

Оглавление

Задание № 2.3. Настройка политик безопасности в ViPNet Policy Manager	1
Формулировка задания	1
2.3.1. Установка ViPNet Policy Manager	1
2.3.2. Создание подразделений Центральный офис, Филиал	4
2.3.3. Создание политики безопасности, ограничивающей доступ работников компании к социальным сетям Вконтакте и Одноклассники	5
2.3.4. Создание политики безопасности, блокирующей весь открытый трафик на рабочем месте Сотрудник_1 Центр офис.	10
Задание № 2.4. Дополнительное задание	10

Задание № 2.3. Настройка политик безопасности в ViPNet Policy Manager

Формулировка задания

В настоящем задании необходимо:

- 2.3.1. Установить ViPNet Policy Manager
- 2.3.2. Создать подразделения *Центральный офис, Филиал*.
- 2.3.3. Создать политики безопасности, ограничивающей доступ работников компании к социальным сетям *Вконтакте* и *Одноклассники*.
- 2.3.4. Создать политики безопасности, блокирующей весь открытый трафик на рабочем месте *Помощник глав админа*.

2.3.1. Установка ViPNet Policy Manager

ПО ViPNet Policy Manager допускается развертывать только на клиенте с ролью *Network Control Center*, поэтому клиенту *Главный администратор* была автоматически назначена роль *Policy Manager*.

1. На рабочем месте *Главный администратор* запустите установочный файл программного обеспечения ViPNet Policy Manager *<имя_файла>.exe*.
2. Следуйте указаниям мастера установки, для этого нажимайте кнопку *Далее*, не меняя параметры по умолчанию.
3. На одном из шагов мастера установки ознакомьтесь с условиями лицензионного соглашения, установите соответствующий флажок и нажмите кнопку *Продолжить*.
4. На странице *Установка базы на Microsoft SQL Server* выберите сервер баз данных – *.\WINNCCSQL*, укажите имя базы данных – *ViPNetPolicyManager* и способ аутентификации – *Аутентификация Windows (Рисунок 111)*.

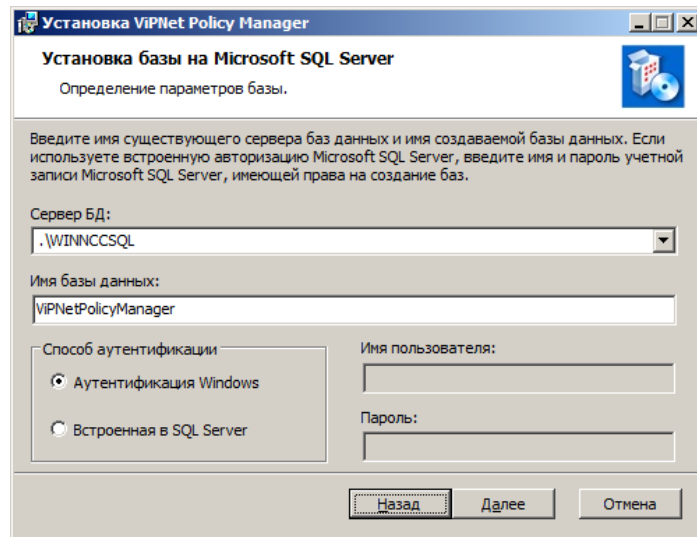


Рисунок 1 – Параметры базы данных при установке ViPNet Policy Manager

5. В процессе установки может появиться окно со списком приложений, которые требуется закрыть. Выберите *Закреть приложения и попытаться перезапустить их* и нажмите кнопку *ОК*. Для обеспечения нормальной работы продукта ViPNet Policy Manager выполните следующие действия:

1. В окне *ViPNet Центр управления сетью* перейдите в раздел *Клиенты*.
2. В свойствах клиента *Главный администратор* выберите *Роли узла > Policy Manager > Свойства* и добавьте в список все узлы сети (Рисунок 112).

