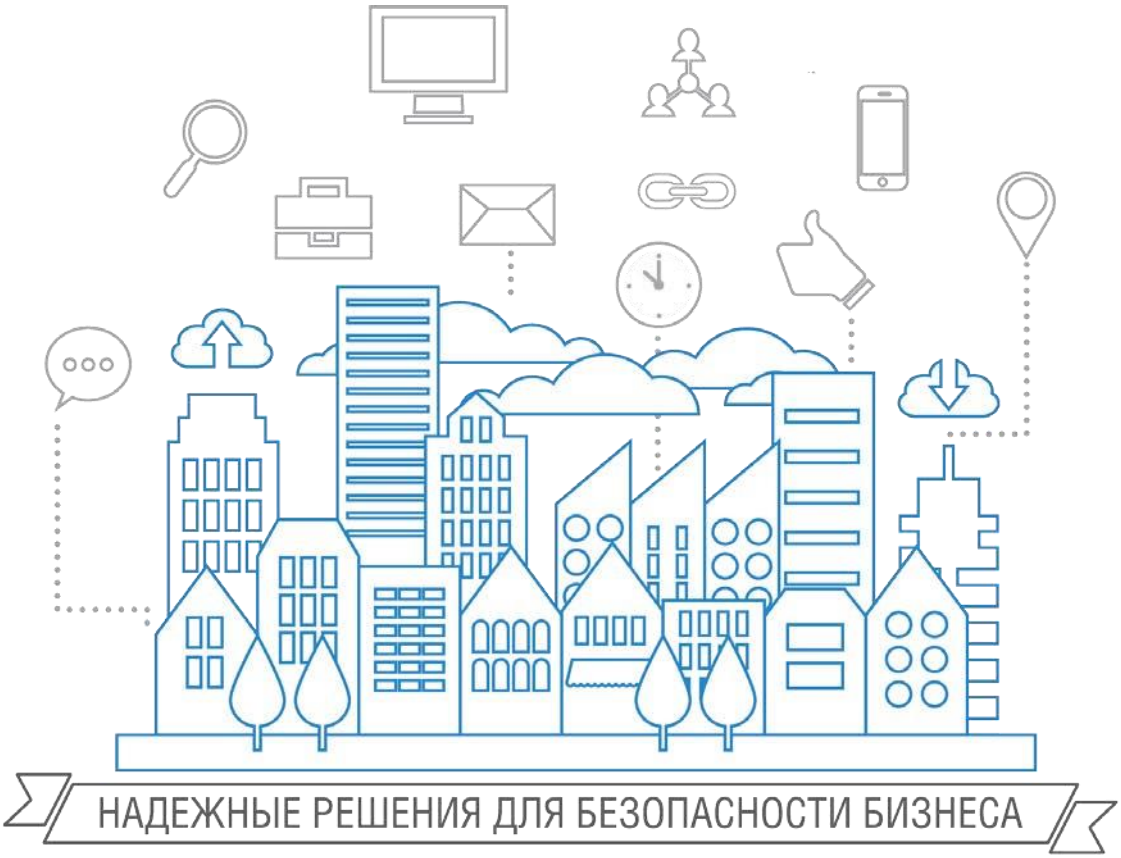
ГАЗИНФОРМСЕРВИС

198096, г. Санкт-Петербург, ул. Кронштадтская, д.10, лит. А, тел.: (812) 677-20-50, факс: (812) 677-20-51 Почтовый адрес: 198096, г.Санкт-Петербург, а/я 59, e-mail: resp@gaz-is.ru, www.gaz-is.ru
р/с 40702810800000001703 Ф-л Банка ГПБ (АО) в г. Санкт -Пет ербу рге БИК 044030827,
к/с 30101810200000000827, ОКПО 72410666, ОГРН 1047833006099, ИНН/КПП 7838017968/783450001

Средство защиты информации от несанкционированного доступа «Блокхост-сеть 2.0»

Руководство администратора
Межсетевой экран



Санкт-Петербург, 2018

Аннотация

Настоящее руководство предназначено для администраторов средства защиты информации от несанкционированного доступа «Блокхост-сеть 2.0» (далее по тексту – СЗИ «Блокхост-сеть 2.0») и содержит описание работы с персональным межсетевым экраном далее по тексту – персональным МЭ), входящим в состав СЗИ «Блокхост-сеть 2.0».

Знаки, расположенные на полях руководства, указывают на примечания. Степени важности примечаний:

 Важная информация, информация предостерегающего характера.

 Дополнительная информация, примеры.

Содержание

1. Общие положения

Персональный межсетевой экран в составе СЗИ реализует защиту ПК, функционирующего автономно или подключенного к ЛВС, от НСД к его ресурсам из внешних источников, разграничение доступа пользователя ПК к ресурсам сети и фильтрацию сетевого трафика.

Персональный межсетевой экран входит в состав автономного и с удаленным управлением вариантов поставки СЗИ «Блокхост-сеть 2.0», устанавливается и функционирует совместно с СЗИ. Настройка функций защиты МЭ осуществляется администратором безопасности с использованием графического интерфейса СЗИ «Блокхост-сеть 2.0».

Состав файлов персонального МЭ приведен в таблице 1.1.

Таблица 1.1. Состав файлов персонального МЭ для ОС Windows

№ п.п.	Наименование файла	Назначение файла
1	DIFxAPI.dll	Библиотека, реализующая функционал по установке драйверов модулей безопасности СЗИ
2	DIFxCmd.exe	Процесс командной строки для установки драйверов модулей безопасности СЗИ
3	DrvFltIP.sys	Драйвер персонального МЭ
4	DrvFltIP.inf	Файл конфигурации для установки драйвера
5	DrvFltIP.cat	Файл с контрольными суммами, подписанный сертификатом
6	gis_publisher.cer	Сертификат издателя для проверки подписи
7	gis_publisher.sha1.cer	Сертификат издателя для проверки подписи МЭ по алгоритму SHA1RSA
8	reg_driver.bat	Командный файл установки (удаления) МЭ в системе в процессе инсталляции СЗИ

2. Описание контролируемых функций

Функции защиты информации от НСД персонального МЭ соответствуют четвертому классу защищенности согласно РД «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997).

В персональном МЭ реализованы следующие функциональные возможности:

- фильтрация пакетов на сетевом уровне на основе 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 средства проверки подлинности сетевых адресов;
- фильтрация с учетом любых значимых полей сетевых пакетов;
- регистрация и учет фильтруемых пакетов.

Средства персонального межсетевого экрана используются для защиты информации поступающей в ПЭВМ и выходящей из нее, посредством фильтрации сетевого трафика, обеспечения безопасного подключения ПЭВМ к сетям общего пользования (в том числе Интернет) и разграничение доступа к сетевым ресурсам ПЭВМ (сетевым дискам, сетевым принтерам и др.).

3. Руководство по настройке и конфигурированию персонального МЭ

3.1 Понятие профиля персонального МЭ. Описание настроек профиля

Для перехода к настройке персонального МЭ администратору безопасности в консоли администрирования СЗИ необходимо:

1. В окне **«Список машин»** консоли администрирования выбрать рабочую станцию, для которой будет производиться настройка персонального межсетевого экрана, раскрыв пункт ***Все машины***;
2. В окне **«Настройки машины»**, раскрыв пункт ***Список пользователей***, двойным щелчком выбрать пользователя, для которого будет производиться настройка, и затем выбрать пункт ***Персональный экран*** или, выделив пользователя, щелкнуть в **Основной панели настроек клиентов** по названию ***Персональный экран***. В обоих случаях в **Основной панели настроек клиентов** откроются настройки выбранного механизма:

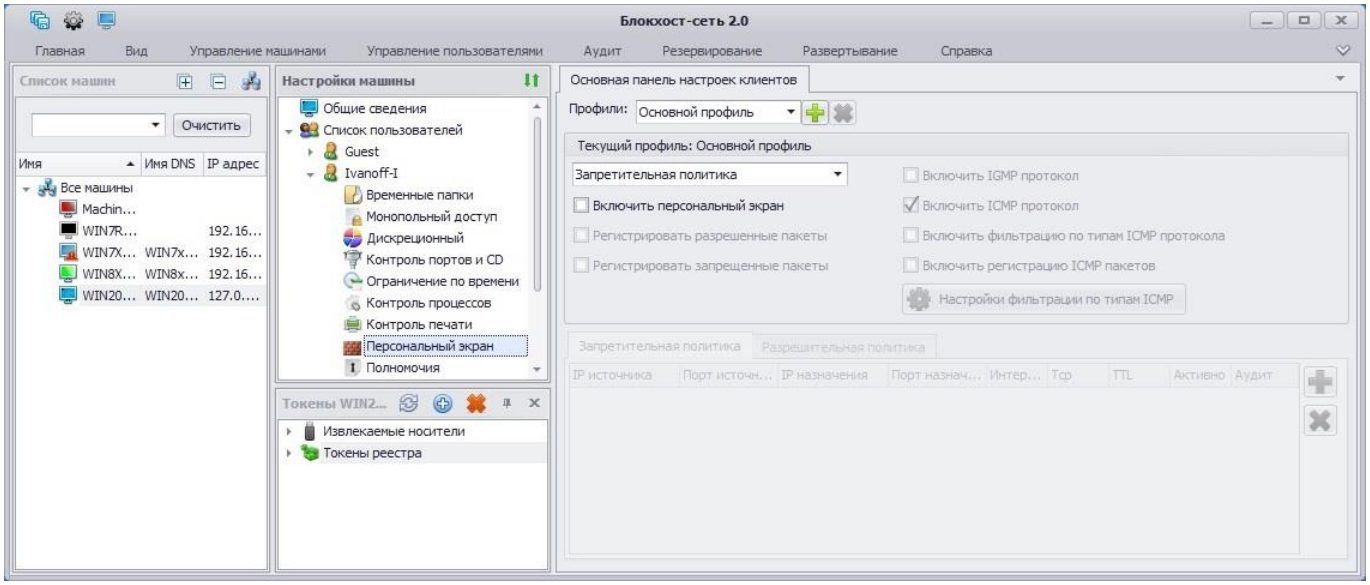


Рисунок 3.1. Настройка персонального МЭ

Настройка персонального МЭ заключается в создании одного или нескольких профилей для пользователя. Каждый профиль МЭ включает в себя *общие настройки* профиля, применяемые независимо от типа выбранной политики, *и настройки правил* фильтрации, которые обеспечивают фильтрацию сетевого трафика в зависимости от вида выбранной политики – разрешительной или запретительной.

3.1.1 Общие настройки профиля персонального МЭ

К **общим настройкам профиля** персонального МЭ относятся следующие параметры (см. пример на рис. 3.1):

- «*Наименование профиля*». Для создания нового профиля необходимо нажать кнопку добавления профиля  , в открывшемся окне **«Добавить профиль»** (рис. 3.2) ввести имя профиля и нажать кнопку ***Добавить*** (по умолчанию в системе создан пустой профиль с именем *«Основной профиль»*). Для удаления созданного профиля следует выбрать его из раскрывающегося списка и нажать кнопку

удаления профиля . Нельзя удалить единственный существующий профиль.

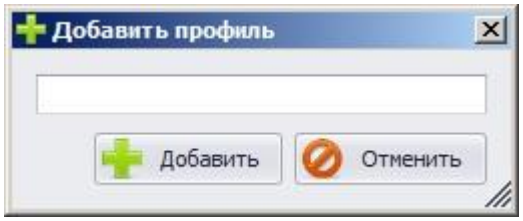


Рисунок 3.2. Окно добавления профиля персонального МЭ

- *«Политика»*. Выбранный тип политики ***Запретительная политика*** или ***Разрешительная политика*** будет распространяться только на параметры, заданные в правилах персонального МЭ (настройка правил описана в пункте 3.1.2 настоящего документа);

Разрешительная политика реализуется по принципу ***«запрещено все, что не разрешено»*** на основе создания правил доступа к сетевым ресурсам, к которым пользователю разрешен доступ, и разрешает прохождения сетевого трафика с указанными параметрами. Доступ к остальным сетевым ресурсам и прохождение сетевых пакетов, которые явно не указаны в правилах доступа, будет запрещен.

Запретительная политика реализуется по принципу ***«разрешено все, что не запрещено»*** на основе создания правил доступа к сетевым ресурсам, к которым пользователю доступ запрещен, и запрещает прохождения сетевого трафика с указанными параметрами. Доступ к остальным сетевым ресурсам и прохождение сетевых пакетов, которые явно не указаны в правилах доступа, будет разрешен.

- *«Включить персональный экран»*. Параметр предназначен для того, чтобы после входа пользователя в систему применялись созданные для него настройки профиля персонального МЭ.
- «*Регистрировать разрешенные пакеты»*. Параметр предназначен для включения регистрации всех событий, связанных с доступом пользователя к разрешенным сетевым ресурсам, а также – для регистрации разрешенного к прохождению сетевого трафика.
- *«Регистрировать запрещенные пакеты»*. Параметр предназначен для включения регистрации всех событий, связанных с доступом пользователя к неразрешенным сетевым ресурсам, а также - для регистрации запрещенного к прохождению сетевого трафика.
- *«Включить IGMP протокол»*. Параметр включает фильтрацию сетевых пакетов, передаваемых по протоколу IGMP.
- *«Включить ICMP протокол»*. Параметр включает фильтрацию сетевых пакетов, передаваемых по протоколу ICMP. После выбора этой настройки станут активными пункты ***Включить фильтрацию по типам ICMP протокола***, ***Включить регистрацию ICMP пакетов*** и кнопка ***Настройки фильтрации по типам ICMP***.
- *«Включить фильтрацию по типам ICMP протокола»*. Параметр включает фильтрацию сетевых пакетов, передаваемых по протоколу ICMP, в соответствии с настройками, заданными в окне **«Настройки ICMP»** (рис. 3.3), которое появляется при нажатии на кнопку ***Настройки фильтрации по типам ICMP***.

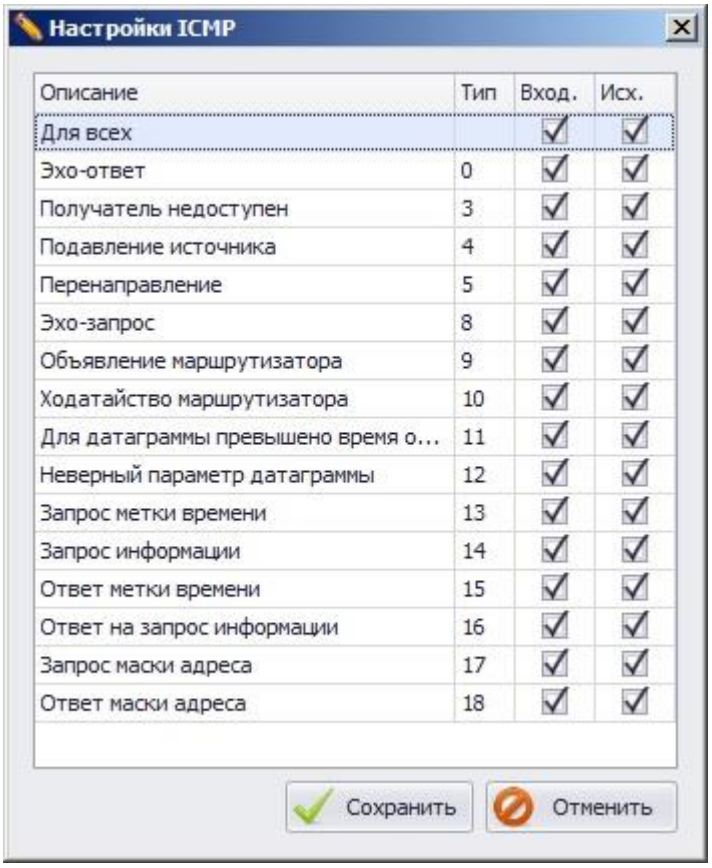


Рисунок 3.3. Настройка фильтрации по типам ICMP-протокола

- *«Включить регистрацию ICMP пакетов».* Данный параметр включает регистрацию в журнале аудита СЗИ типов фильтруемых ICMP-пакетов.

Для каждого пользователя может быть создано несколько профилей в зависимости от режимов его работы (например, в режиме работы с доступом в Internet и без доступа в Internet). Каждому профилю можно сопоставить только один тип политики – разрешительную или запретительную.

3.1.2 Настройки правил фильтрации профиля персонального МЭ

Профиль персонального МЭ может содержать одно или несколько правил фильтрации сетевого трафика. Для создания правила фильтрации необходимо:

1. Включить персональный МЭ, установив в **Основной панели настроек клиентов** параметр ***Включить персональный экран***.
2. Из выпадающего списка поля ***Профили*** выбрать редактируемый профиль или создать новый (подробнее о создании профиля МЭ см. п. 3.1.1 настоящего руководства).
3. Из выпадающего списка раздела редактируемого профиля выбрать тип политики: ***Запретительная политика*** или ***Разрешительная политика*** – в зависимости от того, какая политика будет соответствовать профилю с создаваемым правилом.
4. Установить требуемые параметры общих настроек редактируемого профиля (см. п. 3.1.1 настоящего Руководства).
5. В области создания правил фильтрации нажать кнопку ***Добавить*** .
6. В открывшемся окне **«Настройки правила»** (рис. 3.4) ввести необходимые параметры правила доступа к сетевым ресурсам и фильтрации сетевого трафика.

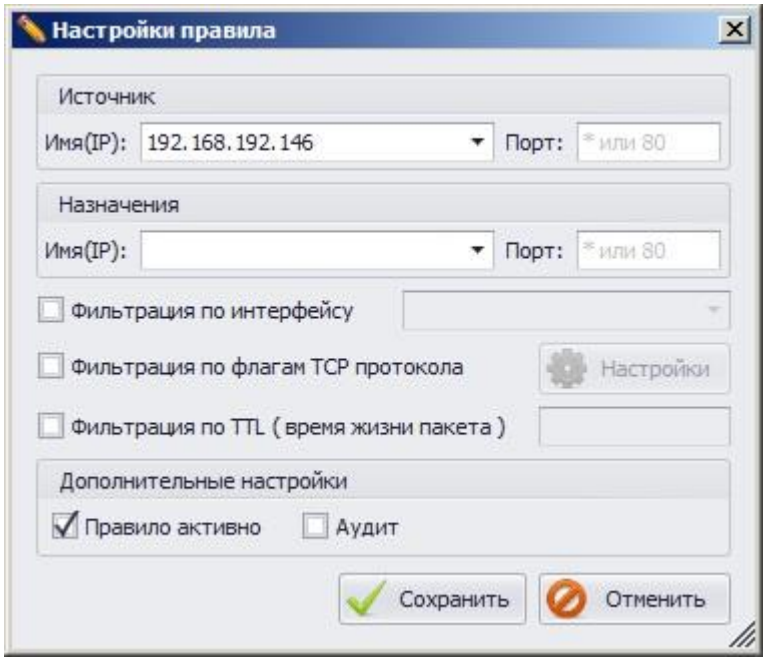


Рисунок 3.4. Добавление правила профиля персонального МЭ

Возможные настройки в окне **«Настройки правила»**:

- ***Имя (IP-адрес) и порт источника и узла назначения***. Настройка позволяет активировать фильтрацию по IP-адресу и номеру порта источника и узла назначения. Ввод символа «*» в поле ***Порт*** будет обозначать выбор всех портов.
  IP-адреса источника и узла назначения, расположенных в одной подсети, могут быть заданы также диапазоном или маской, например:
  192.168.0.1-255
  192.168.0.0/24

  При указании имен узлов фильтрации не следует использовать DNS-имена рабочих станций.

- ***Фильтрация по интерфейсу***. Настройка позволяет указать интерфейс рабочей станции, по которому должна производиться фильтрация сетевого трафика при выполнении данного правила. Применение настройки позволяет осуществлять проверку подлинности сетевых адресов.

  Данный параметр предполагает фильтрацию по IP-адресу выбранного сетевого подключения – при изменении IP-адреса сетевого адаптера (например, при использовании в локальной сети сервера DHCP) правило будет по-прежнему осуществлять фильтрацию по IP-адресу, присвоенному сетевому адаптеру в момент создания правила.

- ***Фильтрация по флагам TCP протокола***. При выборе данного параметра станет активной кнопка ***Настройки***, по нажатию которой появится окно с перечнем TCP-флагов (рис. 3.5).

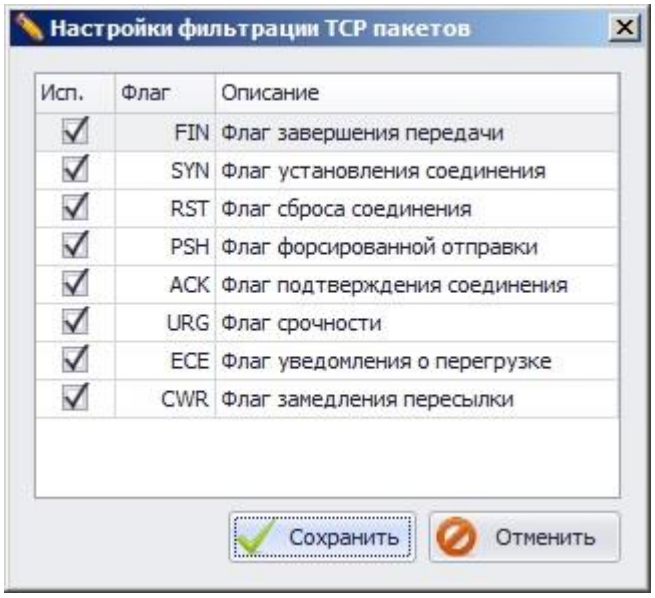


Рисунок 3.5. Настройка TCP

- ***Фильтрация по TTL (Время жизни пакета)***. Выбор данной настройки позволяет осуществлять фильтрацию пакетов по времени их жизни (TTL). Необходимо указать конкретное значение для TTL пакета, разрешенного или запрещенного к прохождению.
- *Дополнительные настройки:*
  1) ***Правило активно***. Пункт предназначен для применения (активации) сохраненных администратором настроек правила МЭ при входе пользователя в систему.
  2) ***Аудит***. При необходимости регистрации событий, относящихся к данному правилу, следует отметить этот пункт.

7. Для сохранения созданного правила следует нажать кнопку ***Сохранить*** в окне **«Настройки правила»** (рис. 3.4). В результате в области создания правил появятся два правила фильтрации (рис. 3.6) – одно созданное администратором и второе, созданное автоматически, в котором заменены между собой параметры узлов ***Источник*** и ***Назначения*** для возможности обратного прохождения сетевых пакетов через МЭ. В случае отсутствия необходимости созданное автоматически правило можно удалить или отредактировать.

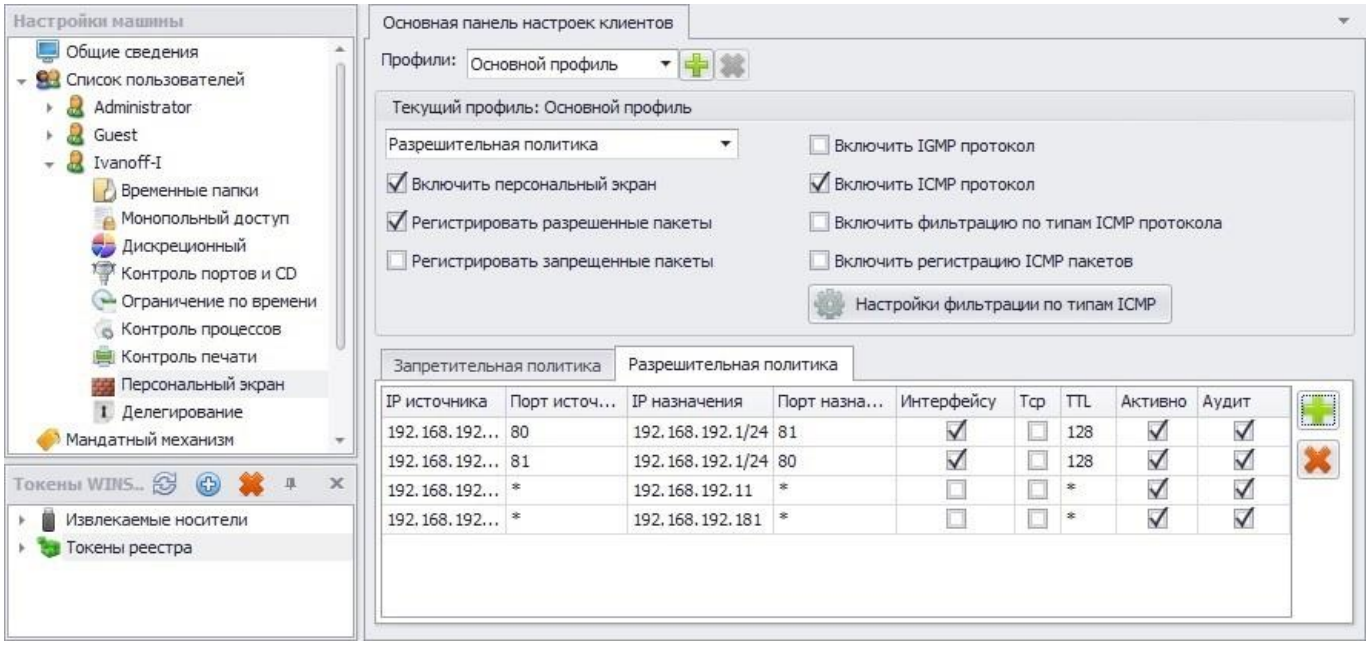


Рисунок 3.6. Созданные правила персонального МЭ

8. Для редактирования правил фильтрации необходимо два раза щелкнуть на строке с выбранным правилом. И в открывшемся окне «**Настройки правила**» можно изменить настройки, описанные в п. 6.
9. Для удаления правил из списка достаточно выбрать в области настроек требуемое правило и нажать кнопку ***Удалить*** , расположенную в области создания правил (для удаления правила можно также воспользоваться клавишей <**Del**>).
10. Сохранить произведенные настройки с помощью кнопки ***Сохранить все*** , расположенной в левом верхнем углу консоли администрирования СЗИ, или воспользоваться пунктом меню ***Главная→ Сохранить***.

Созданные правила будут разрешать или запрещать прохождение пакетов с указанными настройками в зависимости от того, какой тип политики указан – ***Разрешительная*** или ***Запретительная***.
Созданные правила разграничения доступа и фильтрации трафика активны, когда на соответствующем ПК в операционную систему (ОС) вошел пользователь, для которого они были заданы и в СЗИ в его настройках отмечен пункт ***Включить персональный экран***.
Пользователь, добавляемый в СЗИ для создания правил персонального МЭ, не должен быть встроенным администратором ОС, для учетной записи встроенного администратора настроенные правила действовать не будут.
Произведенные настройки персонального МЭ вступают в силу после перезагрузки ОС на рабочей станции с настроенным МЭ или после завершения текущего сеанса пользователя, для которого были заданы правила персонального МЭ.

3.1.3 Синтаксическая структура вводимых данных

При создании правил фильтрации персонального МЭ могут быть использованы цифры и символы «*» и «-» при указании диапазона IP-адресов или номеров портов.

3.2 Регистрация прохождения сетевого трафика

Регистрация сетевого трафика выполняется согласно установленным общим параметрам профиля персонального МЭ (см. п. 3.1.1), а также опции ***Аудит*** для каждого отдельно взятого

правила (см. п. 3.2.2).

Аудит сетевого трафика может выполняться как посредством записи соответствующих событий в журнал СЗИ «Блокхост-сеть 2.0» с помощью службы диспетчера аудита СЗИ (*GIS.Client.LogDispatcher.exe*), так и отправкой сообщений на Syslog-сервер.

