

НАСТОЙКА МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕРВЕРОВ ЭЛЕКТРОННОЙ ПОЧТЫ

Безопасная настройка почтовой службы SMTP

**E-mail
сервер**



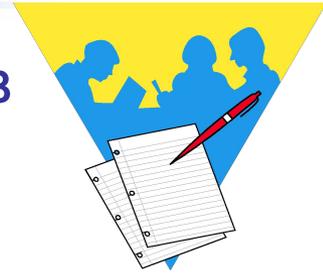
Безопасная настройка SMTP сервера

С точки зрения безопасности интерес представляют следующие возможности конфигурирования:

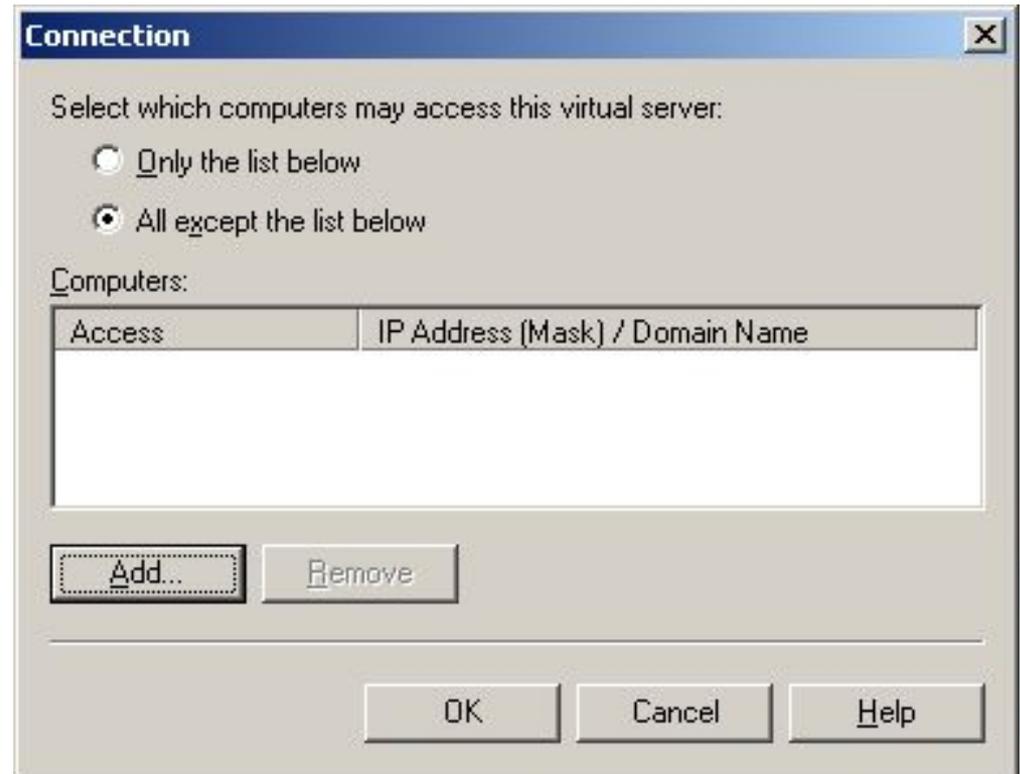
- Разграничение доступа к SMTP серверу в зависимости от IP-адресов хостов, сетей или имен доменов
- Настройка вариантов аутентификации на сервере SMTP
- Настройка ретрансляции почтовых сообщений через сервер
- Фильтрация сообщений по адресу отправителя
- Удаление информации о версии из заголовка службы SMTP
- Управление автоматической генерацией ответов
- Управление регистрацией событий в логах на сервере
- Введение ограничений на почтовые сообщения

Безопасная настройка SMTP сервера

Разграничение доступа к SMTP серверу в зависимости от IP-адресов хостов, сетей или имен доменов



Эта возможность защищает от угрозы маскировки нарушителя под другого пользователя (клиента), когда нарушителю отказывают в обслуживании по SMTP по критерию почтового адреса отправителя.



Безопасная настройка SMTP сервера

Настройка вариантов аутентификации клиентов на SMTP сервере



Анонимный
доступ



Базовая
аутентификация
(имя и пароль в
открытом виде)



Аутентификация по
правилам Windows



Authentication

Select acceptable authentication methods for this resource.

Anonymous access
No user name or password required.

Basic authentication
The password will be sent over the network in clear text using standard commands.

Requires TLS encryption

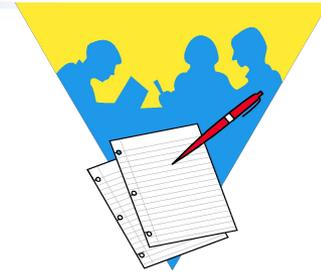
Default domain:

Integrated Windows Authentication
The client and server negotiate the Windows Security Support Provider Interface.

OK Cancel Help

Безопасная настройка SMTP сервера

Outbound security



Анонимный
доступ



Базовая
аутентификация
(имя и пароль в
открытом виде)

