Настройка выполняется посредством оснастки «Локальная политика безопасности» (Панель управления/Администрирование/Локальная политика безопасности):

1) для создания политики IP-безопасности выделить пункт Политики IP-безопасности и средствами контекстного меню для данного элемента выбрать команду Создать политику IP-безопасности;

Файл Действие Вид Справка Файл Действие Вид Справка Создать политику IP-безопасности Создать политику IP-безопасности Управление списками IP-фильтра и действиями фильтра Все задачи Вид Вид	🦂 Локальная политика безопасности		
<ul> <li>Политики открытого ключа</li> <li>Политики ограниченного исп</li> <li>Политики управления прилож</li> <li>Политики IP-безопасности на</li> <li>Конфигурация расширенной политики аудита</li> <li>Обновить</li> <li>Экспортировать список</li> </ul>	Файл Действие Вид Справка Файл Действие Вид Справка Параметры безопасности Политики учетных записей Локальные политики Брандмауэр Windows в режим Политики диспетчера списка Политики диспетчера списка Политики открытого ключа Политики открытого ключа Политики ограниченного исп Политики управления прилож Конфигурация расширенной пол	Создать политику IP-безопасности Управление списками IP-фильтра и действиями фильтра Все задачи Вид Обновить Экспортировать список Справка	
Создание политики ID-безопасности	Создание политики ID-Безопасности		4

2) в появившемся диалоговом окне *Мастер* политики IP- безопасности нажать Далее;

3) в появившемся окне ввести имя новой политики и нажать *Далее,* 

4) в следующем окне включить опцию использования правила по умолчанию;

5) на следующем шаге работы мастера выбрать способ проверки подлинности пользователя: с помощью протокола Kerberos, с помощью сертификата пользователя либо на основании строки для защиты обмена ключами;

6) изменить свойства можно по завершении работы мастера либо позже, выделив нужную политику и выбрав из контекстного меня пункт *Свойства,* 

7) для создания правила безопасности открыть свойства созданной политики безопасности IP, отменить опцию Использовать мастер и на вкладке Правила нажать кнопку Добавить,

8) на закладке Тип подключения выбрать, для каких сетевых подключений будет применяться создаваемое правило;

9) на закладке Методы проверки подлинности добавить несколько методов проверки и изменить порядок их предпочтения;

10) после выбора типа подключений и методов проверки подлинности воспользоваться вкладкой *Список фильтров IP* для выбора списка фильтров IP либо для создания нового фильтра;

11) для создания нового фильтра нажать кнопку Добавить, после чего откроется окно Список фильтров IP, в котором следует отменить опцию Использовать мастер, ввести имя списка фильтров и нажать кнопку Добавить,

12) в появившемся диалоговом окне *Свойства: IP-Фильтр* указать адреса источника и получателя пакетов, к которым будет применяться фильтр, протокол и порты источника и получателя;

13) определить действие фильтра на закладке Действие фильтра,

14) для создания нового действия фильтра отменить опцию Использовать мастер и нажать кнопку Добавить. На вкладке Методы безопасности открывшегося окна Свойства: создание действия фильтра указать, нужно ли разрешить прохождение данных, заблокировать их либо согласовать безопасность;

15) если выбран пункт Согласовать безопасность, добавить методы безопасности и изменить порядок их предпочтения. При добавлении методов безопасности следует выбрать, будет ли использоваться АН, ЕБР, либо настроить безопасность вручную, выбрав пункт Настраиваемая безопасность безопасность (таким образом, можно задействовать и АН и ЕБР);

16) С помощью пункта Настраиваемая безопасность выбрать алгоритмы проверки целостности и шифрования, а также параметры смены ключей сеанса.

/кажите параметры для особого ме	етода безопасности.
ПЦелостность данных и адресов б	без шифрования (АН):
Алгорити проверки целостност	MANDER OF BUILDING AND
SHA1	
Иелостность данных с шифрован	нием (ESP):
Алгоритм проверки целостност	W.
SHA1 -	
Алгоритм шифрования:	
3DES 🔹	
Параметры ключей селиса:	
Будет передано данных:	Смена ключа каждые.
100000 KE	3600