Практическое занятие № 5. Защита АРМ пользователя на основе технологии ViPNet

Содержание практического занятия

В данном практическом занятии освещаются основные возможности и вопросы, связанные с настройкой средств защиты информации, в том числе и криптографических. Выполнив все пункты занятия, вы ознакомитесь и сможете настроить ViPNet Client 4, ViPNet CSP, приложение Деловая почта и другие встроенные средства коммуникации ViPNet.

Применение и правильная настройка данных компонентов линейки ViPNet Security Network позволит защитить АРМ пользователя: организовать защищенные каналы связи, ограничить доступ и реализовать механизмы фильтрации трафика, внедрить защищенный электронный документооборот и элементы PKI (инфраструктура открытых ключей).

Занятие включает в себя следующие задания:

5.1. Настройка ViPNet Client 4 – VPN и персональный сетевой экран;

5.2. Работа с криптопровайдером ViPNet CSP;

5.3. Работа с приложениями ViPNet;

5.4. Дополнительное задание.

Предварительные настройки

Для подготовки к выполнению практического занятия № 5 необходимо выполнить следующие действия:

1. На виртуальной машине VM_1 проверить наличие установленного программного обеспечения *ViPNet Administrator*.
2. На виртуальных машинах VM_2 и VM_3 удалить программное обеспечение ViPNet (если установлено).
3. На виртуальной машине VM_2 установить программное обеспечение ViPNet Client и развернуть дистрибутив ключей *Сотрудник_1 Центр офис*.
4. На виртуальной машине VM_3 установить программное обеспечение *ViPNet Client* и развернуть дистрибутив ключей *Сотрудник_2 Филиал*.
5. Проверить доступность клиентов *Сотрудник_1 Центр офис* и *Сотрудник_2 Филиал* друг для друга.

	**Примечание.** Установить дистрибутивы ключей на узле с ViPNet можно несколькими способами: 1. В меню программы *ViPNet Client Монитор* выбрать раздел *Файл > Выход*, после чего повторно запустить программу через меню Пуск или с ярлыка на рабочем столе. В окне авторизации до ввода пароля необходимо нажать на стрелку рядом с кнопкой *Настройка*, в выпадающем меню выбрать пункт *Установить ключи.* 2. Второй способ установки дистрибутива ключей заключается в следующем: необходимо перенести dst-файл на узел с установленным ViPNet, затем два раза кликнуть по файлу, после запуска мастера установки ключей следовать инструкциям. Данный способ может пригодиться в

	случае если по каким-либо причинам не удается произвести установку дистрибутива ключей первым способом.

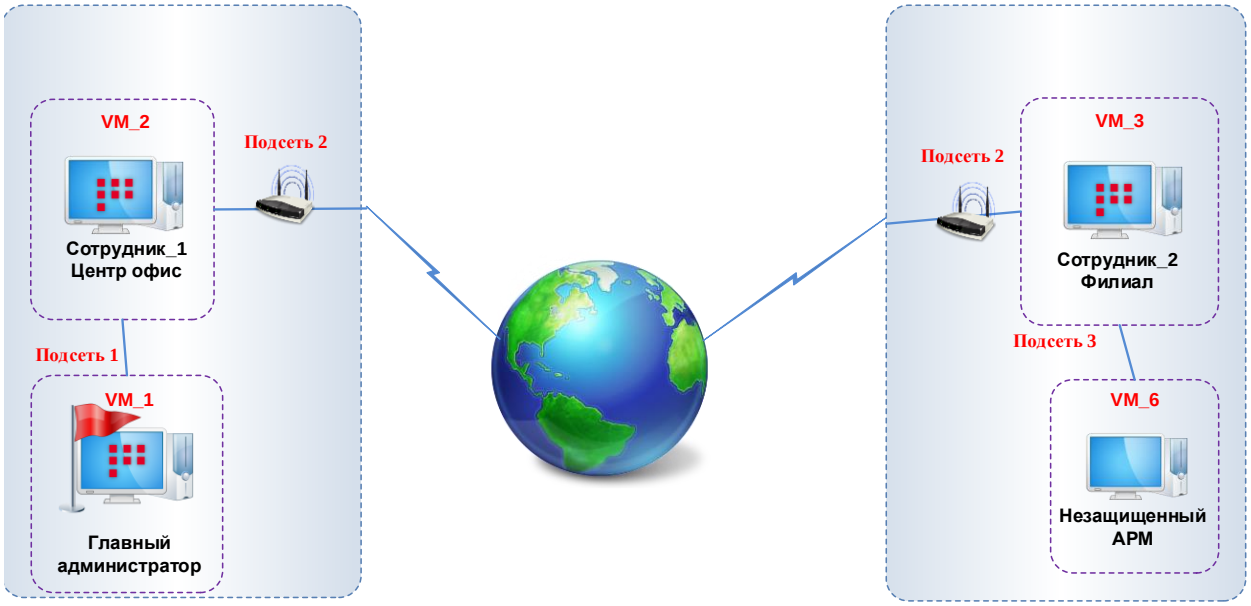

Рисунок 1 – Схема сети для практического занятия № 5.

