Практическое занятие № 20

Настройка средств криптографической защиты сетевого трафика стандартного протокола ipSec в операционной системе MS Windows

Цель: Научиться защищать сетевой трафик средствами шифрования данных через **ipSec (internet protocol security).**

По заказу ФГУ ГНИИ ИТТ «Информика»
Северо-Кавказский государственный технический университет
Кафедра защиты информации, zik@ncstu.ru

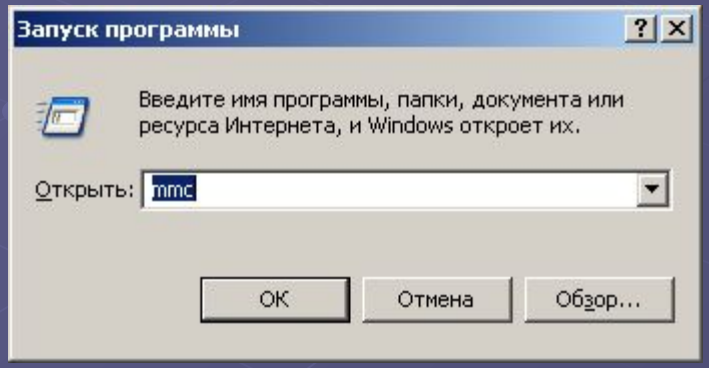
Содержание:

По заказу ФГУ ГНИИ ИТТ «Информика»
Северо-Кавказский государственный технический университет
Кафедра защиты информации, zik@ncstu.ru

Теоретическая часть

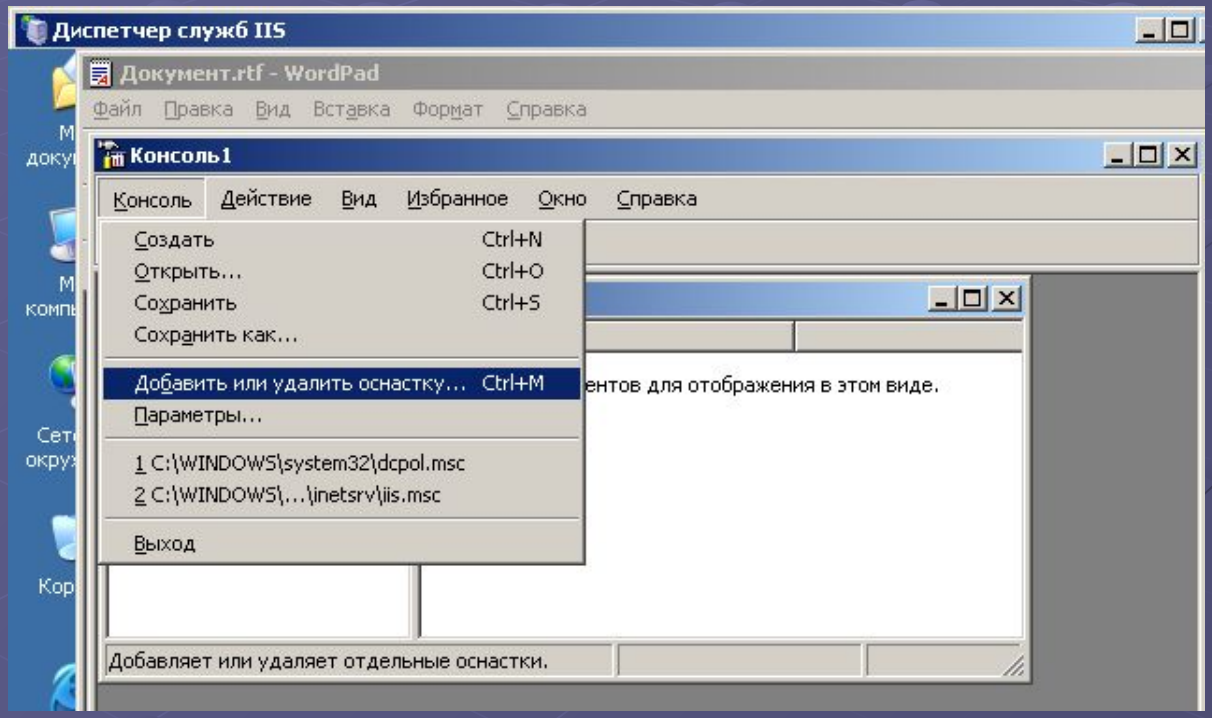
Для управления политикой безопасности **IPSec** с консоли управления Microsoft, выполните следующие действия.

Нажмите кнопку **Пуск**, выберите команду **Выполнить**, введите **MMC** и нажмите кнопку **OK**.



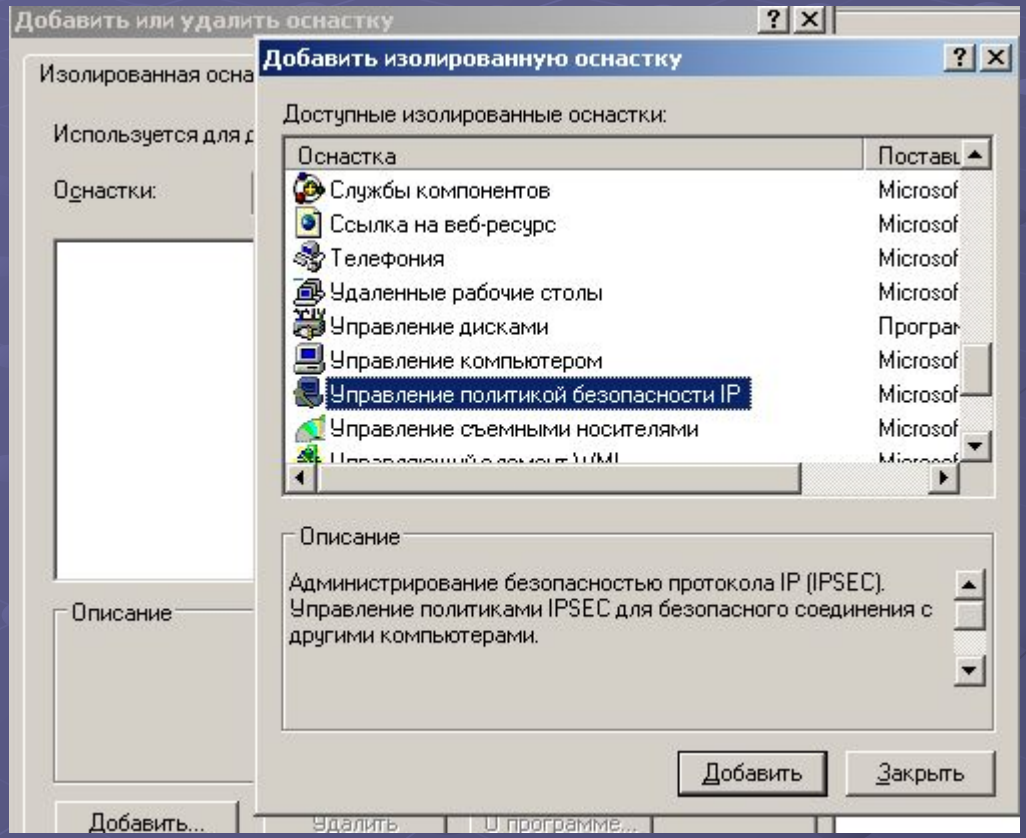
Теоретическая часть

В меню **Консоль** выберите команду **Добавить или удалить оснастку**, затем нажмите кнопку **Добавить**.



