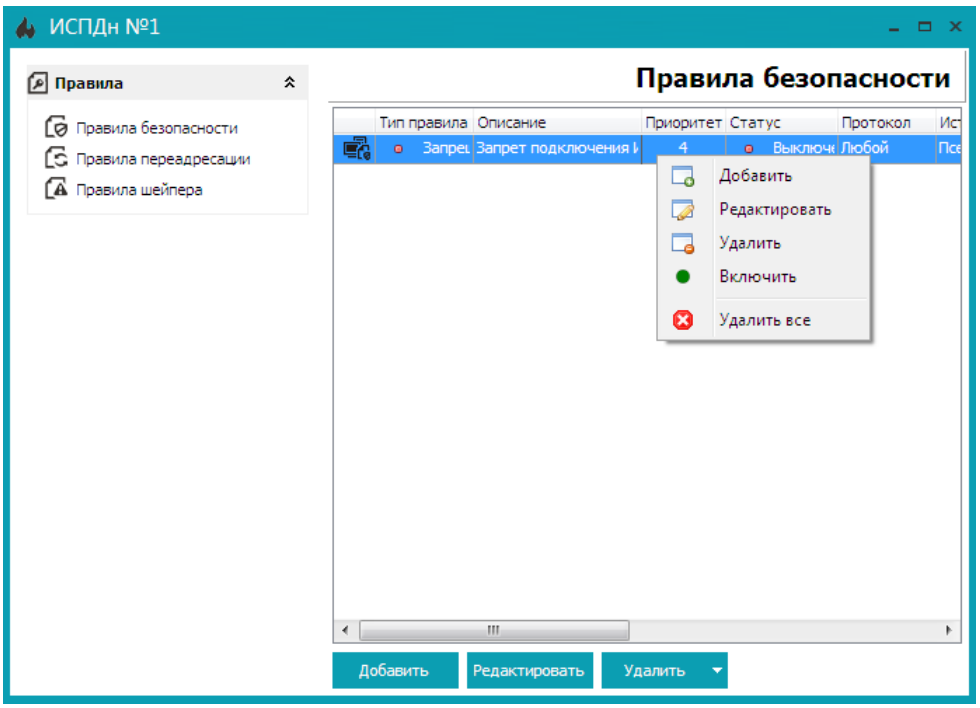

Рис. 10.6. Включаем правила

Созданное нами правило далее на машинах трансформируется в набор правил с конкретными IP-адресами, причем при изменении состава групп или их адресов эти правила автоматически обновляются сервером на клиентах.

Аналогично, вы можете создать и другие группы и установить подобные правила ограничения доступа.

Ограничение скорости для определенной группы

Далее будет показан пример ограничения скорости для определенной группы компьютеров. Представим, что есть группа Test, которая используется только для тестирования программного обеспечения, и компьютерам этой группы нужно ограничить скорость доступа к сети, чтобы эти компьютеры не могли никак повлиять на другие компьютеры.

Необходимые действия:

1. Войдите в программу, как администратор;
2. Выполните команду меню **Файрвол, Панель администрирования**;
3. Выберите группу **Test** и нажмите кнопку **Установить правила**;
4. Перейдите в раздел **Правила шейпера** и нажмите кнопку **Добавить**;
5. На вкладке **Общие** введите описание правила "Ограничение upload для Test";
6. Установите общее и пиковое значения скорости;
7. Перейдите на вкладку **Источник** и выберите переключатель **Псевдоним**, из списка выберите группу **Test**;
8. На вкладке **Получатель** оставьте все как есть (любой получатель, любой порт), нажмите кнопку **ОК**;
9. Щелкните по только что созданному правилу правой кнопкой мыши и выберите команду **Включить**;
10. Снова нажмите кнопку **Добавить**;
11. На вкладке **Общие** введите описание правила "Ограничение download для Test" и установите общее и пиковое значения скорости;
12. На вкладке **Источник** оставьте все, как есть (любой источник, любой порт), а на вкладке **Получатель** установите переключатель **Псевдоним** и выберите из списка группу **Test**;
13. Нажмите кнопку **ОК**;
14. Выделите созданное правило, щелкните по нему правой кнопкой мыши и выберите команду **Включить**;
15. Закройте окно редактора группового правила;

16. Нажмите кнопку **Применить** в окне панели администрирования.

Третий уровень невидимости на сервере

На сервере рекомендуется использовать третий уровень невидимости. Сетевой интерфейс работает по принципу контроля входящих пакетов и проверяет, чтобы адрес, протокол и порт входящего пакета соответствовали вашему запросу. Любой входящий пакет, который не соответствует вашему запросу, будет блокирован. В результате большинство пакетов будет заблокировано, что обеспечит наивысшую степень защиты сервера.

На рис. 10.7 показано, что большинство пакетов на третьем уровне невидимости будут заблокированы.