Задание № 5.1. ViPNet Client 4 – VPN и персональный сетевой экран

Формулировка задания

В настоящем задании необходимо:

5.1.1. Настроить фильтры открытой сети;

5.1.2. Настроить фильтры защищенной сети;

5.1.3. Перевести защищенный сетевой узел в статус незащищенного сетевого узла.

Пояснение к заданию

Персональный сетевой экран при использовании программного обеспечения *ViPNet Client* подразумевает реализацию персональных настроек контроля проходящих сетевых пакетов через сетевой узел с помощью программных средств.

Реализация персонального сетевого экрана в *ViPNet Client* организуется с использованием встроенных сетевых фильтров, которые подразделяются на фильтры для защищенной сети и фильтры для открытой сети.

Но прежде чем рассматривать эти фильтры, необходимо отметить, что в настройках программы имеется возможность блокировать или пропускать определенные виды протоколов.

Для применения данной возможности необходимо в меню *Сервис* выбрать команду **Настройка приложения** (или нажать сочетание клавиш **Ctrl-Alt-S**) и выбрать пункт *Управление трафиком* (Рисунок 160).

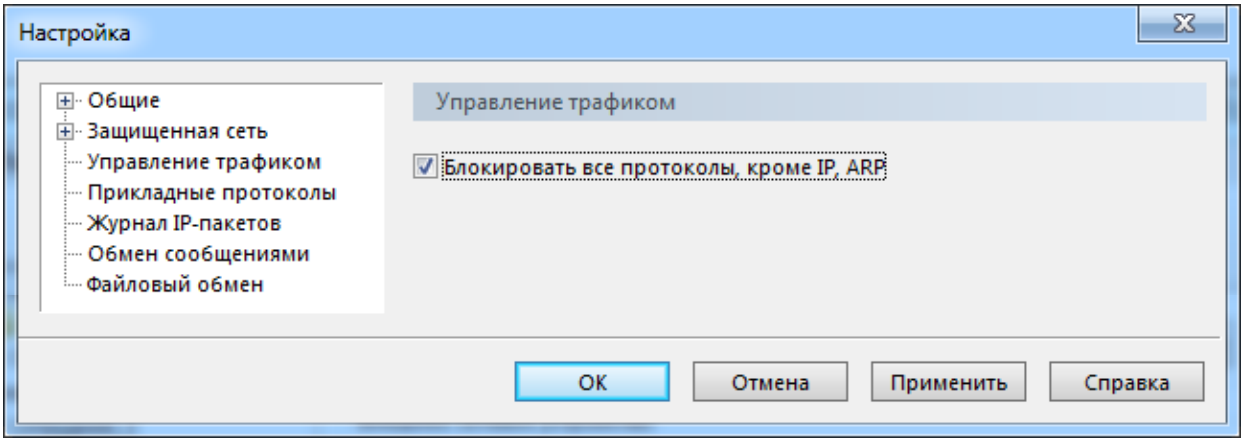

Рисунок 2 – *Управление трафиком* в окне *Настройка*

Из рисунка 160 можно сделать вывод, что при использовании настроек по умолчанию, ViPNet-драйвер будет блокировать весь трафик, за исключением протоколов IPv4 и ARP.

Как было сказано выше, существуют сетевые фильтры как для защищенного, так и для открытого трафика. Они выполняют следующие функции:

− фильтры открытой сети на защищенном узле могут разрешать либо запрещать обмен IP-трафиком с открытыми узлами;

− фильтры защищенной сети могут ограничивать обмен IP-трафиком с защищенными узлами *ViPNet*, с которыми данный узел имеет связь.

В рамках лабораторной работы фильтры, определённые конфигурациями и фильтры политик безопасности, применяться не будут, в связи с этим будут отображены только настраиваемые фильтры и фильтры, заданные по умолчанию (рисунок 161).