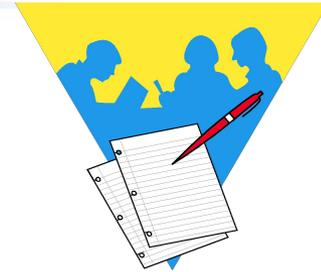


Аутентификация по
правилам Windows



Безопасная настройка SMTP сервера

Выбор соответствующих вариантов аутентификации на клиенте

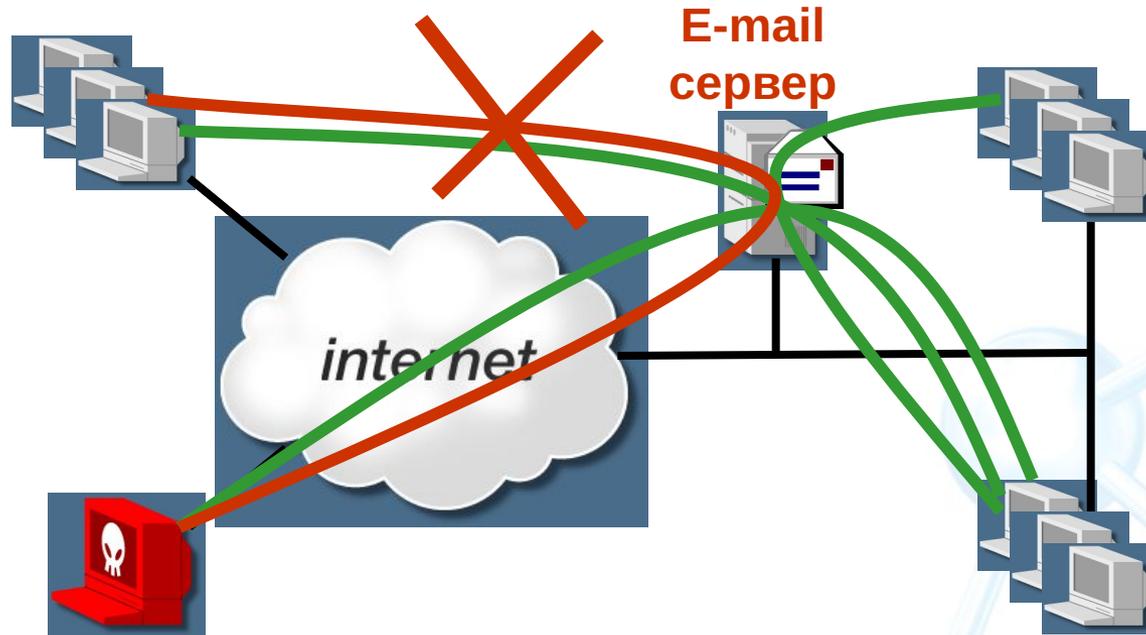
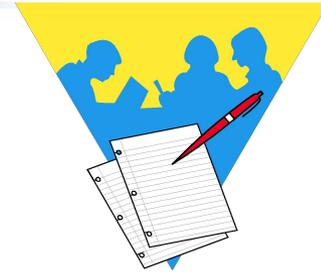


The screenshot shows the 'eadmin Properties' dialog box with the 'Servers' tab selected. The 'Server Information' section indicates the incoming mail server is a POP3 server with the address 'ershov-w2k.edu.infosec.ru'. The outgoing mail (SMTP) address is also 'ershov-w2k.edu.infosec.ru'. Under 'Incoming Mail Server', the account name is 'eadmin' and the password field is empty. There are checkboxes for 'Remember password' (unchecked), 'Log on using Secure Password Authentication' (unchecked), and 'My server requires authentication' (checked). A 'Settings...' button is located next to the authentication checkbox. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

The screenshot shows the 'Outgoing Mail Server' dialog box. Under 'Logon Information', the 'Use same settings as my incoming mail server' radio button is selected. The 'Log on using' radio button is unselected. The 'Account name' field contains 'eadmin' and the 'Password' field is masked with dots. There are checkboxes for 'Remember password' (checked) and 'Log on using Secure Password Authentication' (unchecked). At the bottom are 'OK' and 'Cancel' buttons.

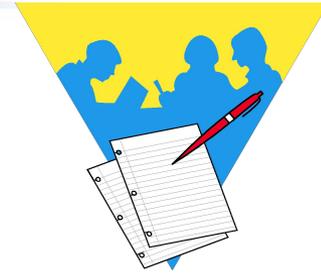
Безопасная настройка SMTP сервера

Настройка ретрансляции (RELAY) почтовых сообщений через сервер

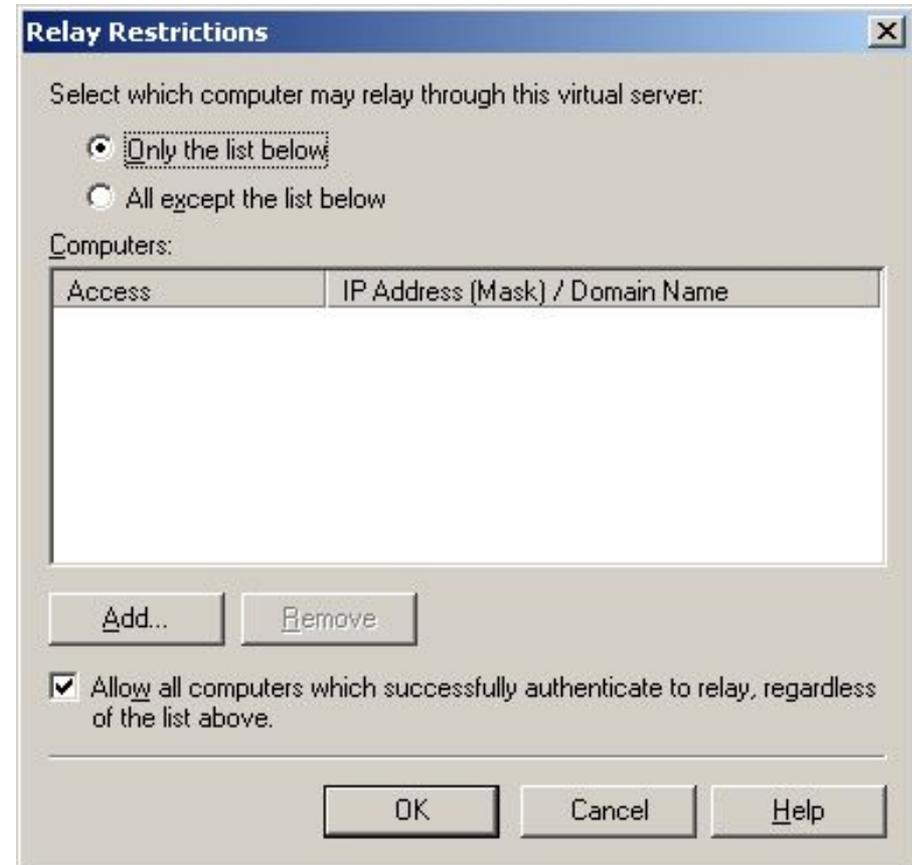


Безопасная настройка SMTP сервера

Настройка ретрансляции (RELAY) почтовых сообщений через сервер

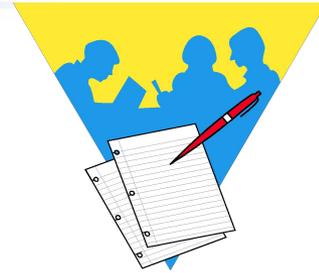


Для предотвращения использования сервера в целях рассылки спама следует выбрать вариант указания списка разрешенных отправителей, поскольку только вполне определенным внешним компьютерам необходимо предоставить возможность отправки сообщений с вашего сервера.



Безопасная настройка SMTP сервера

Фильтрация входящих сообщений по адресу отправителя



Default SMTP Virtual Server Properties

General Access Messages Delivery

Default SMTP Virtual Server

IP address:
[All Unassigned] Advanced...

Limit number of connections to: []

Connection time-out (minutes): 10

Enable logging
Active log format:
W3C Extended Log File Format Properties...