3.3 Настройка правил фильтрации персонального МЭ

Рассмотрим настройку фильтрации сетевых пакетов на примере стенда, схема которого приведена на рисунке 3.7. Стенд представляет собой одну локальную вычислительную сеть (ЛВС), в которой взаимодействуют 4 (четыре) ПЭВМ. В качестве межсетевого экрана выступает ПЭВМ 1, на которой установлено СЗИ «Блокхост-сеть 2.0». Настройка персонального МЭ заключается в создании на ПЭВМ 1 для пользователя, который будет осуществлять вход в ОС, настроек фильтрации сетевого трафика в ЛВС. Созданные правила начинают действовать после входа данного пользователя в ОС.

ПЭВМ 1 имеет 3 (три) сетевые карты с параметрами сетевых интерфейсов, указанными на рисунке 3.7.

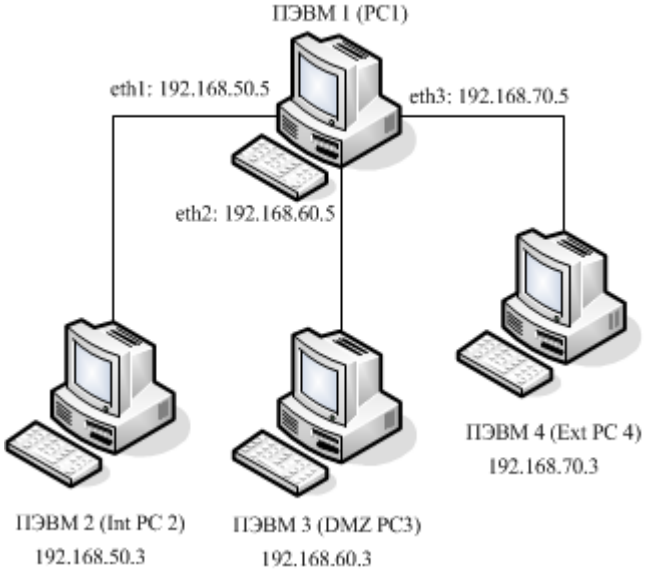


Рисунок 3.7. Пример стенда для настройки правил фильтрации

Брандмауэр Windows на ПЭВМ 2 – ПЭВМ 4 отключен.

В реестре операционной системы ПЭВМ 1 необходимо включить IP-маршрутизацию путем изменения значения параметра реестра ***IPEnableRouter*** (находится в ветке реестра ***HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters***) на ***1*** (по умолчанию параметру присвоено значение ***0***).

Перед началом настройки персонального МЭ должна быть выполнена настройка стенда, приведенная ниже.

Сетевому интерфейсу рабочей станции ПЭВМ 2 необходимо присвоить статический IP-адрес 192.168.50.3, маску подсети 255.255.255.0 и добавить статические маршруты:

- в подсеть 192.168.60.0/255.255.255.0 через шлюз 192.168.50.5 при помощи команды **route -p add 192.168.60.0 mask 255.255.255.0 192.168.50.5;**
- в подсеть 192.168.70.0/255.255.255.0 через шлюз 192.168.50.5 при помощи команды **route -p add 192.168.70.0 mask 255.255.255.0 192.168.50.5.**

Сетевому интерфейсу рабочей станции ПЭВМ 3 необходимо присвоить статический IP-адрес 192.168.60.3, маску подсети 255.255.255.0 и добавить статические маршруты:

- в подсеть 192.168.50.0/255.255.255.0 через шлюз 192.168.60.5 при помощи команды **route -p add 192.168.50.0 mask 255.255.255.0 192.168.60.5;**
- в подсеть 192.168.70.0/255.255.255.0 через шлюз 192.168.60.5 при помощи команды **route -p add 192.168.70.0 mask 255.255.255.0 192.168.60.5.**

Сетевому интерфейсу рабочей станции ПЭВМ 4 необходимо присвоить статический IP-адрес 192.168.70.3, маску подсети 255.255.255.0 и добавить статические маршруты:

- в подсеть 192.168.50.0/255.255.255.0 через шлюз 192.168.70.5 при помощи команды **route -p add 192.168.50.0 mask 255.255.255.0 192.168.70.5;**
- в подсеть 192.168.60.0/255.255.255.0 через шлюз 192.168.70.5 при помощи команды **route -p add 192.168.60.0 mask 255.255.255.0 192.168.70.5.**

Первому сетевому интерфейсу (eth1) ПЭВМ 1 необходимо присвоить статический IP-адрес 192.168.50.5, маску подсети 255.255.255.0. Второму сетевому интерфейсу (eth2) ПЭВМ 1 требуется присвоить статический IP-адрес 192.168.60.5, маску подсети 255.255.255.0. Третьему сетевому интерфейсу (eth3) ПЭВМ 1 необходимо присвоить статический IP-адрес 192.168.60.5, маску подсети 255.255.255.0. Сетевому интерфейсу (eth0) для взаимодействия ПЭВМ 1 с сервером безопасности необходимо присвоить статический IP-адрес 192.168.192.5, маску подсети 255.255.255.0

После установки сетевых параметров интерфейсов ПЭВМ 1 требуется добавить следующие статические маршруты:

- в подсеть 192.168.50.0/255.255.255.0 через шлюз 192.168.50.5 при помощи команды **route -p add 192.168.50.0 mask 255.255.255.0 192.168.50.5;**
- в подсеть 192.168.60.0/255.255.255.0 через шлюз 192.168.60.5 при помощи команды **route -p add 192.168.60.0 mask 255.255.255.0 192.168.60.5;**
- в подсеть 192.168.70.0/255.255.255.0 через шлюз 192.168.70.5 при помощи команды **route -p add 192.168.70.0 mask 255.255.255.0 192.168.70.5**;
- в подсеть 192.168.192.0/255.255.255.0 через шлюз 192.168.192.5 при помощи команды **route -p add 192.168.192.0 mask 255.255.255.0 192.168.192.5**.

Теперь администратор безопасности может из консоли администрирования СЗИ на ПЭВМ 1 переходить к настройкам правил фильтрации.

3.3.1 Настройки фильтрации пакетов на сетевом уровне на основе сетевых адресов отправителя и получателя

В качестве примера настройки фильтрации пакетов на сетевом уровне на основе сетевых адресов отправителя и получателя рассмотрим ситуацию, когда необходимо разрешить прохождение сетевых пакетов только от ПЭВМ 2 (192.168.50.3) к ПЭВМ 4 (192.168.70.3) и обратно.

Для этого администратору безопасности необходимо в консоли администрирования СЗИ на ПЭВМ 1 выполнить следующие настройки механизма межсетевого экрана СЗИ:

1) добавить пользователя (например, **User1**) в СЗИ «Блокхост-сеть 2.0». Для этого:
   - в окне **«Список машин»** консоли администрирования выбрать ПЭВМ 1, раскрыв пункт ***Все машины***.
   - в окне **«Настройки машины»** выбрать пункт ***Список пользователей***.
   - в **Основной панели настроек клиентов** выбрать пункт меню ***Управление***

пользователями→ Добавление пользователей. В появившемся окне **«Добавление пользователей»** (рис. 3.8) в конце списка локальных пользователей редактируемой рабочей станции выбрать пункт - ***Добавить пользователя -***.

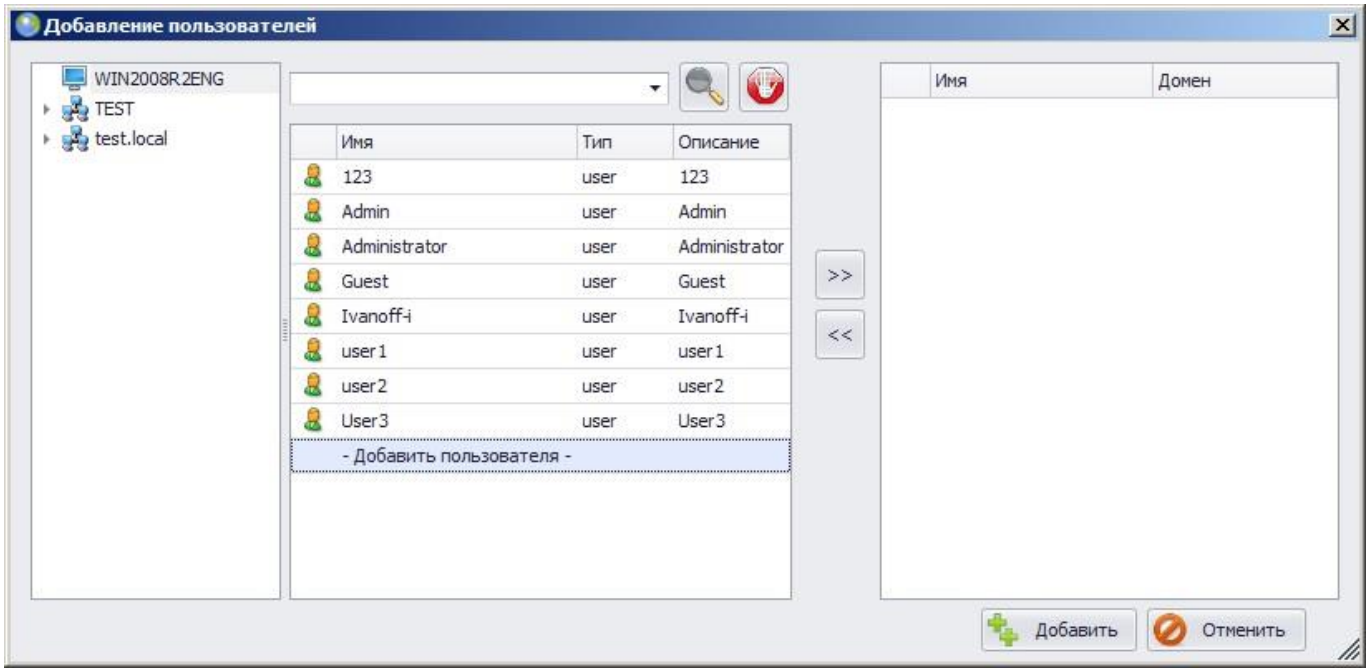


Рисунок 3.8. Добавление пользователя в СЗИ

- в открывшемся окне **«Создание локального пользователя»** (рис. 3.9) ввести имя пользователя, выбрать группу, в которую он будет включен, и задать его пароль. После указания всех необходимых параметров для создания нового локального пользователя нажать кнопку ***Создать***.

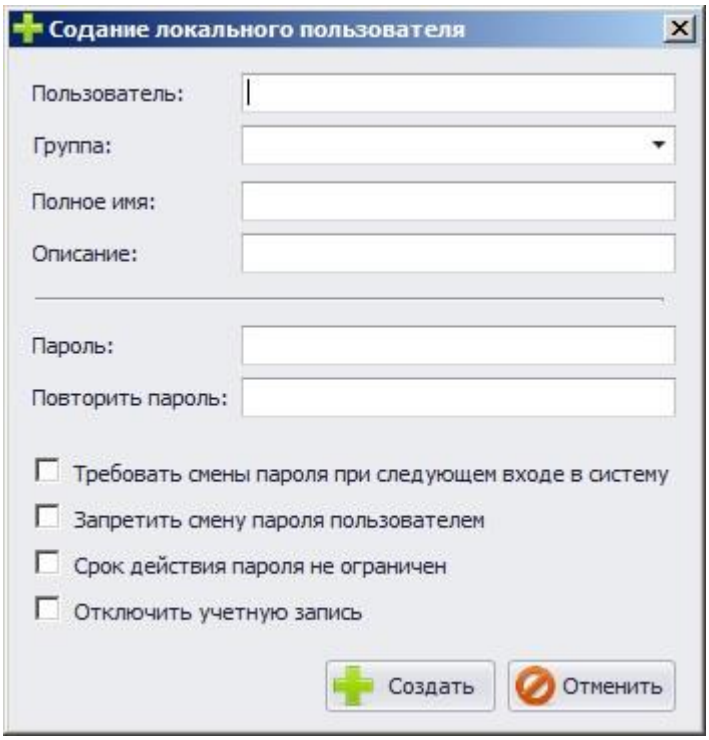


Рисунок 3.9. Окно «Создание локального пользователя»

- в окне добавления пользователей (см. рис. 3.8) выделить созданную учетную

запись, с помощью кнопки >> перенести ее в поле добавляемых в СЗИ пользователей и нажать кнопку ***Добавить***. Созданная учетная запись локального пользователя появится в списке пользователей СЗИ рабочей станции. Добавленному в СЗИ пользователю автоматически назначается мандатная метка равная ***1***, все типы входа на рабочую станцию и возможность входа в ОС без использования ключевого носителя.

2) в **Основной панели настроек клиентов** консоли администрирования для пользователя **User1** (пункт ***Персональный экран*** окна **«Настройки машины»**) при помощи кнопки добавить профиль персонального МЭ с именем *Profile1* со следующими параметрами:
   - установить параметр ***Включить персональный экран***;
   - выбрать значение ***Разрешительная политика***;
   - установить параметр ***Регистрировать разрешенные пакеты***;
   - установить параметр ***Регистрировать запрещенные пакеты***;
   - установить параметр ***Включить IGMP протокол***;
   - установить параметр ***Включить ICMP протокол***;
   - установить параметр ***Включить фильтрацию по типам ICMP протокола***;
   - установить параметр ***Включить регистрацию ICMP пакетов***;
   - в окне **«Настройки ICMP»** установить галочки для всех полей.
3) добавить в созданный профиль *Profile1* правило фильтрации разрешающее прохождение TCP пакетов от ПЭВМ 2 к ПЭВМ 4 (рис. 3.10):
   - IP источника *192.168.50.3*;
   - порт источника *«*»*;
   - IP узла назначения *192.168.70.3*;
   - порт узла назначения *«*»*;
   - установить параметр ***Правило активно***;
   - установить параметр ***Аудит***;
   - нажать кнопку ***Сохранить***.

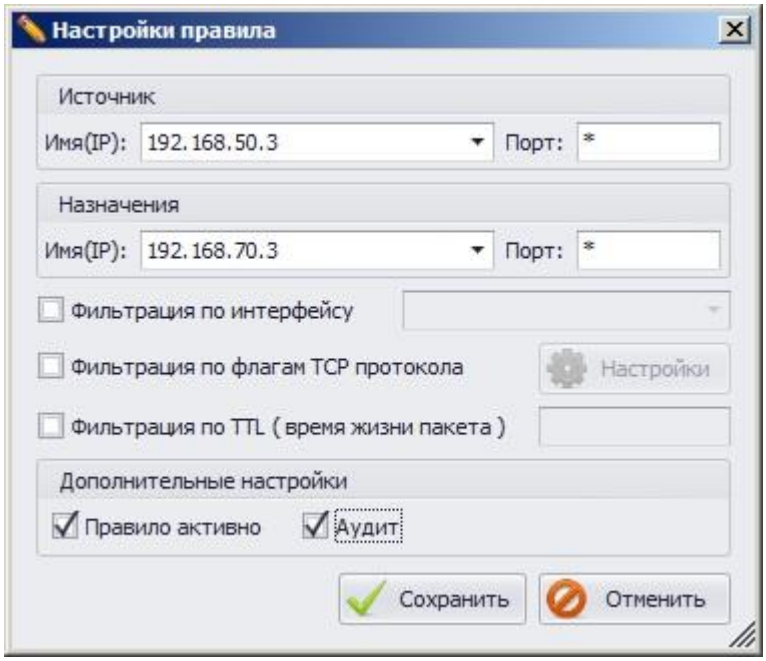


Рисунок 3.10. Правило фильтрации TCP-пакетов от ПЭВМ 2 к ПЭВМ 4

4) в результате сохранения этого правила автоматически будет создано правило, разрешающее прохождение TCP пакетов от ПЭВМ 4 к ПЭВМ 2 (в котором произведена замена установленных параметров узлов ***Источника*** и ***Назначения***). Добавленные правила персонального МЭ отобразятся в консоли администрирования СЗИ:

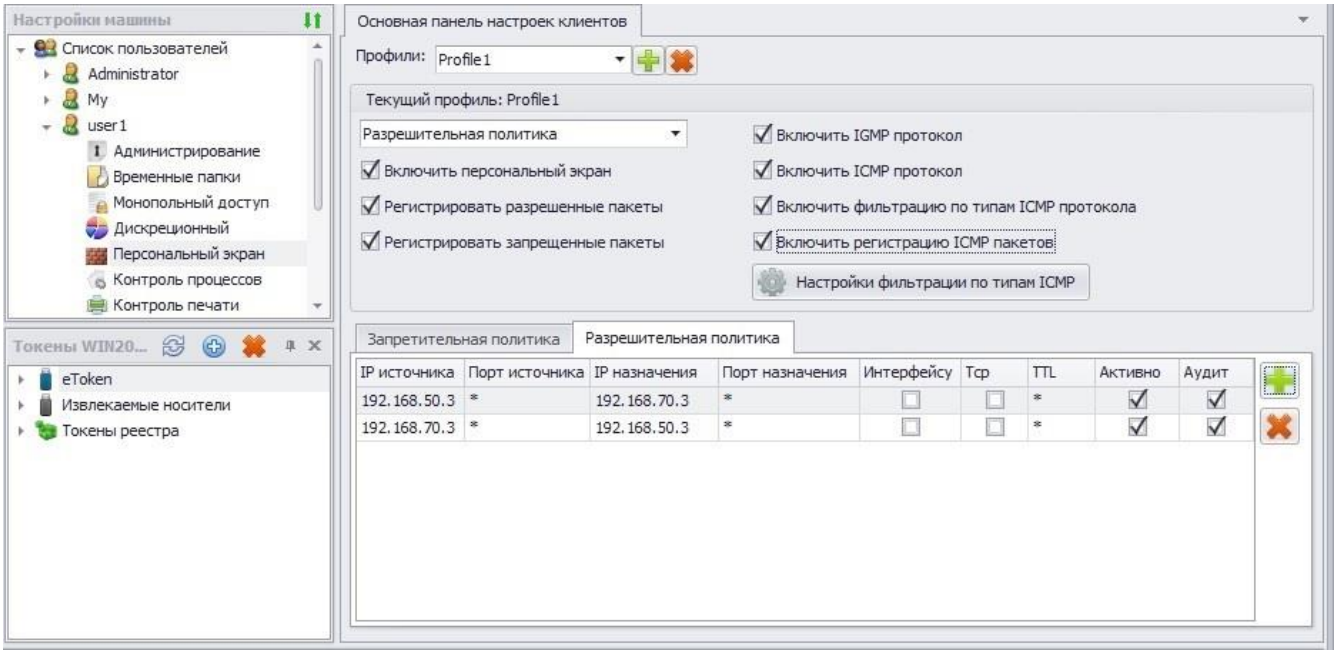


Рисунок 3.11. Правила фильтрации сетевых пакетов на основе IP-адресов отправителя и получателя

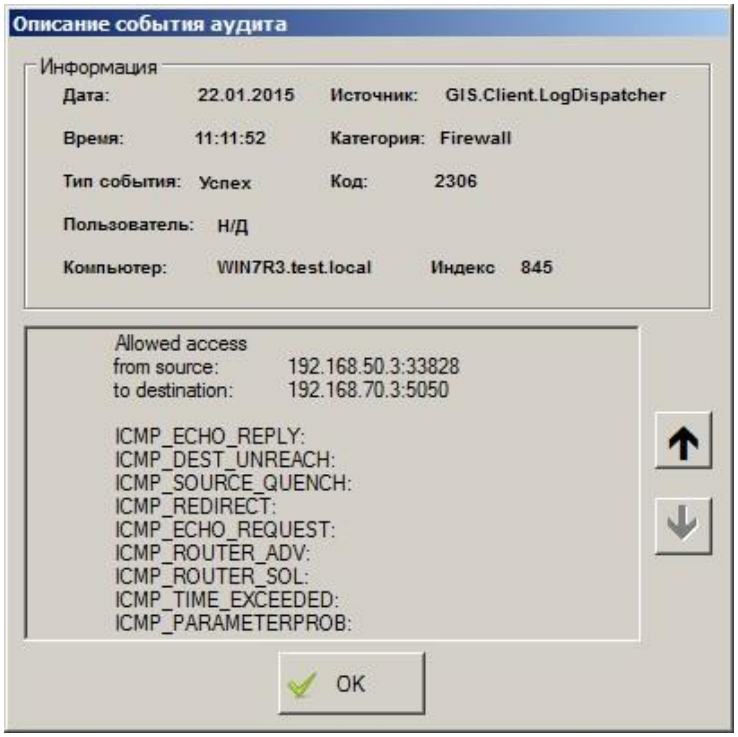
5) сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

После входа пользователя **User1** на ПЭВМ 1 фильтрация TCP-пакетов в ЛВС будет осуществляться следующим образом:

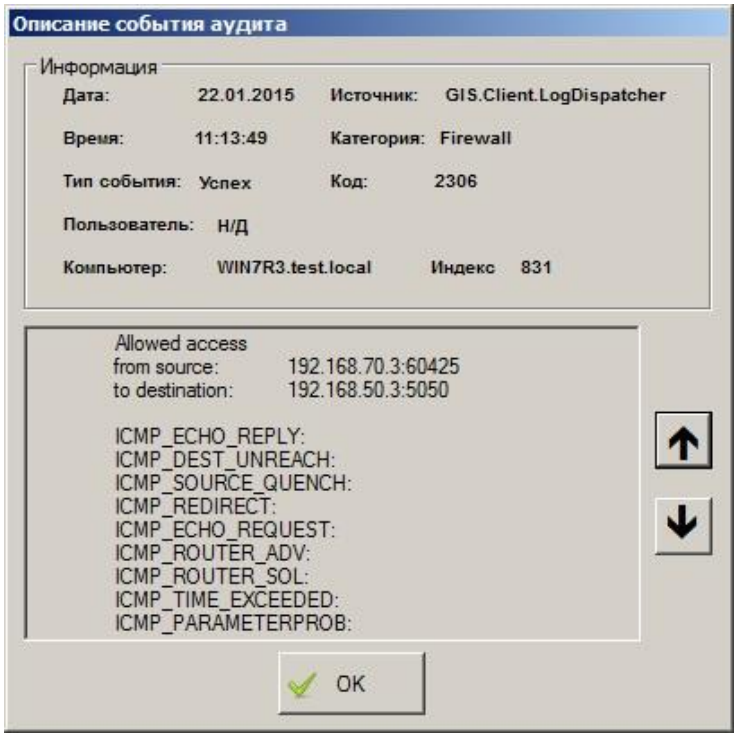
- прохождение TCP-пакетов от ПЭВМ 2 к ПЭВМ 4 и обратно будет разрешено;
- прохождение TCP-пакетов от ПЭВМ 2 к ПЭВМ 3 и обратно будет запрещено;
- прохождение TCP-пакетов от ПЭВМ 4 к ПЭВМ 3 и обратно будет запрещено.

В журнале аудита СЗИ на ПЭВМ 1 фиксируются события прохождения/блокировки сетевого трафика (в консоли администрирования СЗИ в окне **«Список машин»** выбрана ПЭВМ 1, в окне **«Настройки машины»** выбран пункт ***Аудит***). По двойному щелчку по событию в его описании можно увидеть:

1) регистрацию прохождения TCP пакетов от ПЭВМ 2 к ПЭВМ 4 и обратно (рис. 3.12);



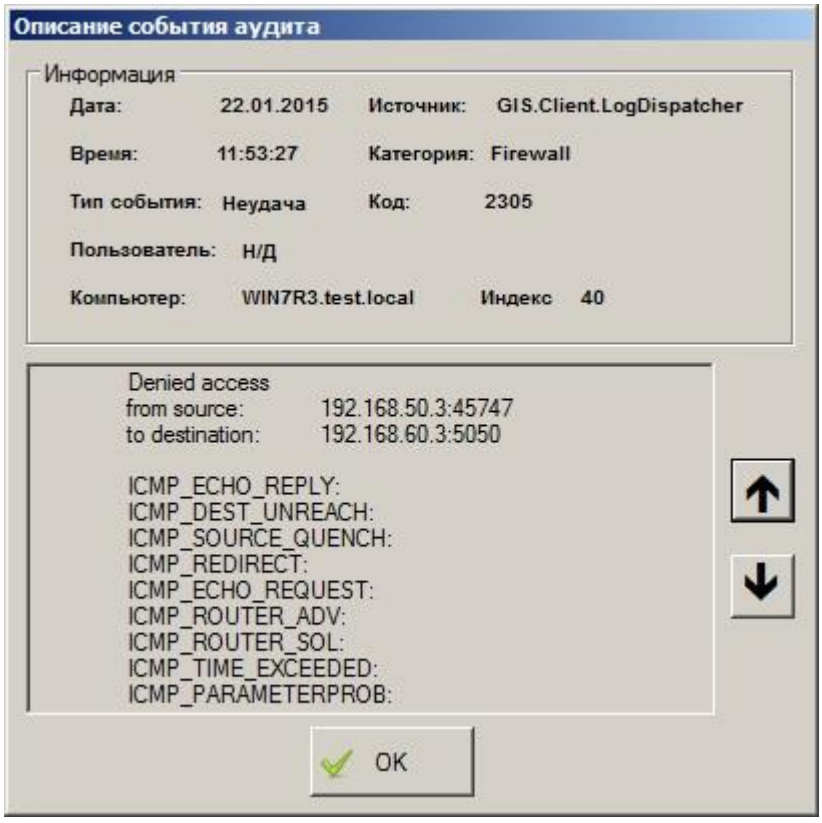
а)



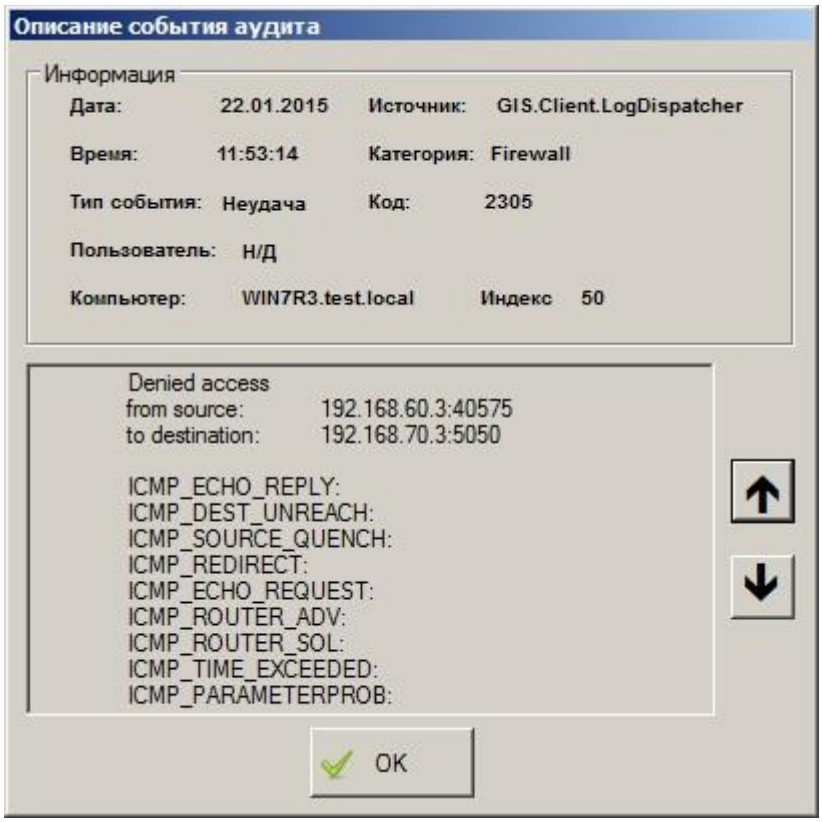
б)