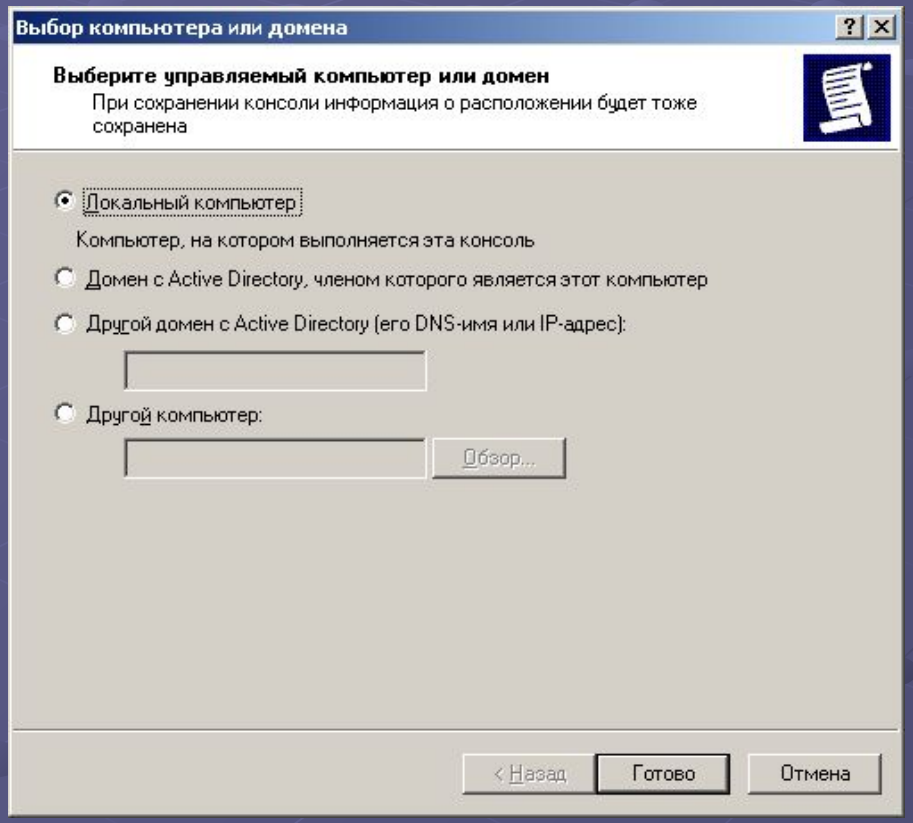
Теоретическая часть

Выберите **Управление политикой безопасности IP** и нажмите кнопку **Добавить**.



Теоретическая часть

Выберите компьютер, политиками **IPSec** которого требуется управлять.

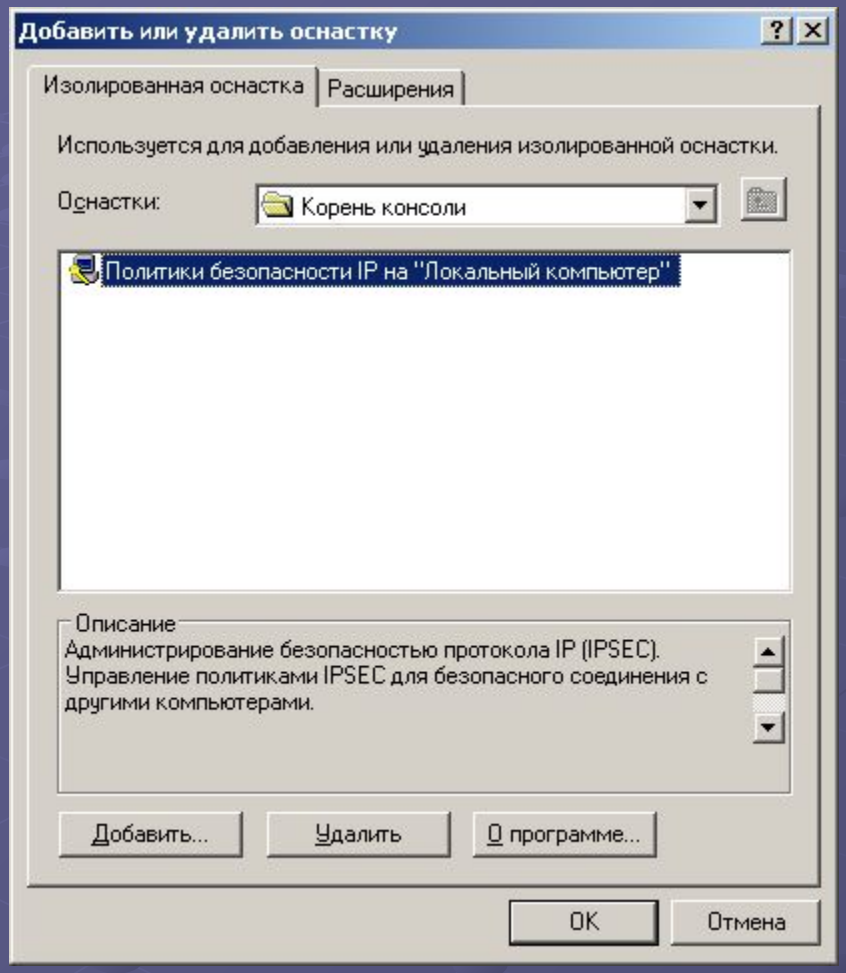


Теоретическая часть

Чтобы	Выполните следующее действие
Управлять только компьютером, на котором выполняется консоль	Выберите **Локальный компьютер**
Управлять политиками и IPSec для любого члена домена	Выберите **Домен с Active Directory,** членом которого является этот компьютер.
Управлять политиками **IPSec** для домена, членом которого компьютер, на котором выполняется консоль, не является	Выберите **Другой домен с Active Directory**.
Управлять удаленным компьютером	Выберите **Другой компьютер**