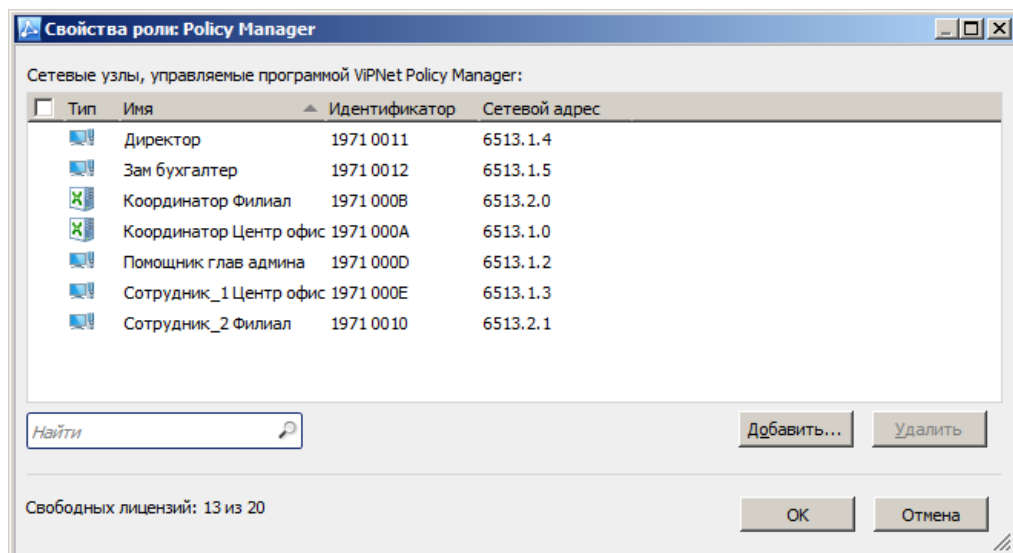


Рисунок 2 – Добавление узлов для роли Policy Manager

3. Создайте и отправьте справочники на все узлы сети. Дождитесь пока обновятся справочники на узле *Помощник глав админа*.

4. Откройте программу ViPNet Policy Manager (*Пуск > Все программы > ViPNet > ViPNet Policy Manager*) и введите имя пользователя и пароль – *Supervisor* (Рисунок 113).

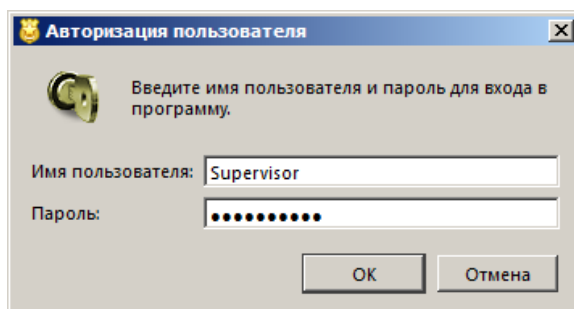


Рисунок 3 – Вход в программу ViPNet Policy Manager

5. На экран будет выведено предупреждение о необходимости смены пароля пользователя *Supervisor* (Рисунок 114).

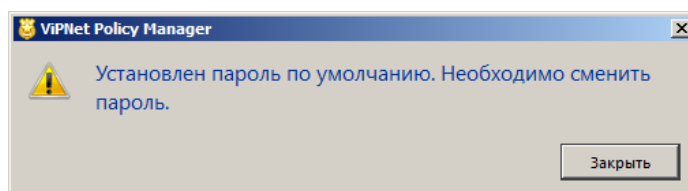


Рисунок 4 – Предупреждение о необходимости смены пароля

6. После авторизации под стандартным паролем перейдите в раздел *Файл>Сменить пароль пользователя* и задайте пароль – 11111111 (восемь единиц).
7. В окне программы *ViPNet Policy Manager* перейдите в раздел *Сетевые узлы*. Если предыдущие шаги выполнены верно, то в списке будут отображены все узлы сети ViPNet (Рисунок 115).

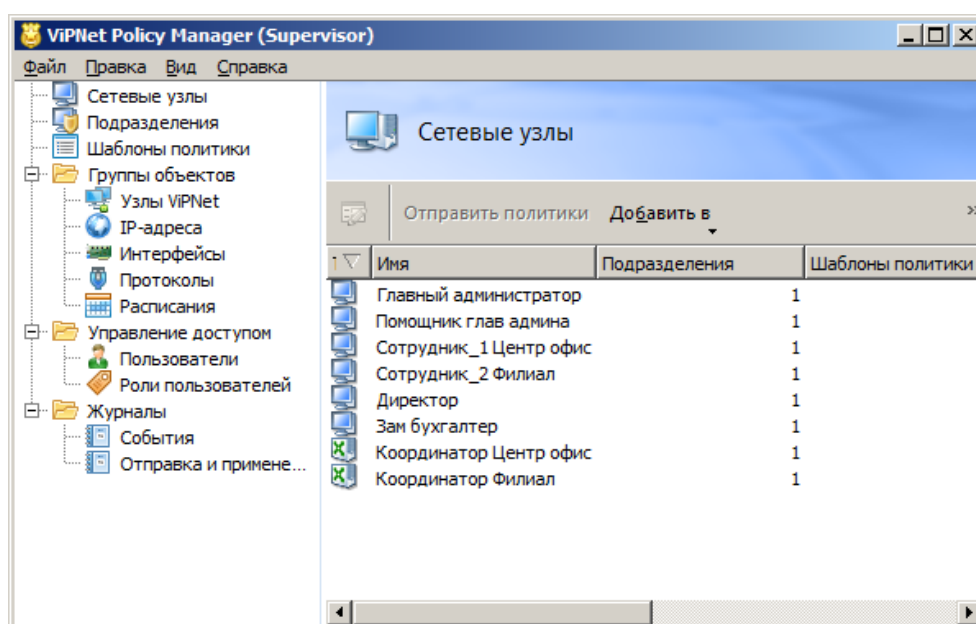


Рисунок 5 – Раздел *Сетевые узлы* программы ViPNet Policy Manager

Теперь можно приступить к управлению узлами ViPNet через *ViPNet Policy Manager*.