Рисунок 3.12. Регистрация прохождения TCP пакетов от ПЭВМ 2 к ПЭВМ 4 и обратно

2) регистрацию блокировки TCP пакетов от ПЭВМ 2 к ПЭВМ 3 и обратно (рис. 3.13);



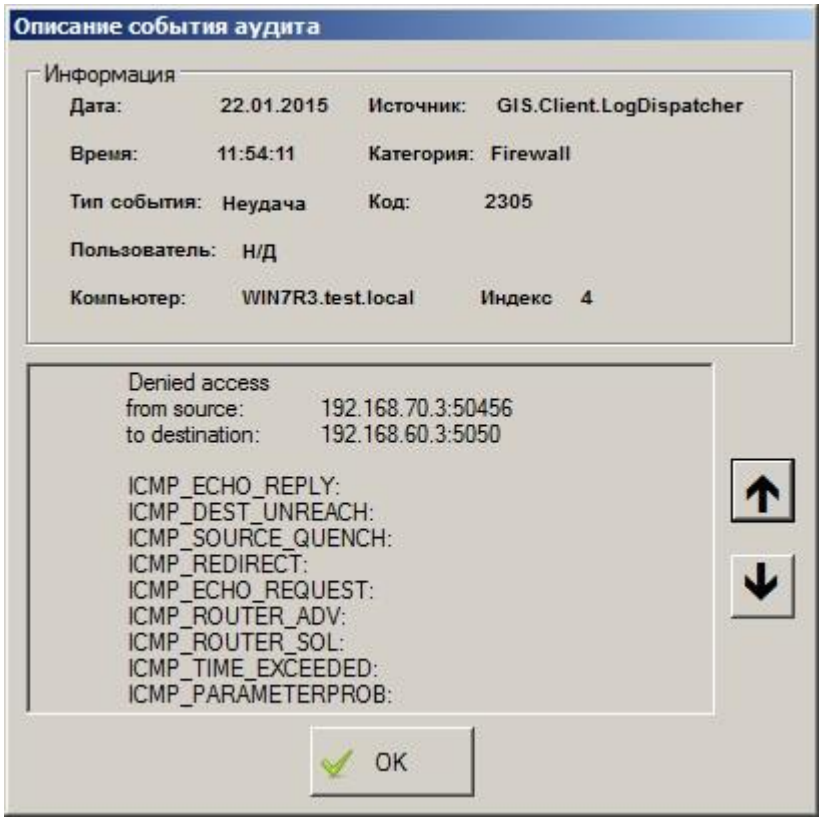
а)



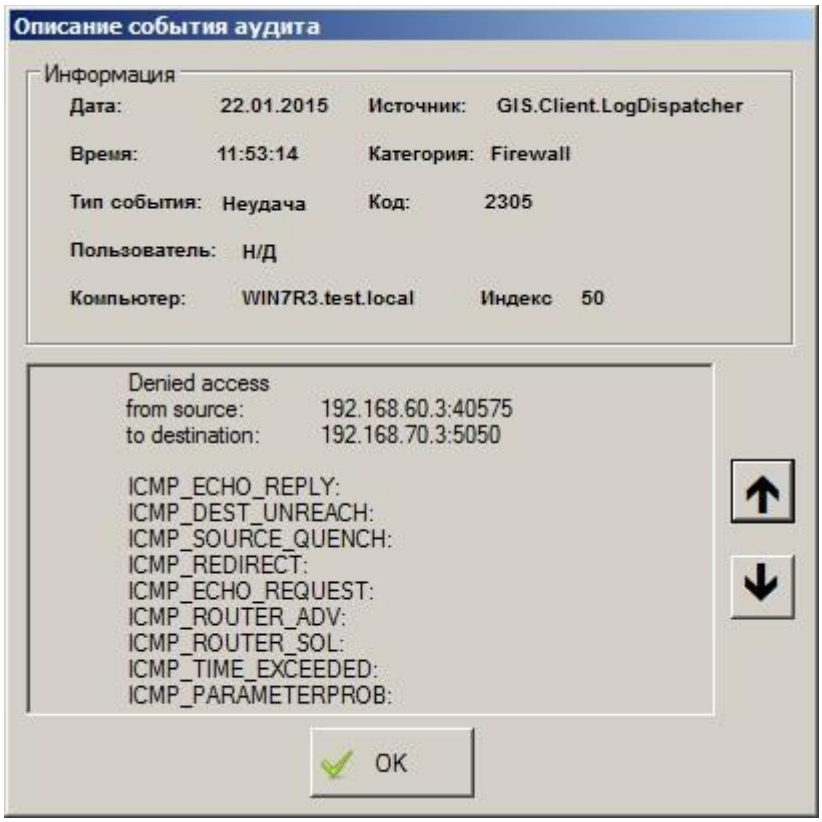
б)

Рисунок 3.13. Регистрация блокировки сетевых пакетов от ПЭВМ 2 к ПЭВМ 3 и обратно

3) регистрацию блокировки сетевых пакетов от ПЭВМ 4 к ПЭВМ 3 и обратно (рис. 3.14).



а)



б)

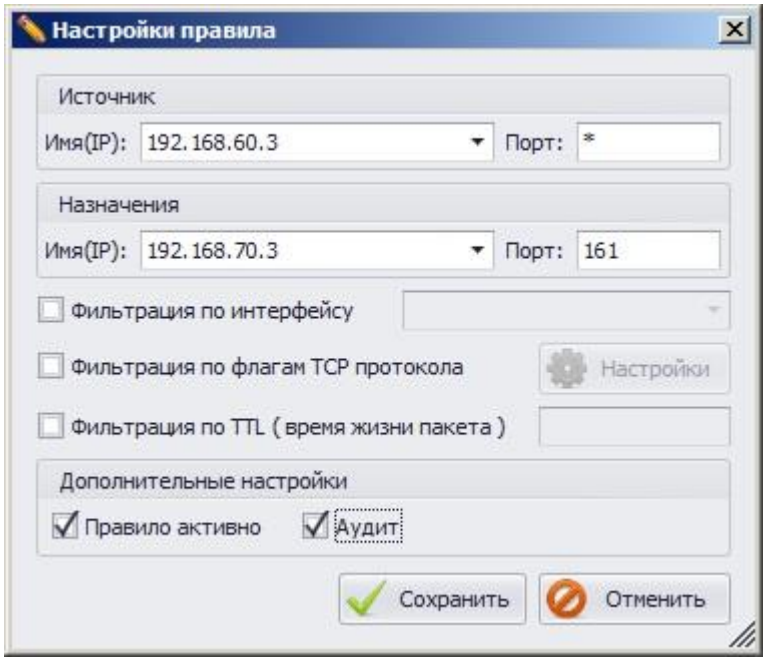
Рисунок 3.14. Регистрация блокировки сетевых пакетов от ПЭВМ 4 к ПЭВМ 3 и обратно

3.3.2 Настройки фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств

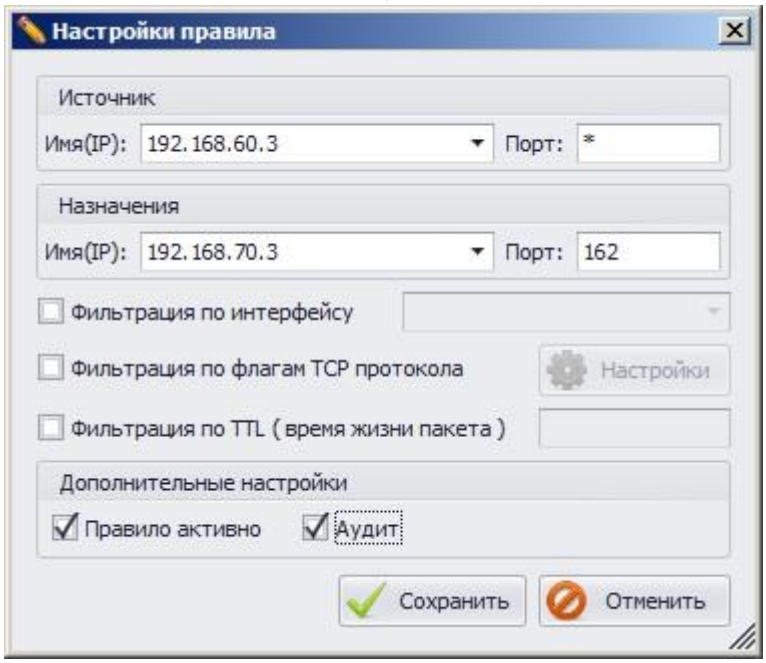
Настройку фильтрации пакетов служебных протоколов рассмотрим на примере настройки фильтрации протокола SNMP, который используется для управления сетевыми устройствами. Выполним настройку персонального МЭ в режиме разрешения прохождения SNMP-пакетов от ПЭВМ 3 к ПЭВМ 4 и в обратном направлении, при этом прохождение всех остальных IP-пакетов запретим.

Для настройки фильтрации протокола SNMP администратору безопасности в консоли администрирования СЗИ выполнить следующие настройки для ПЭВМ 1, использующейся в качестве межсетевого экрана:

1) в **Основной панели настроек клиентов** консоли администрирования для пользователя **User1** (пункт ***Персональный экран*** окна **«Настройки машины»**) при помощи кнопки ***Добавить*** создать профиль персонального МЭ с именем *Profile2* со следующими параметрами:
   - выбрать значение ***Разрешительная политика***;
   - установить параметр ***Включить персональный экран***;
   - установить параметр ***Регистрировать разрешенные пакеты***;
   - установить параметр ***Регистрировать запрещенные пакеты***;
   - установить параметр ***Включить IGMP протокол***;
   - установить параметр ***Включить ICMP протокол***;
   - установить параметр ***Включить фильтрацию по типам ICMP протокола***;
   - установить параметр ***Включить регистрацию ICMP пакетов***;
   - в окне **«Настройки ICMP»** установить галочки для всех полей.
2) разрешить прохождение SNMP пакетов от ПЭВМ 3 к ПЭВМ 4, для чего добавить в созданный профиль *Profile2* следующее правило фильтрации (рис. 3.15):
   - IP источника *192.168.60.3*;
   - порт источника *«*»*;
   - IP узла назначения *192.168.70.3*;
   - порт узла назначения *161 (162*);
   - установить параметр ***Правило активно***;
   - установить параметр ***Аудит***;
   - нажать кнопку ***Сохранить***.



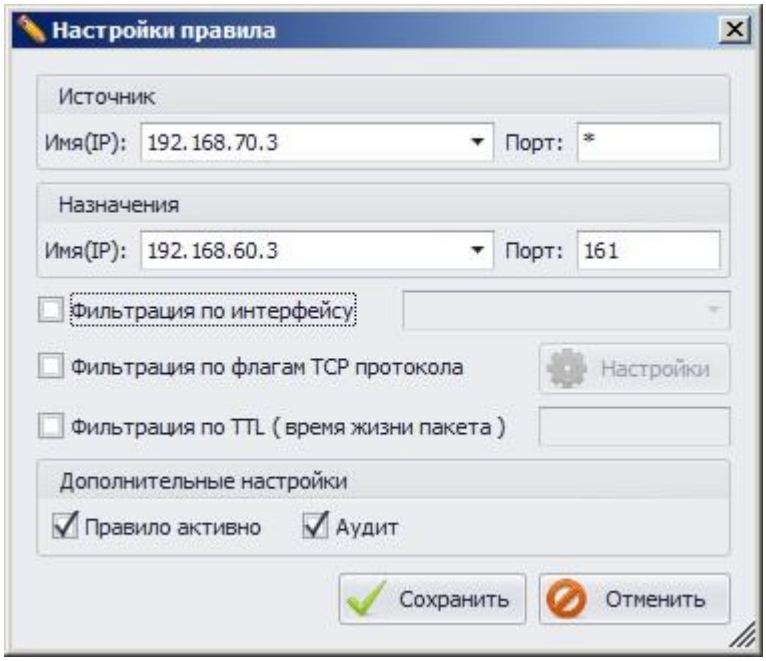
а)



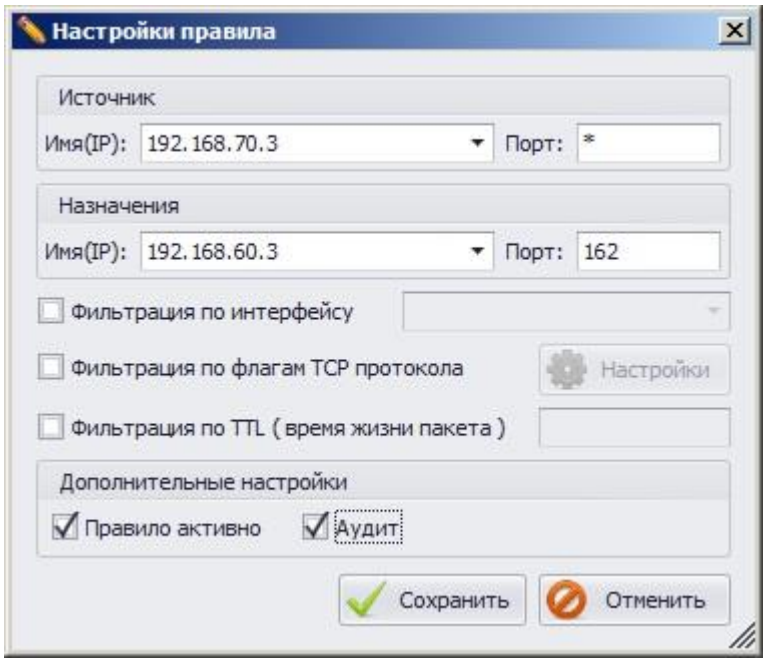
б)

Рисунок 3.15. Правила фильтрации SNMP пакетов от ПЭВМ 3 к ПЭВМ 4

3) разрешить прохождение SNMP пакетов от ПЭВМ 4 к ПЭВМ 3, для чего изменить в профиле *Profile2* созданные автоматически при сохранении правил фильтрации пакетов от ПЭВМ 3 к ПЭВМ 4, обратные им правила фильтрации, изменив параметры поля ***Порт*** для ***Источника*** и ***Назначения*** (рис. 3.16):
   - порт источника *«*»*;
   - порт узла назначения *161 (162)*;
   - нажать кнопку ***Сохранить***.



а)



б)

Рисунок 3.16. Правила фильтрации SNMP пакетов от ПЭВМ 4 к ПЭВМ 3

В результате правила фильтрации пакетов протокола SNMP будут добавлены в консоль управления СЗИ (рис. 3.17).

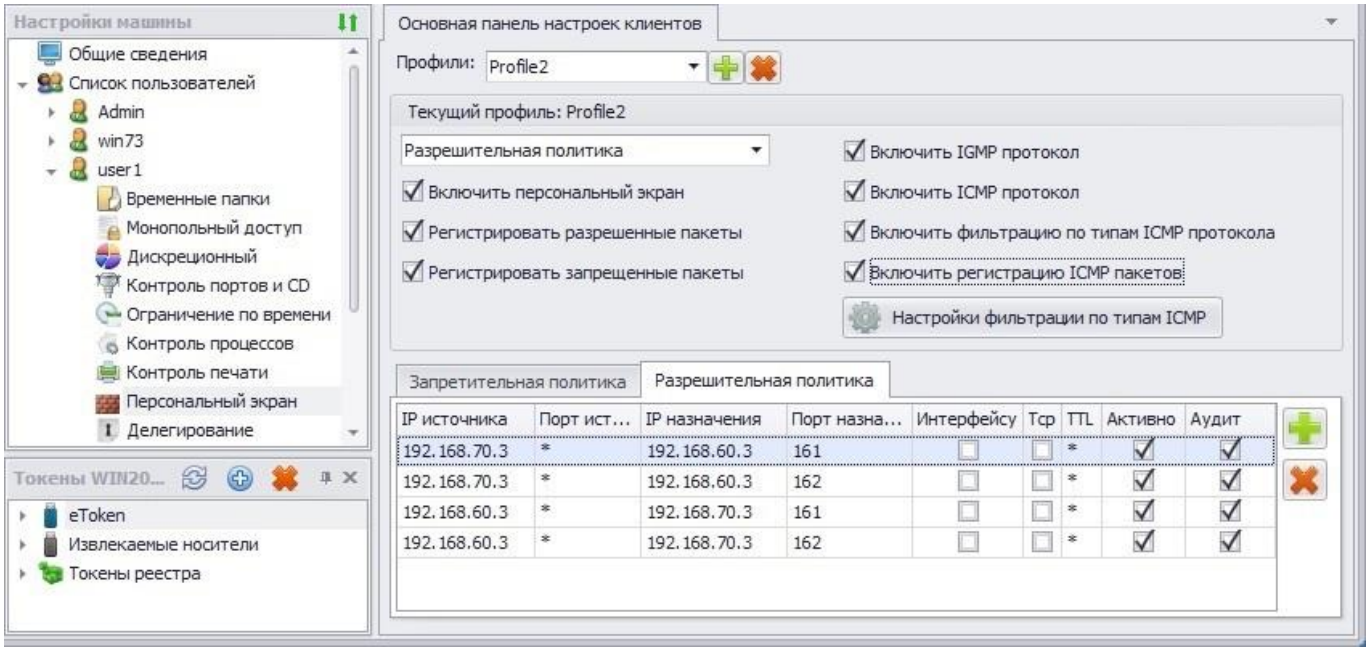


Рисунок 3.17. Правила фильтрации пакетов протокола SNMP

4) сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

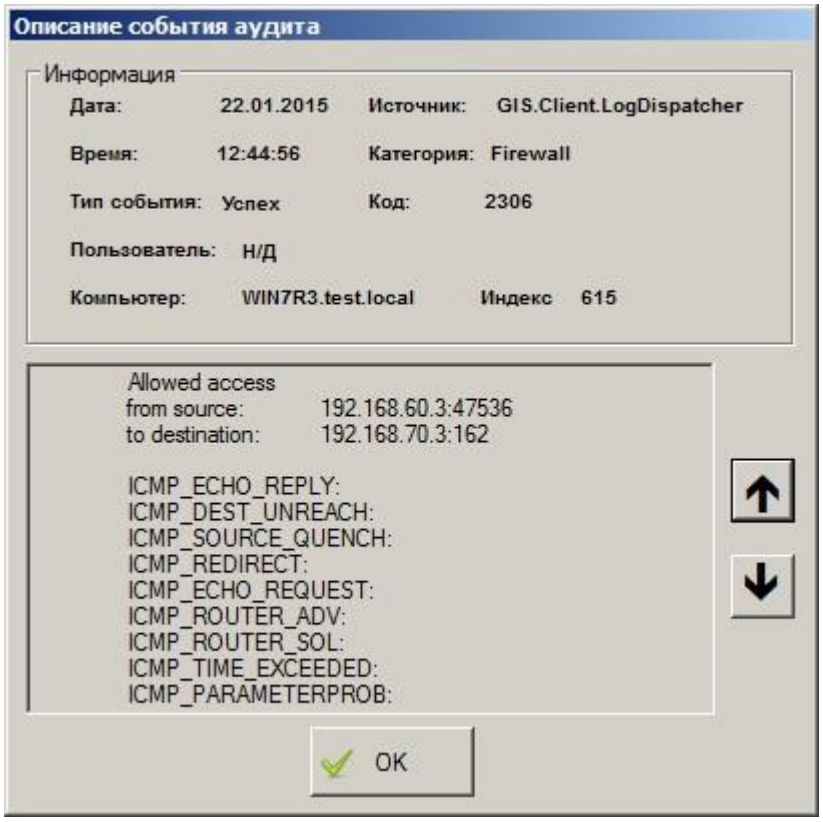
После входа пользователя **User1** на ПЭВМ 1 фильтрация SNMP-пакетов будет осуществляться следующим образом:

- прохождение SNMP-пакетов от ПЭВМ 3 к ПЭВМ 4 и обратно будет разрешено;
- прохождение SNMP-пакетов от ПЭВМ 3 к ПЭВМ 2 и обратно будет запрещено.

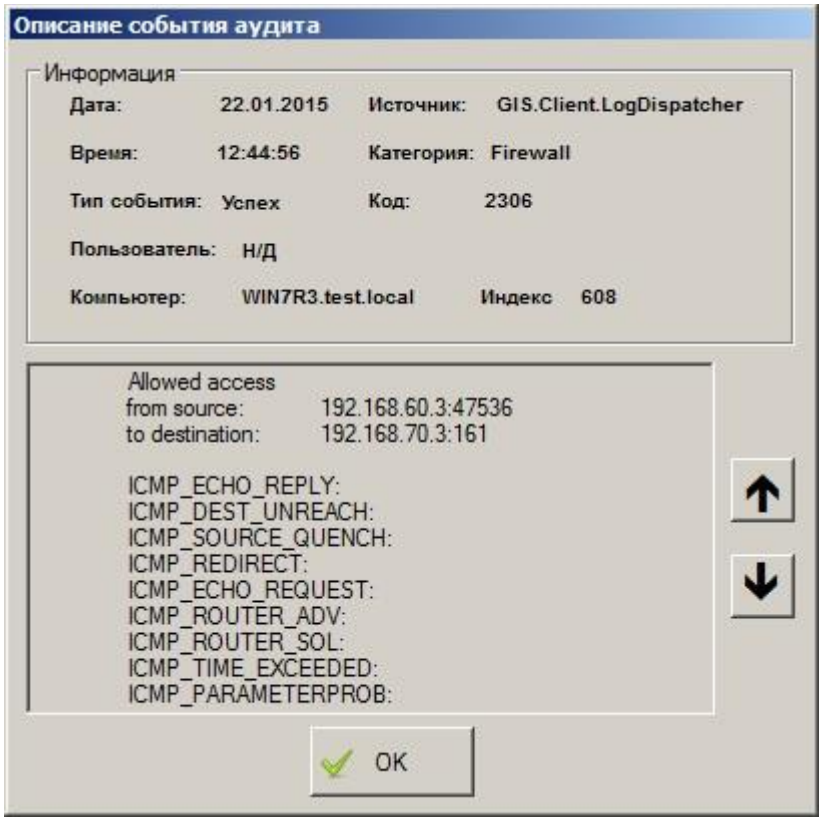
В журнале аудита СЗИ на ПЭВМ 1 фиксируются события прохождения/блокировки сетевого трафика (в консоли администрирования СЗИ в окне **«Список машин»** выбрана ПЭВМ 1, в окне **«Настройки машины»** выбран пункт ***Аудит***). По двойному щелчку по событию в его описании можно увидеть:

1) регистрацию прохождения пакетов протокола SNMP от ПЭВМ 3 к ПЭВМ 4 и обратно:

- с ПЭВМ 3 на ПЭВМ 4 (рис. 3.18):



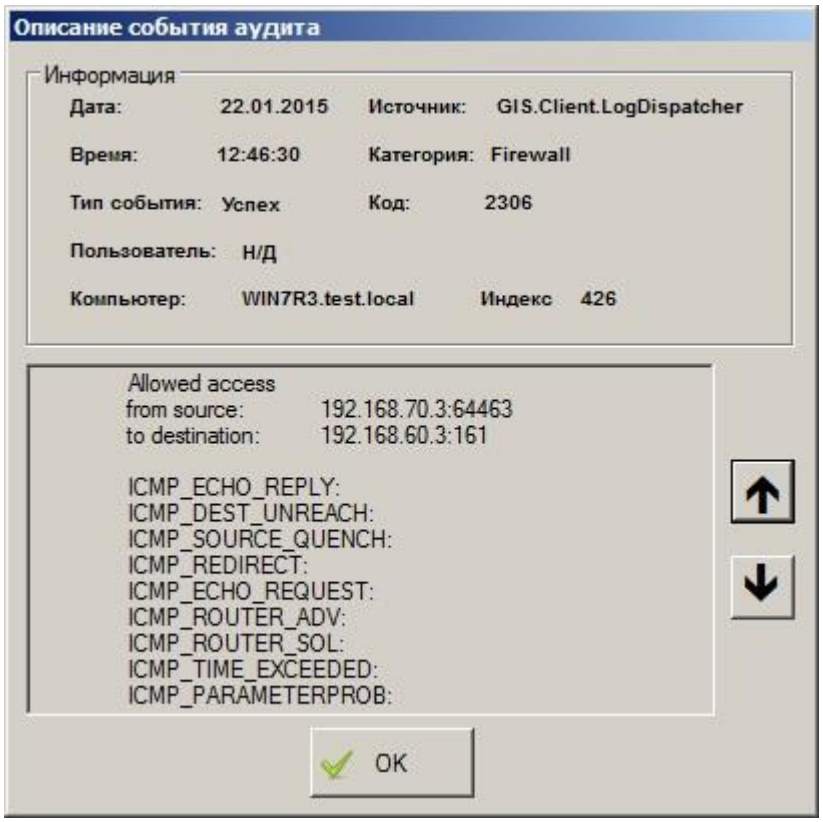
а)



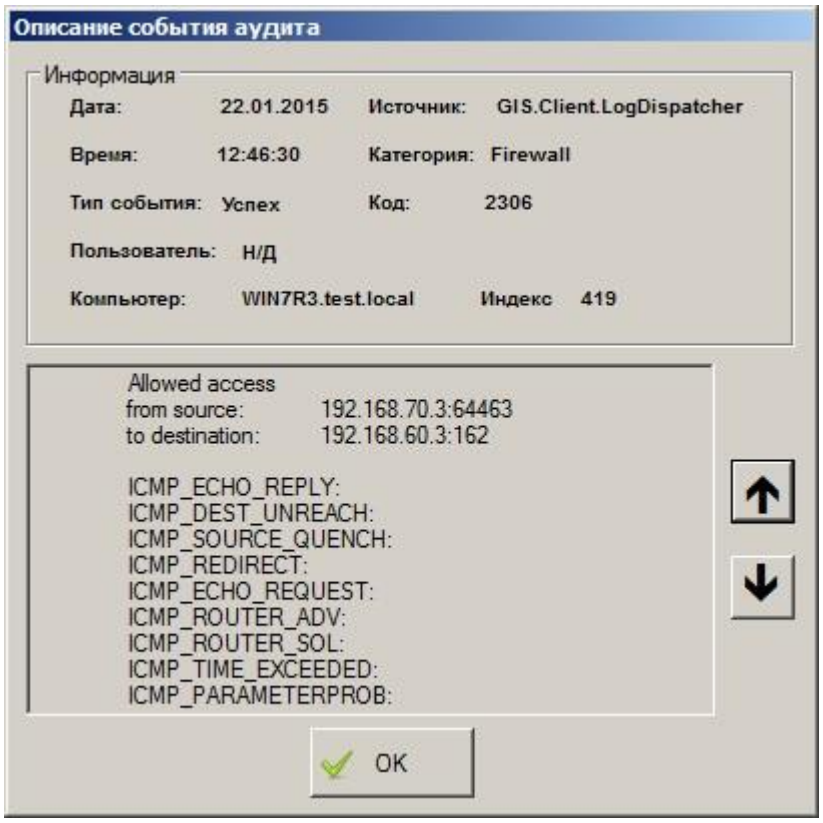
б)

Рисунок 3.18. Регистрация прохождения пакетов протокола SNMP с ПЭВМ 3 на ПЭВМ 4

- с ПЭВМ 4 на ПЭВМ 3 (рис. 3.19):



а)

