

### 5.1.2. Настройка фильтров защищенной сети

При формировании периметра системы защиты информации стоит прорабатывать все возможные векторы атак. Поэтому стоит проводить ревизию не только фильтров открытой сети, но и не забывать про фильтры защищенной сети, так как со стороны других защищенных узлов, которые могут быть потенциально заражены или попасть под контроль злоумышленника в силу ошибок сотрудников (компрометация узла). С таких узлов могут реализовывать внутренние векторы атак.

В связи с этим стоит обратить внимание на настраиваемые предустановленные фильтры защищенной сети, в частности разрешающее правило доступа и подключения со всех узлов связанных с вашим узлом по протоколу RDP.

Чтобы минимизировать риски закрыем доступ по протоколу RDP. Для этого на рабочем месте *Главный администратор* создадим запрещающее правило.

В рамках данного задания перед нами стоит цель не просто отключить существующее правило, а на практике закрепить создание правил фильтрации.

Для создания нового правила необходимо выполнить следующие действия:

1. Удалите существующее правило разрешающее трафик по протоколу RDP. В разделе **Фильтры защищенной сети**→**Настраиваемые фильтры** выделите разрешающее правило и нажмите кнопку **Удалить**;

2. После того как было удалено правило в данное разделе нажмите кнопку **Создать**;

3. В появившемся окне в разделе **Основные параметры** задайте имя фильтра **Запрет подключения по RDP**. Действие **Блокировать трафик**;

4. Раздел **Источник** оставляем неизменным, так как правило будет запрещать весь входящий трафик по протоколу RDP;

5. В разделе **Назначение** нажмите кнопку **Добавить**→**Все координаторы** (это необходимо для того чтобы Главный администратор сети ViPNet мог подключаться к координаторам своей сети по RDP, то есть был разрешен исходящий трафик на защищенные узлы по данному протоколу);

6. Далее в разделе **Протоколы** нажмите кнопку **Добавить**→**Группа протоколов**→**RDP**;

7. После внесения и проверки данных необходимо нажать кнопку **ОК**;

В завершении не забывайте после изменения правил фильтрации или добавления новых нажимать кнопку **Применить**.

### 5.1.3. Перевод защищенного сетевого узла в статус незащищенного сетевого узла

Если возникает необходимость защищенный сетевой узел перевести в разряд незащищенного сетевого узла, то можно сделать это двумя способами:

- удалить программное обеспечение *ViPNet Client*;
- с помощью настроек сделать сетевой узел с установленным программным обеспечением *ViPNet Client* незащищенным.

Так как в дальнейшем потребуется использование программного обеспечения *ViPNet Client*, в рамках лабораторной работы будет выбран второй способ.

В качестве незащищенного узла будет выбрана виртуальная машина *Сотрудник\_2* Филиал.

- 1. Для того, чтобы сделать сетевой узел с установленным программным обеспечением *ViPNet Client* незащищенным, необходимо на в окне программы *ViPNet Client Монитор* зайти в меню *Файл*, выбрать раздел *Конфигурации* и во всплывающем окне выбрать пункт *Отключить защиту* (рисунок 171).

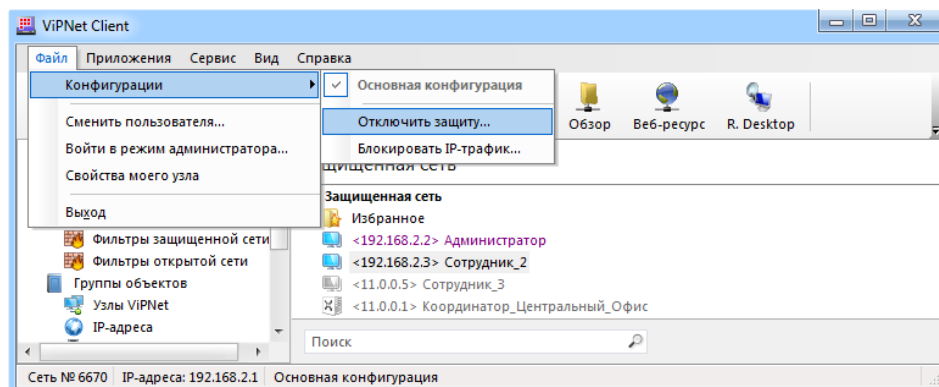


Рисунок 1 – Отключение защиты в окне программы *ViPNet Client Монитор*

- 2. В результате отобразится окно с подтверждением выполнения операции по отключению защиты сетевого узла (Рисунок 172).