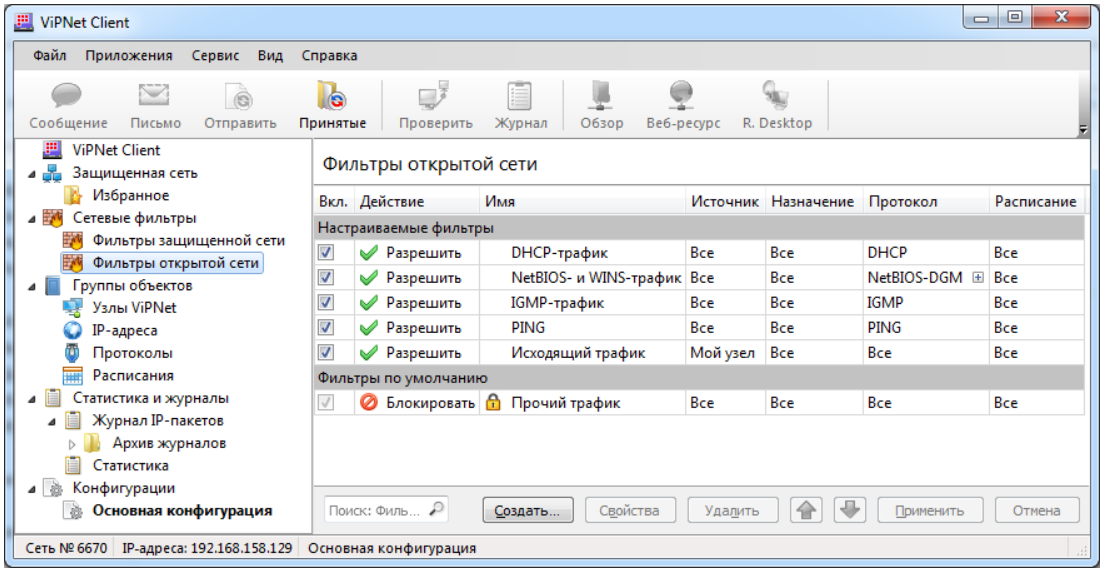

Рисунок 3 – Пример отображения фильтров открытой сети, заданных по умолчанию

Так как наибольшую опасность представляет трафик из открытой сети, поскольку в случае атаки достаточно сложно обнаружить ее источник и

принять оперативные меры по ее пресечению, то в первую очередь разберем параметры персонального сетевого экрана для фильтров открытой сети.

Из рисунка 161 видно, что по умолчанию для настраиваемых фильтров применяются несколько фильтров с разрешающими правилами:

1. Фильтр *DHCP-трафик*.

Данный фильтр разрешает DHCP-трафик от всех источников всем узлам назначения по протоколу DHCP (англ. *Dynamic Host Configuration Protocol* – протокол динамической конфигурации узла) – сетевому протоколу, позволяющему компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

2. Группа фильтров *NetBIOS- и WINS-трафик*.

Данный фильтр разрешает использование *службы WINS* от всех источников ко всем узлам по протоколам *NetBIOS-DGM* и *NetBIOS-NC*.

3. Фильтр *IGMP-трафик*.

Данный фильтр разрешает использование *IGMP-трафика* от всех источников ко всем узлам по протоколу *IGMP*.

4. Фильтр *PING*.

Данный фильтр разрешает использование утилиты *PING* от всех источников ко всем узлам по протоколу *ICMP*.

5. Фильтр *Исходящий трафик*.

Данный фильтр разрешает весь исходящий трафик с конкретного сетевого узла на все другие узлы по всем протоколам.

Исходя из представленной информации по фильтрам открытой сети можно сделать вывод, что из внешней сети обратиться к сетевому узлу практически невозможно, но порой этого достаточно для злоумышленника чтобы начать собирать информацию о узлах в сети, поэтому в первой части задания предлагается настроить фильтр, запрещающий входящий трафик по протоколу ICMP, а также разрешить доступ к общедоступной папке с незащищенной машины из локальной сети организации.

Рассмотрение данного примера позволит в дальнейшем разобраться с основами редактирования правил фильтрации и их настройки. Аналогичным образом можно будет настроить фильтры, например, для запрета доступа с АРМ пользователя к социальным сетям.

Что касается фильтров защищенной сети, принципы создания и настройки схожи с теми, что применяются при создании и редактировании фильтров открытой сети. Поэтому необходимо будет настроить фильтры защищенной сети во второй части задания, то есть запрет или разрешение трафика между узлами с ViPNet Client.