2.3.2. Создание подразделений *Центральный офис*, *Филиал*.

Для создания подразделений *Центральный офис*, *Филиал* выполните следующие действия:

1. В окне программы *ViPNet Policy Manager* перейдите в раздел *Подразделения* и нажмите кнопку *Создать*.
2. В открывшемся окне *Свойства подразделения* на вкладке *Основные параметры* задайте имя *Центральный офис*.
3. На вкладке *Сетевые узлы* добавьте клиентов Центрального офиса: *Координатор Центр офис*, *Главный администратор*, *Помощник глав админа*, *Сотрудник_1 Центр офис*, *Зам бухгалтер*, *Директор* (Рисунок 116).

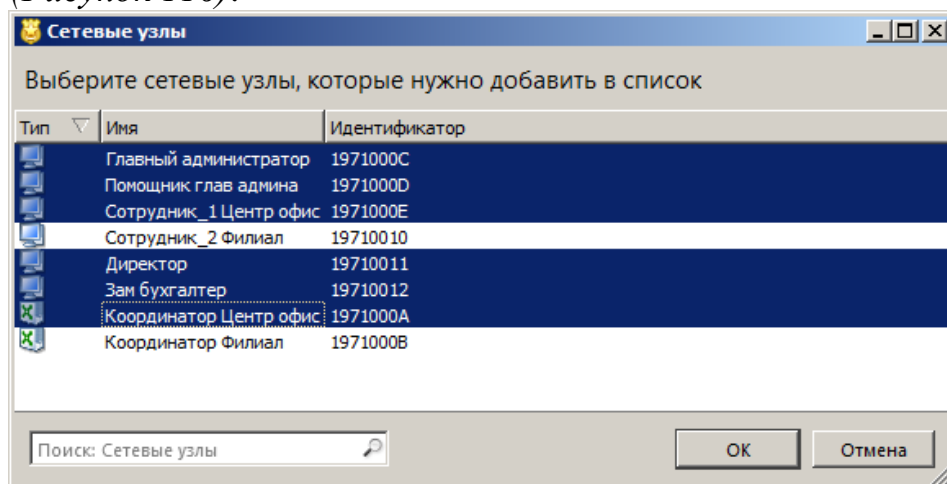


Рисунок 6 – Добавление клиентов в подразделение *Центральный офис*

Остальные настройки в окне *Свойства подразделения* менять не требуется.

Аналогичным образом создайте подразделения *Филиал*, добавив в него сетевые узлы *Координатор Филиал*, *Сотрудник_2 Филиал*.

Если все выполнено правильно, раздел *Подразделения* программы *ViPNet Policy Manager* примет следующий вид (Рисунок 117).

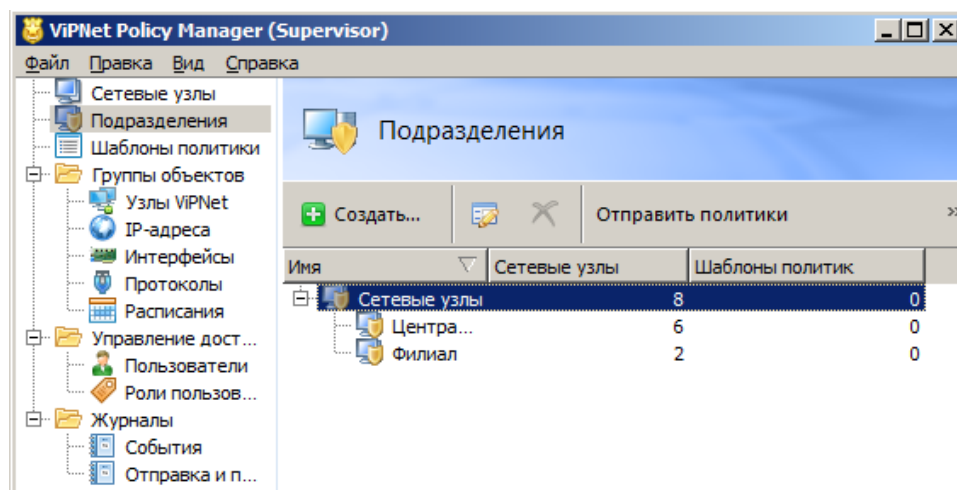


Рисунок 7 – Раздел *Подразделения* программы *ViPNet Policy Manager*

2.3.3. Создание политики безопасности, ограничивающей доступ работников компании к социальным сетям Вконтакте и Одноклассники

Для создания политики безопасности, ограничивающей доступ работников компании к социальным сетям *Вконтакте* и *Одноклассники*, выполните следующие действия:

1. В окне программы *ViPNet Policy Manager* перейдите в раздел *Группы объектов > IP-адреса* и нажмите кнопку *Создать*.
2. В открывшемся окне *Свойства группы IP-адресов* на вкладке *Основные параметры* задайте имя *Социальные сети*.
3. На вкладке *Состав* нажмите кнопку *Добавить > DNS-имя...* и добавьте имя *vk.com*.
4. Аналогичным образом добавьте *DNS-имена* согласно рисунку ниже (в рамках практического занятия не обязательно вбивать все DNS-имена, они приведены в качестве примера, чтобы было понятно, как действовать в реальной ситуации, для эффективного закрытия доступа к ресурсам). Соответствующие IP-адреса будут определены автоматически (*Рисунок 118*).