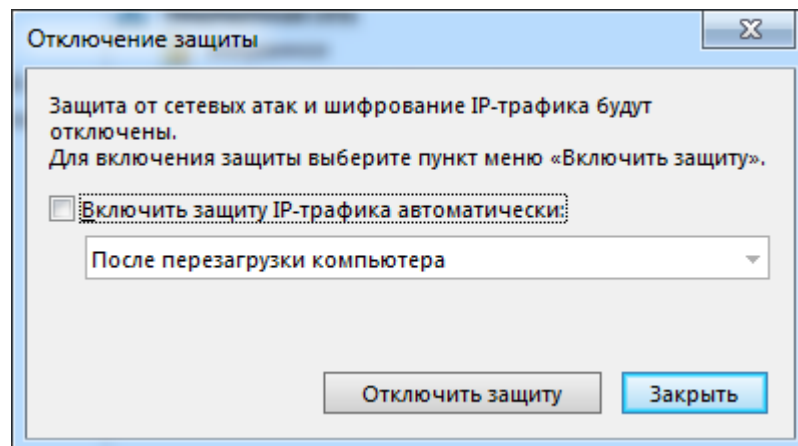


Рисунок 2 – Окно с подтверждением выполнения операции по отключению защиты сетевого узла

- 3. Нажмите кнопку **Отключить защиту**.

Данным действием отключается *ViPNet-драйвер*, в результате чего перестает работать персональный сетевой экран и отключается функция шифрования-расшифрования исходящего и входящего трафика и сетевой узел **Сотрудник\_2 Филиал** станет незащищенным.

Но при этом возникает следующая ситуация.

С одной стороны, раз сетевой узел **Сотрудник\_2 Филиал** стал незащищенным, то на сетевом узле **Сотрудник\_1 Центр офис** трафик, поступающий с сетевого узла **Сотрудник\_2 Филиал**, должен начать обрабатываться фильтрами открытой сети.

Но легко убедиться, что на сетевом узле **Сотрудник\_1 Центр офис**, трафик поступающий от сетевого узла **Сотрудник\_2 Филиал** будет блокироваться.

- 4. Для этого от сетевого узла **Сотрудник\_2 Филиал** в командной строке операционной системы *Windows* выдайте команду **ping** в адрес сетевого узла **Сотрудник\_1 Центр офис** и убедитесь, что сетевой узел **Сотрудник\_1 Центр офис** будет не доступен по протоколу *ICMP*.
- 5. Для того, чтобы понять, почему так происходит, необходимо на сетевом узле **Сотрудник\_1 Центр офис** войти в раздел *Журнал IP-пакетов*, выбрать событие *Блокированные IP-пакеты* и нажать кнопку **Поиск**. В открывшемся *Журнале регистрации IP-пакетов* можно увидеть, что трафик по протоколу *ICMP* от источника с IP-адресом сетевого узла **Сотрудник\_2 Филиал** к назначению с IP-адресом сетевого узла **Сотрудник\_1 Центр офис** был заблокирован фильтром защищенной сети событием: **22-незашифрованный IP-пакет от сетевого узла** (Рисунок 173).