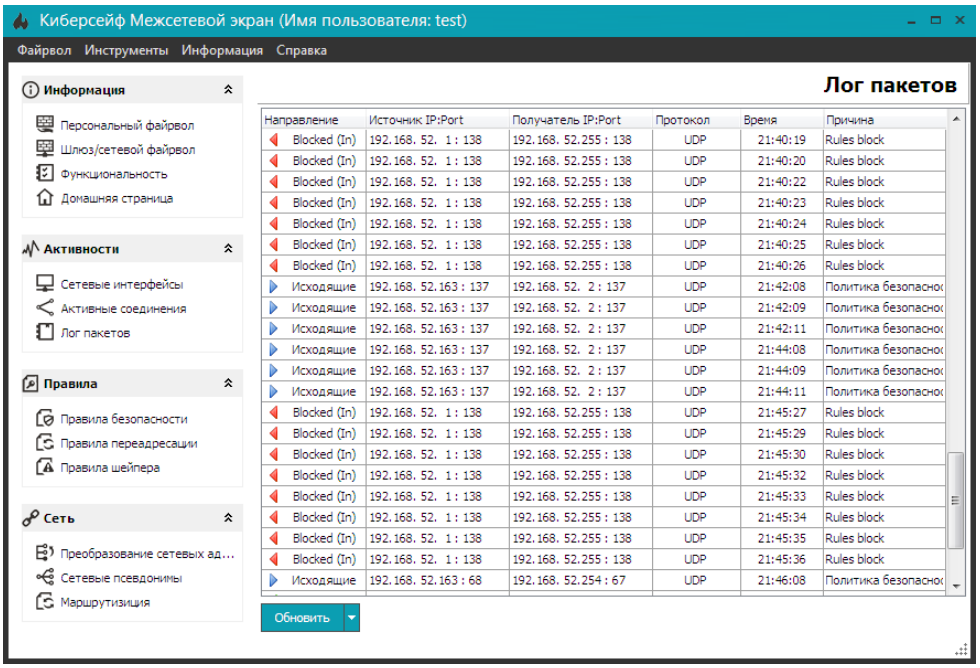

Рис. 10.7. Лог пакетов на сервере

Подробно уровни безопасности уже были рассмотрены в разделе 4.

Переадресация RDP

В этом примере рассматривается переадресация RDP. Представим, что у нас есть следующая конфигурация сети: на машине с IP-адресом 192.168.1.15 есть два сетевых интерфейса. Один из них - это соединение с провайдером Интернета, а второй, 192.168.2.1, подключен к WiFi-роутеру, который "раздает" беспроводную сеть на ноутбуки внутри офиса.

Получается, что у нас есть две подсети - компьютеры, которые подключаются Ethernet-кабелем, находятся в одной подсети, а ноутбуки (которые подключаются по WiFi) - в другой подсети. IP-адрес WiFi-роутера - 192.168.2.2.

Задача следующая: при подключении с ноутбука к реальному IP нашего офиса 91.224.205.158 перенаправить RDP на компьютер 192.168.1.91 (без перенаправления произойдет подключение к рабочему столу сервера 91.224.205.158/192.168.1.222).

Первым делом нужно настроить NAT. На рис. 10.8 представлена конфигурация NAT для нашей задачи.

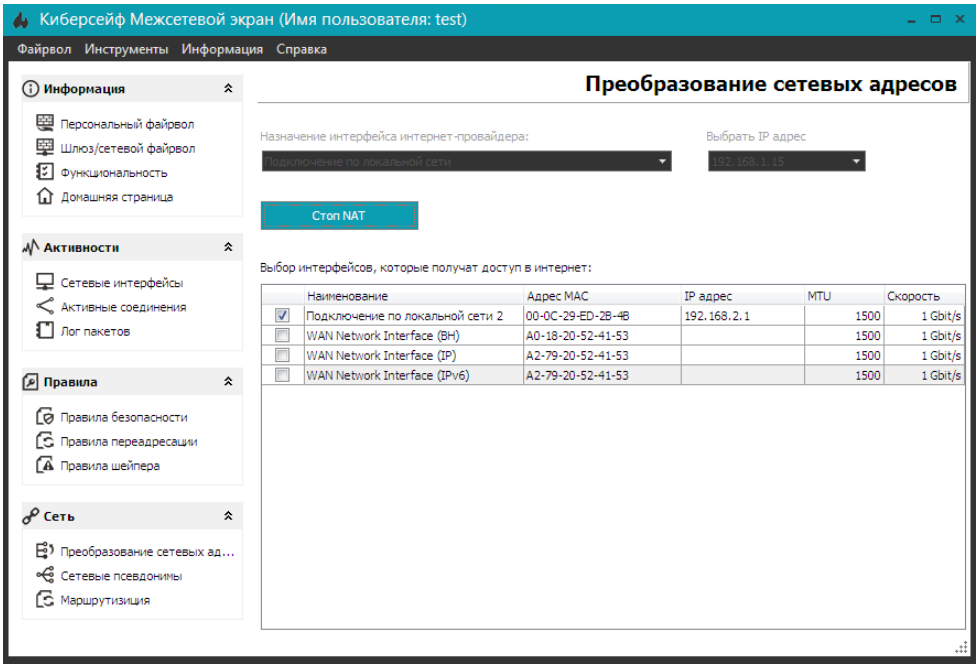

Рис. 10.8. Конфигурация NAT

Затем нужно создать правило переадресации RDP. Перейдите в раздел **Правила, Правила переадресации** и нажмите кнопку **Добавить**. На вкладке **Общие** введите описание правила "RDP", обязательно выберите правильный сетевой интерфейс ("смотрящий" в локальную сеть), укажите IP-адрес, на который нужно перенаправить RDP (192.168.1.91) и порт 3389 (используется RDP). Также обязательно укажите протокол TCP.