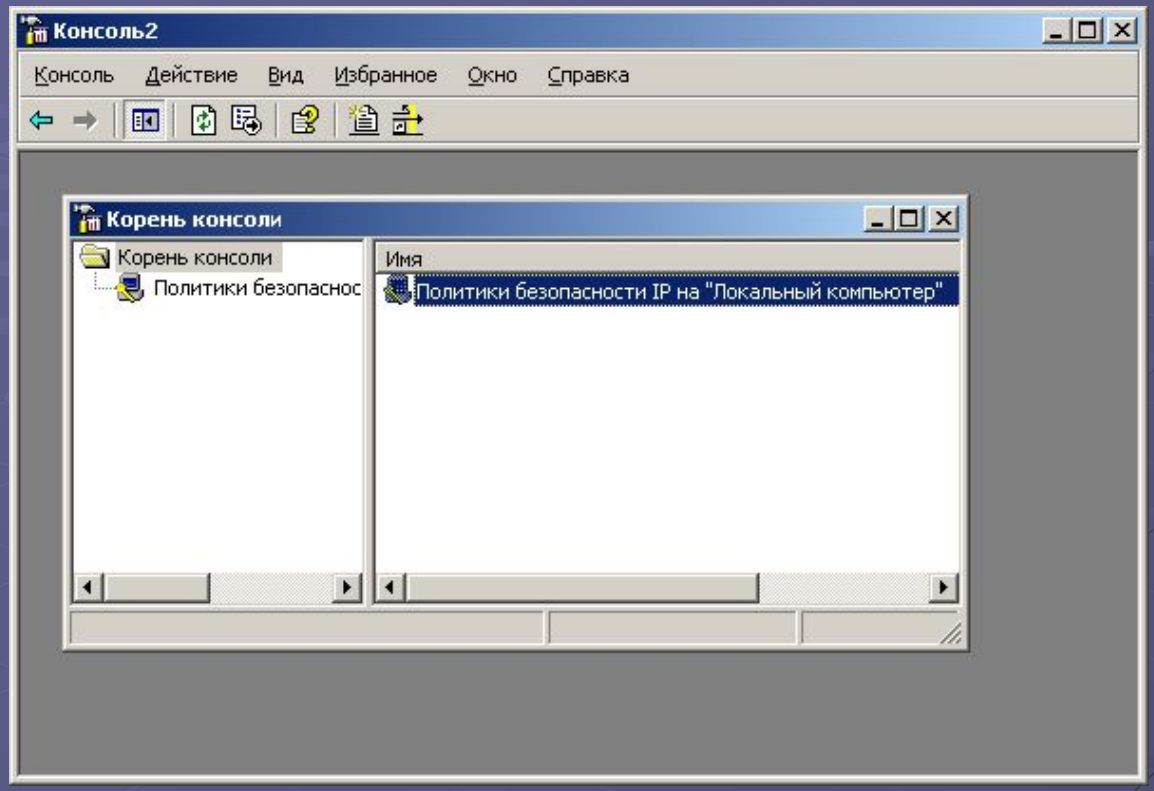
Нажмите **ОК**

Теоретическая часть



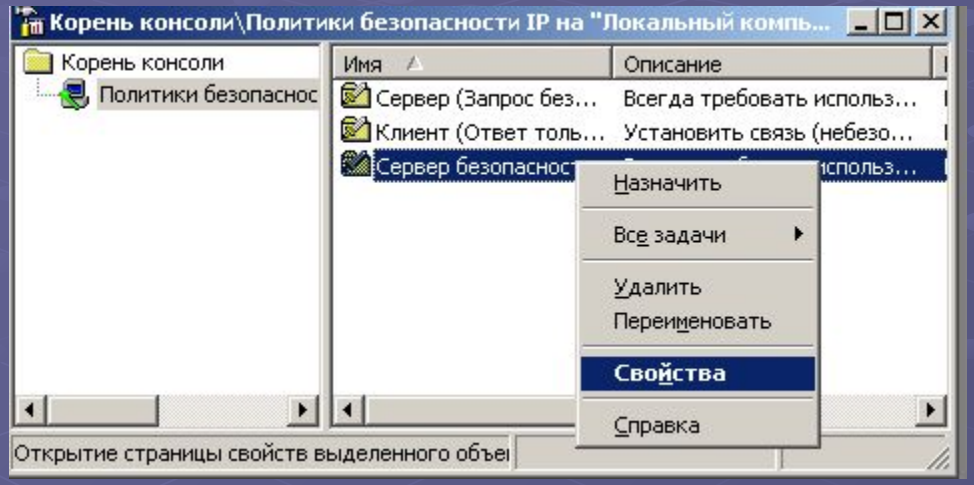
Сделать двойной клик на **Политики безопасности** на **"Локальный компьютер"**

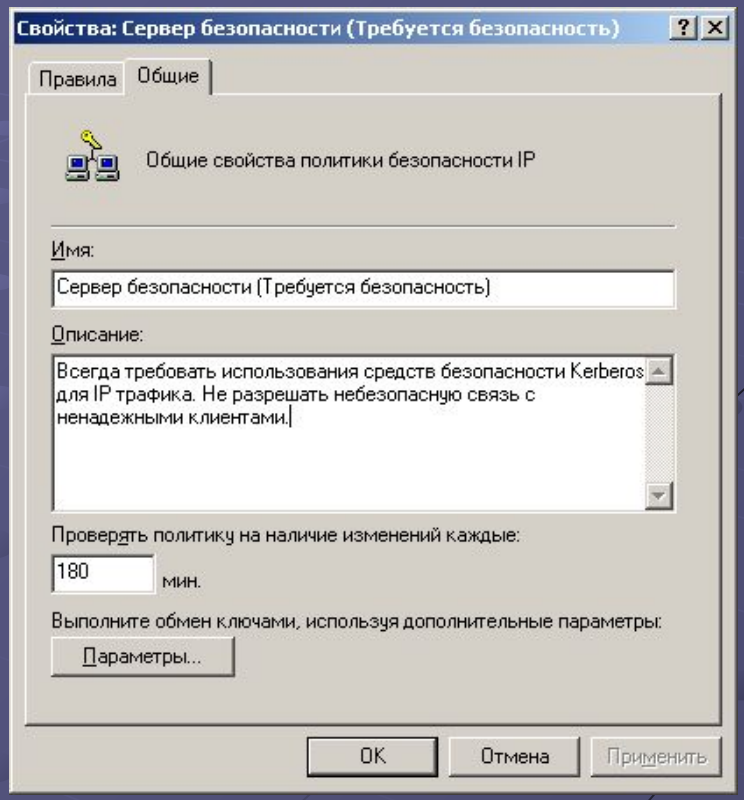
Теоретическая часть



Выбрать свойства "**Сервер безопасности**"

Теоретическая часть

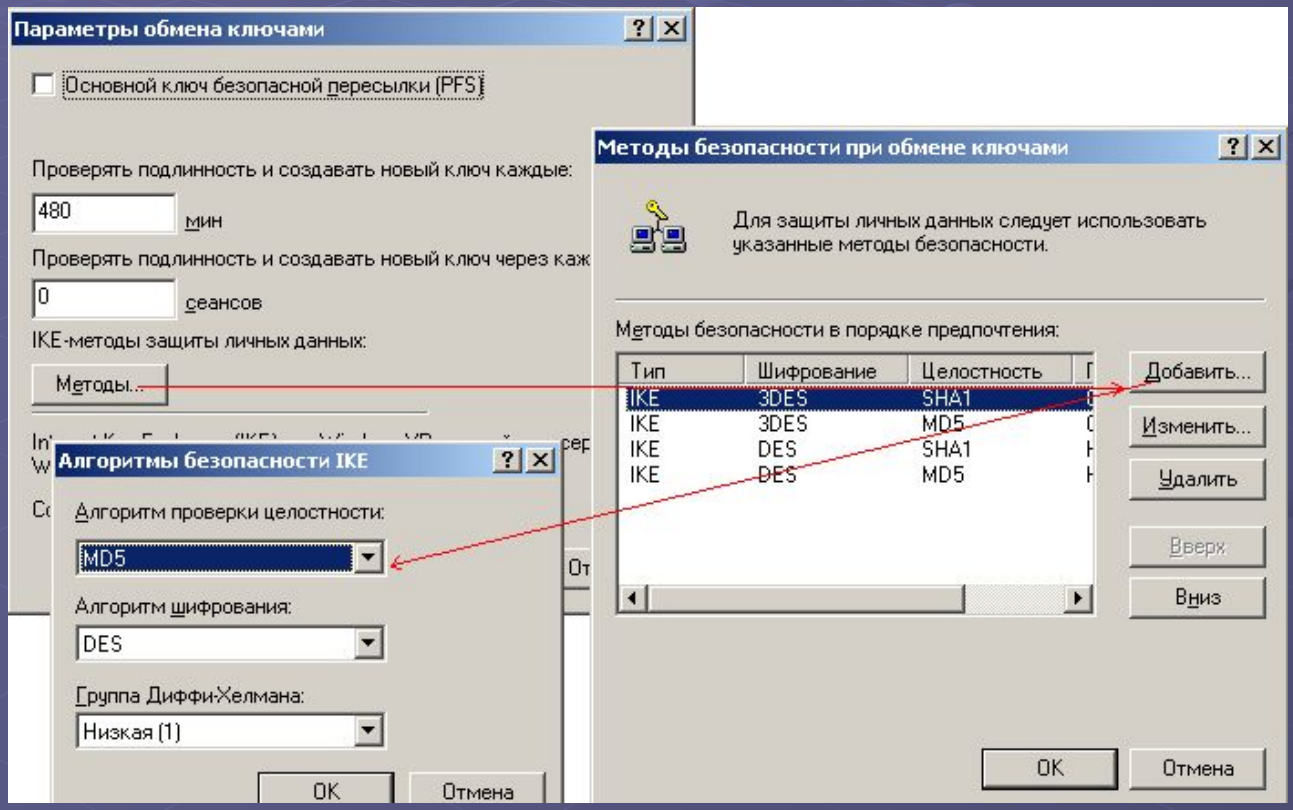




Во вкладке **Общие** указать настройки:

Теоретическая часть

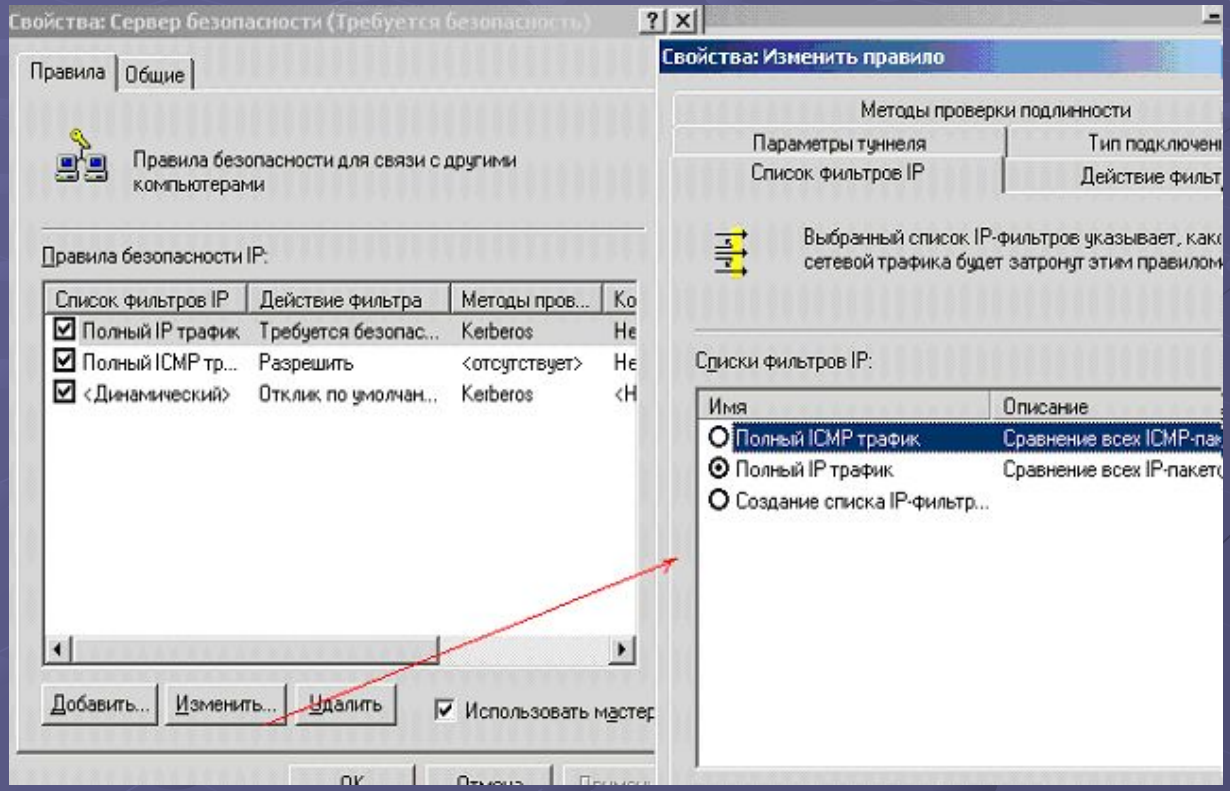
Указать используемые методы шифрования данных



Теоретическая часть

После этого необходимо определить правила и фильтры **ipSec**

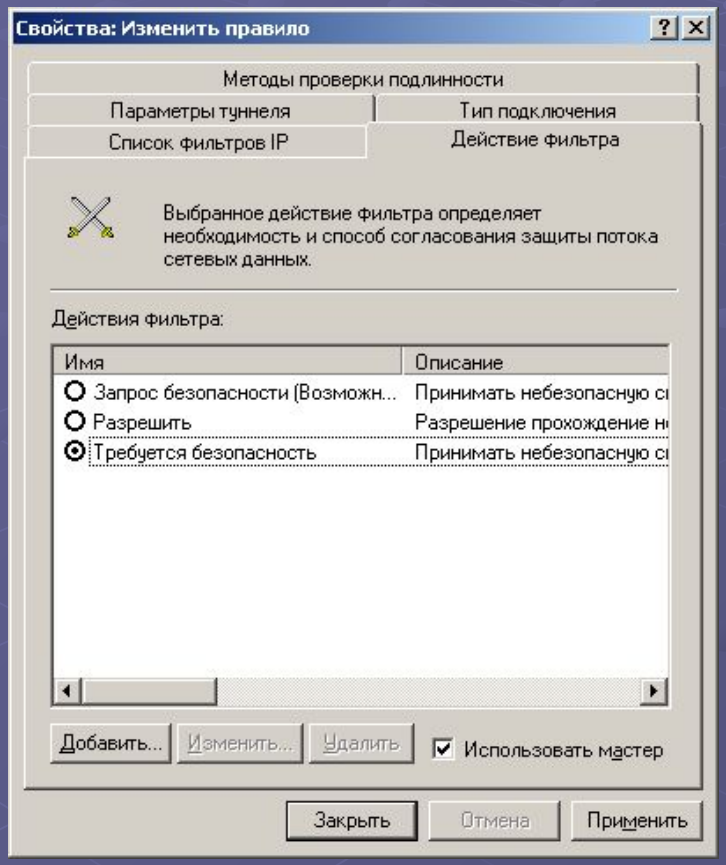
Для создания новых правил или изменения старых необходимо выбрать вкладку **Правила → Список фильтров IP.**



Полный IP трафик - отфильтровывать весь трафик

Теоретическая часть

Вкладка **Действие фильтра**. Выбрать один из предлагаемых действий фильтра:



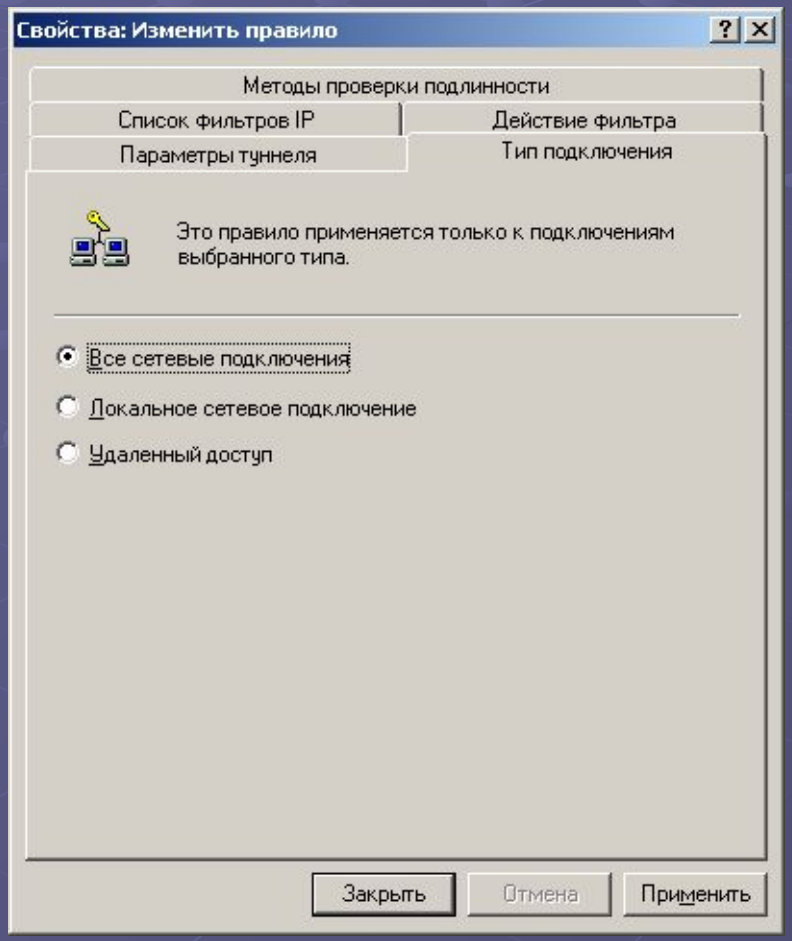
Запрос безопасности - Принимать небезопасную связь, но требовать от клиентов применения методов доверия и безопасности. Будет поддерживаться небезопасная связь с ненадежными клиентами, если клиенты не выполнят требование безопасности;

Разрешить - Разрешение прохождения небезопасных **ip**-пакетов;

Требуется безопасность - Принимать небезопасную связь, но всегда требовать от клиентов применение методов доверия и безопасности. Не будет поддерживаться связь с ненадежными клиентами.