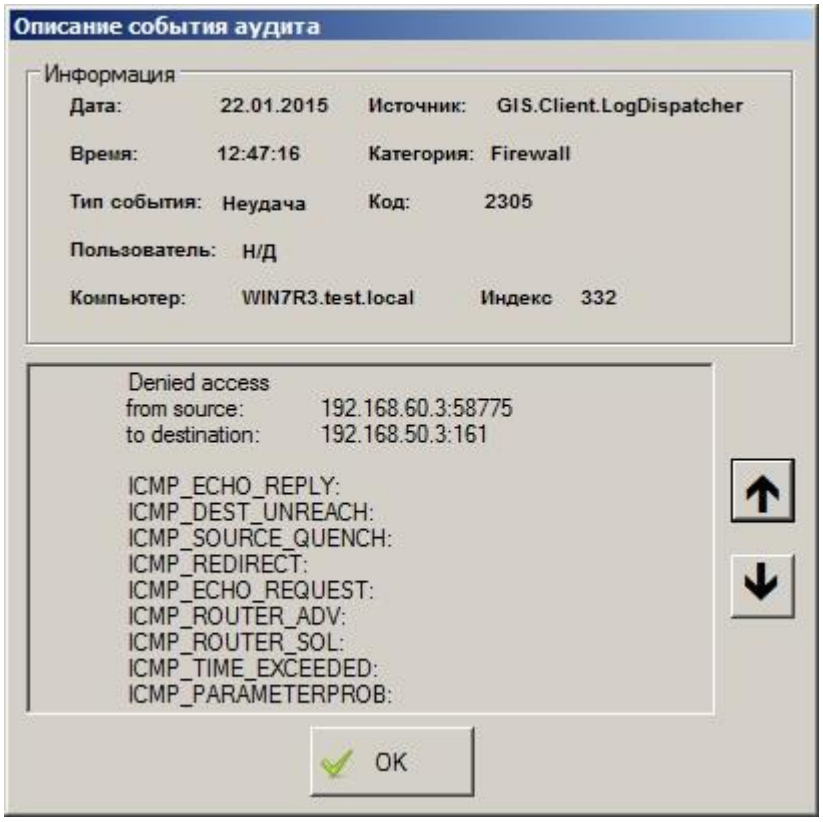


б)

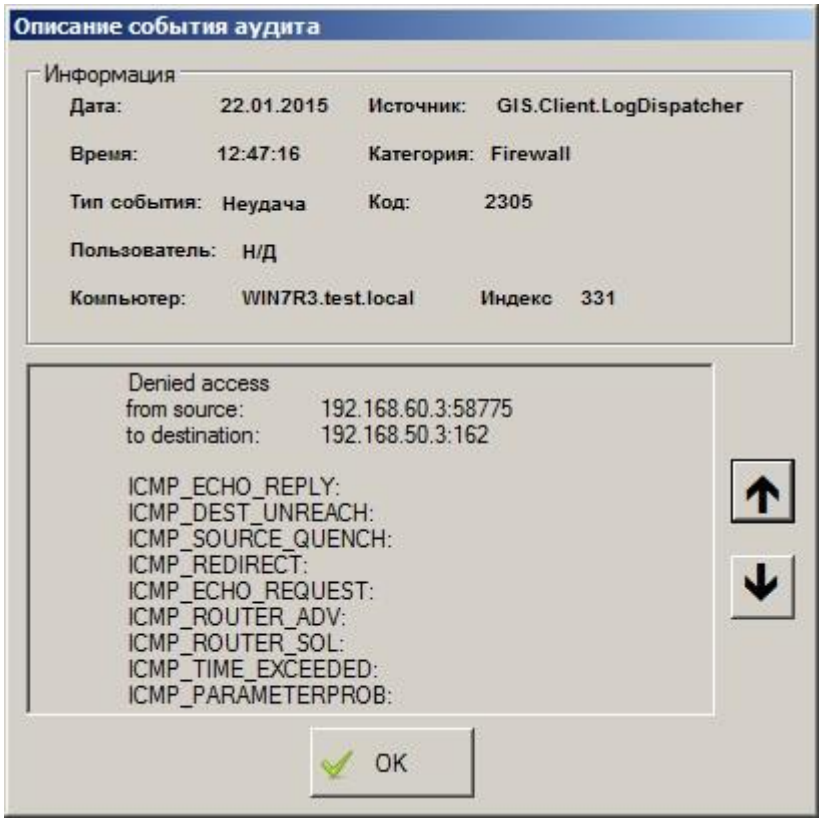
Рисунок 3.19. Регистрация прохождения пакетов протокола SNMP с ПЭВМ 4 на ПЭВМ 3

2) регистрацию блокировки сетевых пакетов от ПЭВМ 3 к ПЭВМ 2 и обратно:

- с ПЭВМ 3 на ПЭВМ 2 (рис. 3.20):



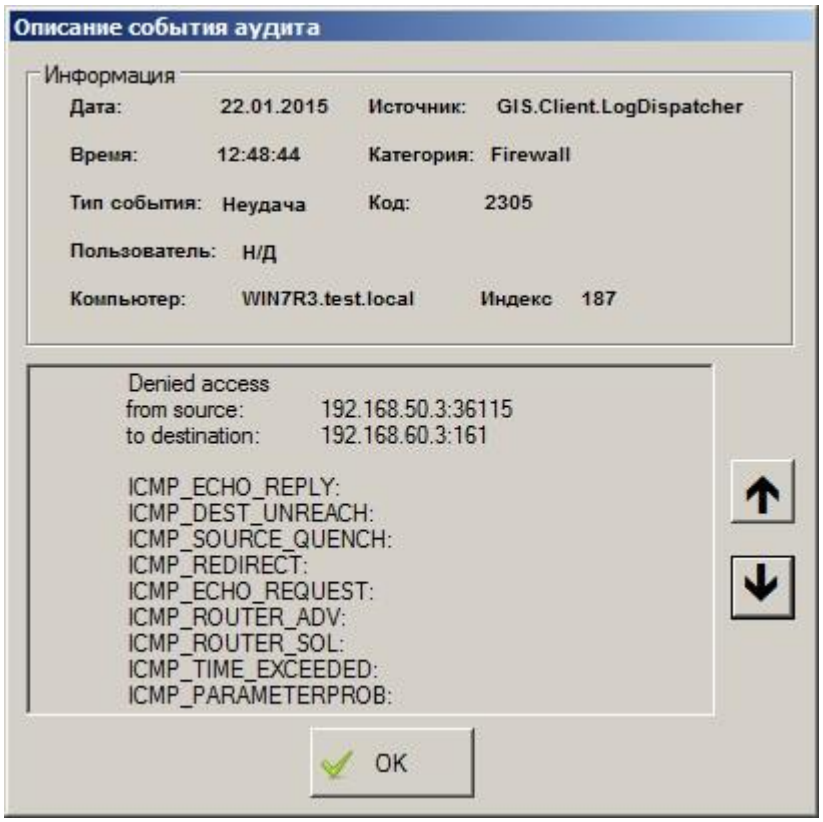
а)



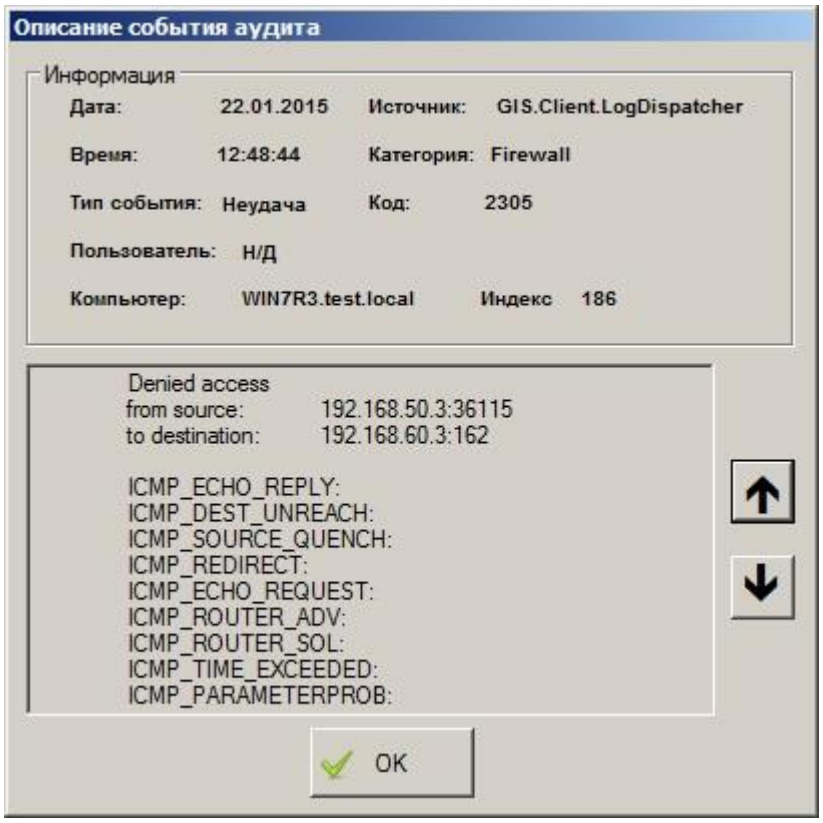
б)

Рисунок 3.20. Регистрация блокировки SNMP пакетов от ПЭВМ 3 к ПЭВМ 2

- с ПЭВМ 2 на ПЭВМ 3 (рис. 3.21):



а)



б)

Рисунок 3.21. Регистрация блокировки SNMP пакетов от ПЭВМ 2 к ПЭВМ 3

3.3.3 Настройки фильтрации с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов

Персональный МЭ позволяет осуществлять фильтрацию сетевого трафика с учетом входного и выходного сетевого интерфейса ПЭВМ и может быть использован как средство проверки подлинности сетевых адресов.

Предположим, разрешено прохождение TCP-пакетов от ПЭВМ 2 к ПЭВМ 3 и обратно без учета фильтрации по интерфейсам (описание организации сетевого взаимодействия ПЭВМ приведено в подразделе 3.3 настоящего документа). В этом случае при отправке пакетов с ПЭВМ 4 к ПЭВМ 3 с подменой адреса источника (от имени ПЭВМ 2) будет разрешено прохождение сетевых пакетов от ПЭВМ 4 к ПЭВМ 3 и на ПЭВМ 2 будет получен ответ от ПЭВМ 3.

Избежать атак с подменой адреса позволяет настройка фильтрации по интерфейсу. Для стенда, приведенного на рисунке 3.6, необходимо выполнить следующие настройки СЗИ для ПЭВМ 1, использующейся в качестве межсетевого экрана:

1) в **Основной панели настроек клиентов** консоли администрирования для пользователя **User1** (пункт ***Персональный экран*** окна **«Настройки машины»**) при помощи кнопки ***Добавить***  добавить профиль персонального МЭ с именем *Profile3* со следующими параметрами:
   - выбрать значение ***Разрешительная политика***;
   - установить параметр ***Включить персональный экран***;
   - установить параметр ***Регистрировать разрешенные пакеты***;
   - установить параметр ***Регистрировать запрещенные пакеты***;
   - установить параметр ***Включить IGMP протокол***;
   - установить параметр ***Включить ICMP протокол***;
   - установить параметр ***Включить фильтрацию по типам ICMP протокола***;
   - установить параметр ***Включить регистрацию ICMP пакетов***;
   - в окне **«Настройки ICMP»** установить галочки для всех полей.
2) разрешить прохождение пакетов от ПЭВМ 3 на ПЭВМ 2 с учетом входного сетевого интерфейса eth 2 ПЭВМ 1, для чего добавить в созданный профиль *Profile3* следующее правило фильтрации (рис. 3.22):
   - IP источника *192.168.60.3*;
   - порт источника *«*»*;
   - IP узла назначения *192.168.50.3*;
   - порт узла назначения *«*»*;
   - активизировать фильтр по интерфейсу (из выпадающего списка выбрать сетевое подключение с именем *DMZ* и IP = *192.168.60.5*, соответствующее интерфейсу e*th2*);
   - установить параметр ***Правило активно***;
   - установить параметр ***Аудит***;
   - нажать кнопку ***Сохранить***.

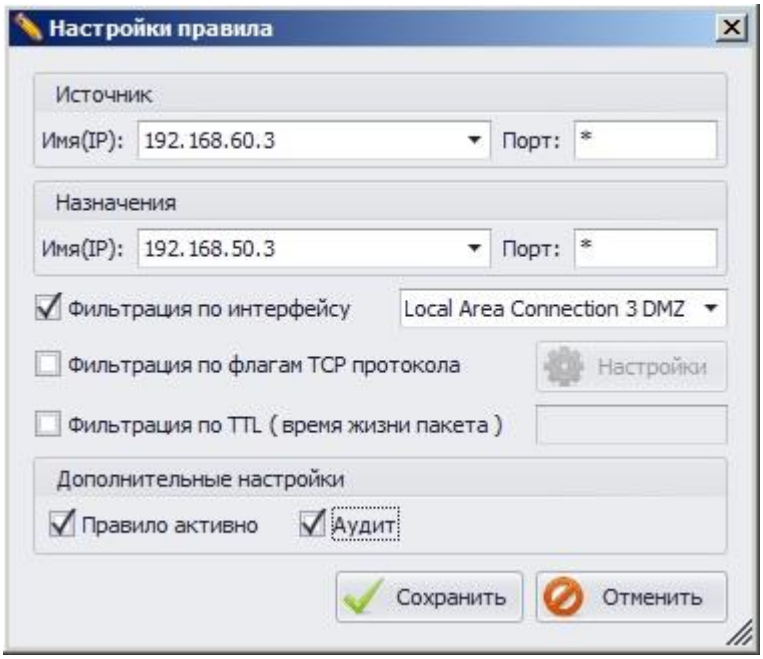


Рисунок 3.22. Правило фильтрации пакетов от ПЭВМ 3 к ПЭВМ 2 с учетом сетевого интерфейса eth2 ПЭВМ 1

3) разрешить прохождение пакетов с ПЭВМ 2 на ПЭВМ 3 с учетом выходного сетевого интерфейса eth1 ПЭВМ 1, для чего изменить в профиле *Profile3* созданное автоматически при сохранении правила фильтрации пакетов от ПЭВМ 3 к ПЭВМ 2, обратное ему правило фильтрации, изменив параметры поля ***Фильтрация по интерфейсу*** (рис. 3.23):
   - выпадающего списка выбрать сетевое подключение с именем *Internal* и IP = *192.168.50.5*, соответствующее интерфейсу e*th1*;
   - нажать кнопку ***Сохранить***.

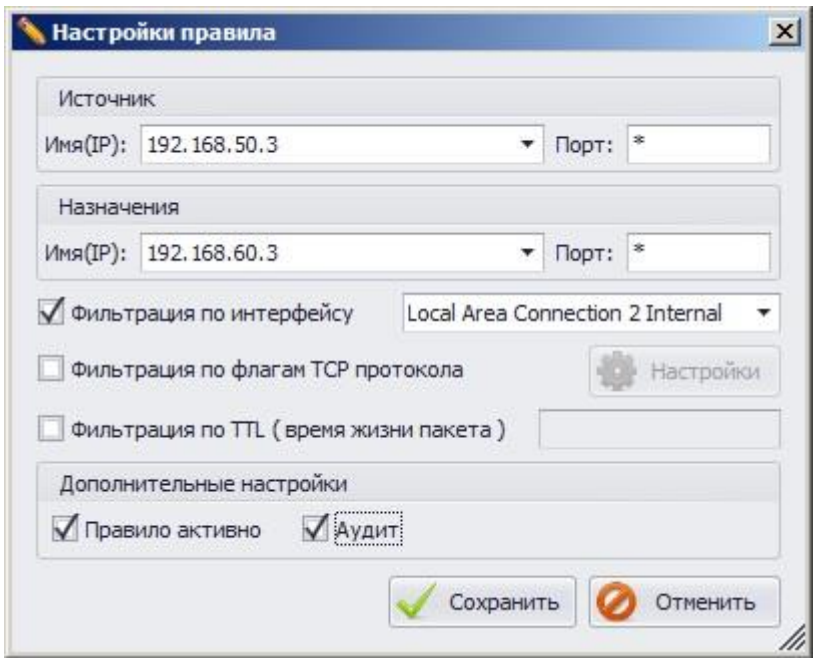


Рисунок 3.23. Правило фильтрации пакетов с ПЭВМ 2 на ПЭВМ 3 с учетом сетевого интерфейса eth1 ПЭВМ 1

В результате правила фильтрации сетевого трафика с учетом сетевых интерфейсов eth1 и eth2 ПЭВМ1 будут добавлены в консоль управления СЗИ (рис. 3.24).

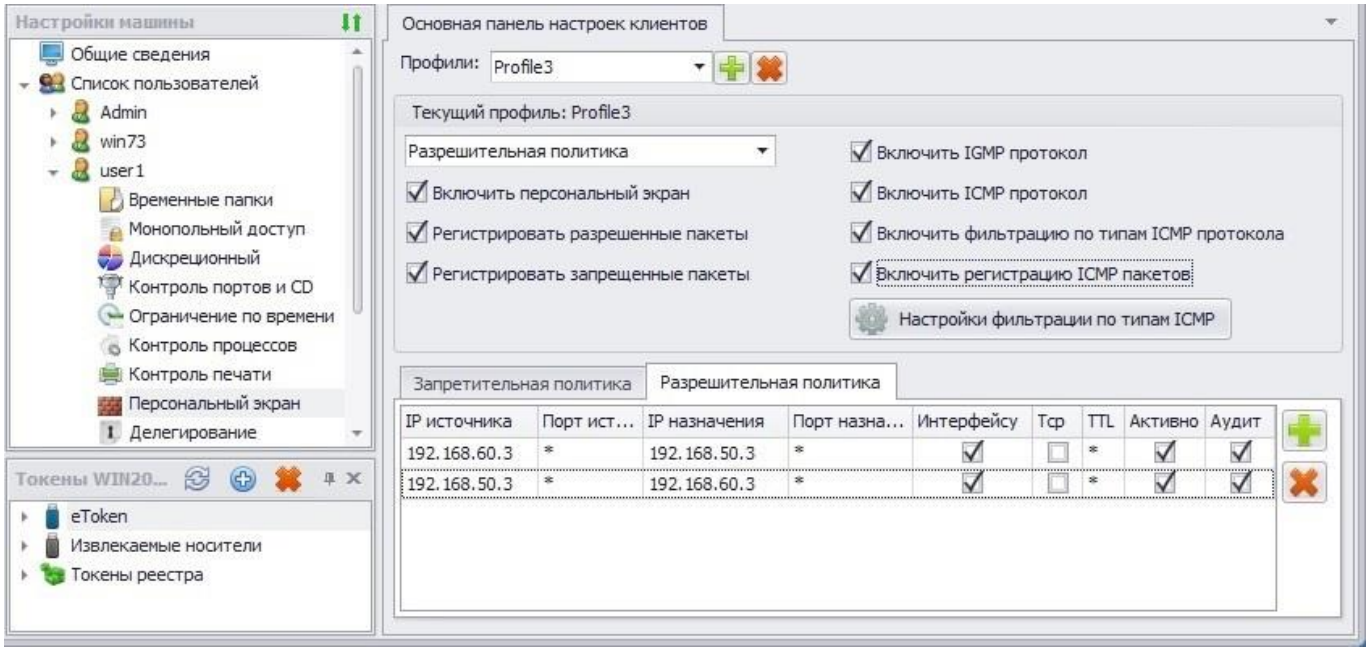


Рисунок 3.24. Правила фильтрации сетевого трафика с учетом сетевых интерфейсов eth1 и eth2 ПЭВМ 1

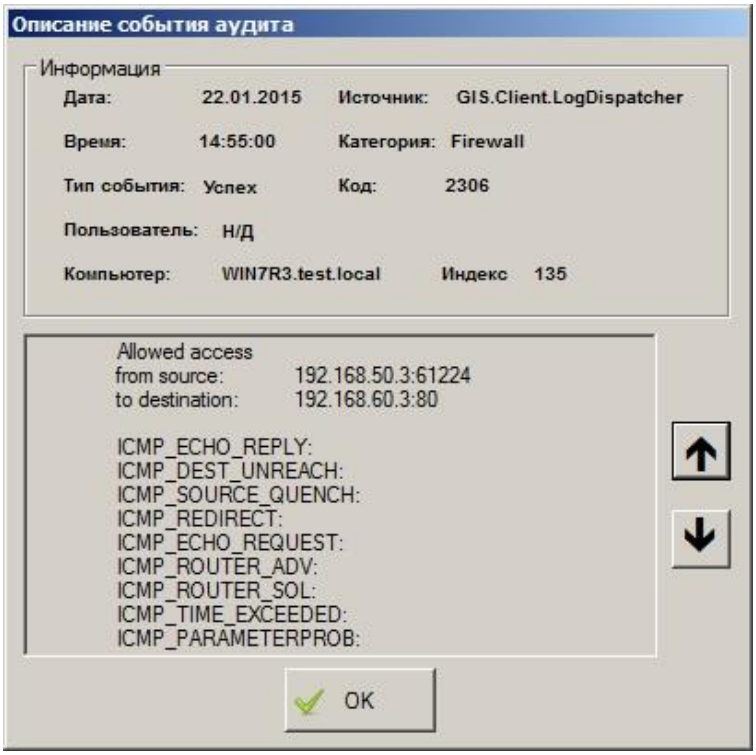
4) сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все*** , расположенной в левом верхнем углу консоли администрирования СЗИ.

После входа пользователя **User1** на ПЭВМ 1 фильтрация TCP-пакетов в ЛВС будет осуществляться следующим образом:

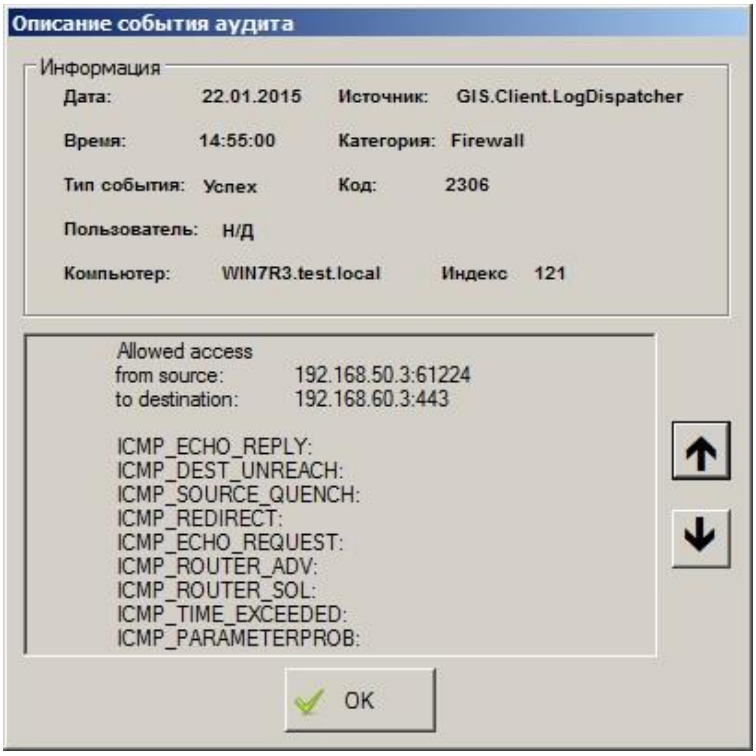
- прохождение TCP-пакетов от ПЭВМ 2 к ПЭВМ 3 и обратно будет разрешено при фильтрации с учетом интерфейсов и генерации пакетов на ПЭВМ 2;
- при отправке TCP-пакетов с ПЭВМ 4 на ПЭВМ 3 с подменой адреса источника (от имени ПЭВМ 2) будет осуществляться их блокирование.

В журнале аудита СЗИ на ПЭВМ 1 фиксируются события прохождения/блокировки сетевого трафика (в консоли администрирования СЗИ в окне **«Список машин»** выбрана ПЭВМ 1, в окне **«Настройки машины»** выбран пункт ***Аудит***). По двойному щелчку по событию в его описании можно увидеть:

1) регистрацию прохождения сетевых пакетов от ПЭВМ 2 к ПЭВМ 3 при фильтрации с учетом интерфейсов и генерации TCP пакетов на ПЭВМ 2 (рис. 3.25).



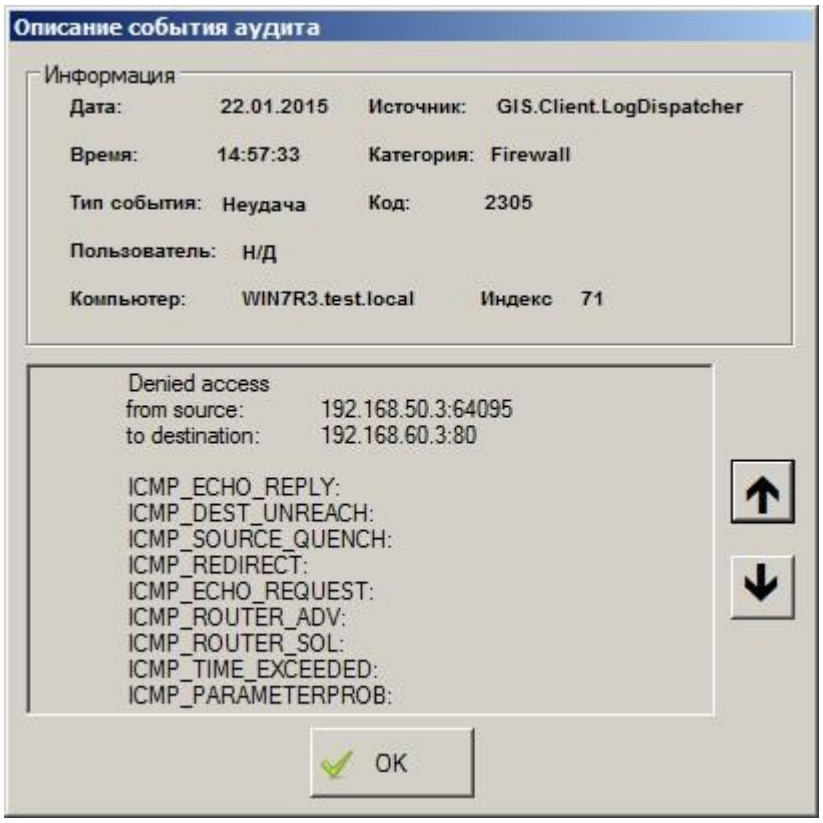
а)



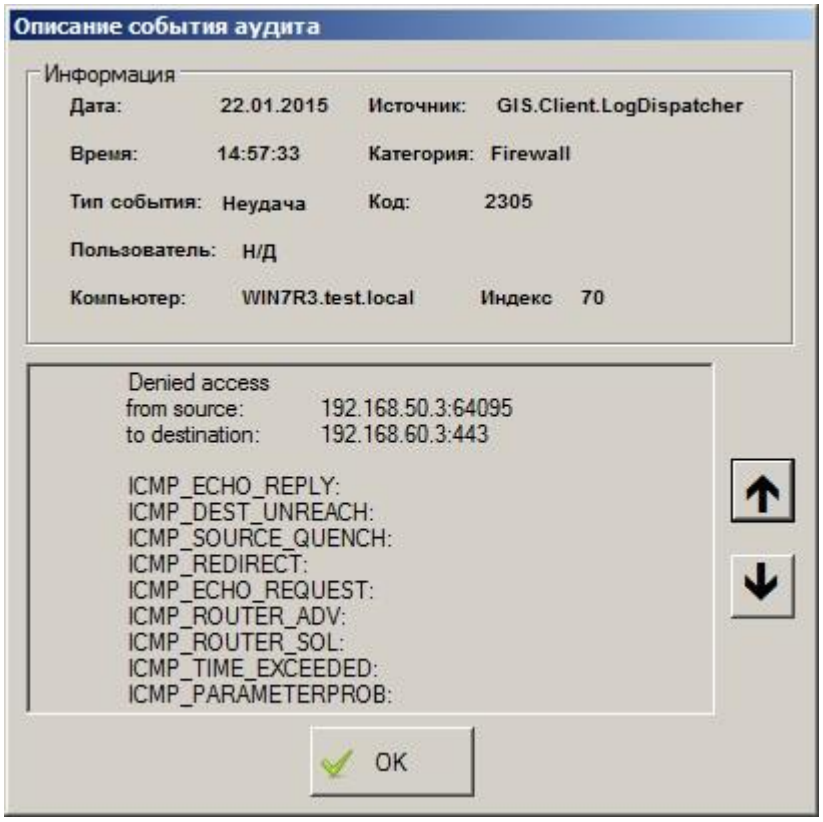
б)

Рисунок 3.25. Регистрация прохождения TCP пакетов при фильтрации с учетом интерфейсов

2) регистрацию блокировки сетевых пакетов от ПЭВМ 2 к ПЭВМ 3 при фильтрации с учетом интерфейсов и генерации TCP пакетов на ПЭВМ 4 (рис. 3.26):



а)



б)

Рисунок 3.26. Регистрация блокировки TCP пакетов при фильтрации с учетом интерфейсов

3.3.4 Настройки фильтрации с учетом значимых полей сетевых пакетов

Персональный МЭ позволяет осуществлять фильтрацию с учетом следующих значимых полей сетевых пакетов:

- номер порта;
- флаг TCP-протокола;
- время жизни сетевого пакета (TTL).