Порядок выполнения задания

5.1.1. Настройка фильтров открытой сети

Настройку фильтров открытой сети необходимо произвести на виртуальной машине Сотрудник_2 Филиал (VM_3), в качестве незащищенного узла будет выступать виртуальная машина VM_6.

Запрет проверки доступности защищенного узла по протоколу ICMP

- **1.** На виртуальной машине VM_6 нажмите сочетание клавиш ***Win+R*** и в открывшейся командной консоли *Windows* наберите команду ***cmd*** (Рисунок 162) и нажмите на кнопку ***Enter***.

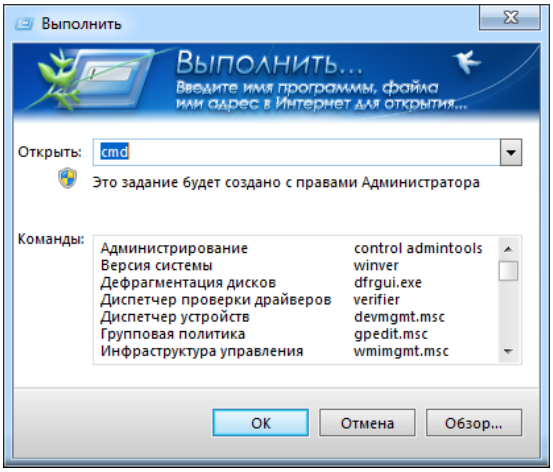

Рисунок 4 – Ввод команды ***cmd*** в командной консоли *Windows*

2. В результате откроется командная строка *Windows*. В командной строке наберите команду ***ping***, через пробел введите IP-адрес виртуальной машины Сотрудник_2 Филиал (VM_3) и убедитесь, что виртуальные машины доступны и обмениваются пакетами по протоколу ICMP (Рисунок 163).

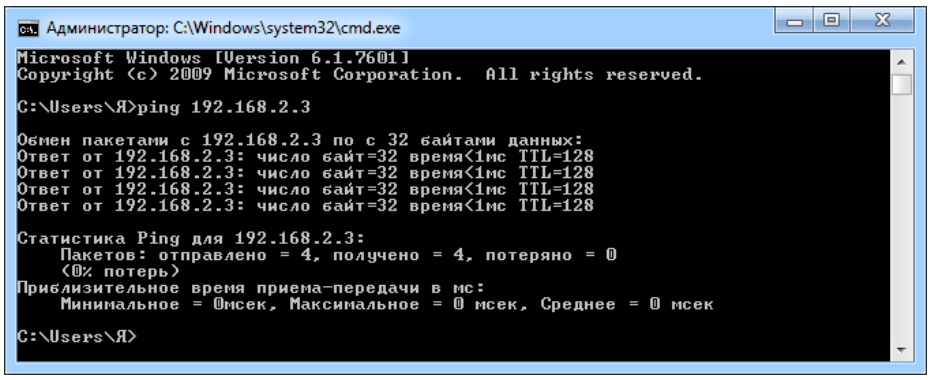

Рисунок 5 – Пример командной строки Windows, где отображено, что сетевой узел доступен по протоколу ICMP

- **3.** На сетевом узле ***Сотрудник_2 Филиал*** в разделе *Сетевые фильтры – Фильтры открытой сети* выделите настраиваемый сетевой фильтр ***Ping*** (рисунок 164).