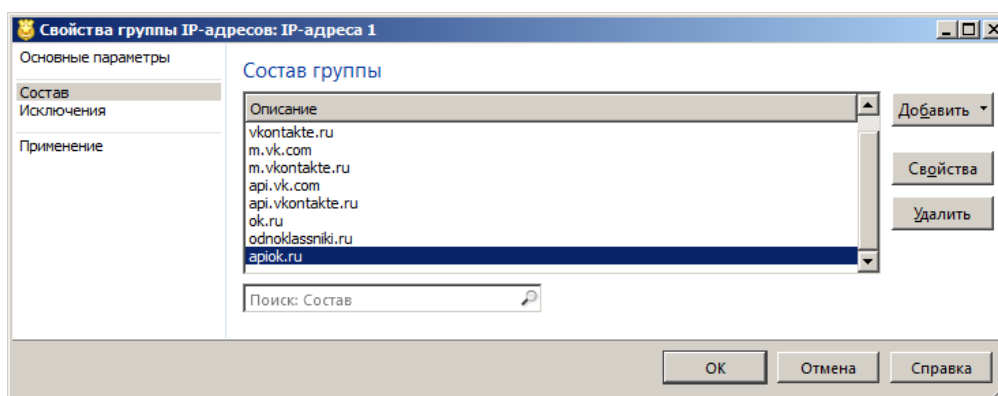


Рисунок 8 – Список *DNS-имен* социальных сетей *Вконтакте* и *Одноклассники*

5. В окне программы *ViPNet Policy Manager* перейдите в раздел *Шаблоны политики* и нажмите кнопку *Создать*.
6. В открывшемся окне *Свойства шаблона политики* на вкладке *Основные параметры* задайте имя *Запрет социальных сетей*.
7. На вкладке *Подразделения* отметьте подразделения *Центральный офис* и *Филиал* (Рисунок 119).

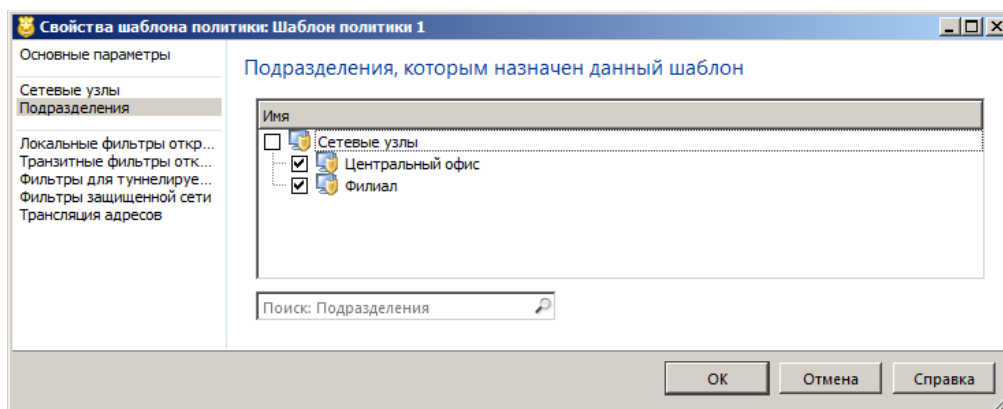


Рисунок 9 – Вкладка *Подразделения* окна *Свойства шаблона политики*

8. На вкладке *Локальные фильтры открытой сети* нажмите кнопку *Создать...*
9. В открывшемся окне *Свойства фильтра открытой сети* на вкладке *Основные параметры* задайте имя фильтра *Запрет социальных сетей* и установите переключатель в положение *Блокировать трафик* (Рисунок 120).

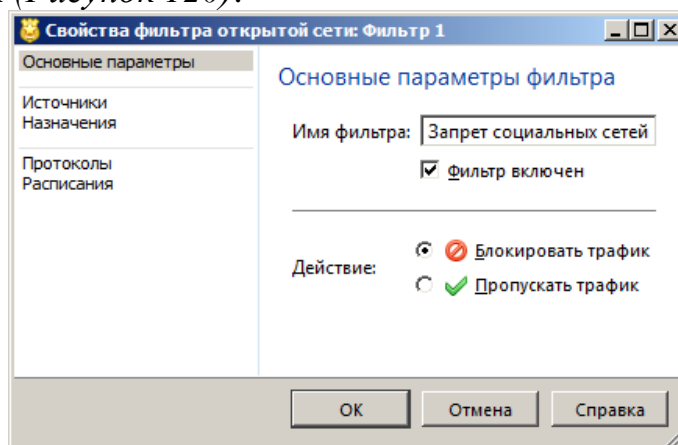


Рисунок 10 – Вкладка *Основные параметры* окна *Свойства фильтра открытой сети*

10. На вкладке *Назначения* нажмите кнопку *Добавить...* > *Группы IP-адресов* и выберите группу *Социальные сети* (Рисунок 121).