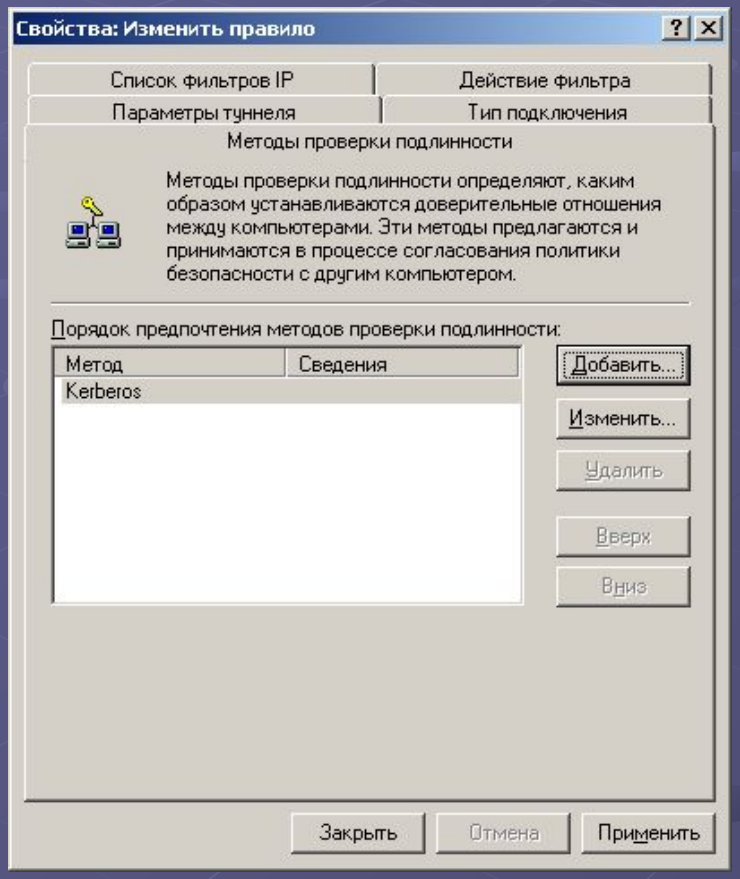
Теоретическая часть

Тип подключения - вкладка, на которой указывается тип сетевого подключения, на которое распространяется данное правило.



Методы проверки подлинности

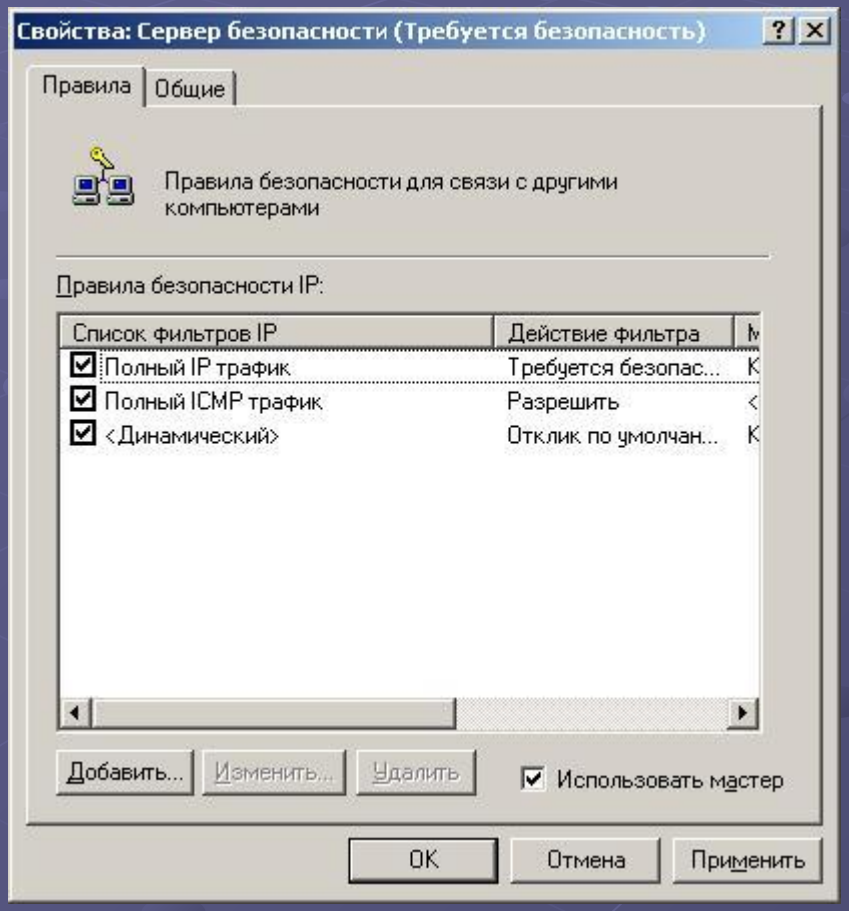
Для пары компьютеров необходимо установить одинаковый способ проверки подлинности, чтобы избежать конфликтов.



Методы проверки подлинности

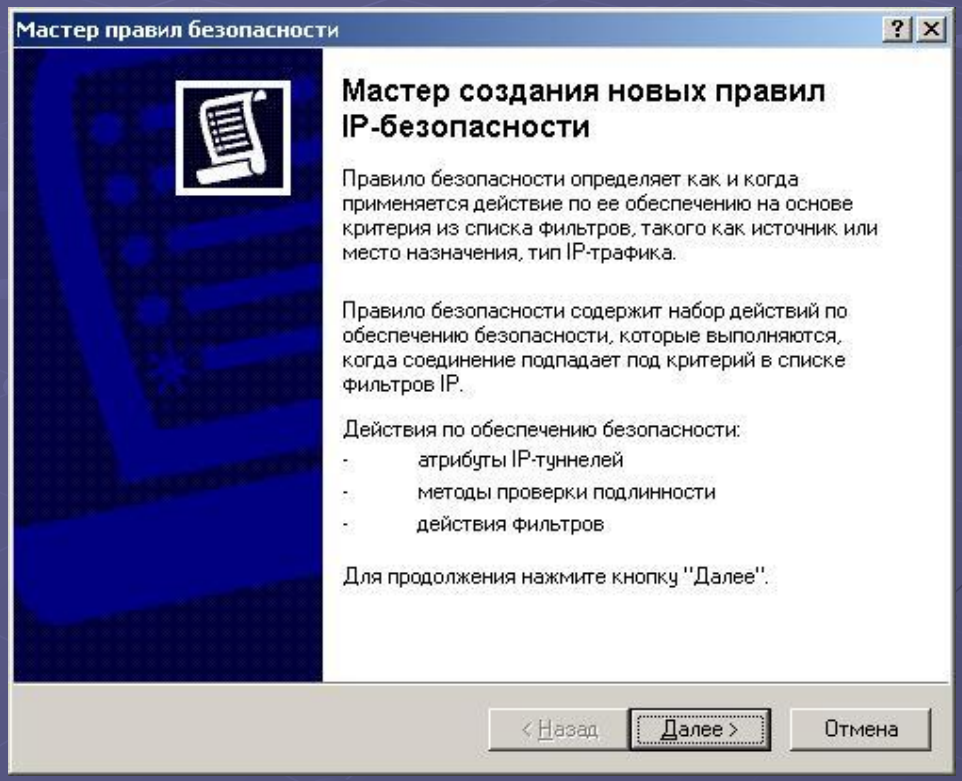
Пример разрешения связи по протоколу **http**