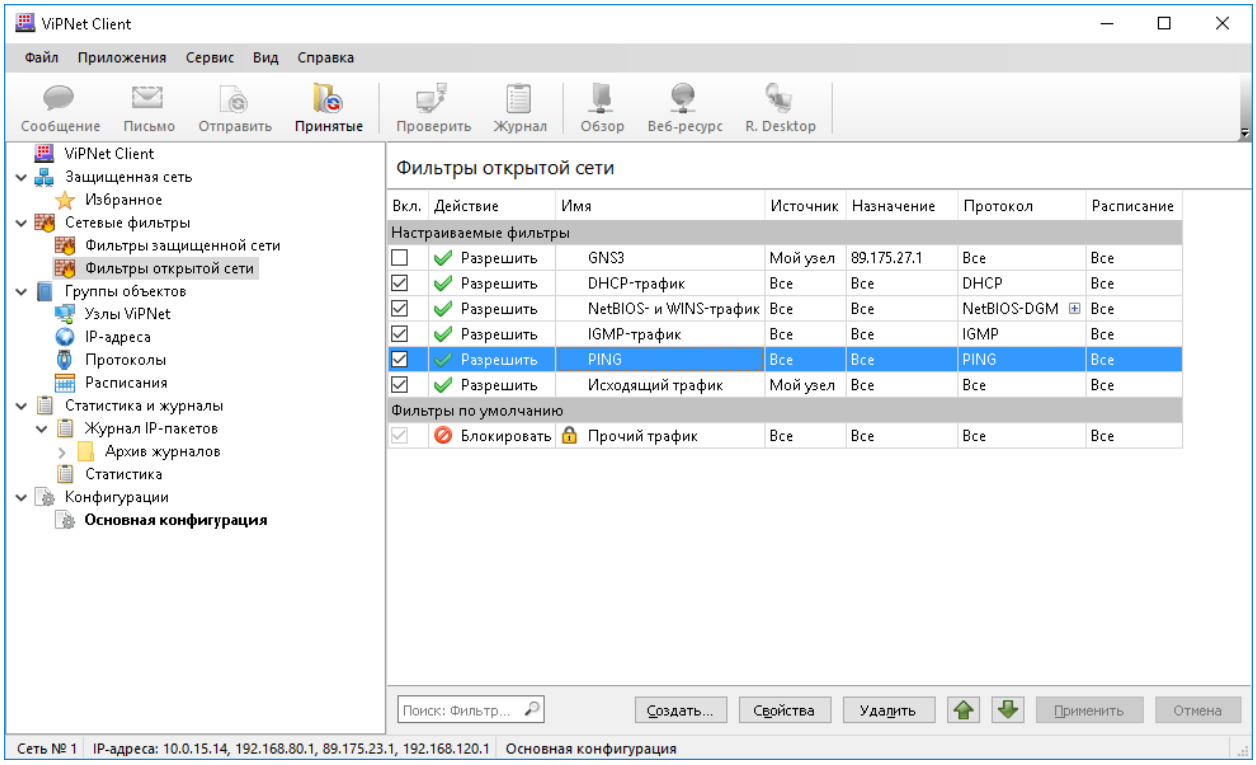

Рисунок 6 – Пример выделения настраиваемого сетевого фильтра ***Ping***

- **4.** Дважды щелкните указателем мышки по выбранному сетевому фильтру, в результате откроется окно *Свойства фильтра открытой сети: Ping* (рисунок 165).
- **5.** В открывшемся окне активируйте действие: *Блокировать трафик* и нажмите кнопку **ОК** (Рисунок 166).