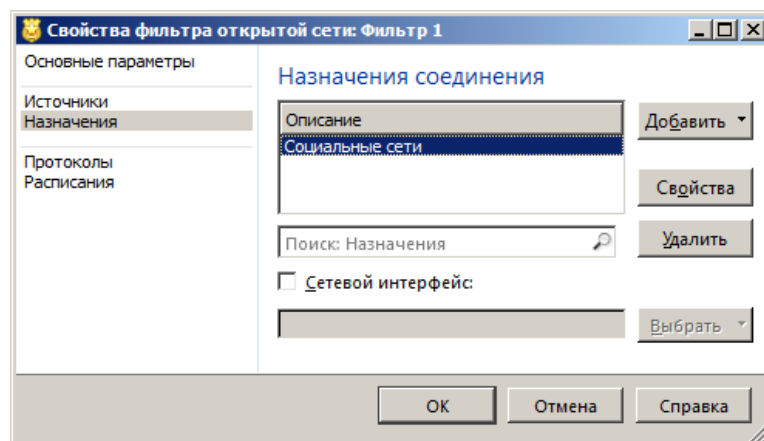


Рисунок 11 – Вкладка *Назначения* окна *Свойства фильтра открытой сети*

11. Остальные параметры окна *Свойства фильтра открытой сети* и *Свойства шаблона политики* менять не требуется.

После создания политики *Запрет социальных сетей* раздел *Шаблоны политики* примет следующий вид (Рисунок 122).

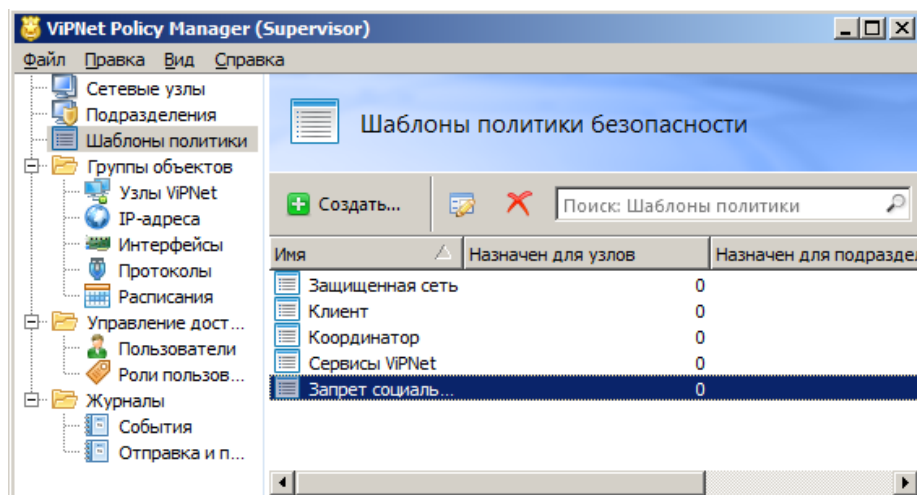


Рисунок 12 – Раздел *Шаблоны политики* с политикой *Запрет социальных сетей*

12. Отправьте политики на узлы. Для этого в окне программы *ViPNet Policy Manager* перейдите в раздел *Подразделения*.

13. Выделите подразделения *Центральный офис* и *Филиал*, нажмите кнопку *Отправить политики* (Рисунок 123).