OK Cancel Apply Help

Advanced

Configure multiple identities for this virtual server.

Address:

IP Address	TCP Port	Filter Enabled
[All Unassigned]	25	No
200.0.0.34	25	Yes

Add... Edit... Remove

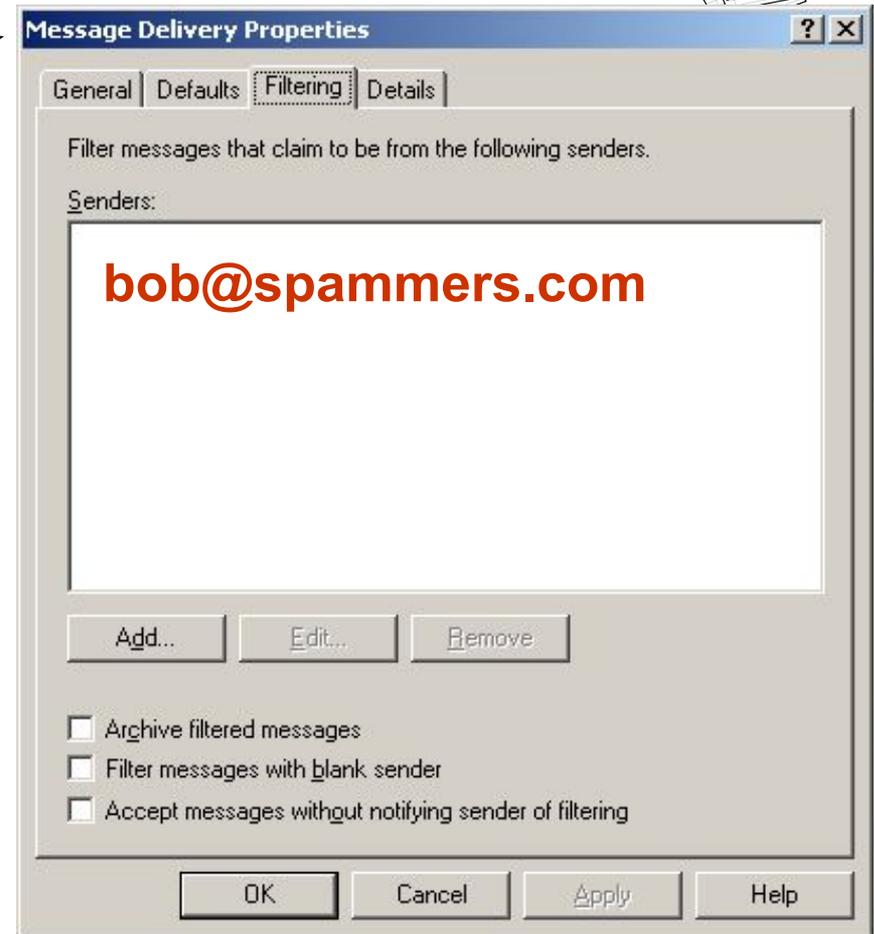
OK Cancel Help

Безопасная настройка SMTP сервера

Фильтрация входящих сообщений
по адресу отправителя

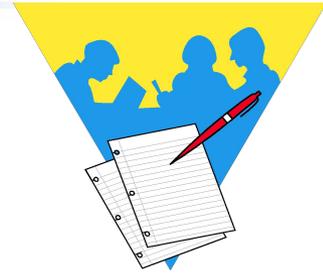


В контейнере Organization
Global Settings >
Message Delivery >
закладка Filtering.

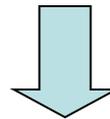


Безопасная настройка SMTP сервера

Удаление информации о версии из
заголовка службы SMTP



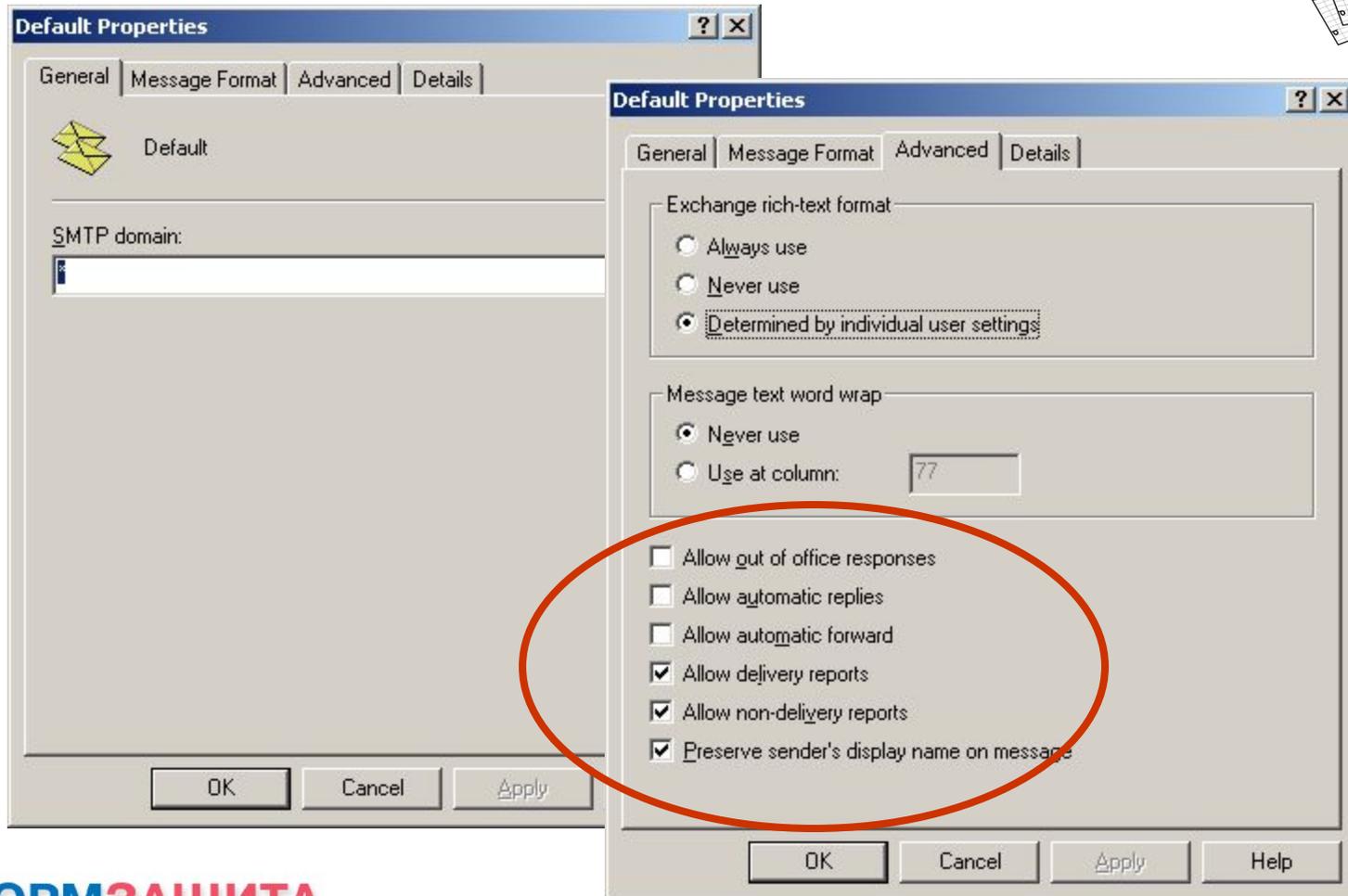
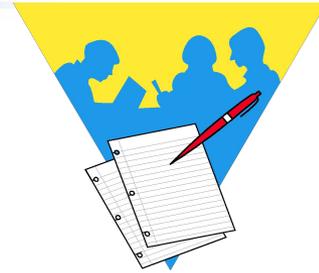
```
C:\WINNT\System32\cmd.exe - telnet localhost 25
220 ershov-w2k.edu.infosec.ru Microsoft ESMTP MAIL Service, Version: 5.0.2195.29
66 ready at Tue, 10 Sep 2002 12:54:20 +0400
```



```
C:\WINNT\System32\cmd.exe - telnet localhost 25
220 ershov-w2k.edu.infosec.ru New SMTP banner for HACKERS Tue, 10 Sep 2002 15:58
:21 +0400
```