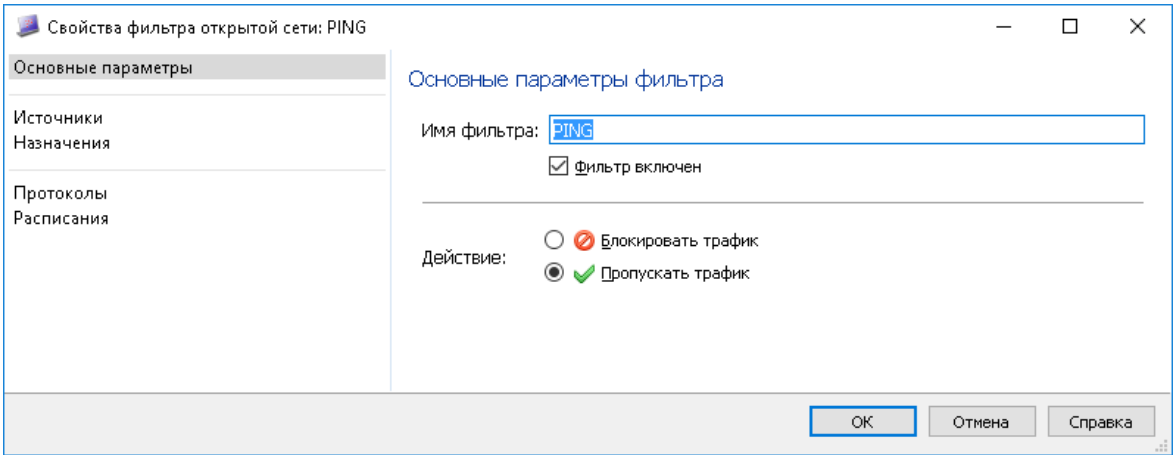

Рисунок 7 – Окно *Свойства фильтра открытой сети: Ping*

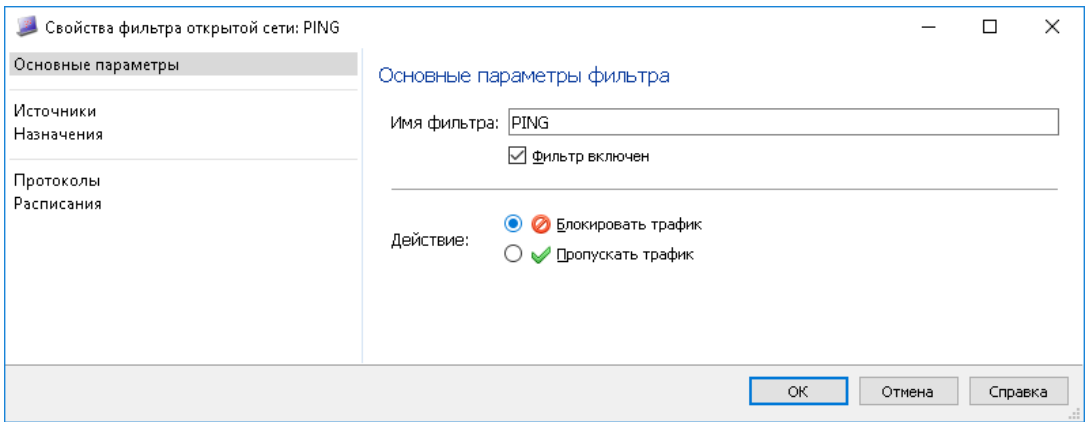

Рисунок 8– Активация действия *Блокировать трафик* в окне *Свойства фильтра открытой сети: Ping*

- **6.** После нажатия кнопки **ОК** обязательно нажмите кнопку **Применить** в разделе *Сетевые фильтры–Фильтры открытой сети* (Рисунок 167).

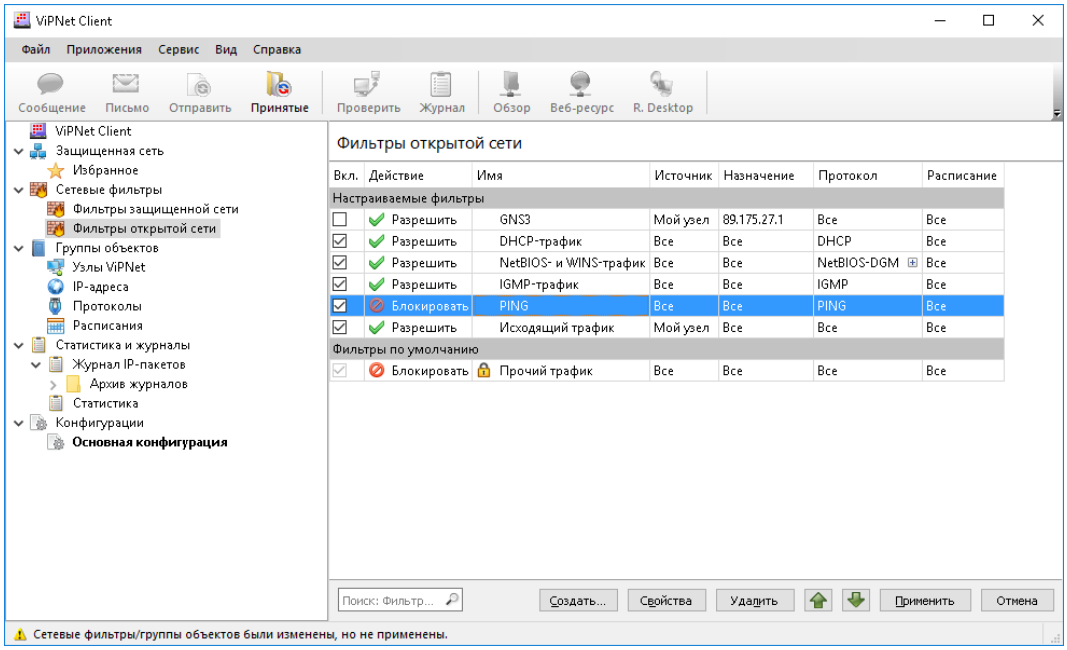

Рисунок 9 – Кнопка **Применить** в разделе *Сетевые фильтры–Фильтры открытой сети*

-

	Примечание. После любого изменения параметра фильтра, всегда нажимайте кнопку Применить. Если вы забудете это сделать, то внесенные вами изменения применены не будут