1) Нажать Добавить



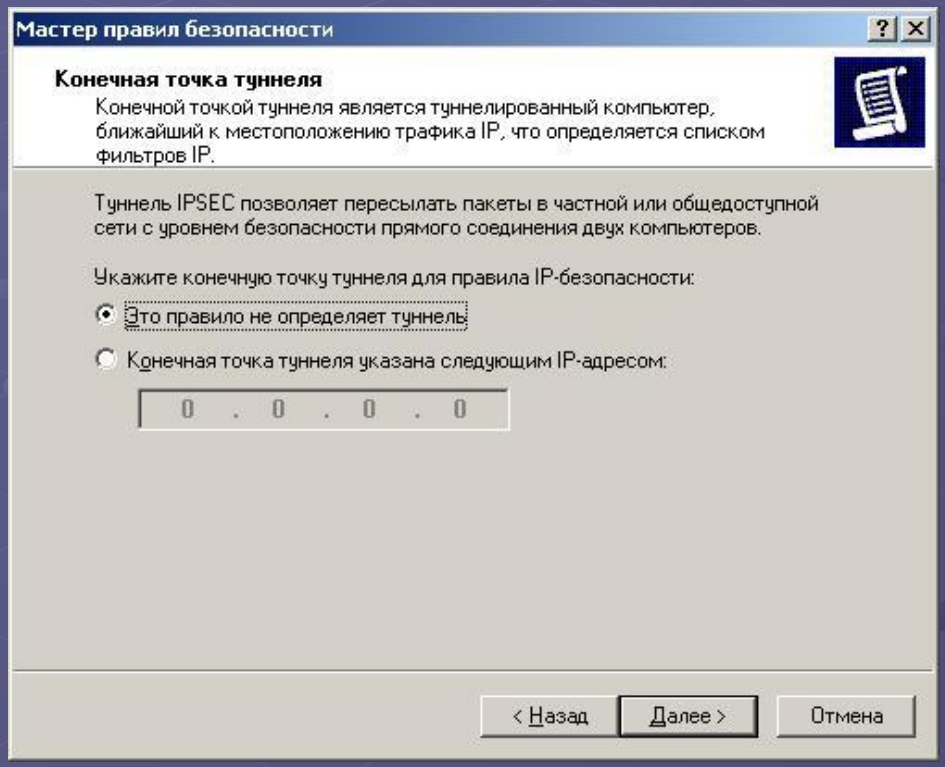
Методы проверки подлинности

2) Запустить **Мастер создания новых правил**.