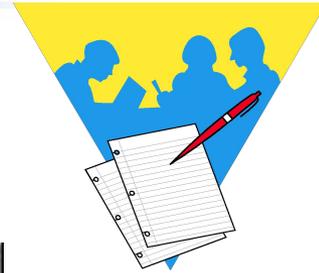
Безопасная настройка SMTP сервера

Управление автоматической генерацией
ответов на почтовые сообщения



Безопасная настройка SMTP сервера

Управление автоматической генерацией ответов на почтовые сообщения



Заместитель [X]

Я нахожусь на работе

Меня нет на работе

Отвечать каждому отправителю единственный раз. Текст ответа:

Извиняйте, нету меня

Правила для обработки сообщений, когда меня нет на работе:

Вкл	Условия	Действия

Вверх

Вниз

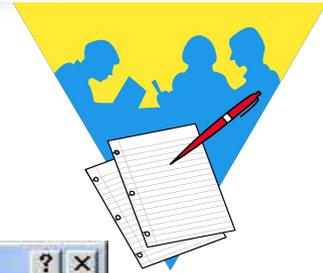
Добавить... Изменить... Удалить

Отображать для всех конфигураций

OK Отмена Справка

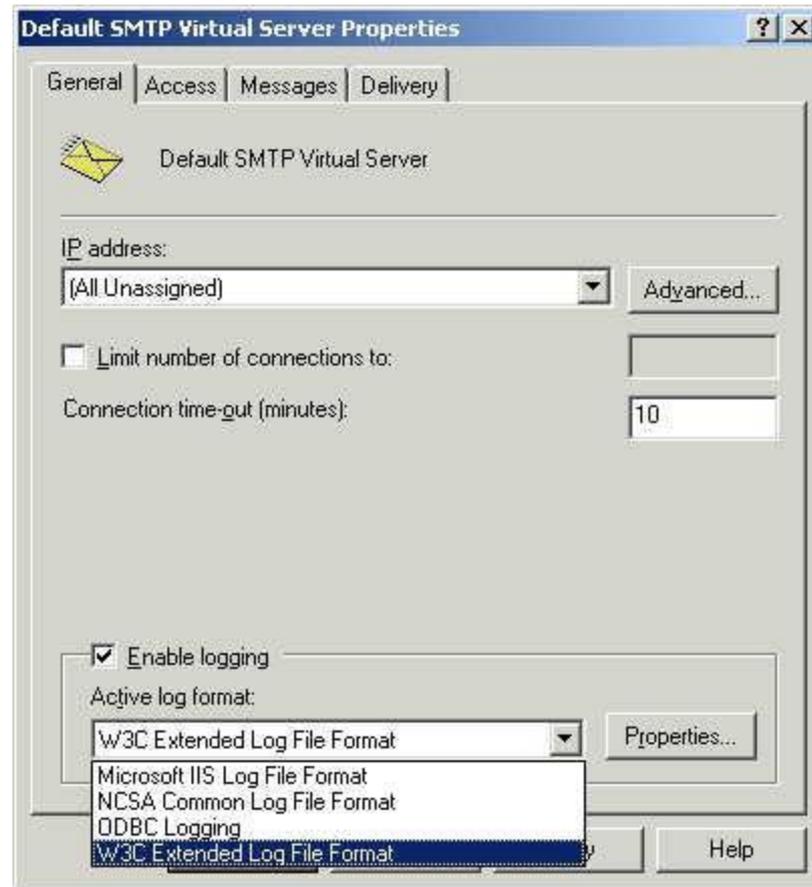
Безопасная настройка SMTP сервера

Управление регистрацией событий
в лог-файлах **на сервере**



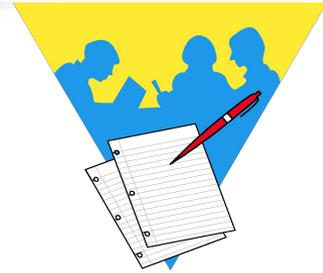
Журналы
сохраняются в
файлах либо в
базе данных
ODBC