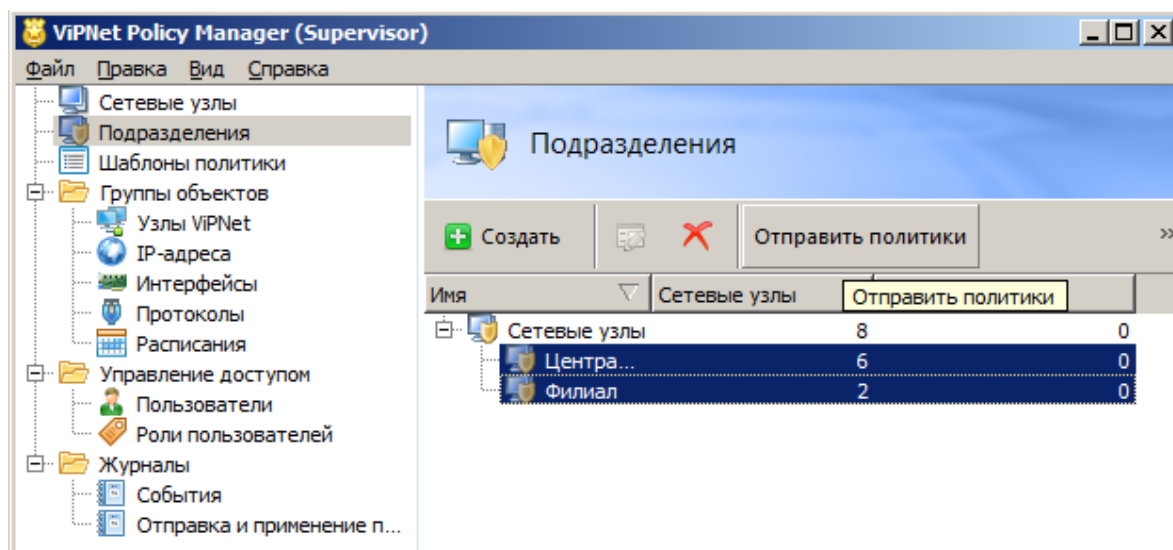


Рисунок 13 – Выбор подразделений для отправки политик безопасности

14. На экран будет выведено окно *Отправка политики*. Не меняя параметров, нажмите кнопку *ОК* (Рисунок 124).

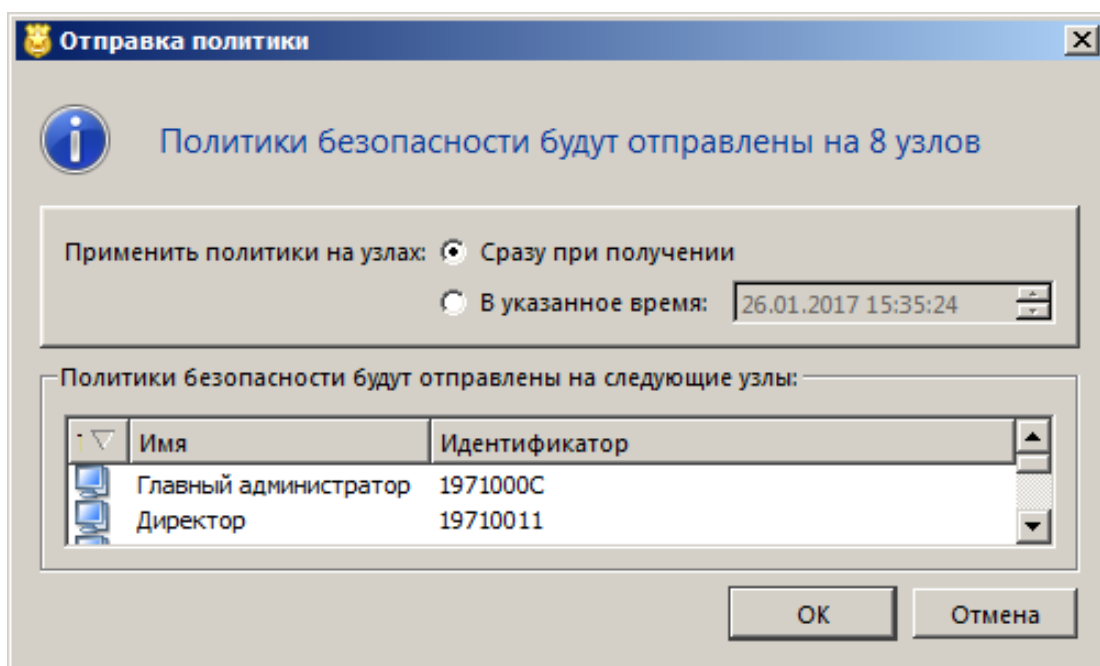


Рисунок 14 – Окно *Отправка политики*

Для контроля за ходом отправки политик на узлы в окне программы *ViPNet Policy Manager* перейдите в раздел *Журналы > Отправка и применение политик*. Статус политик на узлах *Главный администратор* и *Помощник глав админа* должен измениться на *Применена* (Рисунок 125).