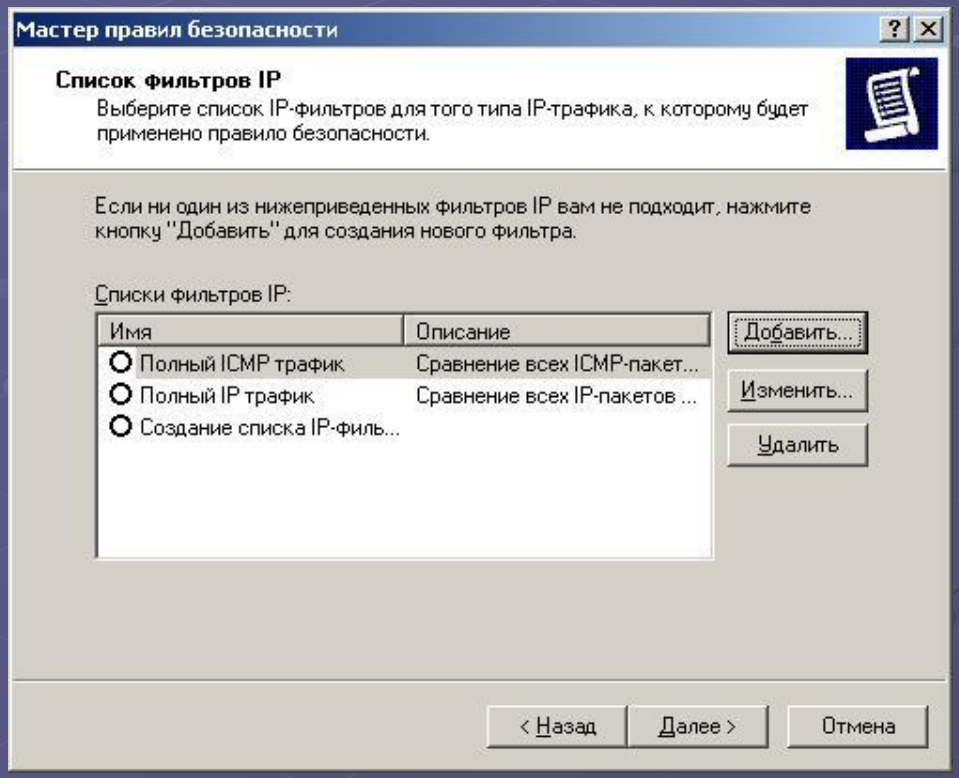
Методы проверки подлинности

3) Нажать **Далее**



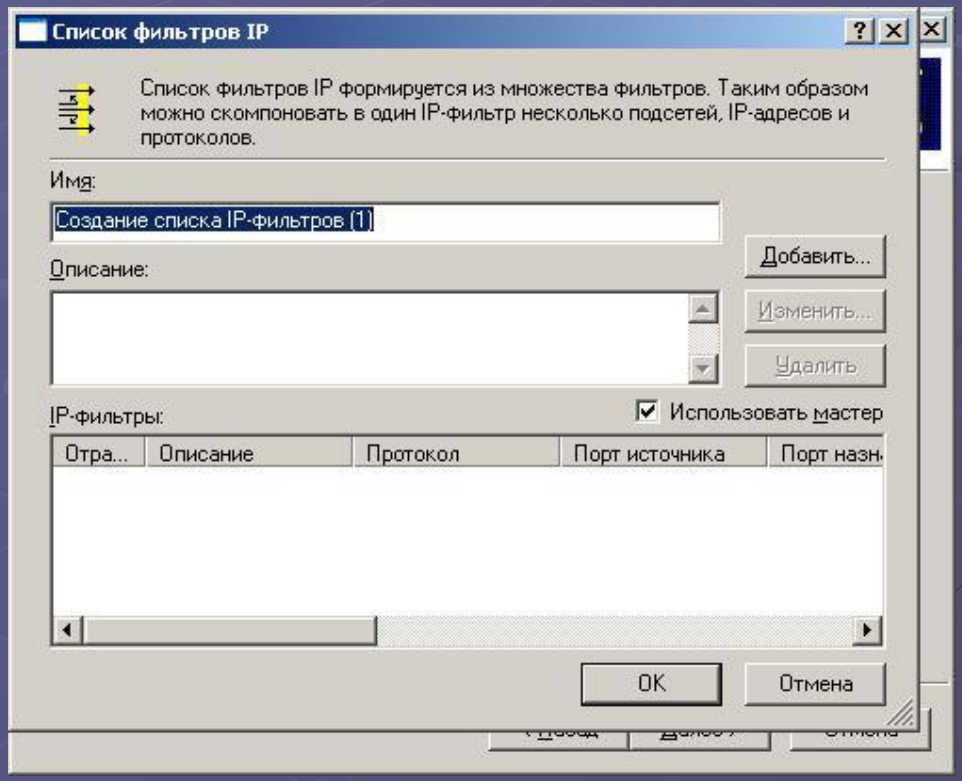
Методы проверки подлинности

4) Нажать **Добавить**



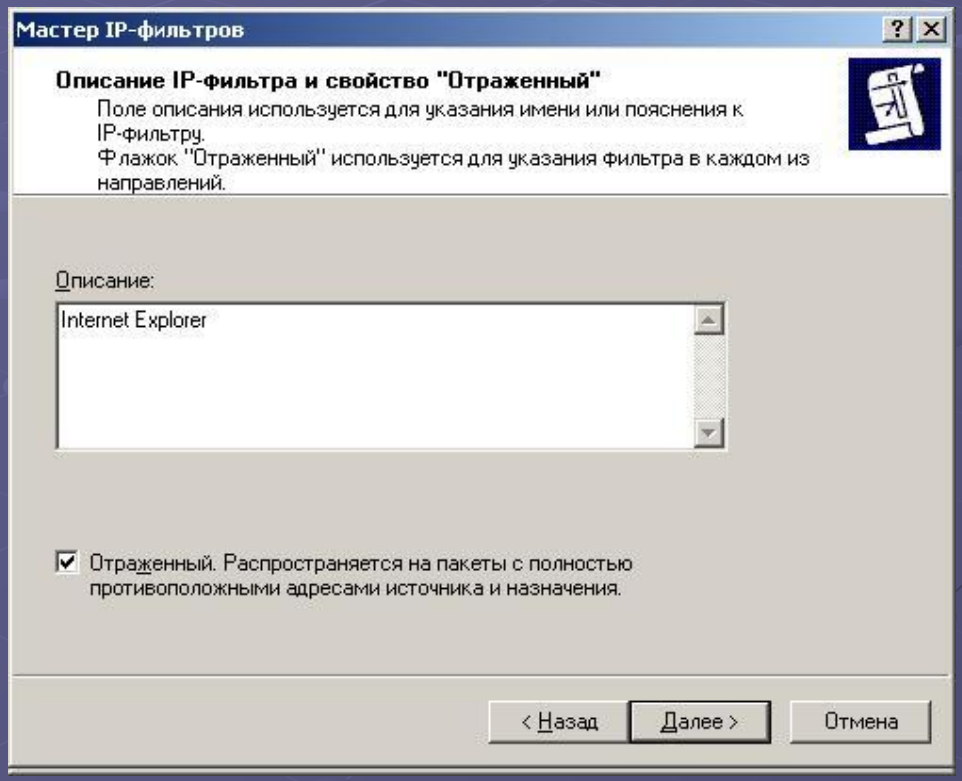
Методы проверки подлинности

5) Создать новый фильтр через **Мастер,** нажав кнопку **Добавить**



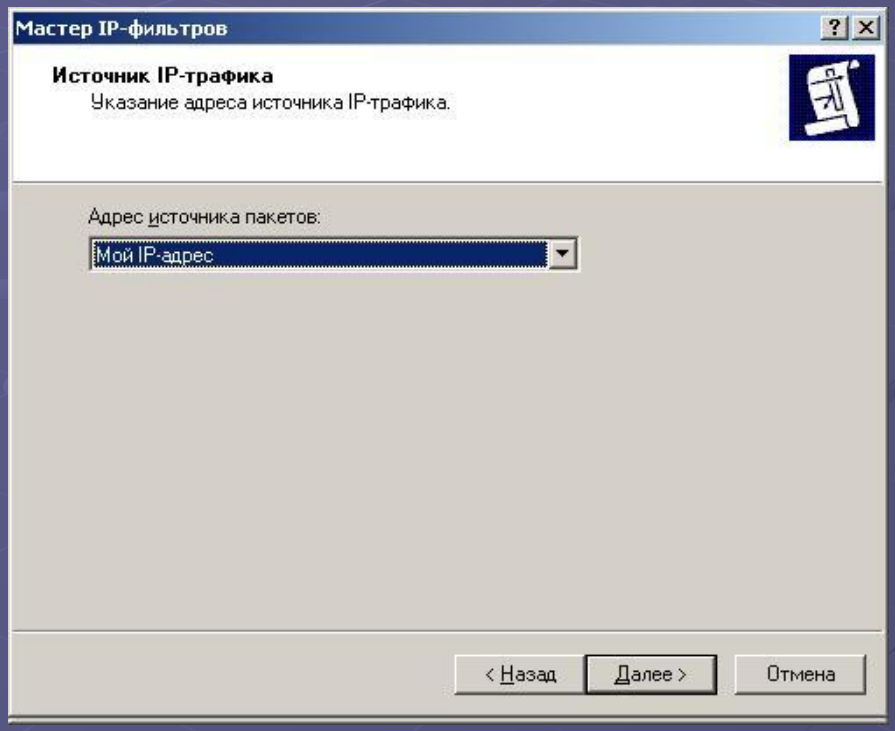
Методы проверки подлинности

6) Нажать **Далее,** если нужно, можно указать **Описание**.



Методы проверки подлинности

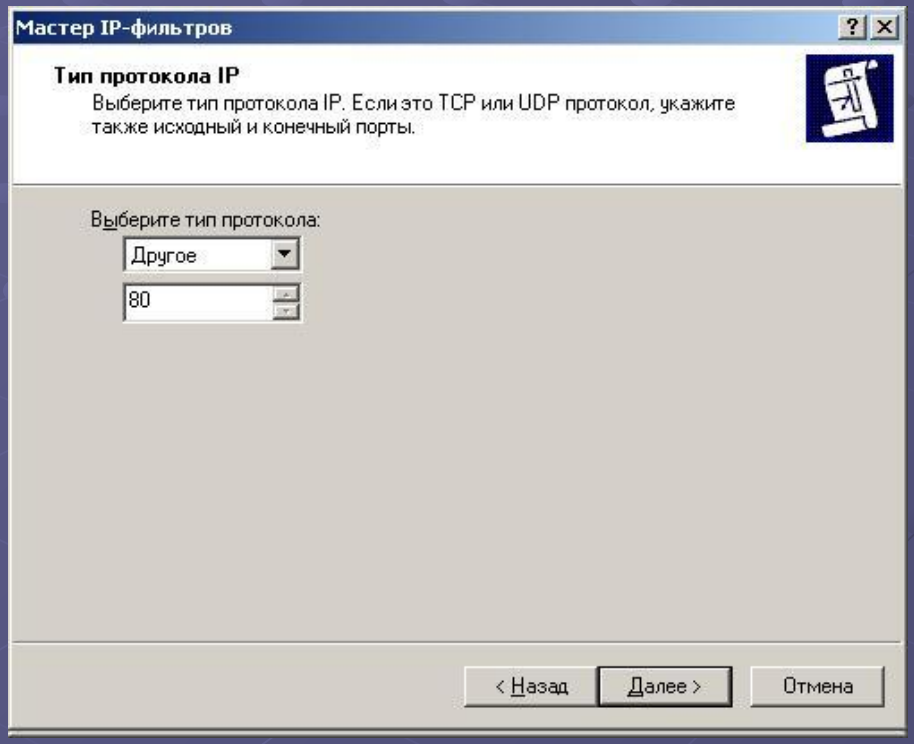
7) Указать **Адрес источника пакетов,** нажать **Далее**.