Три типа
текстовых
журналов



Безопасная настройка SMTP сервера

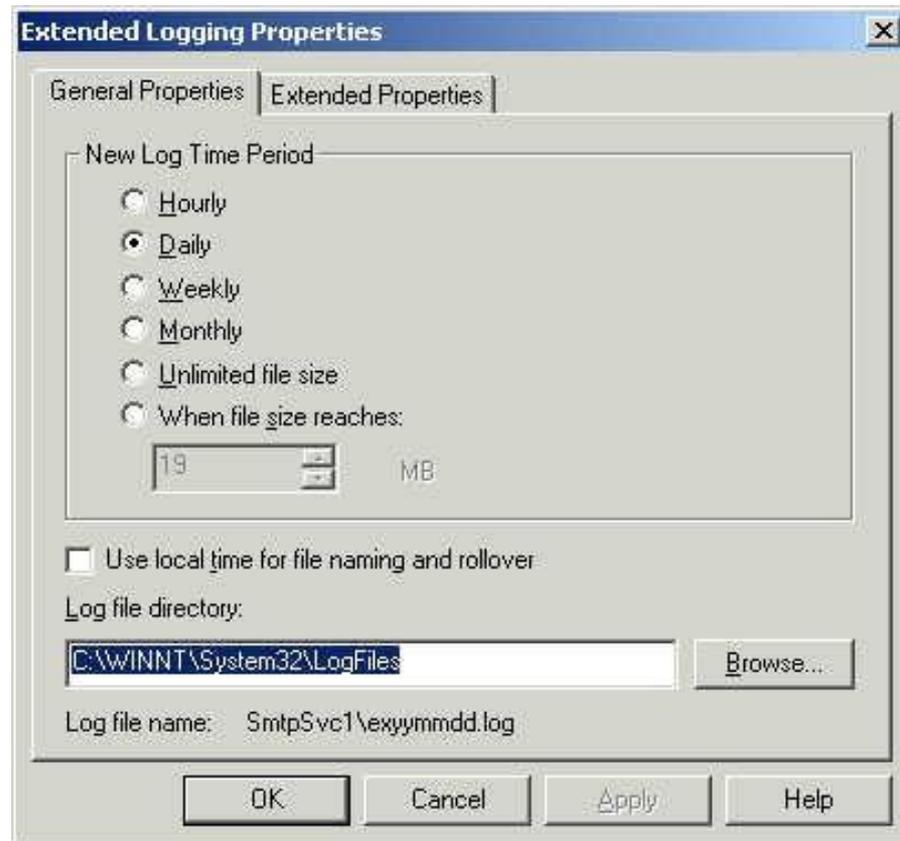
Управление регистрацией событий
в лог-файлах на сервере



Параметры
обработки

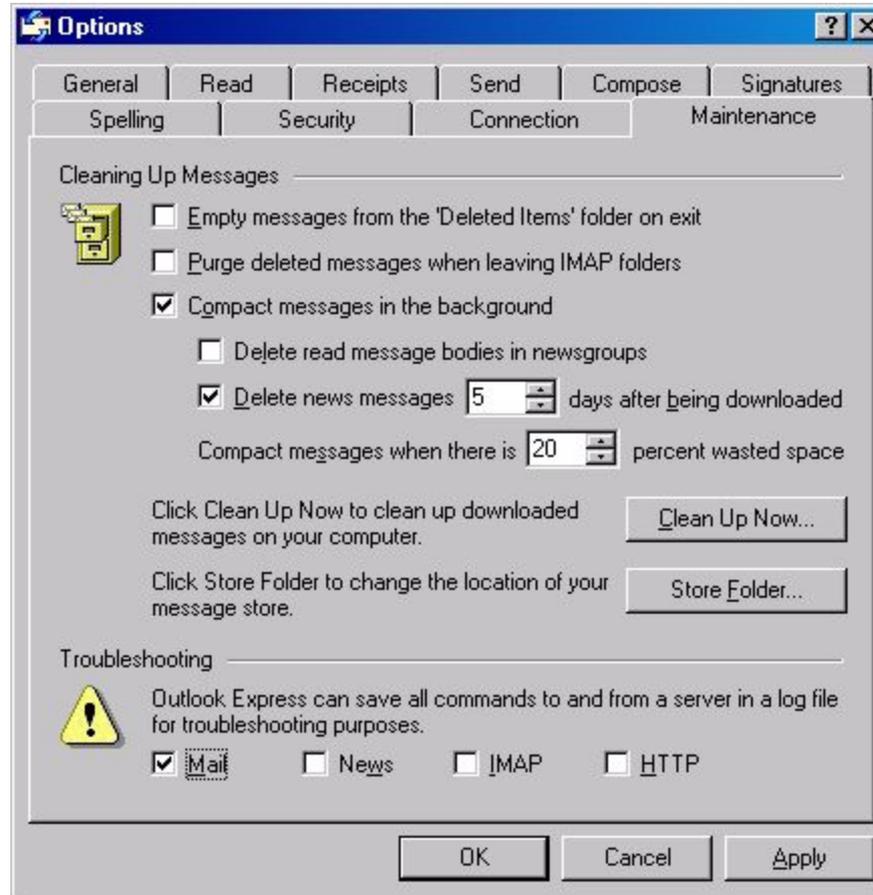
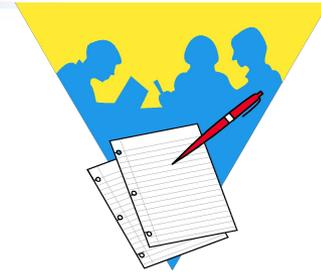
Место
хранения
журналов