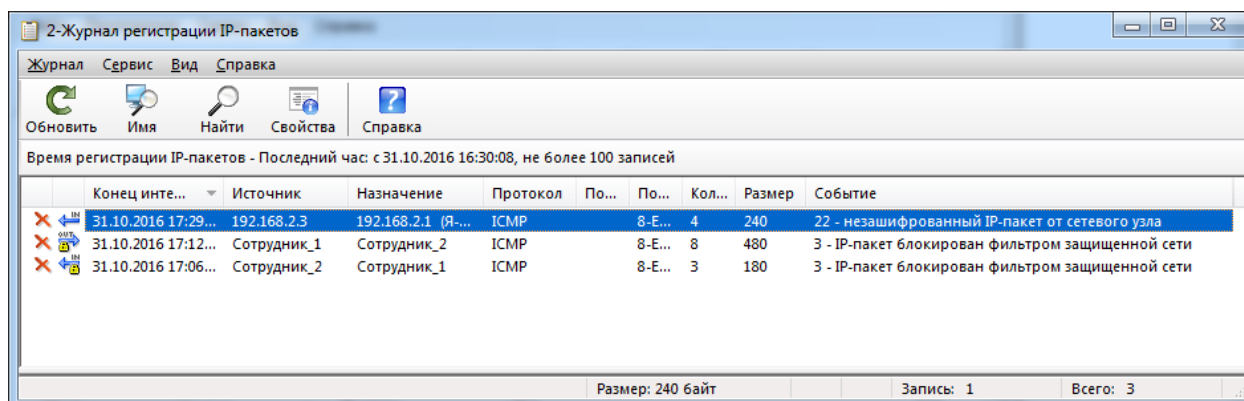


Рисунок 3 – Блокировка фильтром защищенной сети событием **22-незашифрованный IP-пакет от сетевого узла** трафика по протоколу *ICMP* от источника с IP-адресом сетевого узла **Сотрудник\_2 Филиал** к назначению с IP-адресом сетевого узла **Сотрудник\_1 Центр офис**

Таким образом, несмотря на то, что сетевой узел **Сотрудник\_2 Филиал** стал незащищенным, пакеты от него по-прежнему блокируются фильтром защищенной сети сетевого узла **Сотрудник\_1 Центр офис**.

Это происходит из-за того, что в адресных справочниках сетевого узла **Сотрудник\_1 Центр офис**, сетевой узел **Сотрудник\_2 Филиал** сохранился как защищённый узел и по политикам безопасности программного обеспечения *ViPNet*, весь сетевой трафик, поступающий от защищенного узла в открытом (незашифрованном) виде блокируется.

- 6. В этом случае возобновление обмена трафиком можно организовать следующим способом: на сетевом узле **Сотрудник\_1 Центр офис** в разделе Защищенная сеть выбрать сетевой узел **Сотрудник\_2 Филиал** и дважды щёлкнуть по нему указателем мышки. В открывшемся окне *Свойства узла (Сотрудник\_2 Филиал)* войдите во вкладку *IP-адреса*, выделить IP-адрес сетевого узла **Сотрудник\_2 Филиала** и нажать кнопку **Удалить** (рисунок 174).

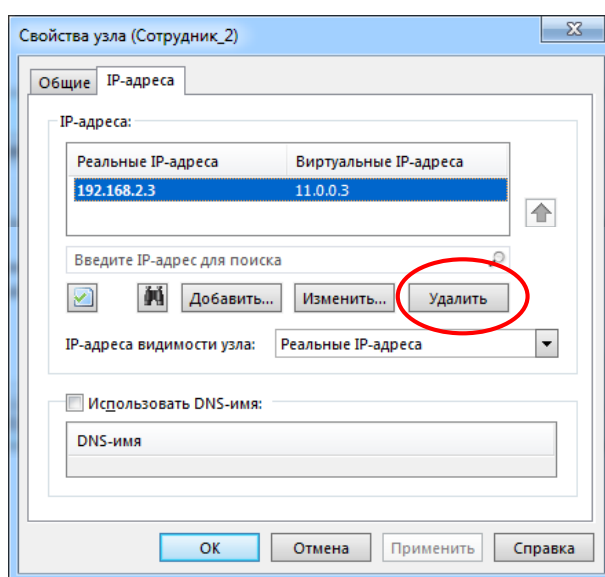


Рисунок 4 – Удаление IP-адреса сетевого узла **Сотрудник\_2 Филиал**

- 7. В появившемся окне *Управление IP-адресами* подтвердить желание об удалении информации с IP-адресом, нажав на кнопку **Да**.
- 8. В окне *Свойства узла (Сотрудник\_2 Филиал)* нажать кнопку **ОК**.  
В результате для сетевого узла **Сотрудник\_1 Центр офис** сетевой узел **Сотрудник\_2 Филиал** будет исключен из перечня защищенных узлов и к нему начнут применяться фильтры открытой сети.
- 9. Для того, чтобы убедиться в этом, с виртуальной машины VM\_3 в командной строке операционной системы *Windows* выдайте команду *ping* в адрес сетевого узла **Сотрудник\_1 Центр офис** и убедитесь, что сетевой узел **Сотрудник\_1 Центр офис** стал доступен по протоколу *ICMP*.
- 10. В разделе *Журнал IP-пакетов* сетевого узла **Сотрудник\_1 Центр офис** установите фильтр по событию *Все IP-пакеты* и ограничьте фильтр выборкой протоколов *ICMP* (рисунок 175).