- **7.** После нажатия кнопки **Применить** отобразится окно, где необходимо указать подтверждения, что вы желаете применить выбранные изменения (Рисунок 168). Нажмите кнопку **Да.**

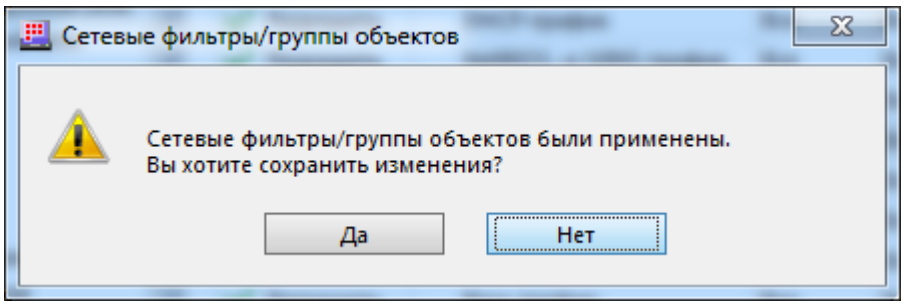

Рисунок 10 – Окно с подтверждением или отменой сохранения изменений в настройках фильтров

- **9.** После нажатия на кнопку **Да** в разделе *Сетевые фильтры–Фильтры открытой сети* будет отображено действие на блокирование трафика от утилиты *Ping*.

10. После введения блокирующего действия к данному фильтру, убедитесь, что виртуальные машины перестали обмениваются пакетами по протоколу *ICMP*.

- **11.** В *Журнале регистрации IP-пакетов* сетевого узла ***Сотрудник_2 Филиал*** убедитесь, что трафик по протоколу ICMP от источника ***VM_6 Незащищенный узел*** к назначению ***Сотрудник_2*** блокирован событием: ***3-IP-пакет блокирован фильтром защищенной сети***.

Открытие доступа к общей папке на защищенном АРМ ViPNet Client 4

Предварительно создайте общую папку с названием **Общие документы** на виртуальной машине **Сотрудник_2 Филиал (VM_3)**.

Система фильтров программы *ViPNet Client Монитор* по умолчанию настроена на запрет подключения к общим папкам защищенного сетевого узла с незащищенных сетевых узлов. Но в некоторых ситуациях возникает необходимость подключения к общим папкам защищенного сетевого узла с незащищённого узла.

Для этого на защищенном узле необходимо настроить разрешающее правило.

Сделать это можно либо созданием нового разрешающего фильтра, либо создав фильтр из *Журнала регистрации IP-пакетов* сетевого узла ***Сотрудник_2 Филиал***.

Ниже представлен способ создания нового фильтра из *Журнала регистрации IP-пакетов*.

- **1.** С виртуальной машины VM_6 попробуйте подключиться к папке **Общие документы** сетевого узла ***Сотрудник_2 Филиал***. Убедитесь, что данная папка недоступна.
- **2.** На сетевом узле ***Сотрудник_2 Филила*** в *Журнале регистрации IP-пакетов* найдите событие блокировки пакета от источника с IP–адресом

виртуальной машины VM_6 на порт 445 по протоколу TCP (событие ***30-IP-пакет блокирован фильтром открытой сети***).

- **3.** Правой кнопкой мыши нажмите на данной событие и во всплывающем окне выберите действие **Создать фильтр** (Рисунок 169).