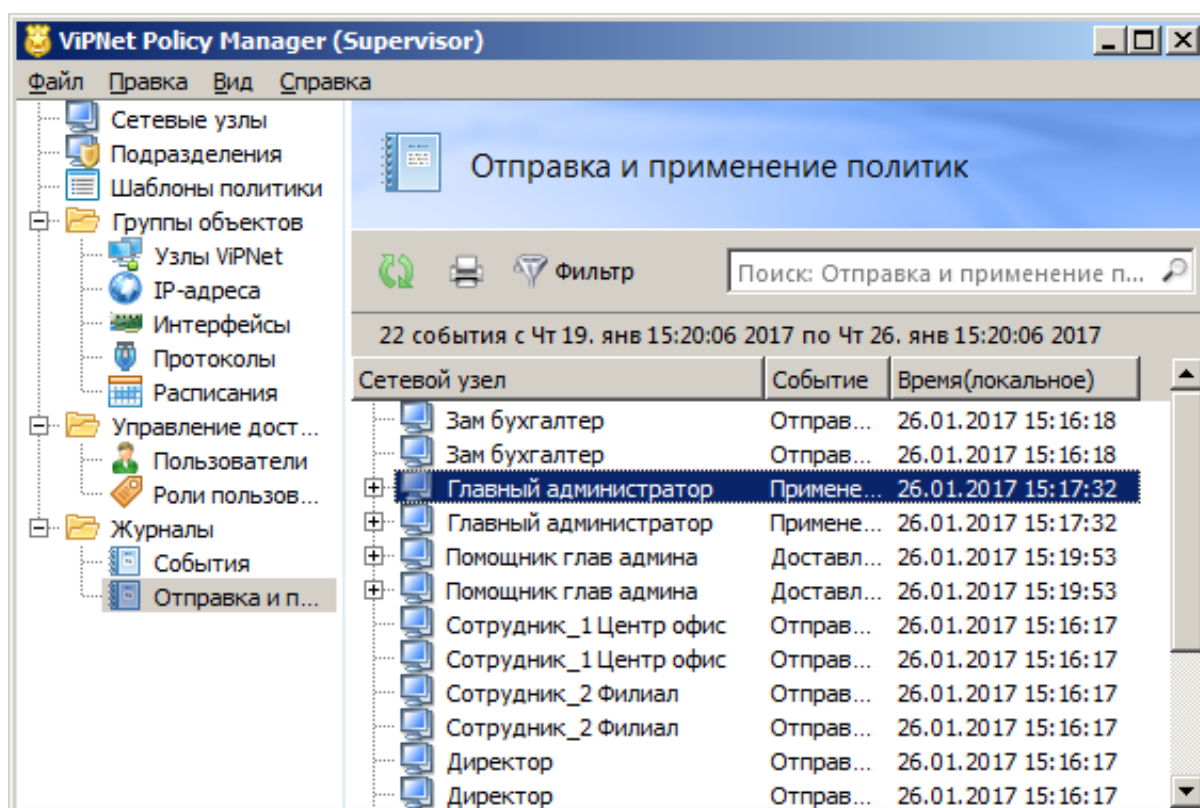


Рисунок 15 – Контроль отправки и применения политик

Для проверки применения политик на рабочих местах *Главный администратор* и *Помощник глав админа* зайдите в программу *ViPNet Client Монитор* > *Сетевые фильтры* > *Фильтры открытой сети*. Убедитесь, что добавлен новый фильтр *Запрет социальных сетей* (Рисунок 126).