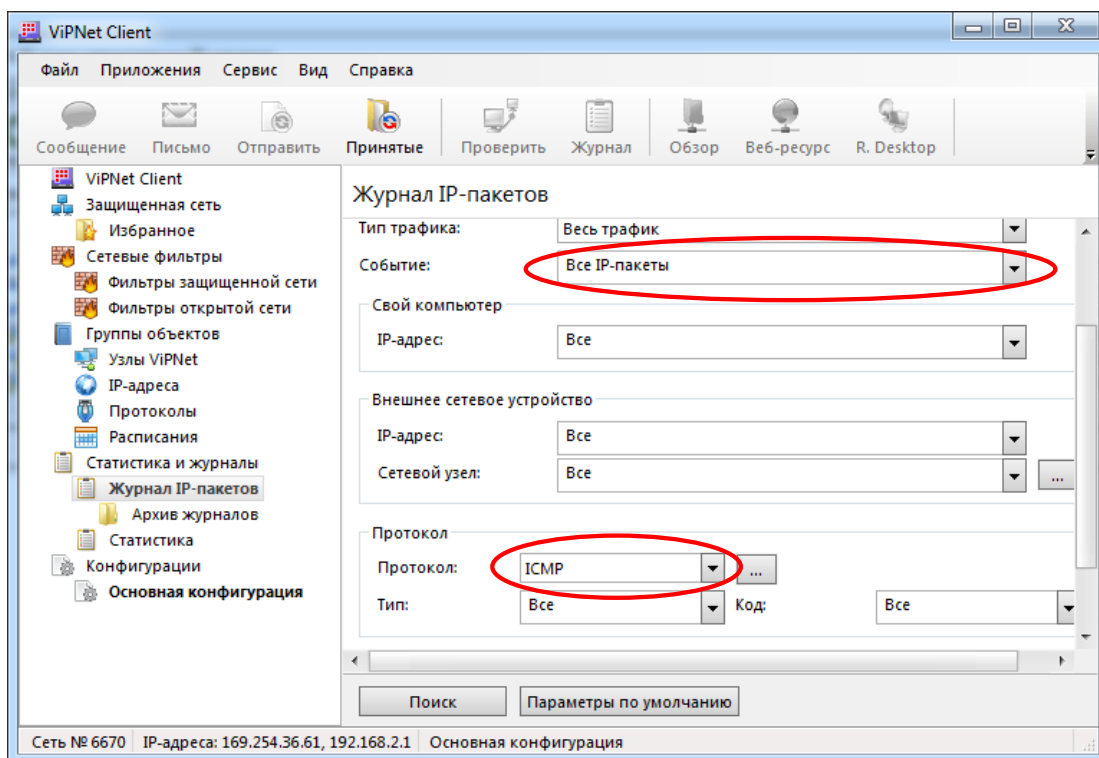


Рисунок 5 – Установка фильтра Журнала IP-пакетов сетевого узла **Сотрудник\_1 Центр офис** по событию *Все IP-пакеты* и ограничение выборкой протоколов *ICMP*

- **11.** После нажатия на кнопку **Поиск** отобразится *Журнал регистрации IP-пакетов*, из которого можно сделать вывод, что от источника с IP-адресом сетевого узла **Сотрудник\_2 Филиал** пакет по протоколу ICMP был пропущен фильтром открытой сети по событию *60-пропущен незашифрованный локальный IP-пакет*.

Таким образом, для сетевого узла **Сотрудник\_1 Центр офис**, сетевой узел **Сотрудник\_2** стал незащищенным, несмотря на то, что он продолжает отображаться в списках защищенной сети, но с IP-адресом 0.0.0.0.