Поля,
сохраняемые в
журналах



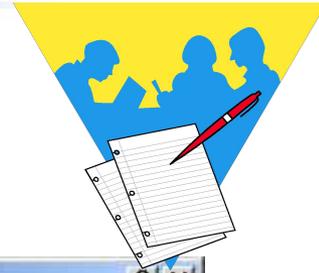
Безопасная настройка SMTP сервера

Управление регистрацией событий в лог-файлах на клиентах



Безопасная настройка SMTP сервера

Введение ограничений на почтовые сообщения

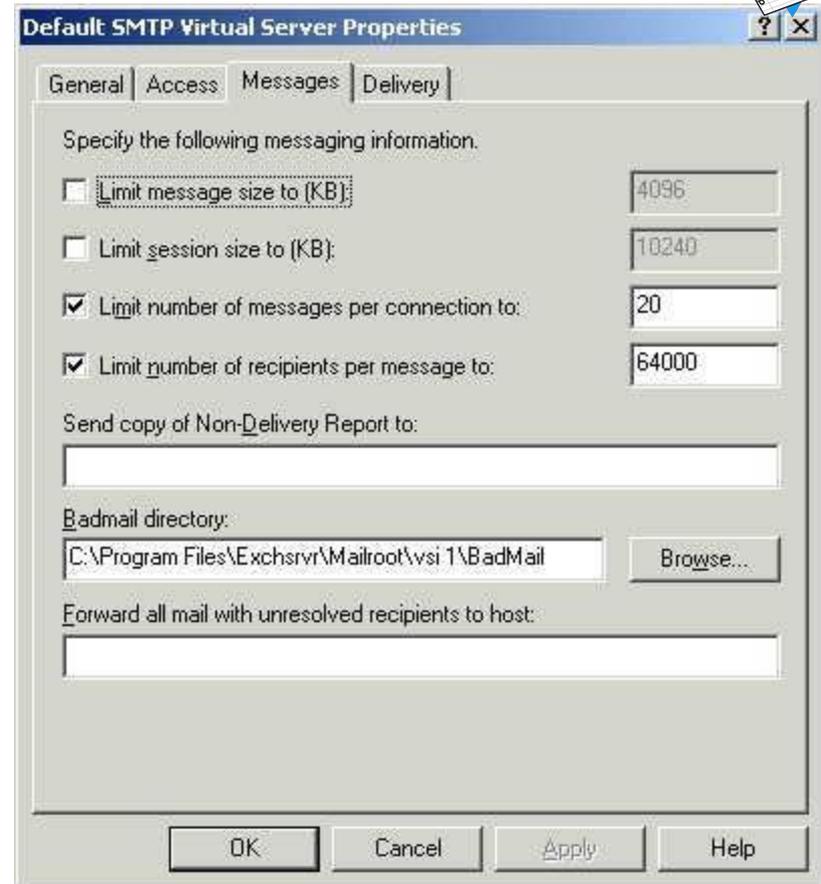


Максимальный размер сообщения

Максимальный размер сессии

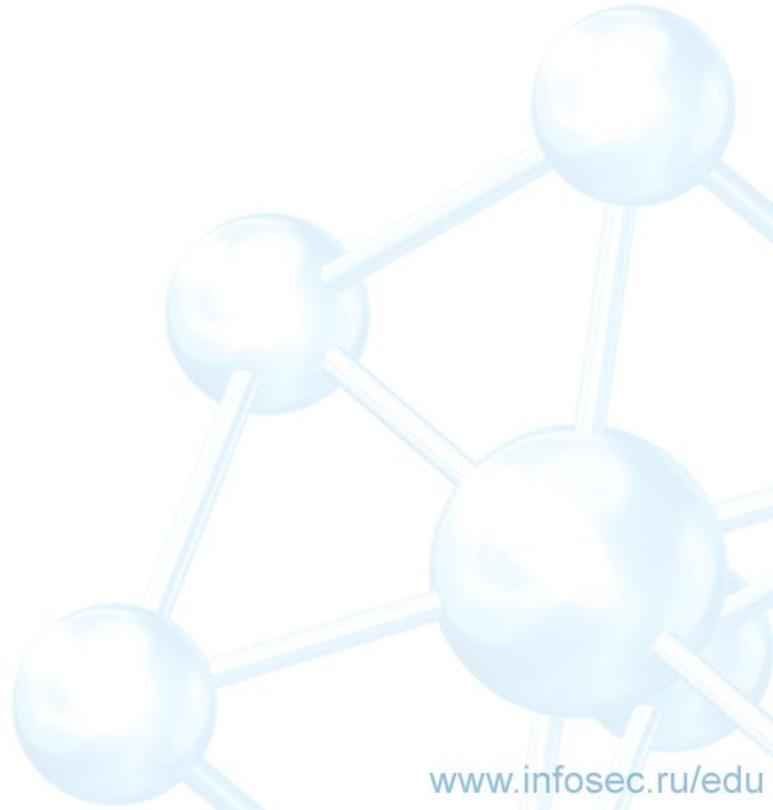
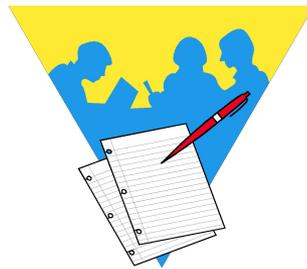
Максимальное количество сообщений в сессии

Максимальное количество получателей сообщения



Практическая работа 10

Безопасная настройка SMTP сервера



Безопасная настройка почтовой службы POP3

**E-mail
сервер**



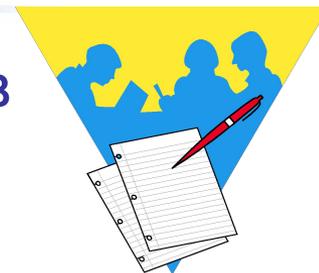
Безопасная настройка POP3 сервера

С точки зрения безопасности интерес представляют следующие возможности конфигурирования:

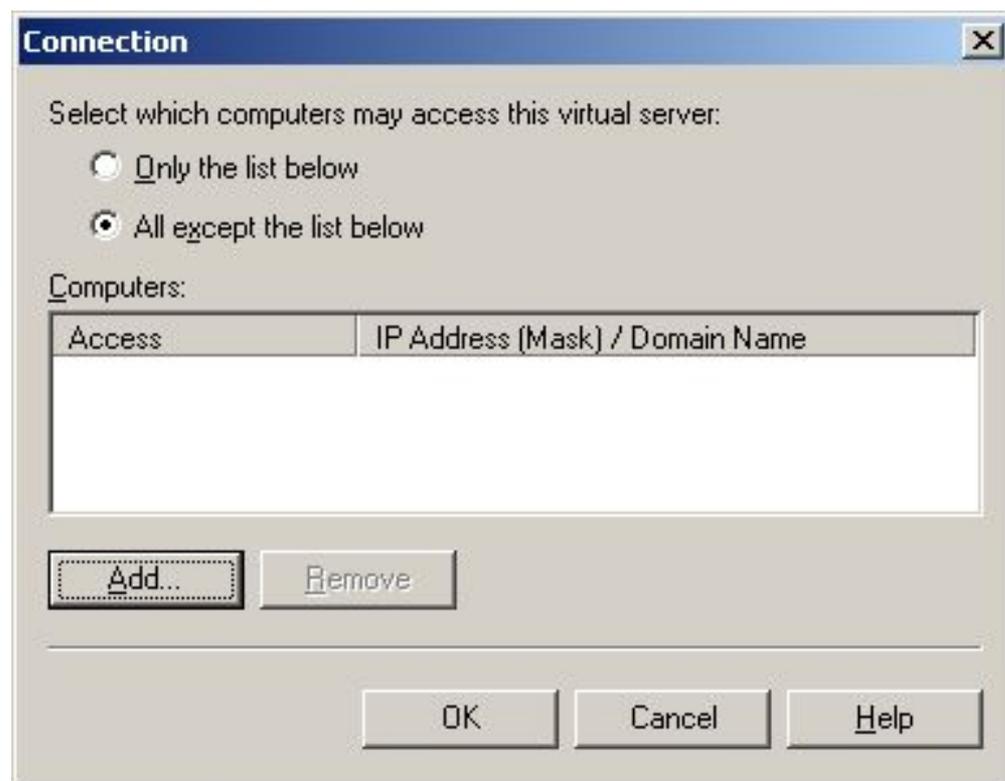
- ❑ Разграничение доступа к POP3 серверу в зависимости от IP-адресов хостов, сетей или имен доменов
- ❑ Настройка вариантов аутентификации на сервере POP3
- ❑ Удаление информации о версии из заголовка и хвостовика службы POP3
- ❑ Управление регистрацией событий в логах на сервере