3.3.4.1 Настройка фильтрации по номеру порта

Фильтрацию с учетом поля ***Порт:*** рассмотрим на примере фильтрации протокола Telnet (протокол TCP, порт 23) в режиме, при котором разрешен обмен по протоколу Telnet только с ПЭВМ 2 (192.168.50.3) на ПЭВМ 3 (192.168.60.3).

В этом случае администратору безопасности в консоли администрирования СЗИ необходимо выполнить следующие настройки СЗИ для ПЭВМ 1:

1) в **Основной панели настроек клиентов** консоли администрирования для пользователя **User1** (пункт ***Персональный экран*** окна **«Настройки машины»**) при помощи кнопки ***Добавить***  добавить профиль персонального МЭ с именем *Profile4* со следующими параметрами:
   - выбрать значение ***Разрешительная политика***;
   - установить параметр ***Включить персональный экран***;
   - установить параметр ***Регистрировать разрешенные пакеты***;
   - установить параметр ***Регистрировать запрещенные пакеты***;
   - установить параметр ***Включить IGMP протокол***;
   - установить параметр ***Включить ICMP протокол***;
   - установить параметр ***Включить фильтрацию по типам ICMP протокола***;
   - установить параметр ***Включить регистрацию ICMP пакетов***;
   - в окне **«Настройки ICMP»** установить галочки для всех полей.
2) разрешить прохождение пакетов протокола Telnet от ПЭВМ 2 к ПЭВМ 3, для чего добавить в созданный профиль *Profile4* следующее правило фильтрации (рис. 3.27):
   - IP источника *192.168.50.3*;
   - порт источника *«*»*;
   - IP узла назначения *192.168.60.3*;
   - порт узла назначения *23*;
   - установить параметр ***Правило активно***;
   - установить параметр ***Аудит***;
   - нажать кнопку ***Сохранить***.

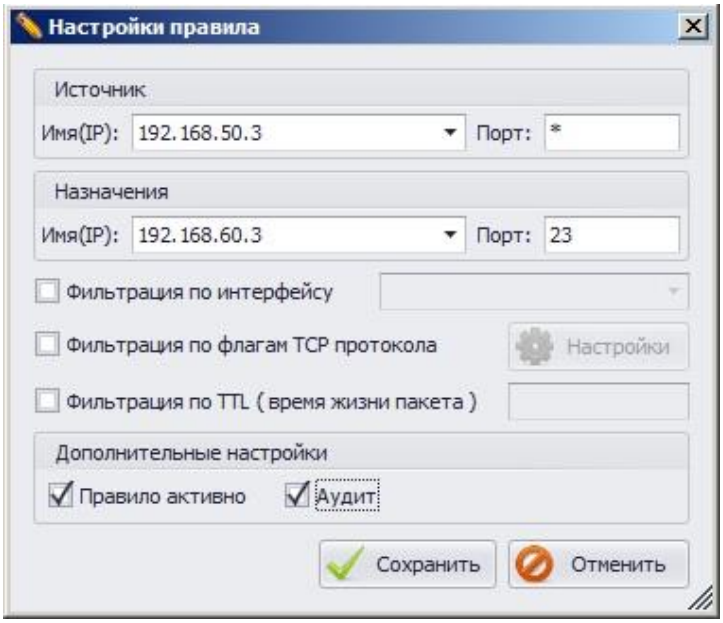


Рисунок 3.27. Правило фильтрации пакетов протокола Telnet от ПЭВМ 2 к ПЭВМ 3

3) в результате добавления этого правила автоматически будет создано правило, разрешающее прохождение TCP пакетов от ПЭВМ 3 к ПЭВМ 2 (в котором произведена замена установленных параметров узлов ***Источника*** и ***Назначения***). Добавленные правила фильтрации сетевых пакетов протокола Telnet отобразятся в консоли администрирования СЗИ:

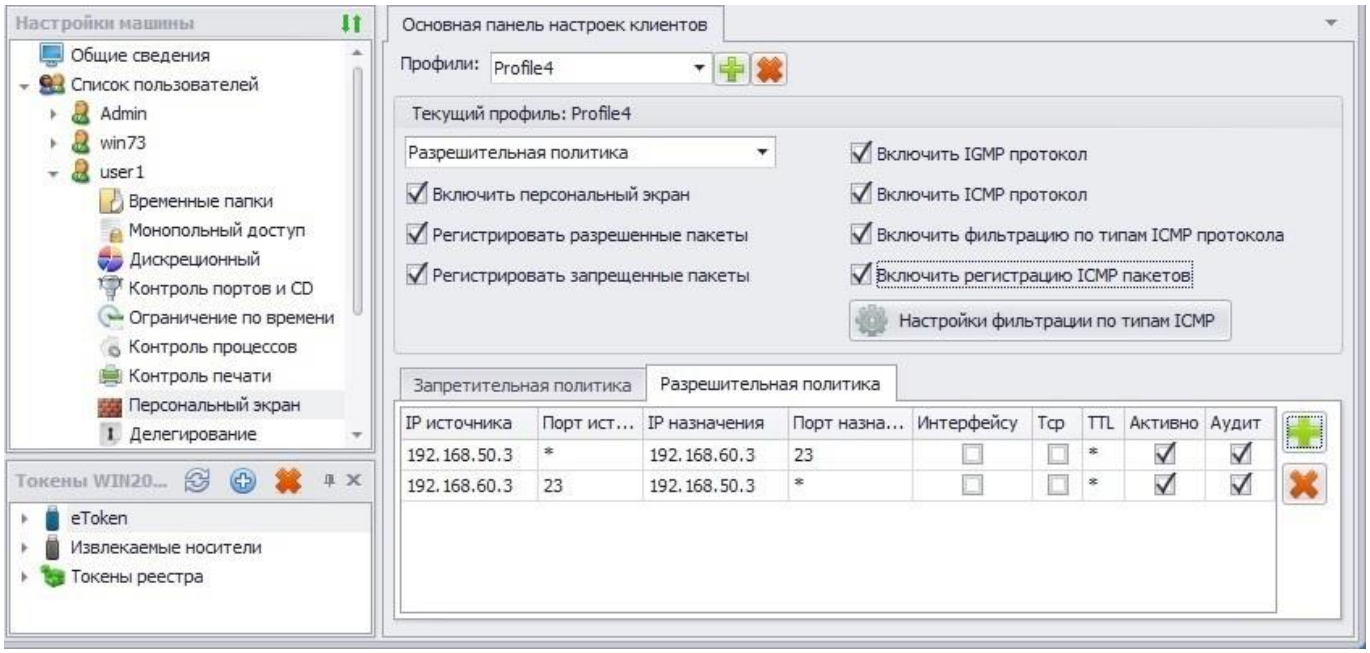


Рисунок 3.28. Правила фильтрации пакетов протокола Telnet

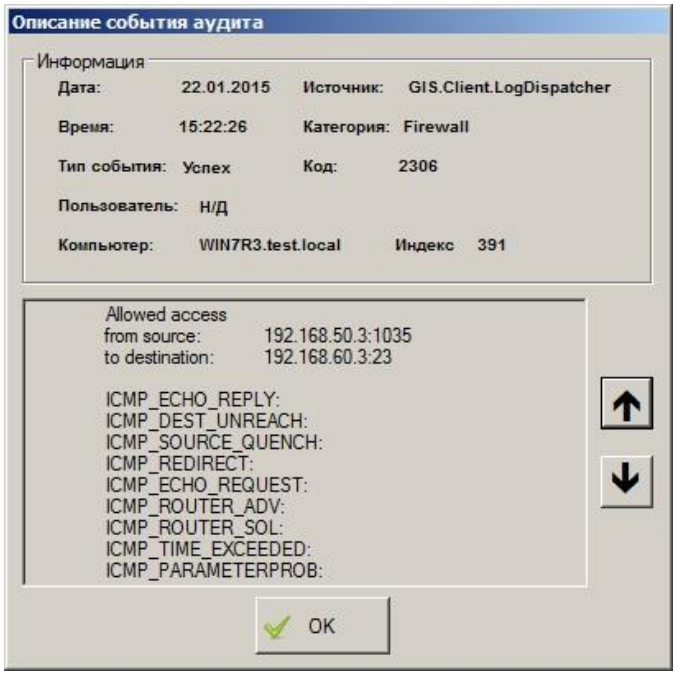
4) сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

После входа пользователя **User1** на ПЭВМ 1 фильтрация пакетов будет осуществляться следующим образом:

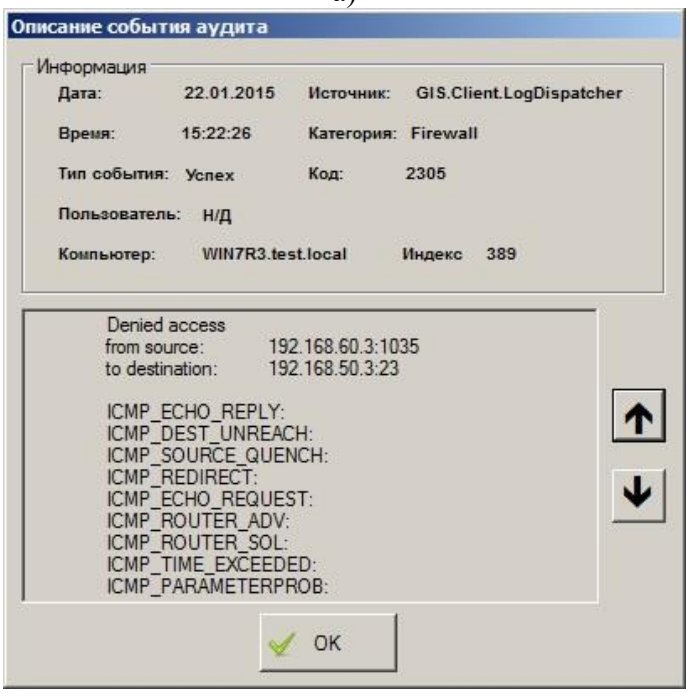
- прохождение пакетов по протоколу Telnet от ПЭВМ 2 к ПЭВМ 3 и обратно будет разрешено;
- прохождение пакетов по протоколу Telnet от ПЭВМ 2 к ПЭВМ 4 и обратно будет запрещено.

В журнале аудита СЗИ на ПЭВМ 1 фиксируются события прохождения/блокировки сетевого трафика (в консоли администрирования СЗИ в окне **«Список машин»** выбрана ПЭВМ 1, в окне **«Настройки машины»** выбран пункт ***Аудит***). По двойному щелчку по событию в его описании можно увидеть:

1) регистрацию прохождения пакетов протокола Telnet от ПЭВМ 2 к ПЭВМ 3 в рамках установленной TCP-сессии (рис. 3.29):



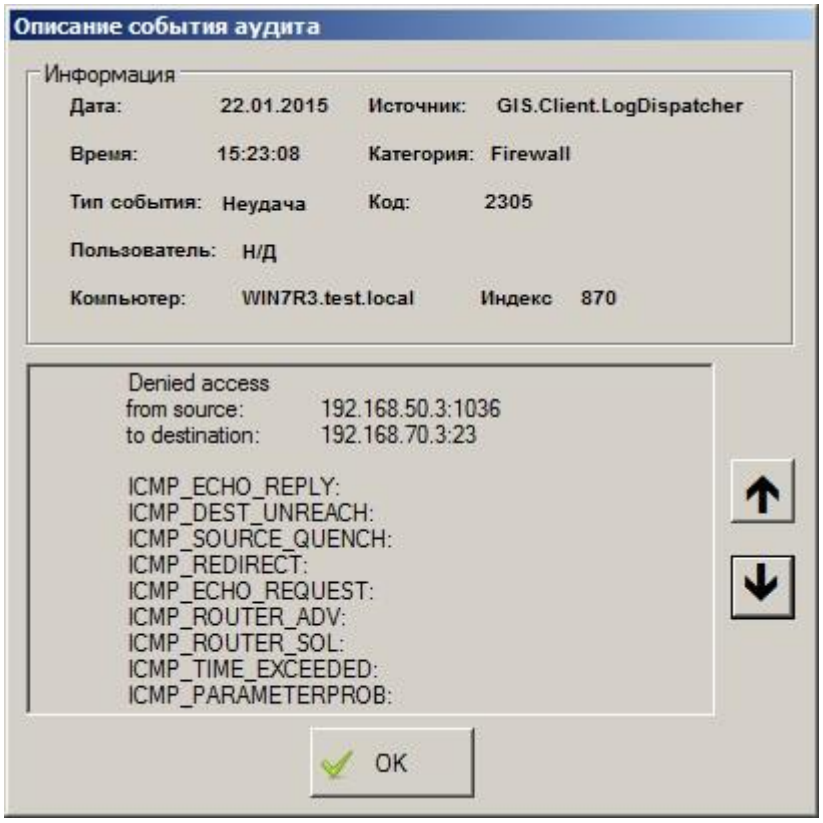
а)



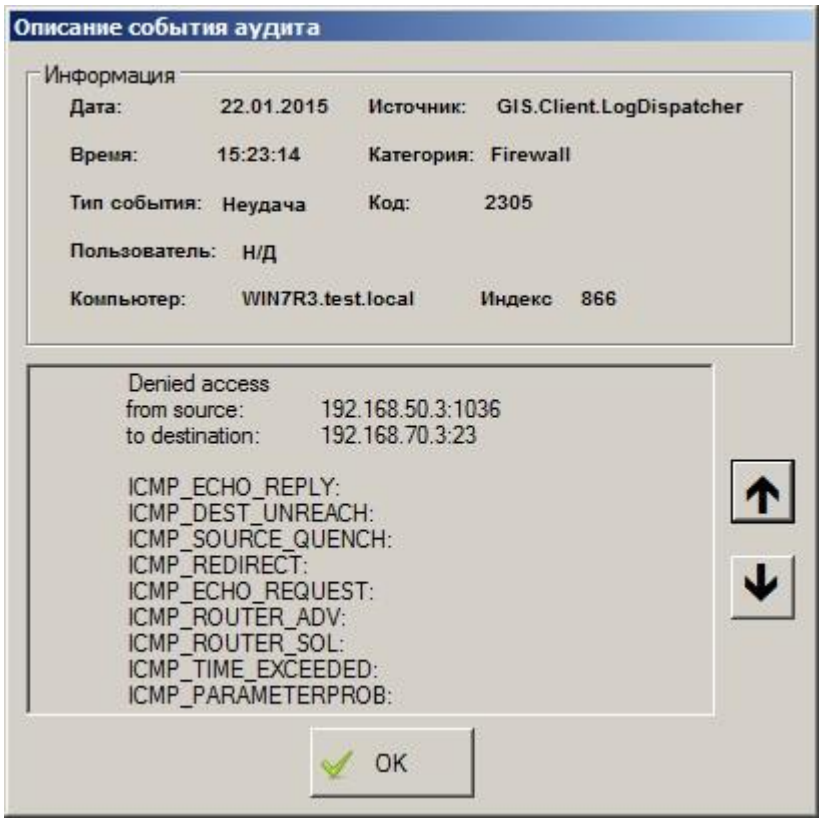
б)

Рисунок 3.29. Регистрация прохождения пакетов протокола Telnet от ПЭВМ 2 к ПЭВМ 3 в рамках установленной TCP-сессии

2) регистрацию блокировки пакетов протокола Telnet от ПЭВМ 2 к ПЭВМ 4 (рис. 3.30):



а)



б)

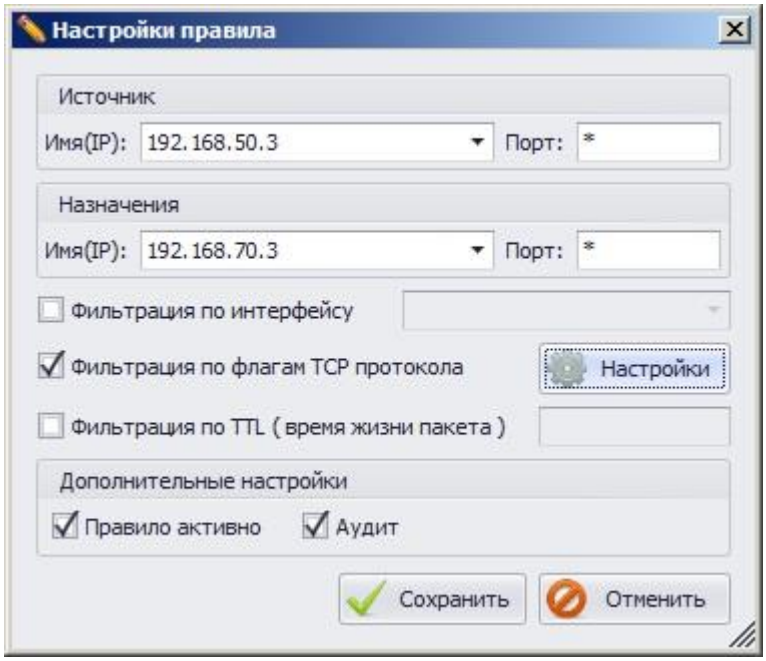
Рисунок 3.30. Блокировка сетевых пакетов от ПЭВМ 2 к ПЭВМ 4

3.3.4.2 Настройка фильтрации по флагам TCP протокола

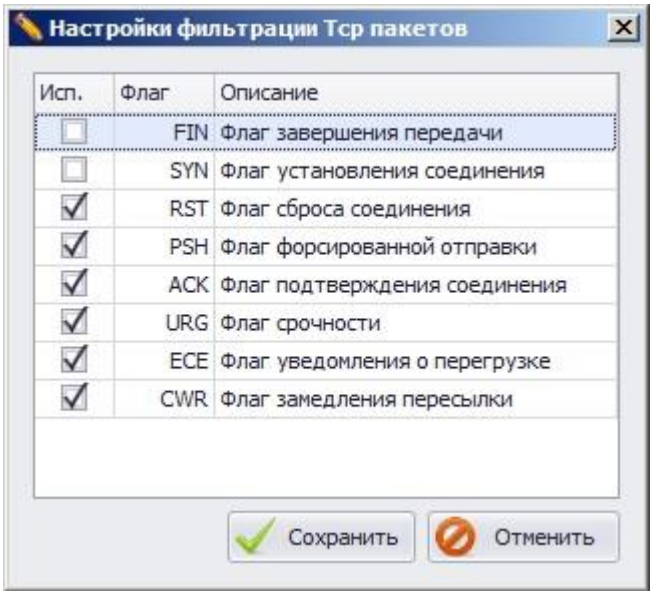
Фильтрацию с учетом флагов TCP-протокола рассмотрим на примере фильтрации между узлами сети ПЭВМ 2 (192.168.50.3) и ПЭВМ 4 (192.168.70.3), когда разрешено прохождение сетевых пакетов протокола TCP со всеми установленными флагами, за исключением флагов SYN и FIN.

Администратору безопасности необходимо выполнить в консоли администрирования СЗИ следующие настройки СЗИ для ПЭВМ 1:

1) в **Основной панели настроек клиентов** консоли администрирования для пользователя **User1** (пункт ***Персональный экран*** окна **«Настройки машины»**) при помощи кнопки ***Добавить*** добавить профиль персонального МЭ с именем *Profile5* со следующими параметрами:
   - выбрать значение ***Разрешительная политика***;
   - установить параметр ***Включить персональный экран***;
   - установить параметр ***Регистрировать разрешенные пакеты***;
   - установить параметр ***Регистрировать запрещенные пакеты***;
   - установить параметр ***Включить IGMP протокол***;
   - установить параметр ***Включить ICMP протокол***;
   - установить параметр ***Включить фильтрацию по типам ICMP протокола***;
   - установить параметр ***Включить регистрацию ICMP пакетов***;
   - в окне **«Настройки ICMP»** установить галочки для всех полей.
2) разрешить прохождение TCP-пакетов со всеми флагами, за исключением *FIN* и *SYN*, от ПЭВМ 2 к ПЭВМ 4. Для этого в консоли администрирования добавить в созданный профиль *Profile5* следующее правило фильтрации (рис. 3.31):
   - IP источника *192.168.50.3*;
   - порт источника *«*»*;
   - IP узла назначения *192.168.70.3*;
   - порт узла назначения *«*»*;
   - включить фильтрацию по флагам TCP протокола – нажать кнопку ***Настройки*** и, в открывшемся окне **«Настройки фильтрации TCP пакетов»**, отметить все флаги, за исключением флагов *FIN* и *SYN*;
   - установить параметр ***Правило активно***;
   - установить параметр ***Аудит***;
   - нажать кнопку ***Сохранить***.



а)



б)

Рисунок 3.31. Правило фильтрации пакетов по флагам TCP протокола от ПЭВМ 2 к ПЭВМ 4

3) в результате сохранения этого правила автоматически будет создано правило, разрешающее прохождение TCP пакетов от ПЭВМ 4 к ПЭВМ 2 (в котором произведена замена установленных параметров узлов ***Источника*** и ***Назначения***). Добавленные правила персонального МЭ отобразятся в консоли администрирования СЗИ (рис. 3.32).

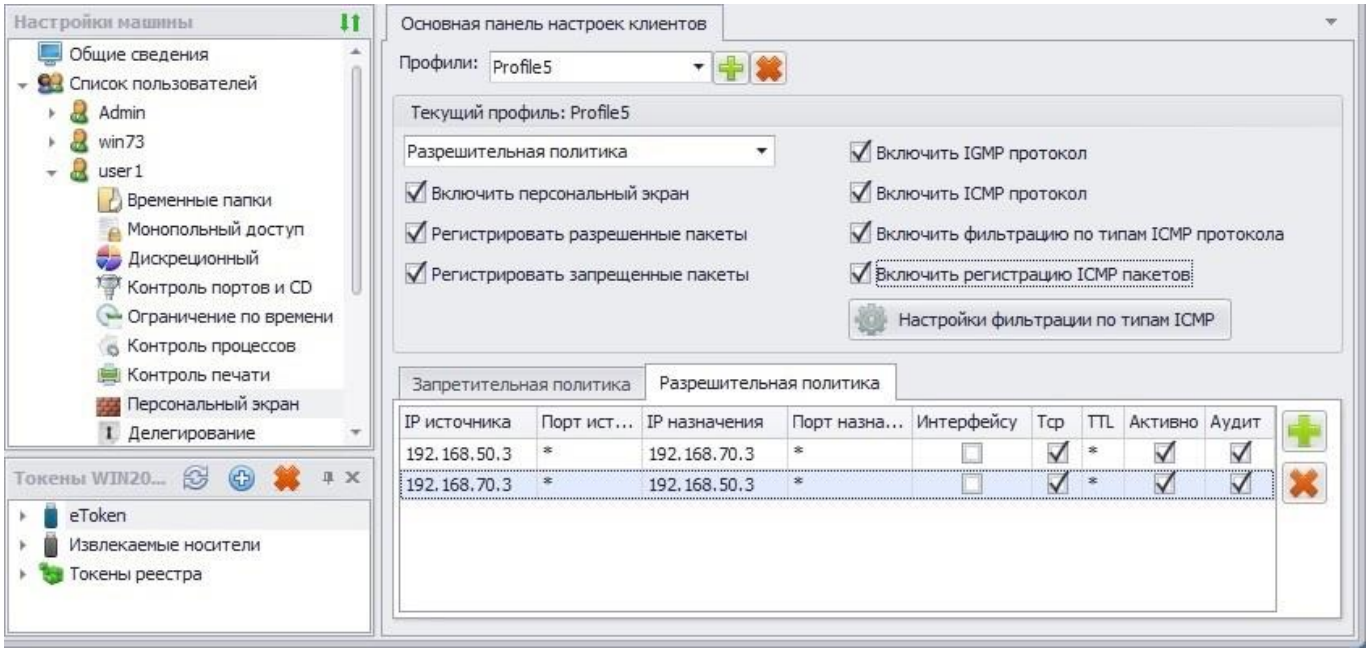


Рисунок 3.32. Правила фильтрации сетевых пакетов по флагам TCP протокола

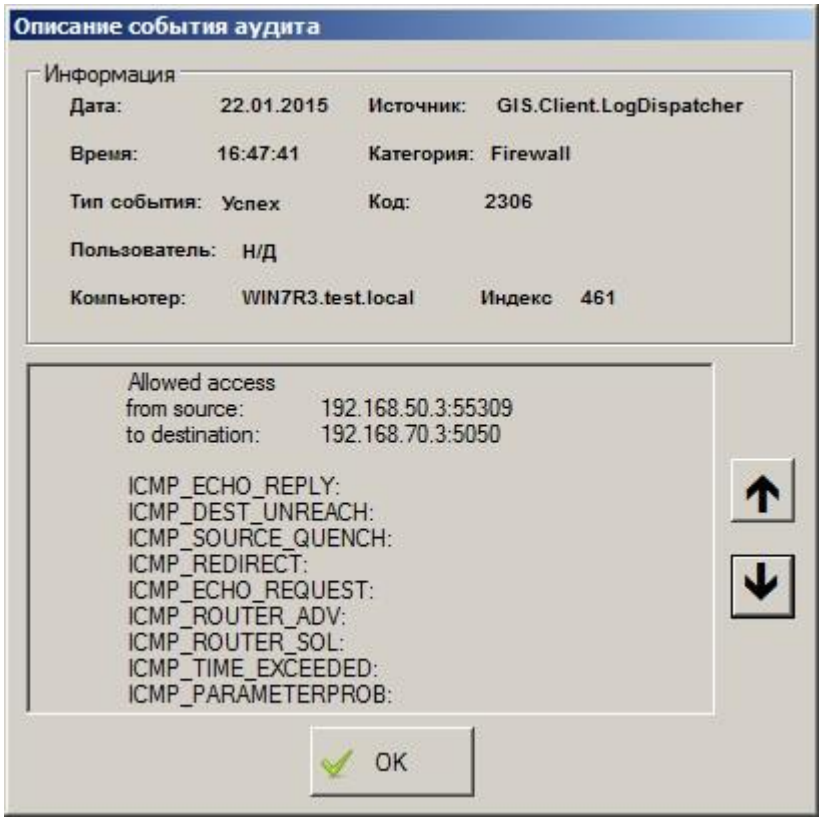
4) сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все*** , расположенной в левом верхнем углу консоли администрирования СЗИ.