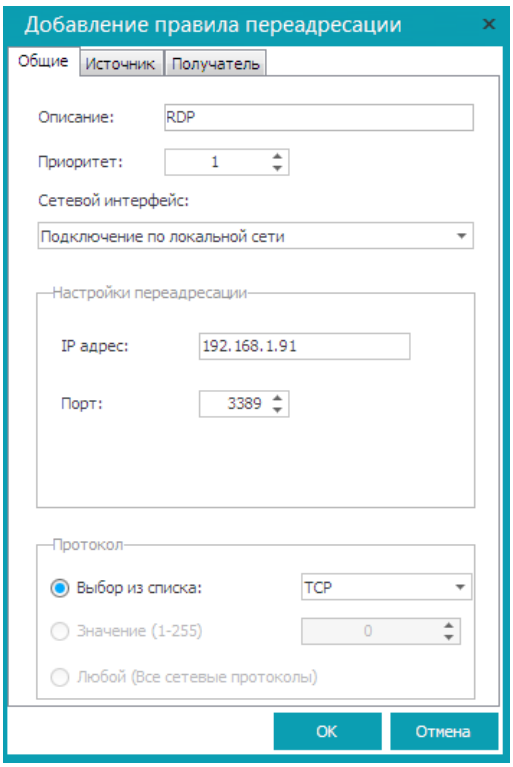

Рис. 10.9. Общие параметры правила переадресации

Параметры на вкладках **Источник** и **Получатель** заполните в соответствии с решаемой задачей (рис. 10.10 и 10.11).

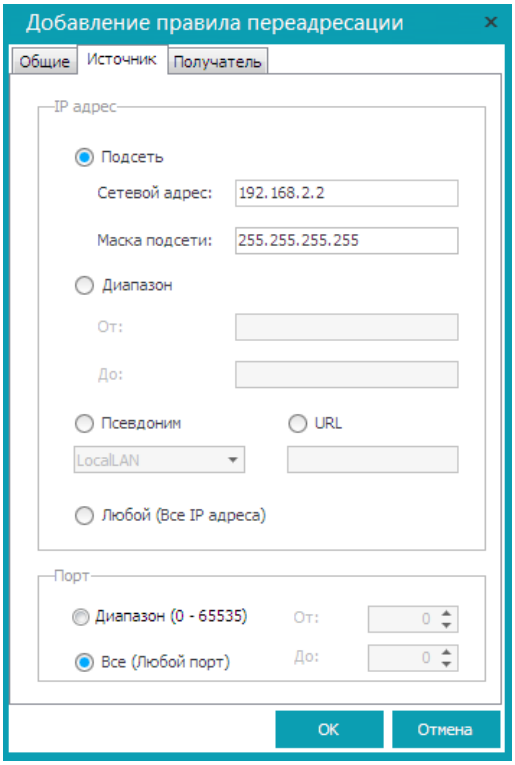

Рис. 10.10. Параметры источника (192.168.2.2 - это WiFi-роутер)

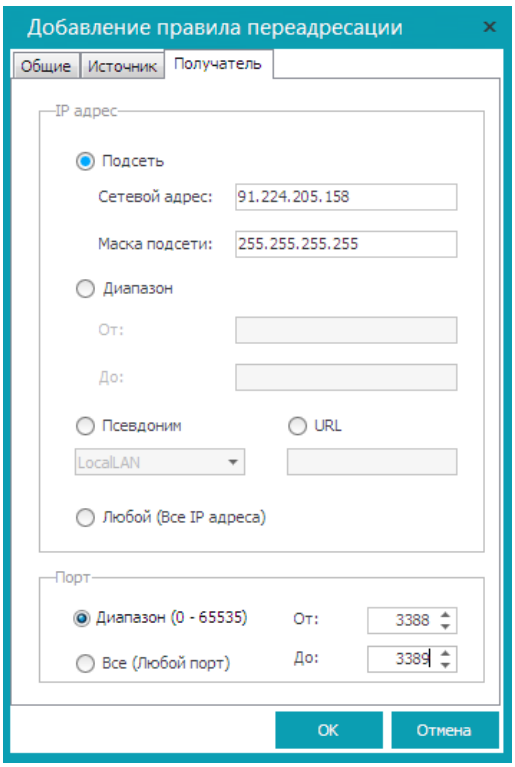

Рис. 10.11. Параметры получателя

Нажмите кнопку **OK** и включите созданное правило. После этого у вас в сети будет работать переадресация RDP.