Безопасная настройка POP3 сервера

Разграничение доступа к POP3 серверу в зависимости от IP-адресов хостов, сетей или имен доменов

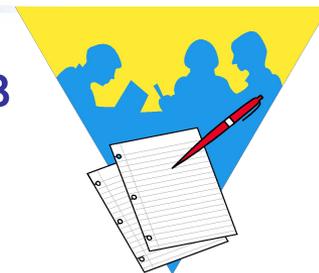


Ограничивает круг лиц, которые могут соединиться с сервером. Поскольку сервер POP используется для получения почты, диапазон адресов обычно известен. Защита от взлома из «чужой» сети.



Безопасная настройка POP3 сервера

Разграничение доступа к POP3 серверу в зависимости от IP-адресов хостов, сетей или имен доменов



IP адрес узла

IP адрес и маска сети

Полное имя домена
(нужен обратный DNS)

Computer

Add one of the following to the list.

Single computer
IP address: [] DNS Lookup...

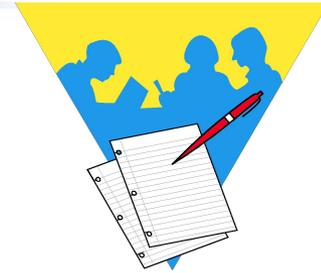
Group of computers
Subnet address: [] Subnet mask: []

Domain
Name: []

OK Cancel Help

Безопасная настройка POP3 сервера

Настройка вариантов аутентификации клиентов на POP3 сервере



Базовая аутентификация (имя и пароль в открытом виде)

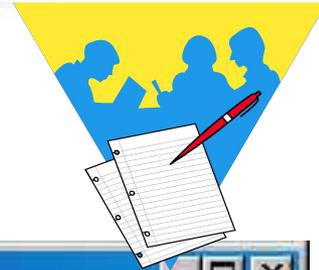


Аутентификация по правилам Windows (NTLM)



Безопасная настройка POP3 сервера

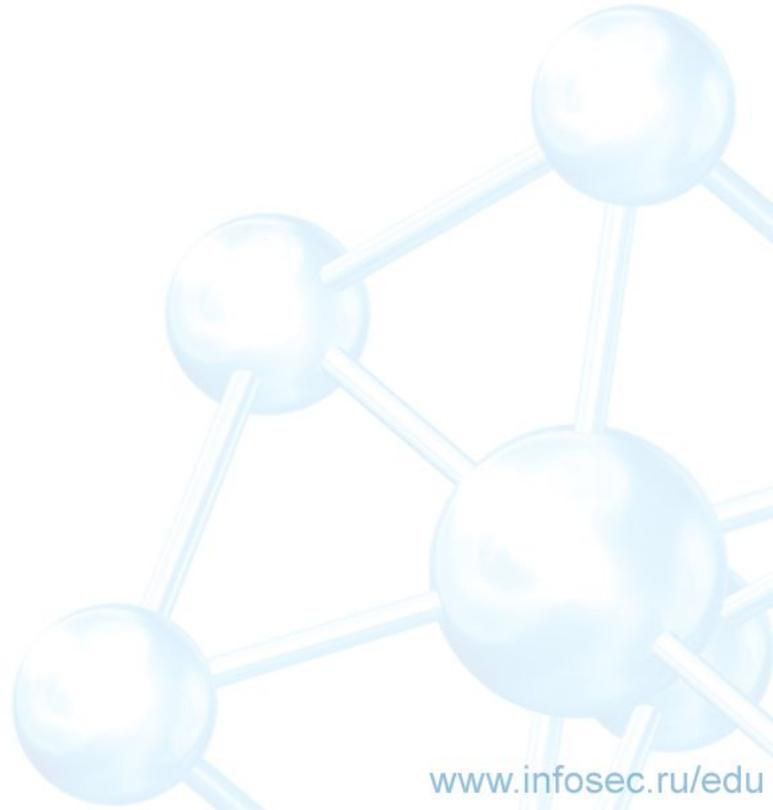
Удаление информации о версии из
заголовка службы POP3



```
C:\WINNT\system32\cmd.exe
+OK Microsoft Exchange 2000 POP3 server ready.
user user1
+OK
pass 1111
+OK User successfully logged on.
stat
+OK 3 7138
retr 1
+OK
Received: from w2kas ([200.1.1.100]) by w2kas.dom.isec with Microsoft SMTPSUC<5.
0.2195.5329>;
quit
+OK Microsoft Exchange 2000 POP3 server version 6.0.6249.0 signing off.
```

Практическая работа 11

Безопасная настройка POP3 сервера



Безопасная настройка почтовой службы IMAP4

**E-mail
сервер**



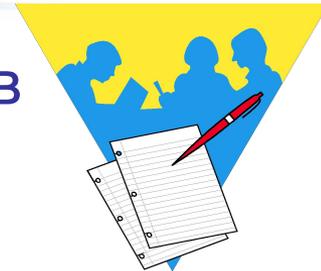
Безопасная настройка IMAP4 сервера

С точки зрения безопасности интерес представляют следующие возможности конфигурирования:

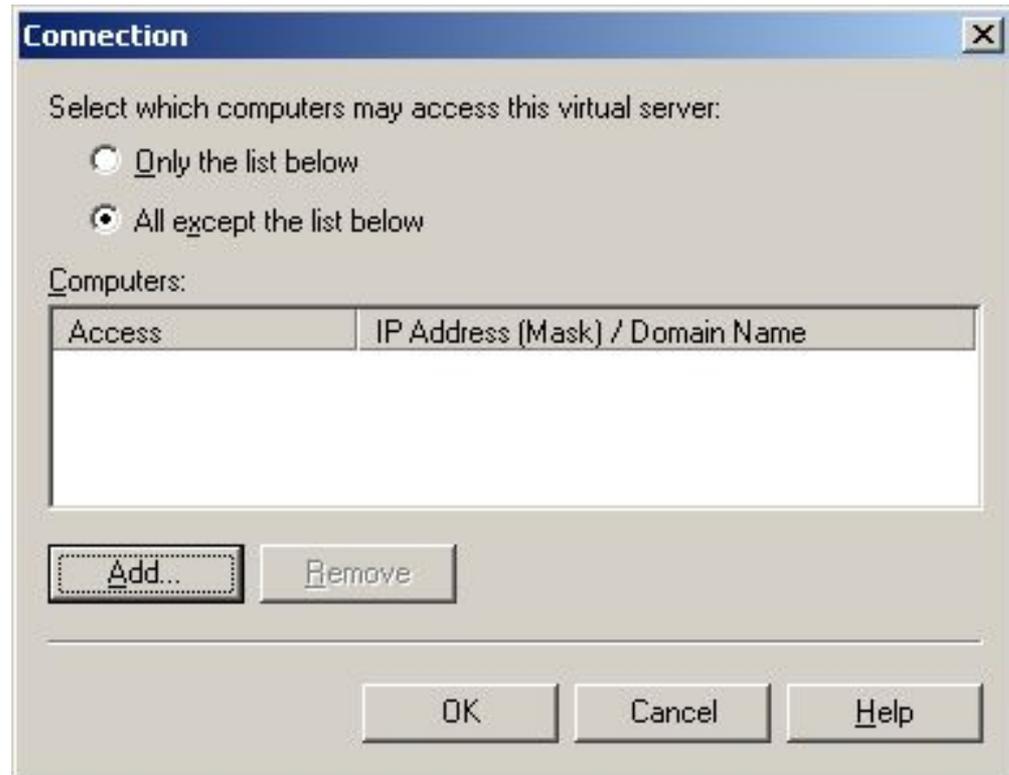
- ❑ Разграничение доступа к IMAP4 серверу в зависимости от IP-адресов хостов, сетей или имен доменов
- ❑ Настройка вариантов аутентификации на сервере IMAP4
- ❑ Удаление информации о версии из заголовка и хвостовика службы IMAP4
- ❑ Управление регистрацией событий в логах на сервере

Безопасная настройка IMAP4 сервера

Разграничение доступа к IMAP4 серверу в зависимости от IP-адресов хостов, сетей или имен доменов

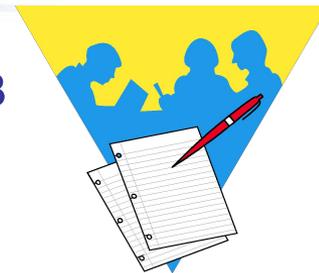


Ограничивает круг лиц, которые могут соединиться с сервером. Поскольку сервер IMAP4 используется для получения почты, диапазон адресов обычно известен. Защита от взлома из «чужой» сети.



Безопасная настройка IMAP4 сервера

Разграничение доступа к IMAP4 серверу в зависимости от IP-адресов хостов, сетей или имен доменов



IP адрес узла

IP адрес и маска сети

Полное имя домена
(нужен обратный DNS)

Computer

Add one of the following to the list.

Single computer
IP address: [] DNS Lookup...

Group of computers
Subnet address: [] Subnet mask: []

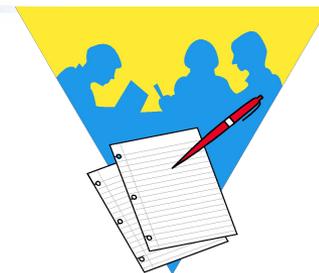
Domain
Name: []

OK Cancel Help



Безопасная настройка IMAP4 сервера

Настройка вариантов аутентификации
клиентов на IMAP4 сервере



Базовая
аутентификация
(имя и пароль в
открытом виде)

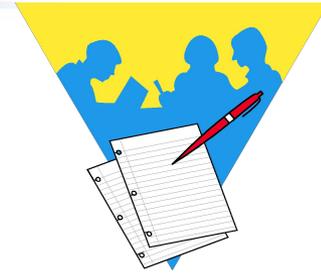


Аутентификация по
правилам Windows
(NTLM)



Безопасная настройка IMAP4 сервера

Удаление информации о версии из
заголовка службы IMAP4

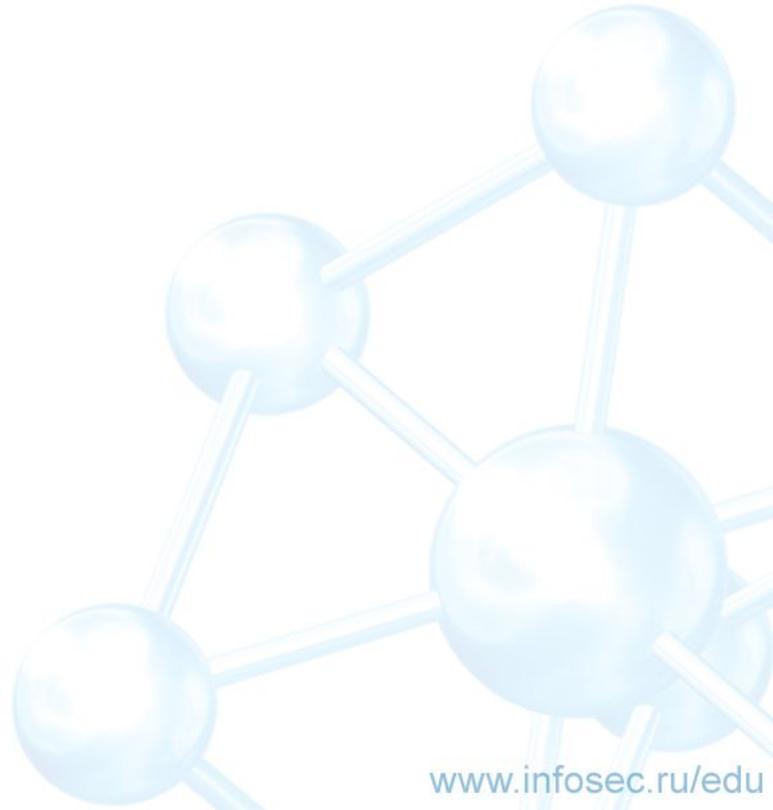


```
C:\WINNT\System32\cmd.exe - telnet localhost 143
* OK Microsoft Exchange 2000 IMAP4rev1 server version 6.0.6249.0 (erшов-w2k.edu
.infosec.ru) ready.
```

```
C:\WINNT\System32\cmd.exe - telnet localhost 143
* OK New banner for IMAP4 (8.22.0555)
```

Практическая работа 12

Изменение заголовков служб POP3 и IMAP4



Вопросы ?