После входа пользователя **User1** на ПЭВМ 1 фильтрация пакетов будет осуществляться согласно установленному правилу:

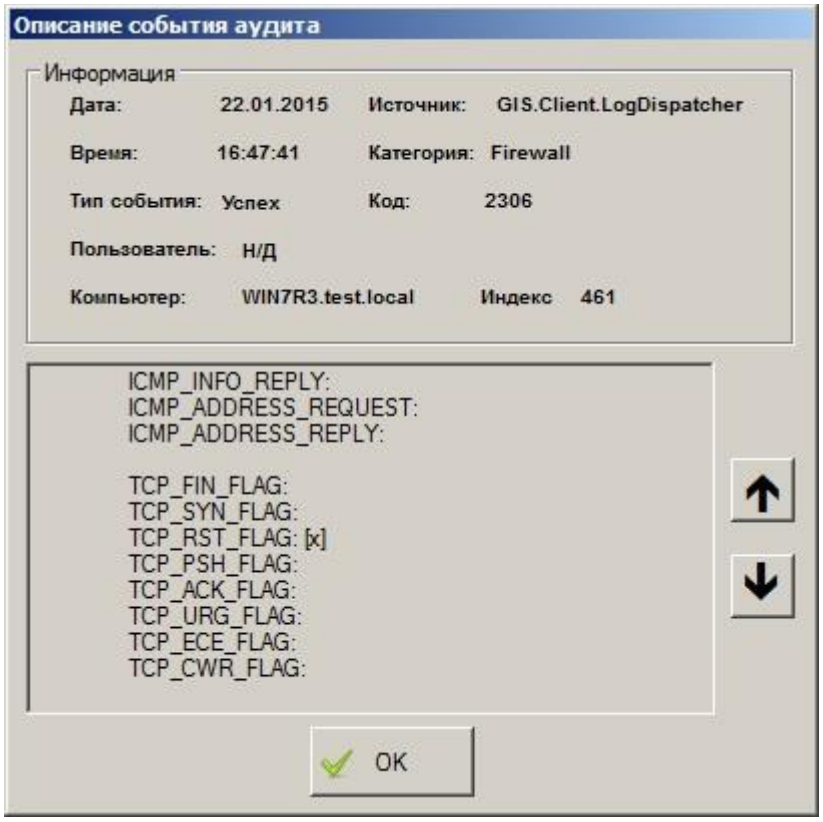
- от ПЭВМ 2 к ПЭВМ 4 и обратно будет разрешено прохождение TCP-пакетов со всеми флагами, за исключением *FIN* и *SYN*;
- прохождение TCP-пакетов с флагами *FIN* и *SYN* от ПЭВМ 2 к ПЭВМ 4 и обратно будет запрещено.

В журнале аудита СЗИ на ПЭВМ 1 фиксируются события прохождения/блокировки сетевого трафика (в консоли администрирования СЗИ в окне **«Список машин»** выбрана ПЭВМ 1, в окне **«Настройки машины»** выбран пункт ***Аудит***). По двойному щелчку по событию в его описании можно увидеть:

1) регистрацию прохождения TCP пакетов, например, с флагом *RST* от ПЭВМ 2 к ПЭВМ 4 (рис. 3.33):



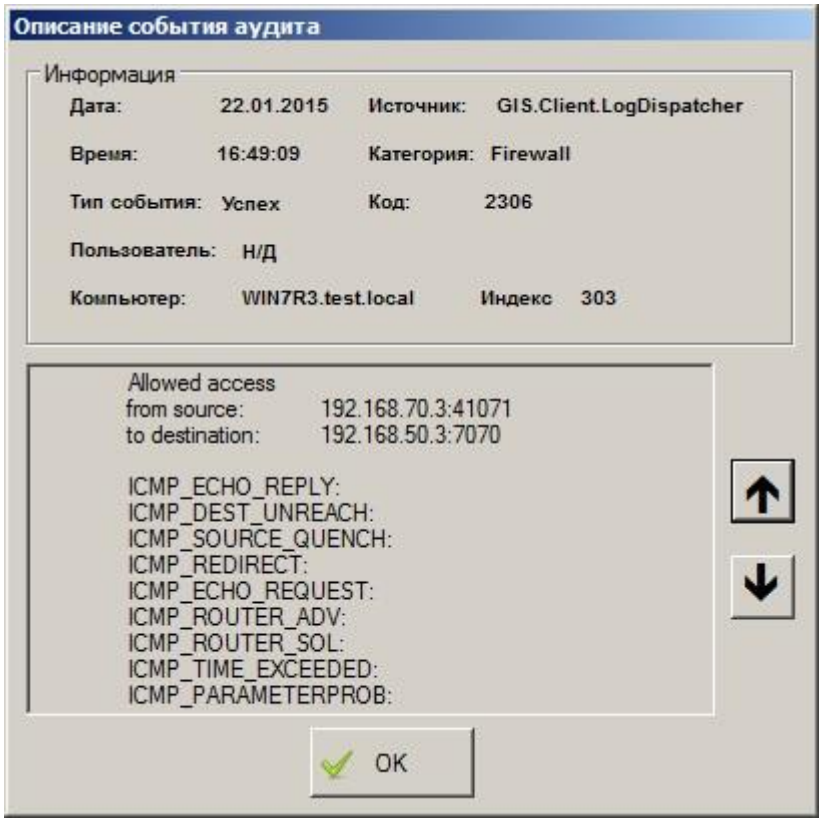
а)



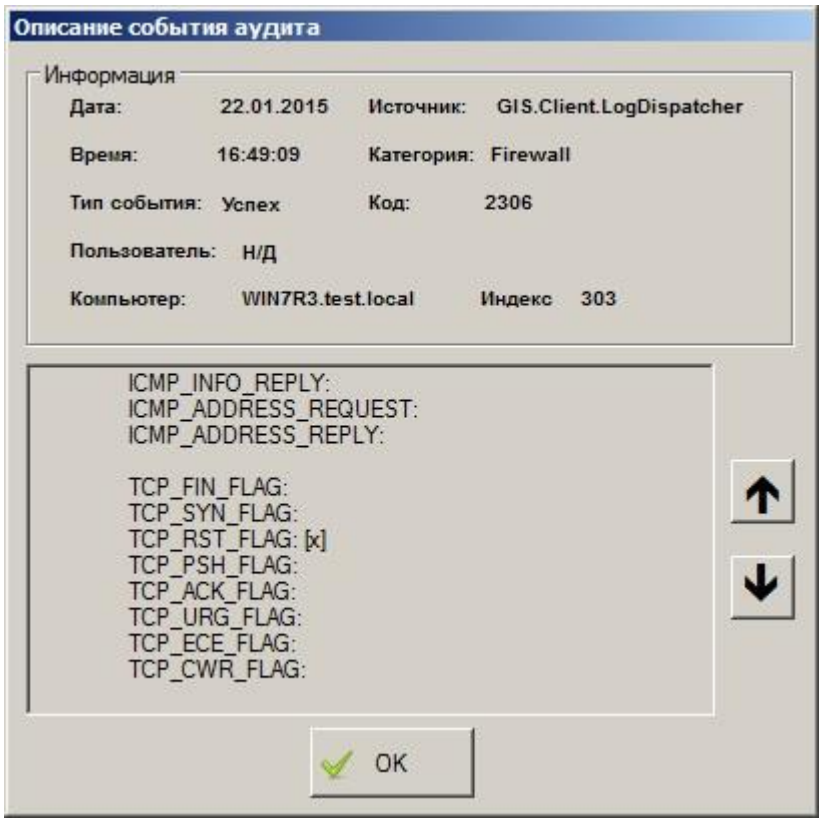
б)

Рисунок 3.33. Регистрация прохождения TCP пакетов с флагом «RST» от ПЭВМ 2 к ПЭВМ 4

2) регистрацию прохождения TCP пакетов, например, с флагом *RST* от ПЭВМ 4 к ПЭВМ 2 (рис. 3.34):



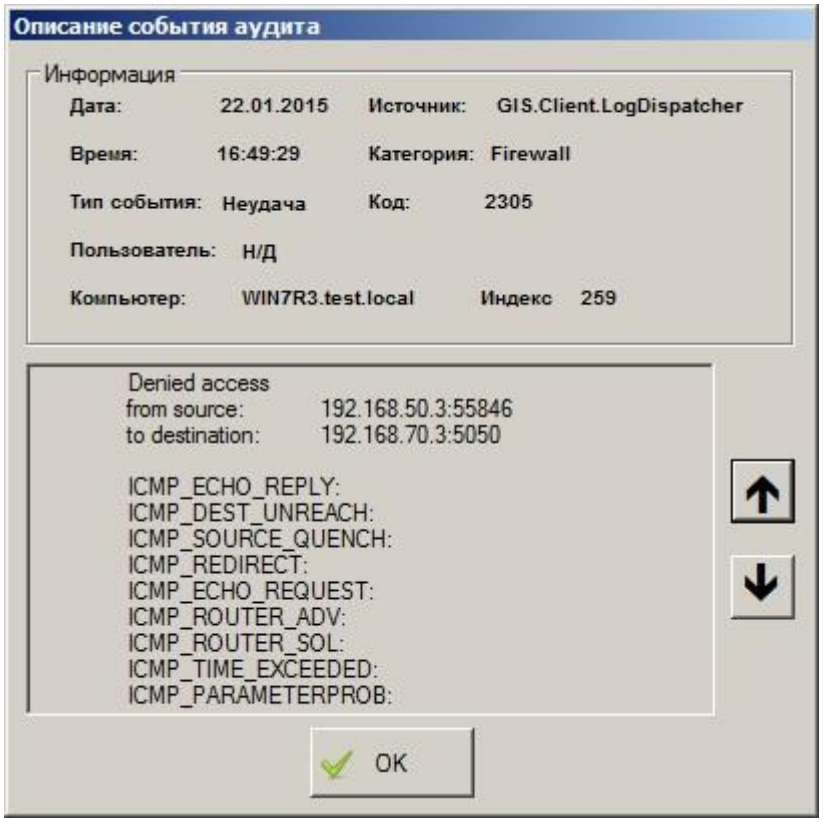
а)



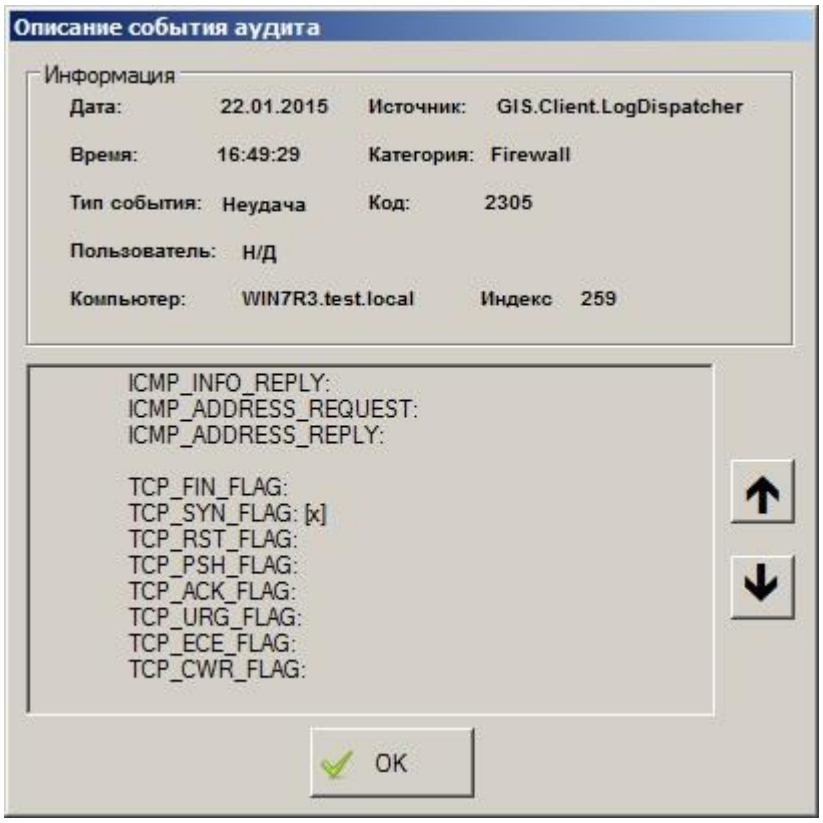
б)

Рисунок 3.34. Регистрация прохождения TCP пакетов с флагом «RST» от ПЭВМ 4 к ПЭВМ 2

3) регистрацию блокировки TCP пакетов с флагом *SYN* от ПЭВМ 2 к ПЭВМ 4 (рис. 3.35):



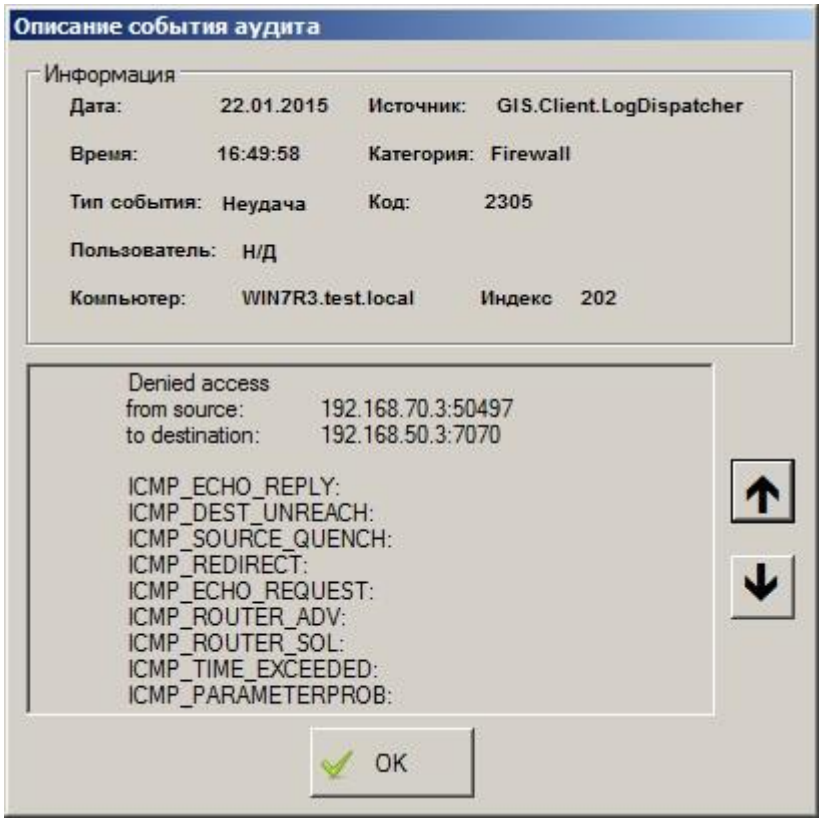
а)



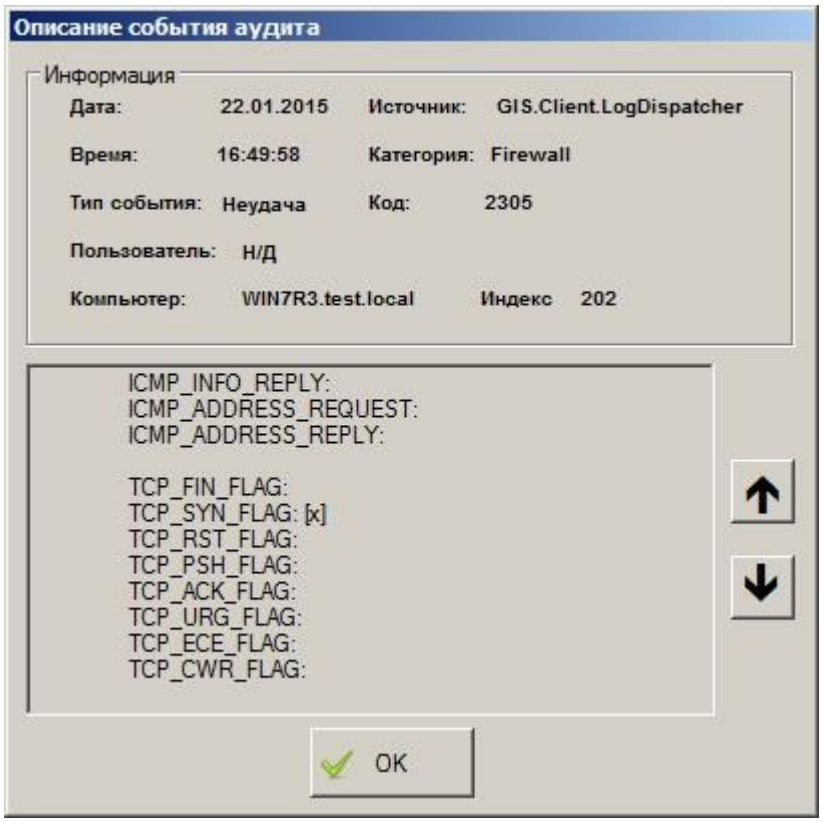
б)

Рисунок 3.35. Регистрация блокировки TCP пакетов с флагом «SYN» от ПЭВМ 2 к ПЭВМ 4

4) регистрацию блокировки TCP пакетов с флагом *SYN* от ПЭВМ 4 к ПЭВМ 2 (рис. 3.36):



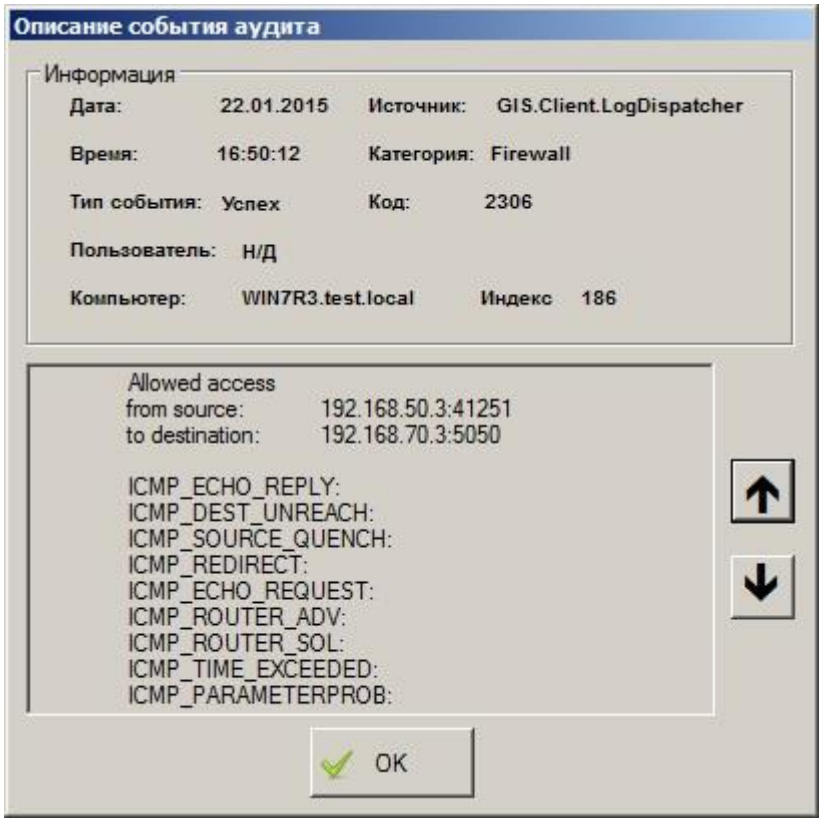
а)



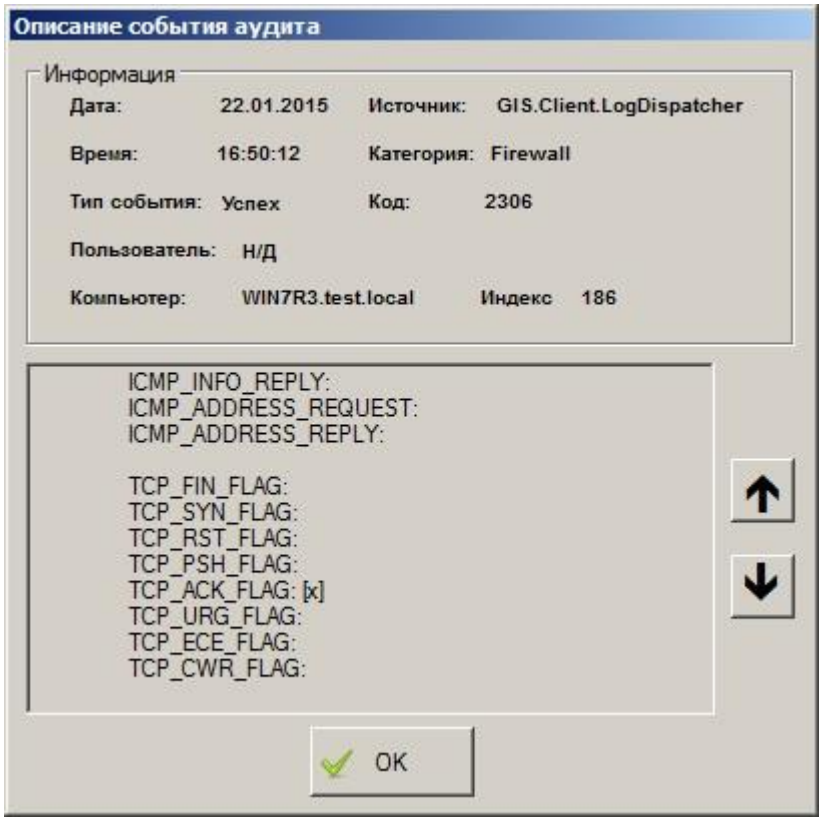
б)

Рисунок 3.36. Регистрация блокировки TCP пакетов с флагом «SYN» от ПЭВМ 4 к ПЭВМ 2

5) регистрацию прохождения TCP пакетов с флагом *ACK* от ПЭВМ 2 к ПЭВМ 4 (рис. 3.37):



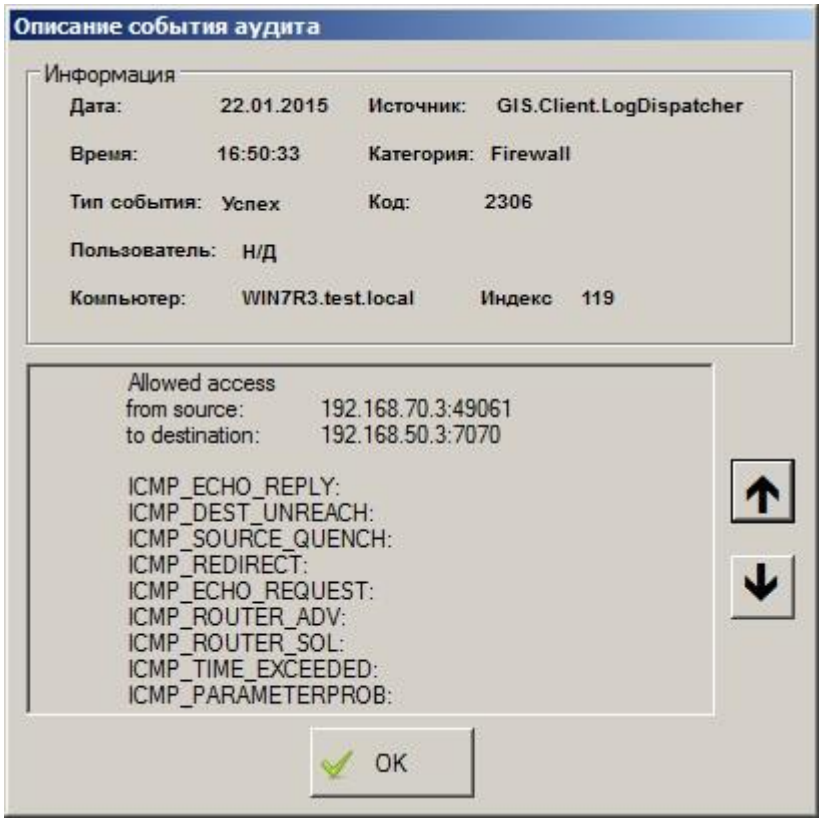
а)



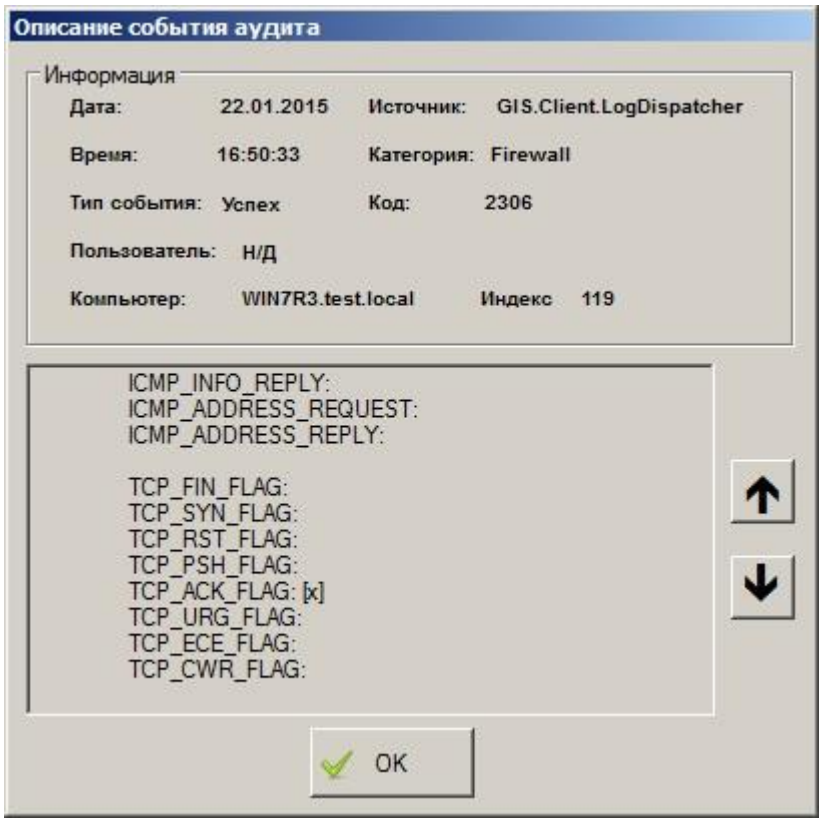
б)

Рисунок 3.37. Регистрация прохождения TCP пакетов с флагом «ACK» от ПЭВМ 2 к ПЭВМ 4

6) регистрацию прохождения TCP пакетов с флагом *ACK* от ПЭВМ 4 к ПЭВМ 2 (рис. 3.38):