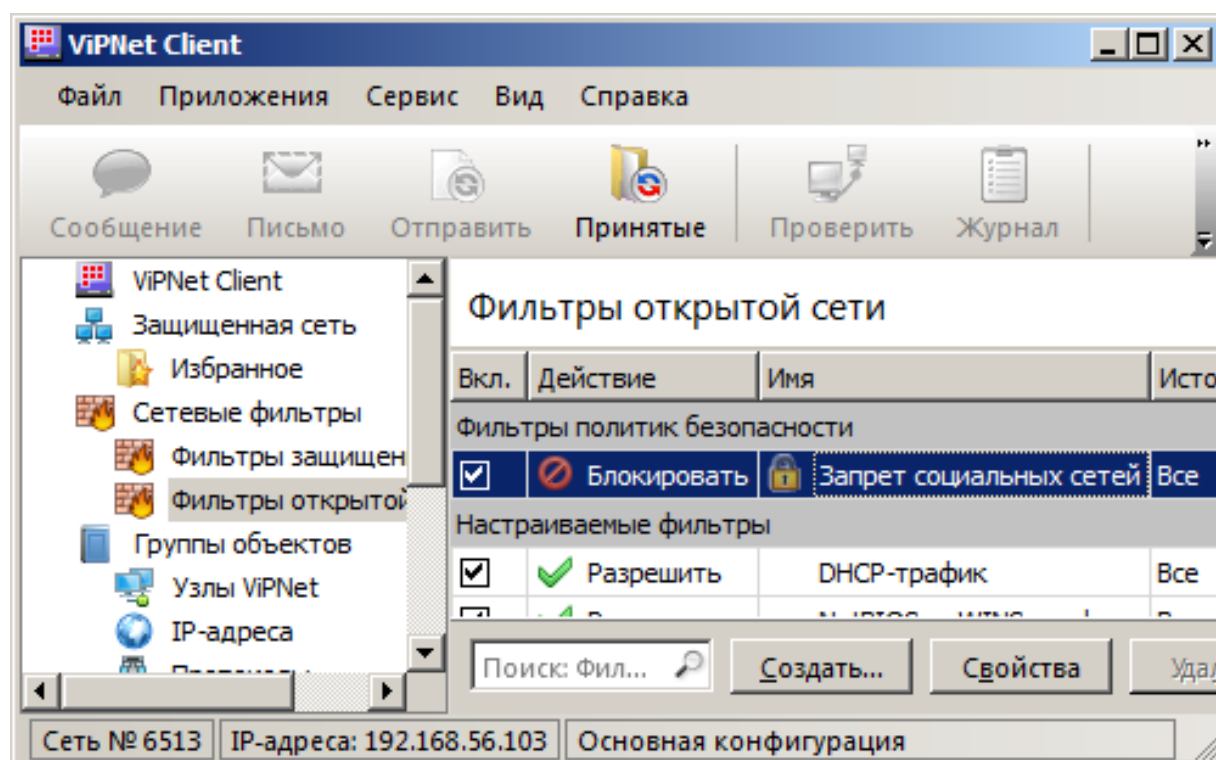


Рисунок 16 – Окно программы *ViPNet Client Монитор* после применения политик

2.3.4. Создание политики безопасности, блокирующей весь открытый трафик на рабочем месте Сотрудник_1 Центр офис.

Для создания политики безопасности, блокирующей весь открытый трафик на рабочем месте *Сотрудник_1 Центр офис*, выполните следующие действия:

1. В окне программы *ViPNet Policy Manager* перейдите в раздел *Шаблоны политики* и нажмите кнопку *Создать*.
2. В открывшемся окне *Свойства шаблона политики* на вкладке *Основные параметры* задайте имя *Блокировка открытого трафика*.
3. На вкладке *Сетевые узлы* добавьте *Сотрудник_1 Центр офис*.
4. На вкладке *Локальные фильтры открытой сети* нажмите кнопку *Создать...*
5. В открывшемся окне *Свойства фильтра открытой сети* на вкладке *Основные параметры* задайте имя фильтра *Блокировка открытого трафика*, установите переключатель в положение *Блокировать трафик* и нажмите *ОК* (Рисунок 127).

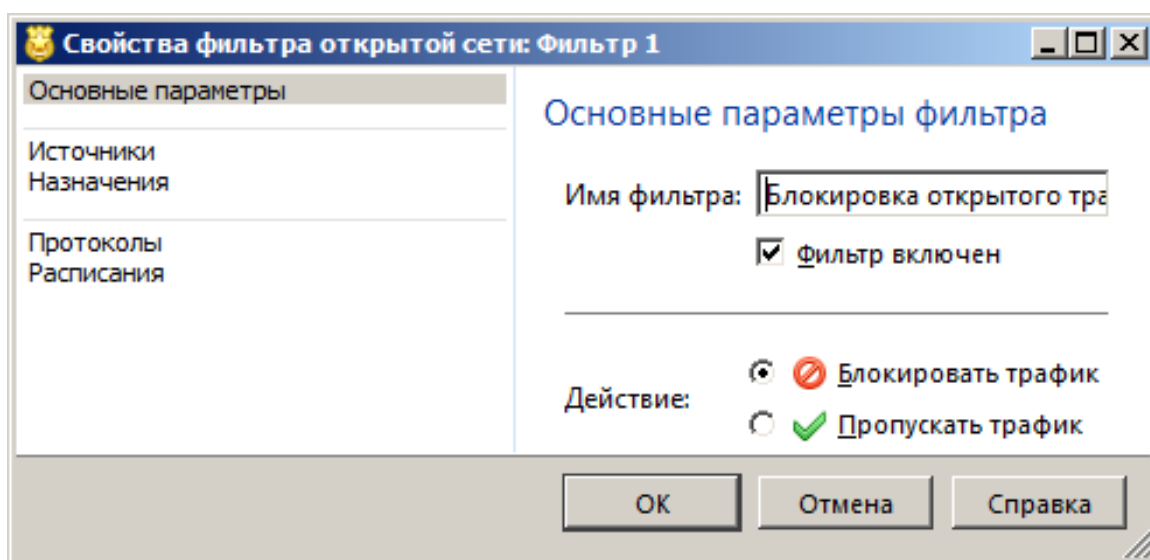


Рисунок 17 – Вкладка *Основные параметры* окна *Свойства фильтра открытой сети*

6. Остальные параметры окна *Свойства фильтра открытой сети* и *Свойства шаблона политики* менять не требуется.
7. Отправьте теперь политики на узел *Сотрудник_1 Центр офис* (в окне программы *ViPNet Policy Manager* раздел *Сетевые узлы* > выбрать узел *Сотрудник_1 Центр офис* > *Отправить политики*).

Проверить были ли приняты политики или нет в данном случае не получится, так как данный узел не был развернут.

Задание № 2.4. Дополнительное задание.

2.4.1. Настройте *ViPNet Удостоверяющий и ключевой центр* таким образом, чтобы ключи узлов автоматически создавались после

формирования справочников в программе *ViPNet Центр управления сетью*.

2.4.2. Просмотреть журнал IP-пакетов узла *Помощник глав админа* с рабочего места *Главного администратора*.