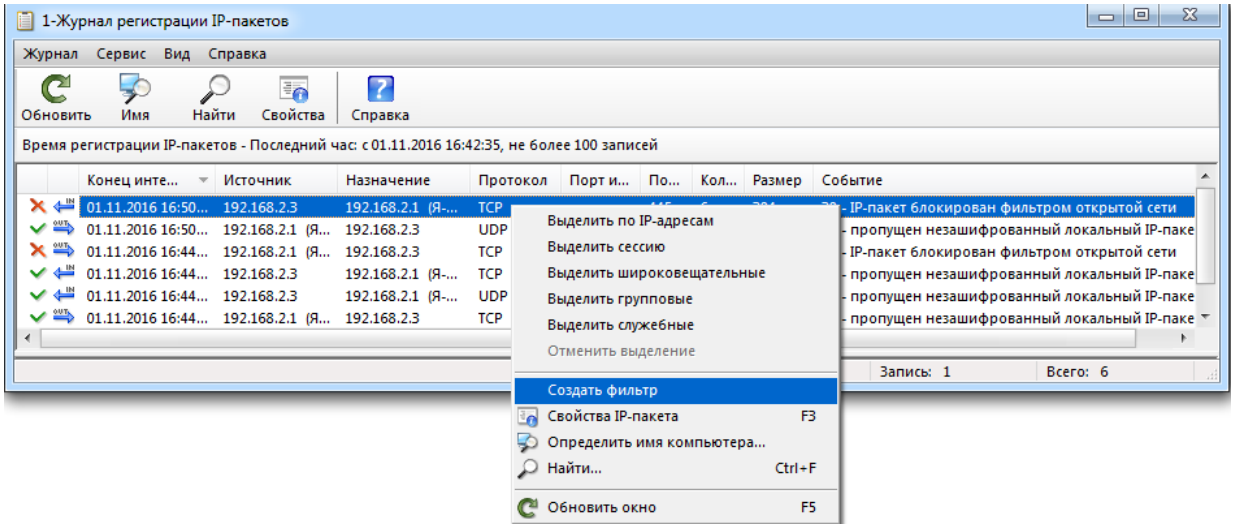

Рисунок 11 – Создание нового фильтра в *Журнале регистрации IP-пакетов*

- **4.** В появившемся окне *Свойства фильтра открытой сети* задайте новому фильтру имя ***Открытие доступа к общим папкам***, проверьте правильность указанных в фильтре источников, назначений и протокола. Убедитесь, что выбрано действие *Пропускать трафик*, установлена галочка *Фильтр включен* и нажмите кнопку **ОК** (Рисунок 170).
- **5.** В разделе *Фильтры открытой сети* программы *ViPNet Client Монитор* убедитесь, что созданный фильтр отобразился в подразделе *Настраиваемые фильтры* и нажмите кнопку **Применить**.

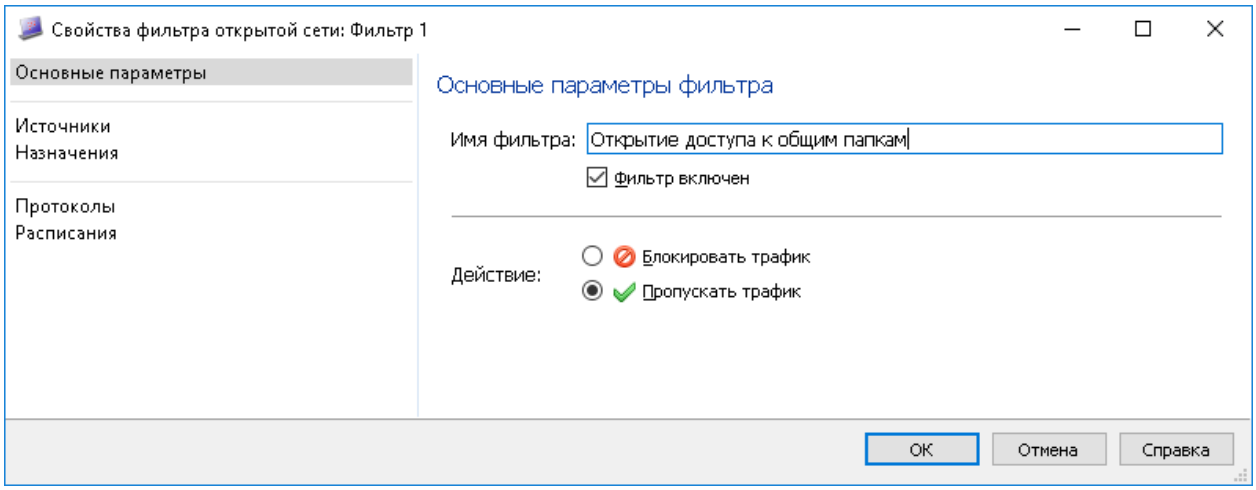

Рисунок 12 – Проверка параметров нового фильтра ***Открытие доступа к общим папкам***

- **6.** В появившемся окне *Сетевые фильтры/группы объектов* нажмите кнопку **Да**.

- **7.** Убедитесь, что папка **Общие документы** сетевого узла ***Сотрудник_2 Филиал*** доступна с незащищенной виртуальной машины VM_6.
- **8.** В *Журнале регистрации IP-пакетов* сетевого узла ***Сотрудник_2 Филиал*** убедитесь, что трафик к порту 445 от *VM_6* пропускается фильтром открытой сети по событию ***60-пропущен незашифрованный локальный IP-пакет***.