Методы проверки подлинности

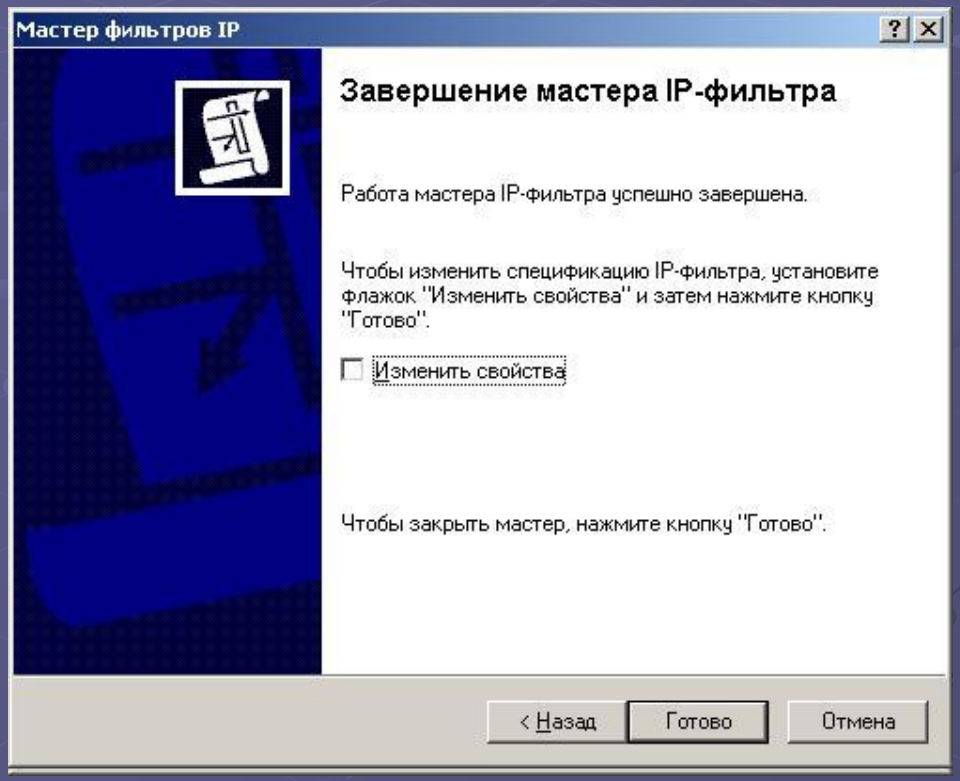
8) По аналогии с **Адресом источника** указать **Адрес назначения**.

9) Указать номер порта, используемый для протокола, в нашем случае **80**.



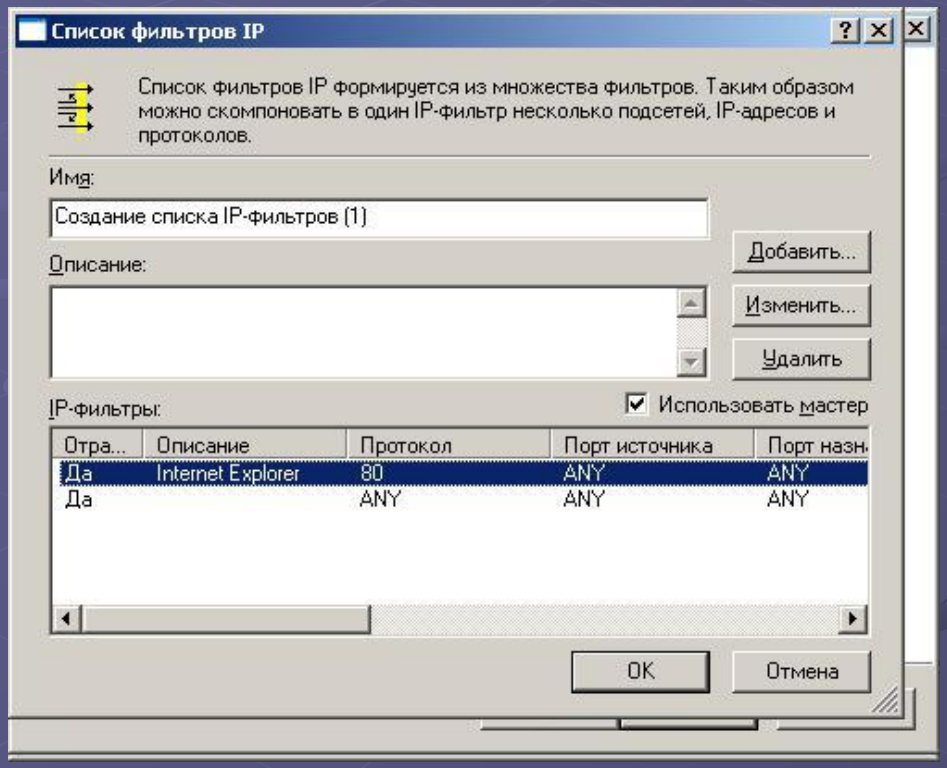
Методы проверки подлинности

10) Завершить работу с **Мастером**.



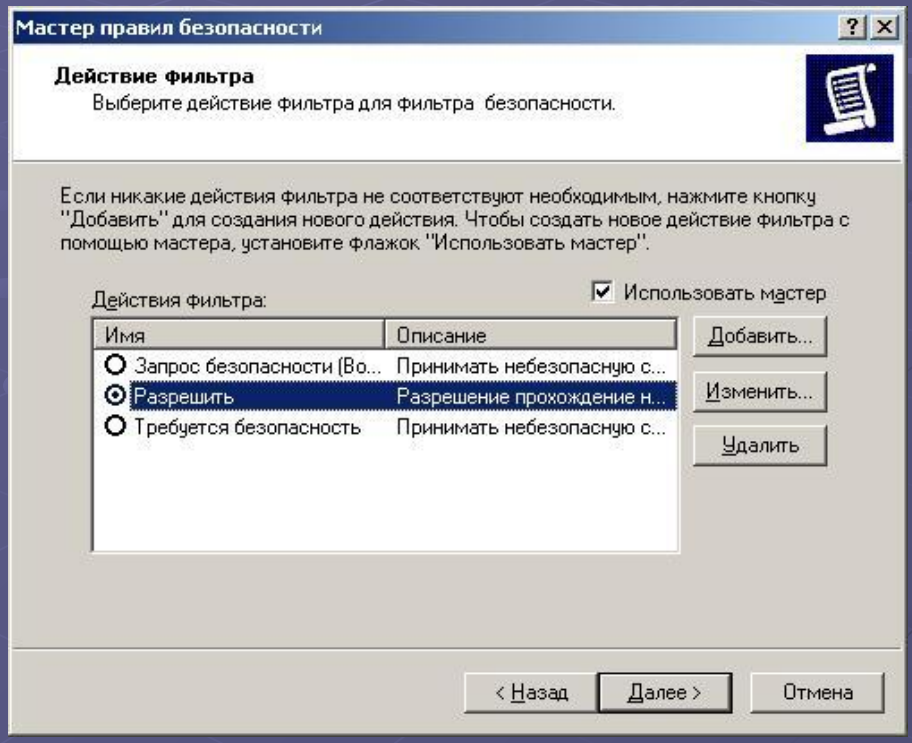
Методы проверки подлинности

11) Убедиться, что правило появилось в списке фильтров.



Методы проверки подлинности

12) Разрешить передачу данных данному протоколу.



Практическая часть

Подготовьте **Internet Explorer** для безопасной работы через **proxy server**, адрес которого **192.168.0.16** порт **8080**.

Результат: Выполнив работу, вы научитесь управлять защитой сетевого трафика с помощью средств стандартного протокола IPSec операционной системы Microsoft Windows.