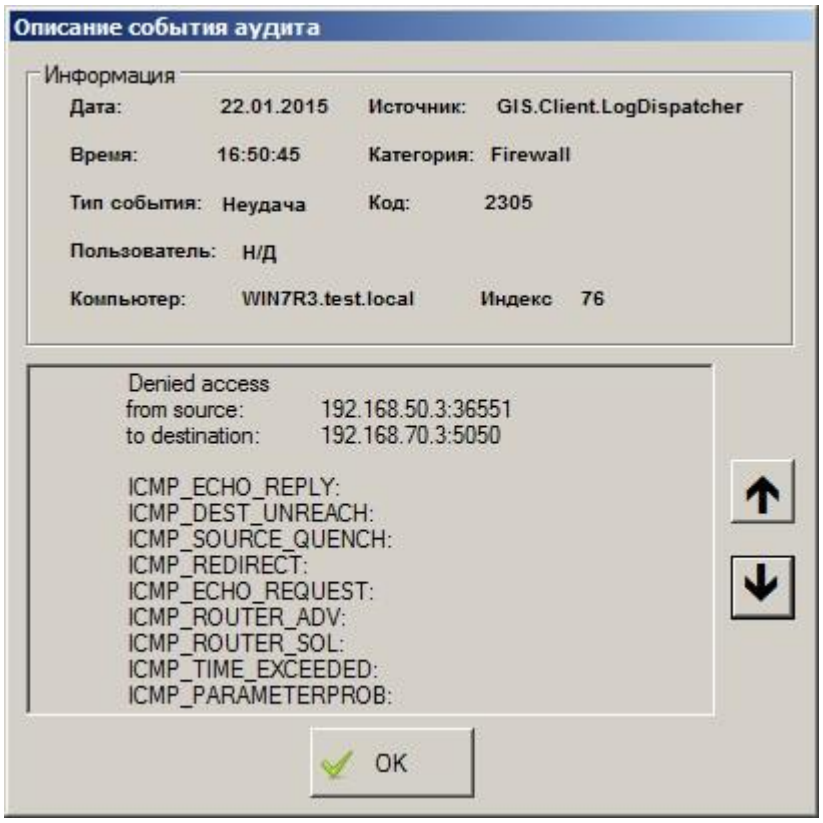
а)



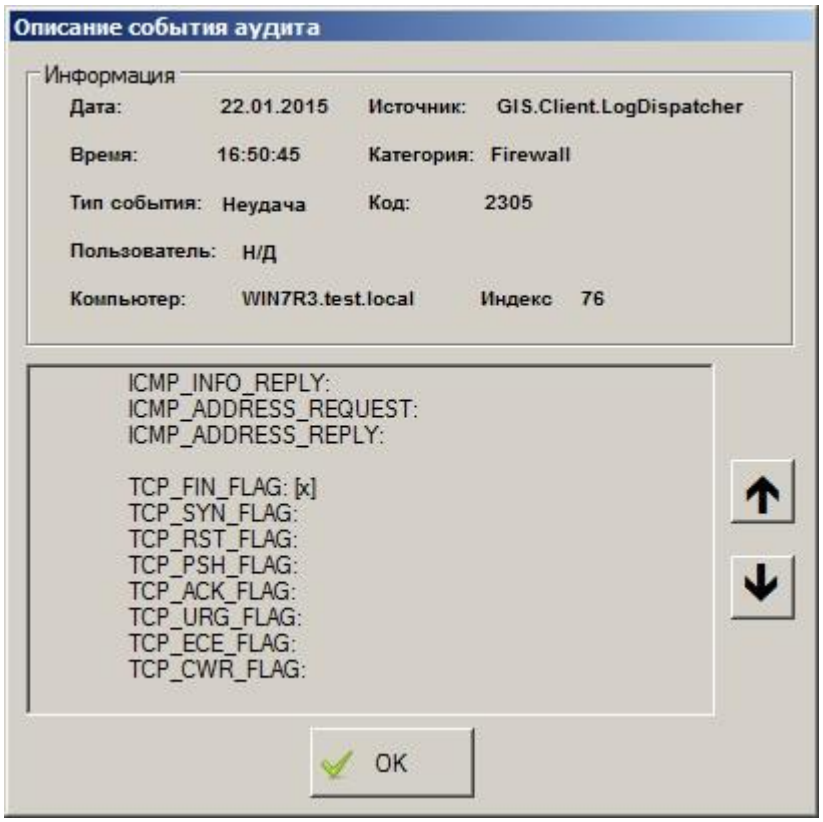
б)

Рисунок 3.38. Регистрация прохождения TCP пакетов с флагом «ACK» от ПЭВМ 4 к ПЭВМ 2

7) регистрацию блокировки TCP пакетов с флагом *FIN* от ПЭВМ 2 к ПЭВМ 4 (рис. 3.39):



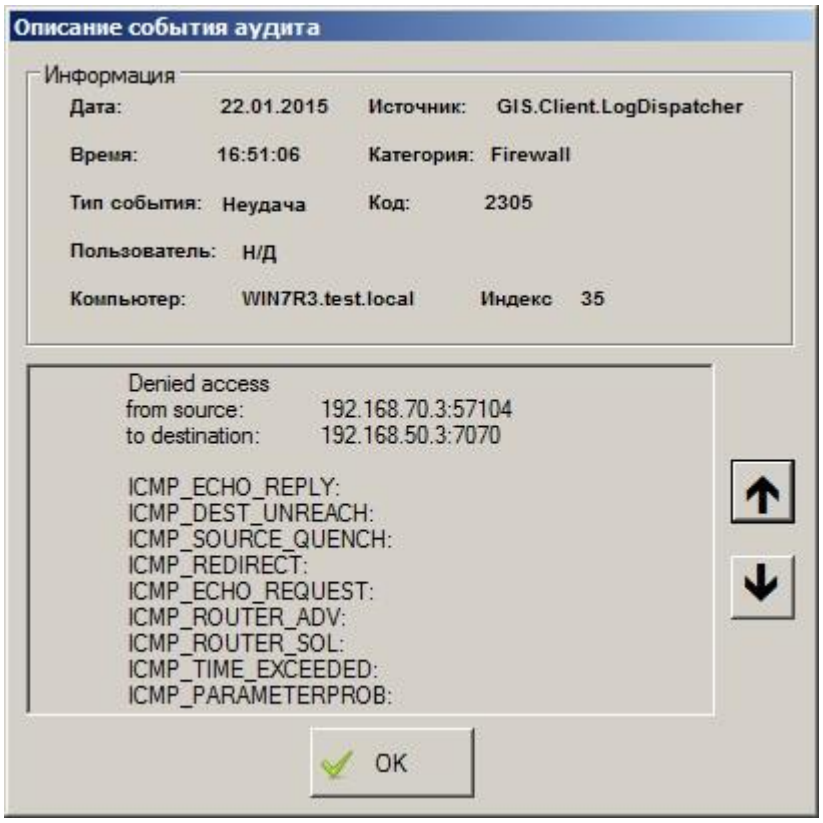
а)



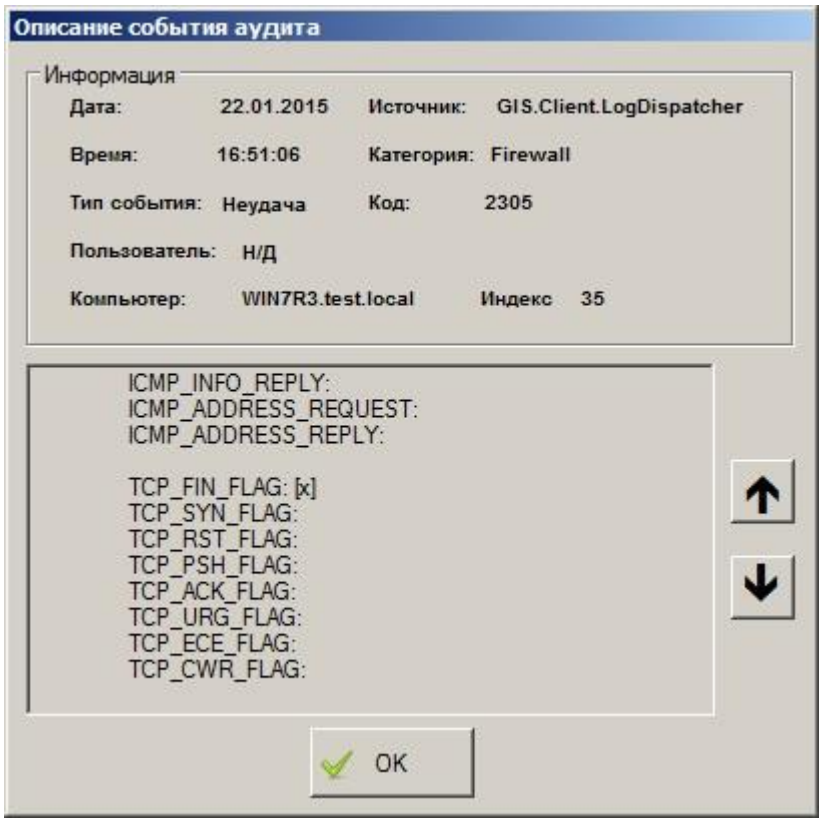
б)

Рисунок 3.39. Регистрация блокировки TCP пакетов с флагом «FIN» от ПЭВМ 2 к ПЭВМ 4

8) регистрацию блокировки TCP пакетов с флагом *FIN* от ПЭВМ 4 к ПЭВМ 2 (рис. 3.40):



а)



б)

Рисунок 3.40. Регистрация блокировки TCP пакетов с флагом «FIN» от ПЭВМ 4 к ПЭВМ 2

3.3.4.3 Настройка фильтрации по времени жизни пакета (TTL)

Фильтрацию с учетом поля ***Фильтрация по TTL (время жизни пакета)*** TCP-протокола рассмотрим на примере фильтрации IP-пакетов между узлами сети ПЭВМ 3 (192.168.60.3) и ПЭВМ 4 (192.168.70.3). Прохождение пакетов, имеющих в IP-заголовке значение ***TTL***, равное *30*, (созданных с использованием программы **nmap** с параметрами *-ttl <30> -pT44,99 -PN <ip-адрес получателя>*) разрешено, прохождение пакетов, имеющих значение ***TTL***, отличное от *30*, запрещено.

Администратору безопасности в консоли администрирования СЗИ необходимо создать соответствующее правило:

1) в **Основной панели настроек клиентов** консоли администрирования для пользователя **User1** (пункт ***Персональный экран*** окна **«Настройки машины»**) при помощи кнопки ***Добавить***  добавить профиль персонального МЭ с именем *Profile6* со следующими параметрами:
   - выбрать значение ***Разрешительная политика***;
   - установить параметр ***Включить персональный экран***;
   - установить параметр ***Регистрировать разрешенные пакеты***;
   - установить параметр ***Регистрировать запрещенные пакеты***;
   - установить параметр ***Включить IGMP протокол***;
   - установить параметр ***Включить ICMP протокол***;
   - установить параметр ***Включить фильтрацию по типам ICMP протокола***;
   - установить параметр ***Включить регистрацию ICMP пакетов***;
   - в окне **«Настройки ICMP»** установить галочки для всех полей.
2) разрешить прохождение сетевых пакетов с ***TTL****=30* от ПЭВМ 3 к ПЭВМ 4, для чего добавить в созданный профиль *Profile6* следующее правило фильтрации (рис. 3.41):
   - IP источника *192.168.60.3*;
   - порт источника *«*»*;
   - IP узла назначения *192.168.70.3*;
   - порт узла назначения *«*»*;
   - включить фильтрацию по полю ***Фильтрация по TTL (время жизни пакета)*** и установить значение поля *30*;
   - установить параметр ***Правило активно***;
   - установить параметр ***Аудит***;
   - нажать кнопку ***Сохранить***.

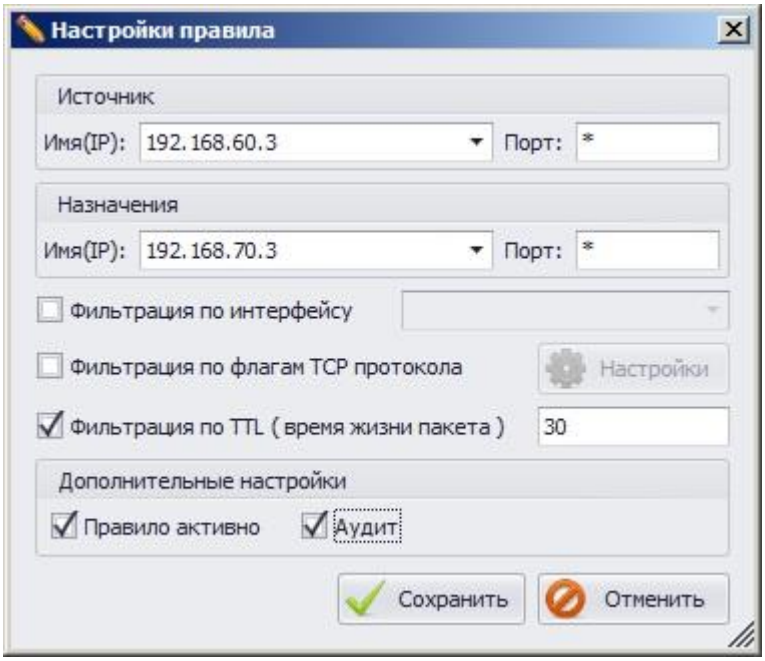


Рисунок 3.41. Правило фильтрации пакетов с TTL=30 от ПЭВМ 3 к ПЭВМ 4

3) разрешить прохождение ответных пакетов от ПЭВМ 4 к ПЭВМ 3, для чего изменить в профиле *Profile6* созданное автоматически при сохранении правила фильтрации пакетов от ПЭВМ 3 к ПЭВМ 4, обратное ему правило фильтрации, изменив параметры поля ***Фильтрация по TTL (время жизни пакета)*** (рис. 3.42):
   - ввести в поле ***Фильтрация по TTL (время жизни пакета)*** значение *128*, как разрешенное для прохождения. В рассматриваемом примере для получения ответного трафика необходимо разрешить прохождение ICMP пакетов с значением поля ***TTL***, равным *128*, так как при формировании эхо-ответов (Echo-Reply) на посланные эхо-запросы (Echo-Request) опрашиваемая станция (ПЭВМ 4) по умолчанию устанавливает значение ***TTL*** = *128*.
   - нажать кнопку ***Сохранить***.

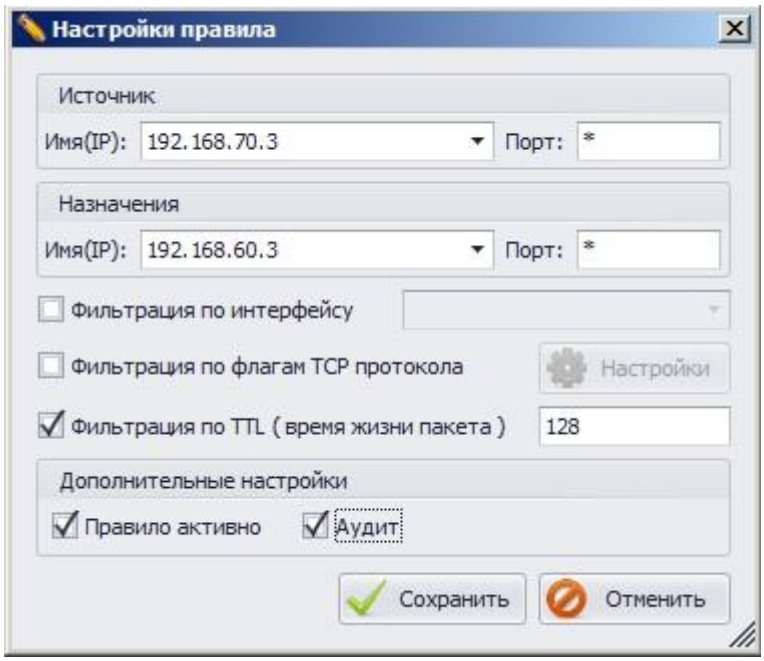


Рисунок 3.42. Правило фильтрации ответных пакетов с ПЭВМ 4 на ПЭВМ 3

Добавленные правила персонального МЭ отобразятся в консоли администрирования СЗИ (рис. 3.43).

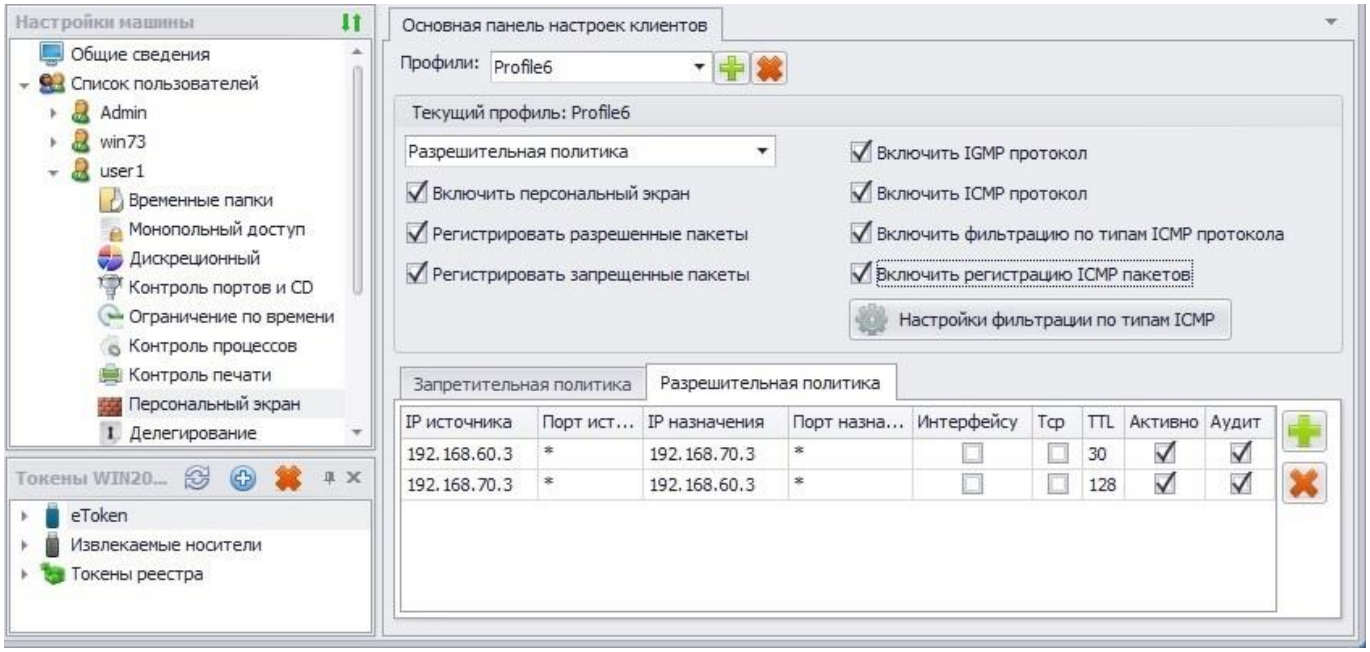


Рисунок 3.43. Правила фильтрации сетевых пакетов по полю «TTL»

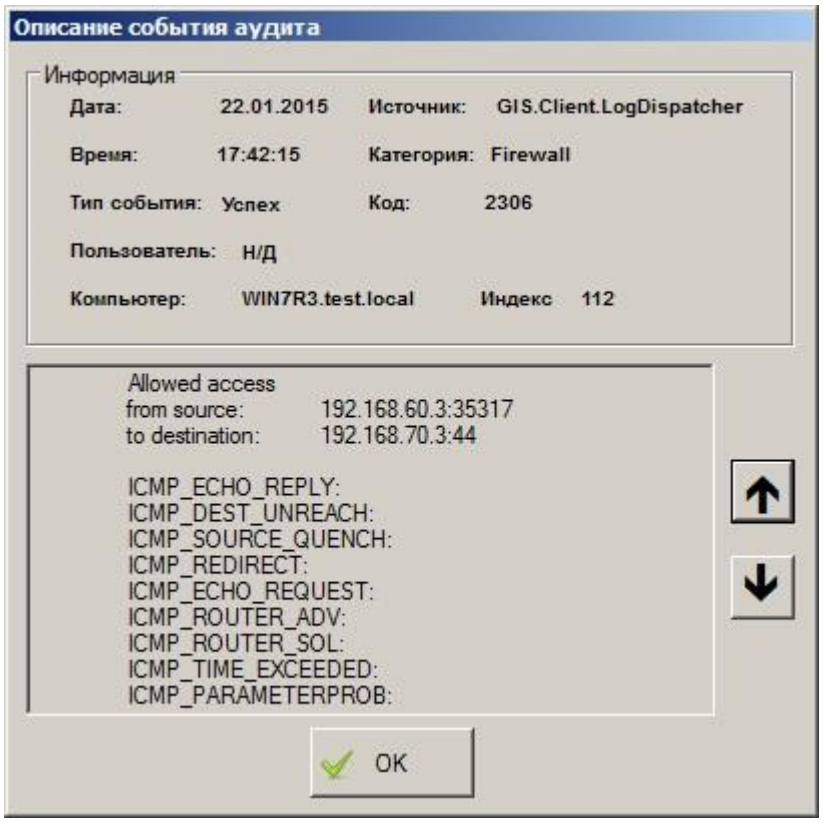
4) сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

После входа пользователя **User1** на ПЭВМ 1 фильтрация сетевого трафика будет осуществляться в соответствии с созданным правилом:

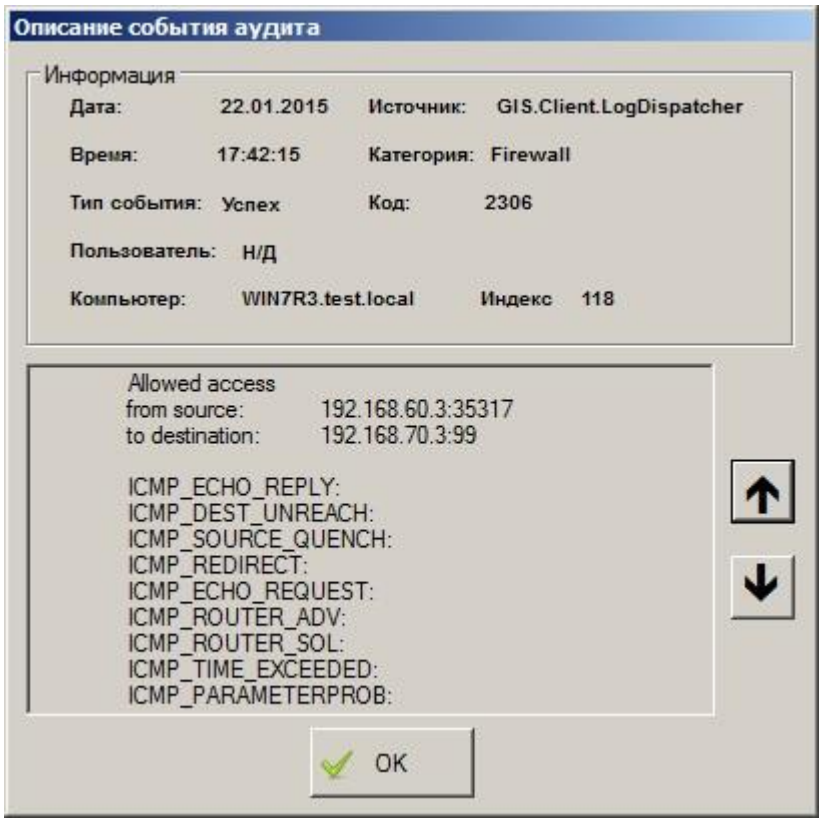
1) пакеты со значением ***TTL*** равным *30* будут разрешены к прохождению с ПЭВМ 3 на ПЭВМ 4;
2) пакеты от ПЭВМ 3 к ПЭВМ 4 со значением ***TTL*** отличным от 30 будут блокироваться.

В журнале аудита СЗИ на ПЭВМ 1 фиксируются события прохождения/блокировки сетевого трафика (в консоли администрирования СЗИ в окне **«Список машин»** выбрана ПЭВМ 1, в окне **«Настройки машины»** выбран пункт ***Аудит***). По двойному щелчку по событию в его описании можно увидеть:

1) регистрацию прохождения пакетов протокола IP со значением поля ***TTL*** = *30* от ПЭВМ 3 к ПЭВМ 4 (рис. 3.44):



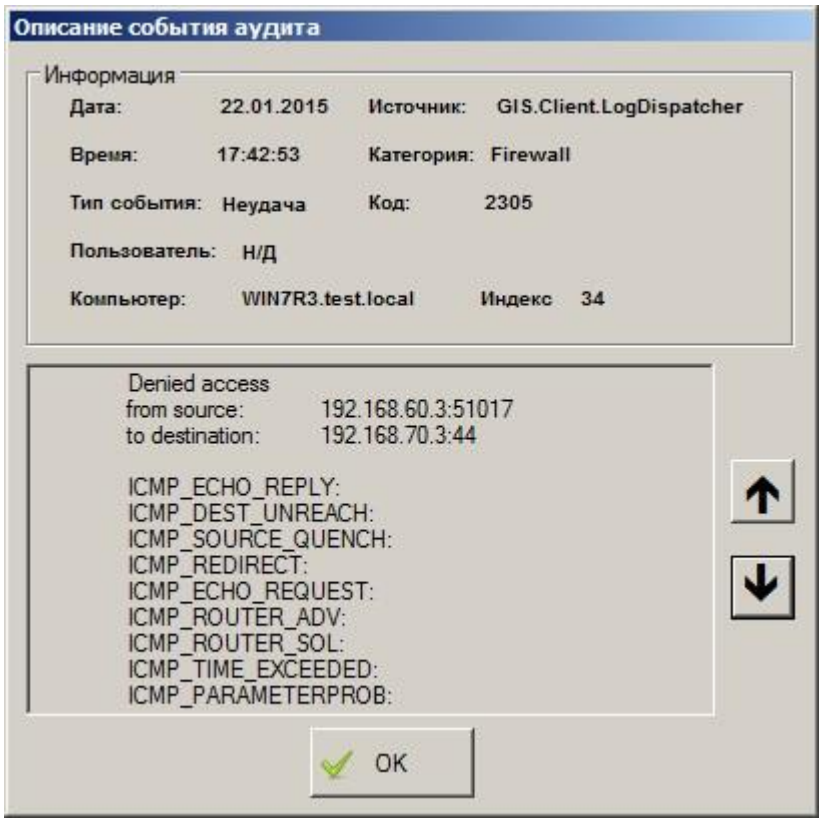
а)



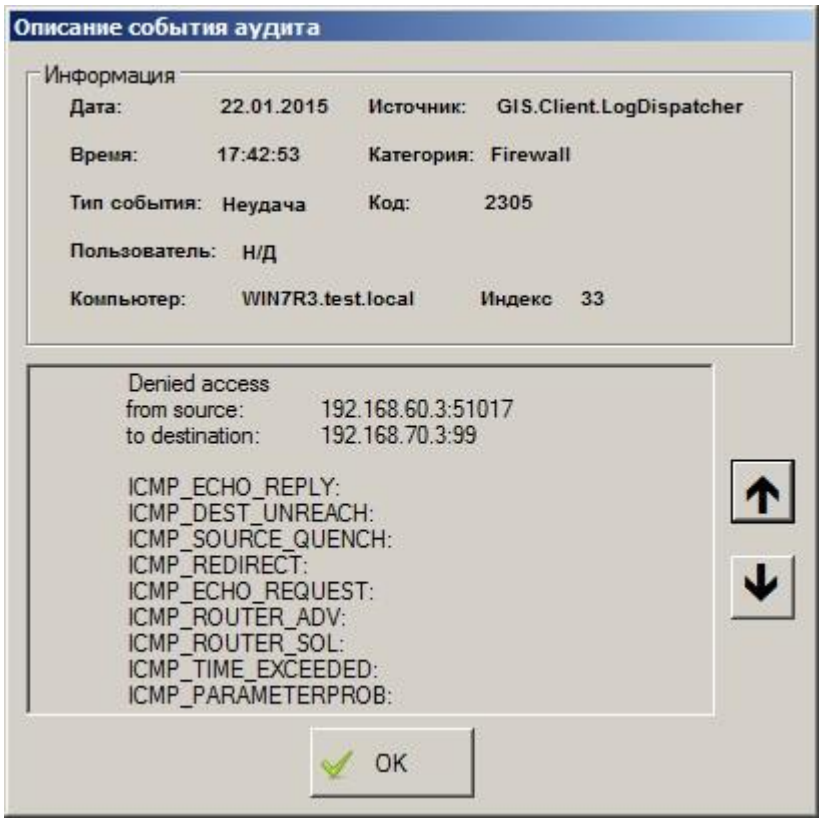
б)

Рисунок 3.44. Регистрация прохождения пакетов протокола IP со значением поля TTL = 30 от ПЭВМ 3 к ПЭВМ 4

2) регистрацию блокировки пакетов протокола IP со значением поля ttl, отличным от 30, от ПЭВМ 3 к ПЭВМ 4 (рис. 3.45):



а)



б)

Рисунок 3.45. Регистрация блокировки пакетов протокола IP со значением поля TTL, отличным от 30, от ПЭВМ 3 к ПЭВМ 4

4. Описание старта персонального МЭ и процедур проверки правильности старта

Модуль персонального экрана СЗИ «Блокхост-сеть 2.0» стартует при загрузке ОС. Модуль загружается после драйвера NDIS, но до регистрации сетевых протоколов. В момент входа пользователя в систему драйверу персонального экрана от модуля идентификации и аутентификации СЗИ приходит конфигурация настроек, согласно которой выполняется дальнейшая фильтрация сетевого трафика. Драйвер персонального экрана регистрируется на этапе инициализации как драйвер-фильтр интерфейса NDIS 6, настраиваются функции обратного вызова, которые гарантируют присоединение фильтра к любому существующему или вновь появляющемуся в системе сетевому адаптеру. В дальнейшем для каждого такого адаптера фильтром обрабатывается любая сетевая активность указанного устройства.

Каждый драйвер персонального МЭ подписан доверенным сертификатом компании ООО «Газинформсервис», который включен в список доверенных распространителей системного ПО компании Verisign и Microsoft. Корректность проверки ЭП гарантирует целостность программной и информационной части ПЭ. Проверка ЭП выполняется автоматически средствами ОС при установке СЗИ «Блокхост-сеть 2.0» и каждый раз при запуске драйвера. Драйвер, подпись которого не была проверена или целостность исполняемого образа которого была нарушена, не будет загружен ОС.

Проверка правильности старта модуля персонального МЭ выполняется следующими способами:

1) вручную – с помощью команды *sc query DrvFltIP* (рис. 4.1). Драйвер персонального МЭ, загруженный корректно, будет иметь соответствующий статус *RUNNING*. Если отображается статус *STOPPED* – драйвер загружен не был.

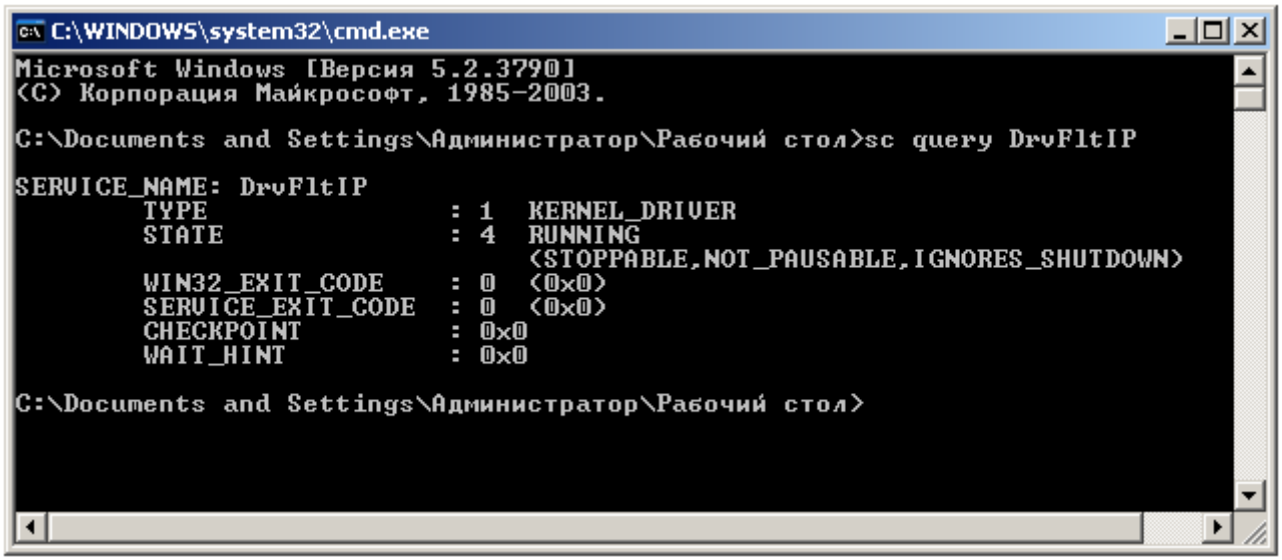


Рисунок 4.1. Проверка старта драйвера персонального экрана при помощи команды sc query DrvFltIP

2) при входе пользователя в систему может появиться сообщение, показанное на рисунке 4.2. Необходимо в окне **«Запуск драйвера firewall»** нажать кнопку ***ОК***, затем войти в ОС от имени учетной записи встроенного администратора и восстановить драйвер способами, приведенными в разделе 5 настоящего руководства.

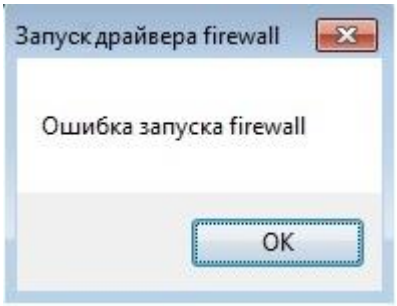


Рисунок 4.2. Ошибка запуска драйвера МЭ в ОС Windows 7

Если драйвер персонального МЭ не был загружен или был загружен некорректно, следует выполнить вход в систему от имени администратора рабочей станции (пользователя с правами администратора) и восстановить драйвер в последовательности, приведенной в разделе 5.

4.1 Автоматический контроль целостности персонального МЭ средствами СЗИ «Блокхост-сеть 2.0»

Контроль целостности персонального МЭ может быть выполнен модулем контроля целостности GIS.Client.IntegrityChecker.exe из состава СЗИ «Блокхост-сеть 2.0». Для этого администратору безопасности в серверной консоли администрирования необходимо:

1) в окне **«Список машин»**, раскрыв пункт ***Все машины***, выбрать рабочую станцию, для которой будет производиться настройка механизма контроля целостности;
2) в окне **«Настройки машины»** выбрать пункт ***Контроль целостности***.
3) в **Основной панели настроек клиента** включить механизм контроля целостности, выбрав пункт ***Включить контроль целостности*** (рис. 4.3)**;**
4) задать интервал контроля целостности (период проверки контрольных сумм), указав в поле ввода ***Периодичность контроля*** соответствующее значение. Можно оставить значение, указанное по умолчанию – 6 секунд;

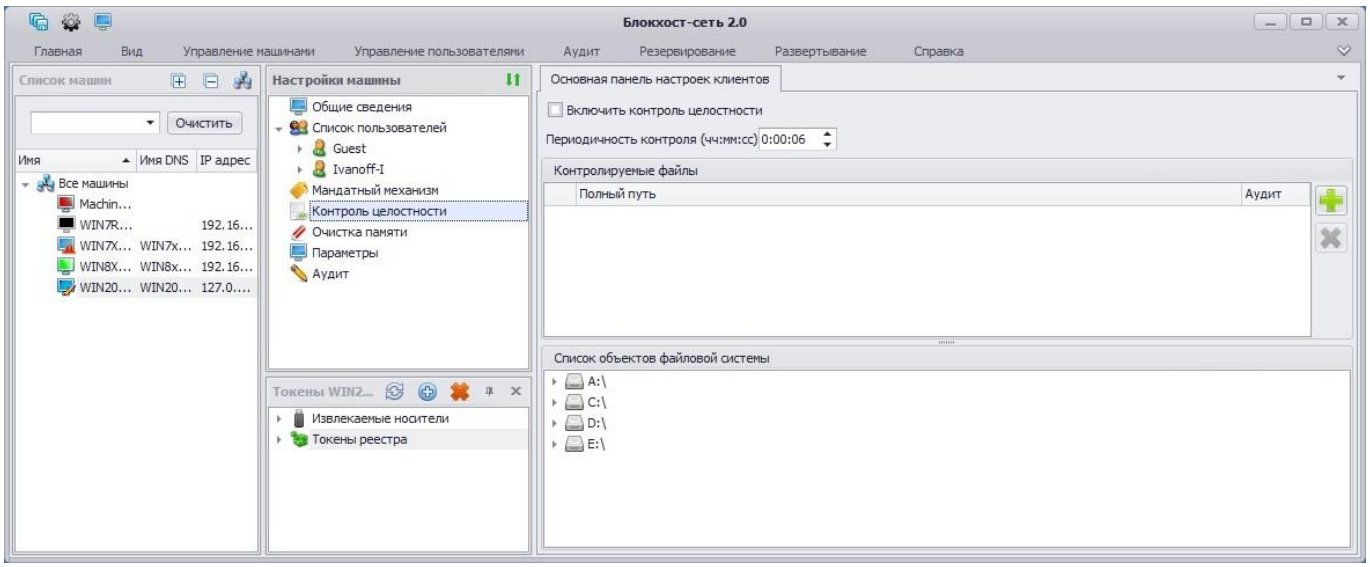


Рисунок 4.3. Настройка механизма контроля целостности

5) в **Основной панели настроек клиента**, раскрыв дерево списка объектов файловой системы, добавить файловые объекты на контроль. Добавление выполняется путем перетаскивания выбранного файла из области списка объектов в область контролируемых файлов. Необходимо добавить следующие объекты:

- C:\BlockHost\bppfw\DrvFltIP.sys;
- C:\BlockHost\bppfw\DrvFltIP.inf;
- C:\BlockHost\bppfw\drvfltip.cat;
- C:\BlockHost\bppfw\gis_publisher.cer;
- C:\Windows\System32\drivers\DrvFltIP.sys.

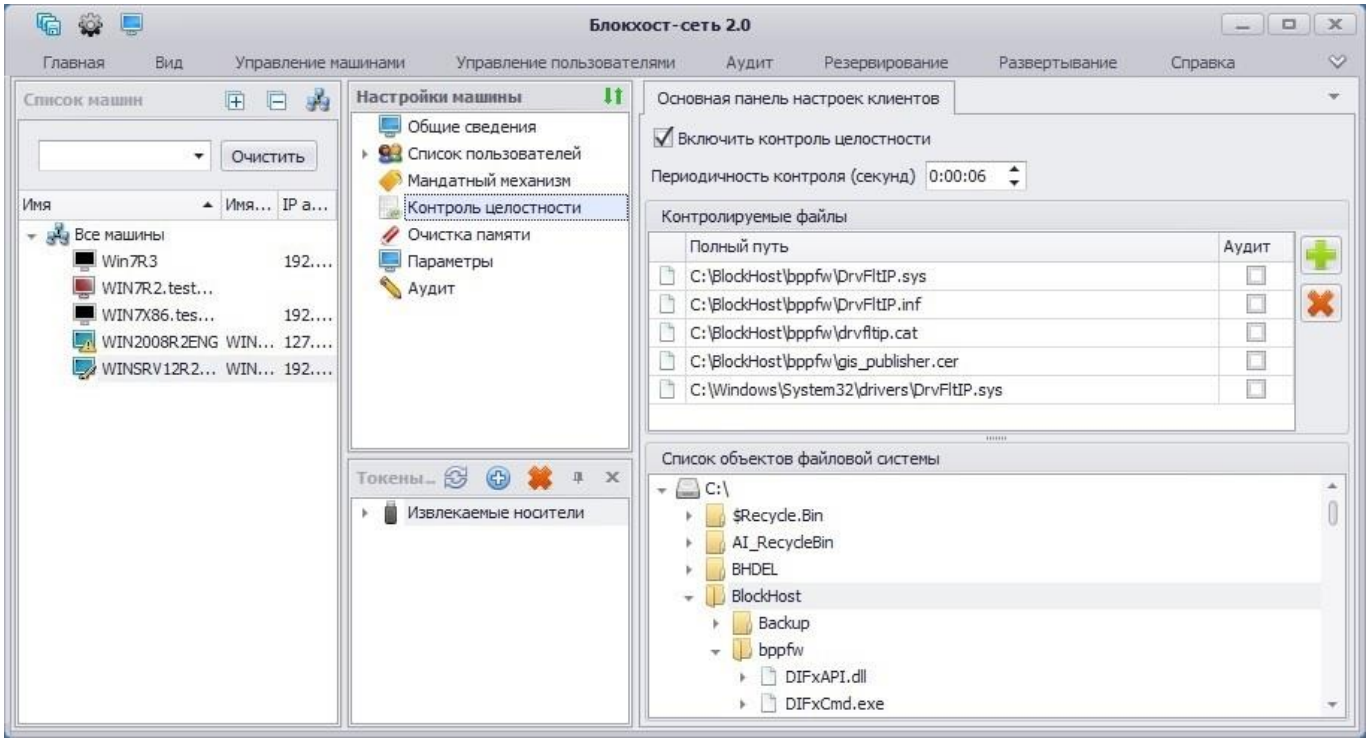


Рисунок 4.4. Постановка на контроль целостности объектов персонального МЭ в ОС Windows 7/2008R2/8.1/2012/2012R2/10/2016

6) при необходимости фиксаций событий, связанных с доступом к контролируемым объектам, отметить напротив них поле ***Аудит***;
7) сохранить произведенные настройки выбрав пункт меню ***Главная→ Сохранить***, или воспользовавшись кнопкой ***Сохранить все***  , расположенной в левом верхнем углу консоли администрирования СЗИ.

После добавления файлов персонального МЭ на контроль целостности будет создана их резервная копия в папке C:\BlockHost\Backup. Контроль целостности указанных файлов будет проводиться с заданной периодичностью. При нарушении их целостности будет выполнено автоматическое восстановление. Для запуска драйвера после его автоматического восстановления компьютер необходимо перезагрузить.

5. Руководство по процедуре восстановления

5.1 Автоматическое восстановление драйвера персонального МЭ

Автоматическое восстановление драйвера персонального экрана происходит, если файлы персонального МЭ были добавлены на контроль целостности (см. пункт 4.1 настоящего документа). Для запуска драйвера после его автоматического восстановления компьютер необходимо перезагрузить.

5.2 Ручное восстановление драйвера персонального МЭ

Для ручного восстановления драйвера используется резервная копия исполняемого образа, которая создается в папке C:\BlockHost\Backup\bppfw при установке СЗИ «Блокхост-сеть 2.0».

При нарушении целостности драйвера персонального экрана администратор безопасности может восстановить его заново установив драйвер персонального экрана из папки *C:\BlockHost\Backup\BlockHost\bppfw*. Для этого необходимо сделать следующее:

1) выбрать пункт ***Панель управления → Сеть и Интернет → Центр управления сетями*** и общим доступом и нажать на ссылку ***Подключение по локальной сети***;
2) в появившемся окне «**Состояние-Подключение по локальной сети»** (рис. 5.1) нажать кнопку ***Свойства***.

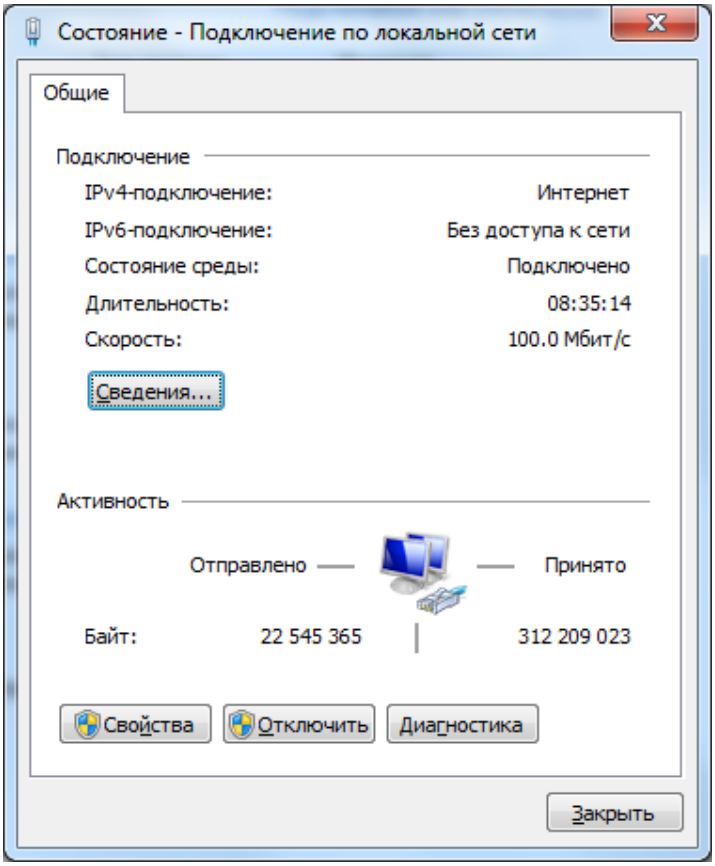


Рисунок 5.1. Окно «Состояние-Подключение по локальной сети»

3) в открывшемся окне свойств подключения по локальной сети нажать кнопку ***Установить*** (рис. 5.2):

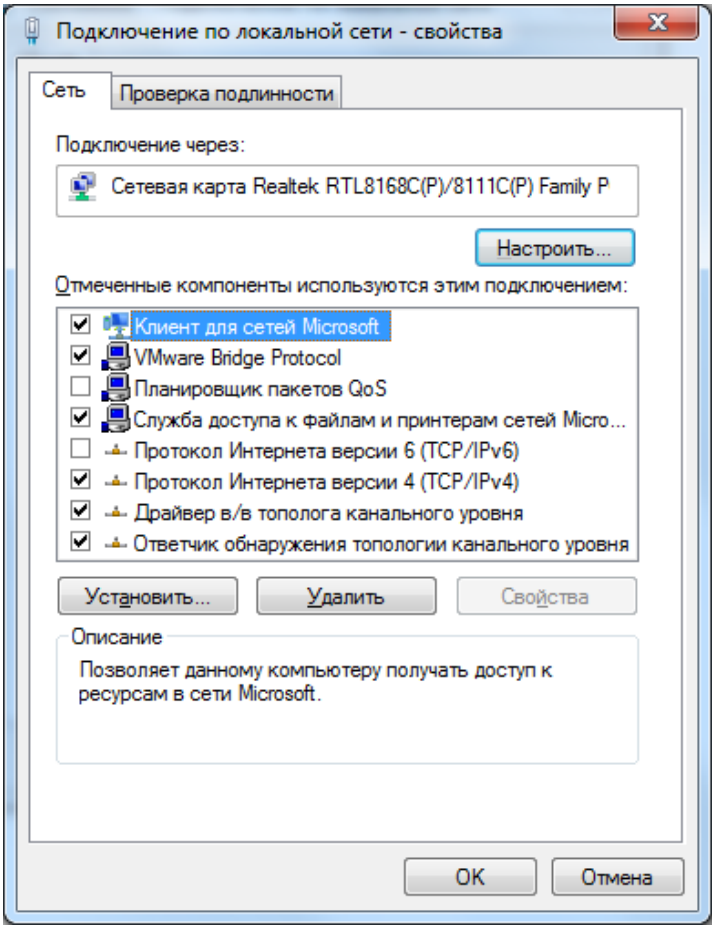


Рисунок 5.2. Выбор пункта «Установить»

4) в открывшемся окне **«Выбор сетевых компонентов»** выбрать сетевой компонент ***Служба*** и нажать кнопку ***Добавить*** (рис. 5.3):

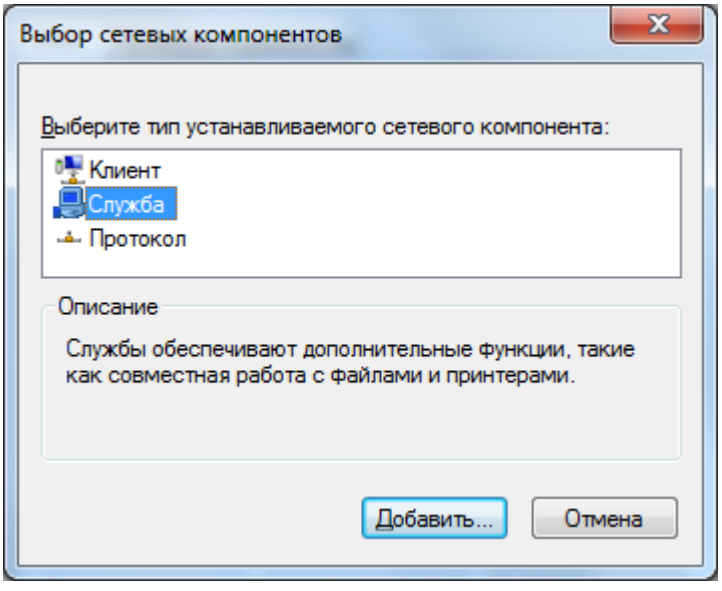


Рисунок 5.3. Выбор компонента «Служба»

5) в окне выбора сетевой службы нажать кнопку ***Установить с диска*** (рис. 5.4):

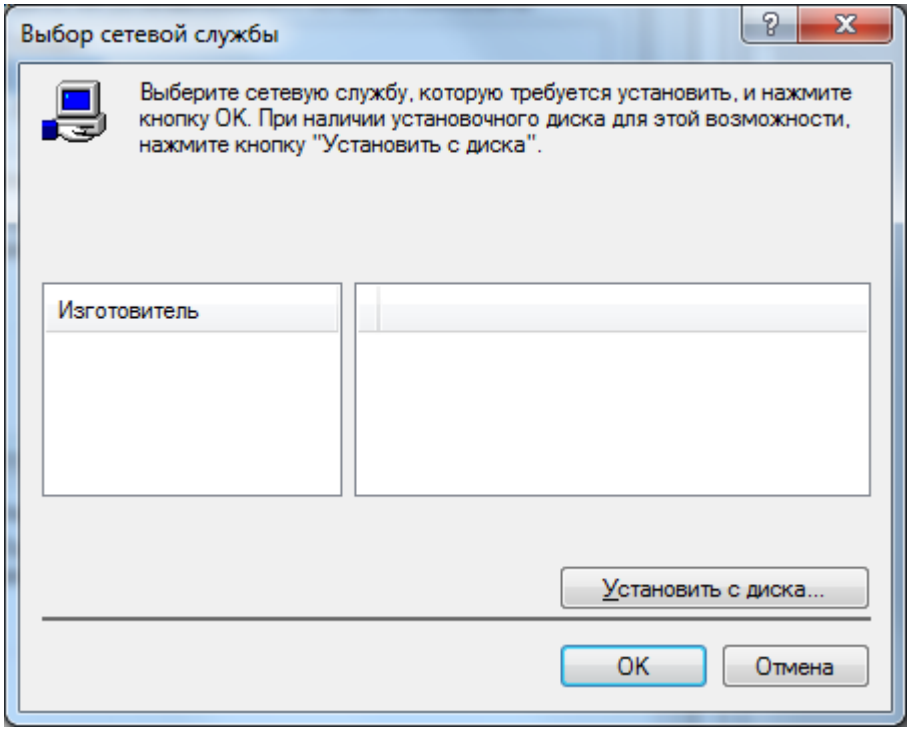


Рисунок 5.4. Окно выбора устанавливаемой службы

6) в открывшемся окне **«Установка с диска»** нажать кнопку ***Обзор*** (рис. 5.5):

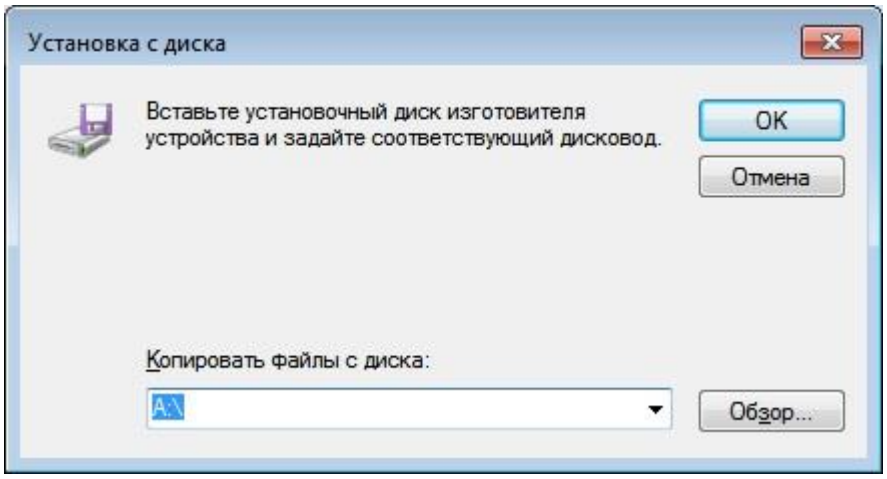


Рисунок 5.5. Окно «Установка с диска»

7) в открывшемся окне **«Поиск файла»** (рис. 5.6) выбрать в папке *C:\BlockHost\Backup\BlockHost\bppfw* файл *DrvFltIP.inf* и нажать кнопку ***Открыть***.

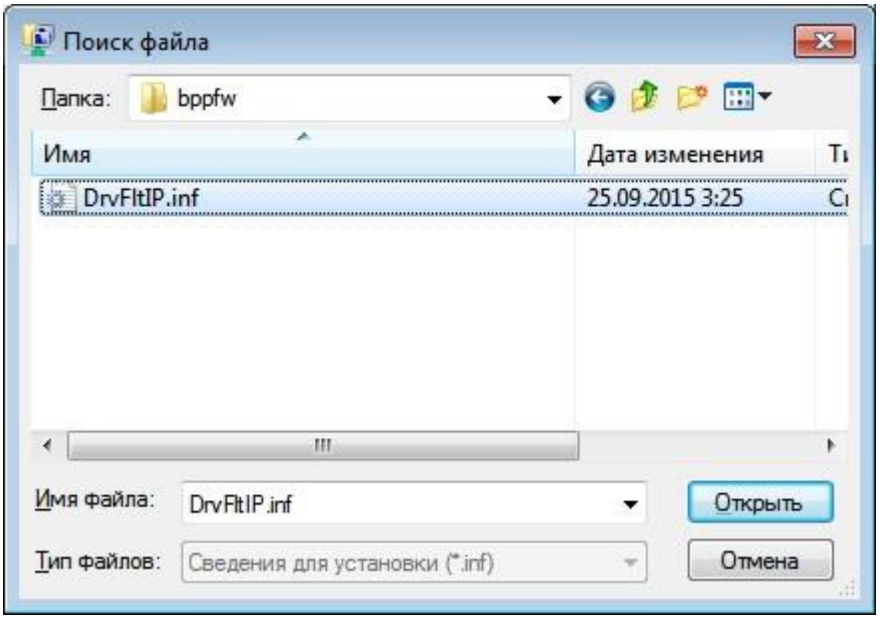


Рисунок 5.6. Выбор файла драйвера персонального МЭ

8) поочередно нажать кнопку ***ОК*** сначала в окне **«Поиск файла»**, а затем в окне **«Выбор сетевой службы»**.
   В результате файл драйвера персонального экрана будет восстановлен из резервной копии.